

Шаблони за стандартно описание и обръщение към API

(Версия 1.3.4)

(в сила от датата на приемане на еврото
като официална валута в Република България)



Документът е част от Националния технически стандарт за Банков Интерфейс за Стандартизирани Разплащания (БИСТРА) и технологична комуникация между системите на банките и лицензираните доставчици на платежни услуги в рамките на разширената директива на Европейския съюз относно платежните услуги – PSD 2 Directive (EU) 2015/2366.

Като база е използван документа на Берлинската група NextGenPSD2 Implementation guide, но с допълнения които отразяват националните специфики при използването на API интерфейс за Достъп до сметка.

Таблиците с описание на съдържанието на параметри, елементи и атрибути са приложени в оригиналния им вид от документа NextGenPSD2 Implementation guide, без превод на български език, с цел да се осигури:

- Унификация при прилагането на стандарта на Берлинската група
- Еднопосочно разбиране от всички ДПУ за целта и съдържанието на всички параметри, елементи и атрибути при използване на API интерфейс за Достъп до сметка.

Съдържание

1. ВЪВЕДЕНИЕ	8
1.1. Предистория	8
1.2. История на документа	8
1.3. Спецификация на интерфейса „Достъп до сметка“	12
2. Използване на символи и нотации	13
2.1. Основни и допълнителни символи	13
2.2. Нотации	13
2.2.1 Нотация при подаване на заявка	13
2.2.2 Нотация при отговор на заявка	14
3. Транспортен слой	15
4. Приложен слой – Водещи принципи	16
4.1. Местоположение на параметрите	16
4.1.1. Кодиране на параметрите в съобщенията на различните нива:	16
4.1.2. Прилагане на параметри за дефиниране на API:	16
4.2. Подписване на съобщения в приложния слой	17
4.3. Допълнително използване на OAuth2 за удостоверяване или авторизация на PSU	18
4.4. Структура на API в интерфейса за Достъп до сметка (XS2A Interface API Structure)	19
4.4.1. Path	19
4.4.2. Query parameter	19
4.4.3. Header	19
4.4.4. Body	19
4.5. Много-валутна сметка	20
4.6. Авторизация като крайна точка в ресурс	20
4.7. Отмяна на плащане като крайна точка в ресурс	23
4.8. Изисквания към контекстните данни на Ползвател	24
4.9. Изисквания за идентификация на ДПУ	26
4.10. Изисквания към URIs на ДПУ	26
4.11. Методи на достъп чрез API (API Access Methods)	26
4.11.1. Крайни точки за Разплащания	27
4.11.2. Крайни точки за Информация по сметка	29
4.11.3. Крайна точка за картова сметка	29
4.11.4. Крайна точка за съгласие	30
4.11.5. Крайна точка за съгласие за Потвърждение на наличност на средства по сметка	31
4.11.6. Крайна точка за подписване на кошница	32
4.11.7. Крайна точка за потвърждение на наличност по сметка	32

4.12.	HTTP Response Codes and Additional Error Information.....	32
4.13.	Допълнителна информация за грешки.....	33
4.13.1.	Header	34
4.13.2.	Body	34
4.13.3.	Допълнителна информация за грешки	34
4.14.	Информация за статус.....	36
4.14.1.	Информация за статус при услуга за инициране на плащане	36
4.14.2.	Информация за статус при услуга за Информация по сметка като процес от предоставяне на съгласие.....	39
4.15.	Хипервръзки за управление на API процеси	40
4.16.	Разширяване на атрибутите за данни.....	41
4.17.	Попълване на атрибутите за данни.....	41
4.17.1.	Идентификатор на сметка	41
4.17.2.	TPP-Redirect-URI Header Parameter	41
4.17.3.	Установяване на съгласие.....	41
4.17.4.	Предоставяне на баланс на сметка	41
4.17.5.	Предоставяне на списък на трансакции от сметка	42
4.18.	Пример.....	43
5.	Услуга за инициране на плащане	45
5.1.	Процес на Инициране на плащане	45
5.1.1.	Redirect подход на ЗУИ – с изрично стартиране на авторизация.....	45
5.1.2.	Redirect подход на ЗУИ – с изрично стартиране на авторизация с код за потвърждаване.....	46
5.1.3.	Redirect подход на ЗУИ – автоматично стартиране.....	46
5.1.4.	Redirect подход на ЗУИ – автоматично стартиране с код за потвърждаване.....	48
5.1.5.	OAuth2 подход на ЗУИ – автоматично стартиране	48
5.1.6.	OAuth2 подход на ЗУИ – автоматично стартиране с код за потвърждаване	50
5.1.7.	Decoupled подход на ЗУИ	50
5.1.8.	Embedded подход без ЗУИ (към сигурен получател).....	52
5.1.9.	Embedded подход при единствен метод на ЗУИ.....	53
5.1.10.	Embedded подход чрез избор на метод за ЗУИ	54
5.1.11.	Комбинация от потоци със смесени ЗУИ подходи.....	54
5.1.12.	Множествена ЗУИ авторизация: Пример за подхода с Redirect ЗУИ	56
5.2.	Обзор на данните за услугата за инициране на плащания	57
5.3.	Заявка за инициране на плащане.....	61
5.3.1.	Инициране на плащане в JSON кодиране.....	61
5.3.2.	Инициране на плащане в XML съобщение pain.001	71
5.3.3.	Инициране на масово плащане (bulk payment)	73
5.3.4.	Инициране на нареждане за периодично плащане	74
5.4.	Заявка за статус на Транзакция за Плащане.....	76

5.4.1.	Отговор за статус на Плащане иницирано в JSON формат.....	76
5.4.2.	Отговор за статус на Плащане иницирано в XML формат.....	77
5.5.	Отговор на искане за плащане Get Payment Request	78
5.6.	Искане за отмяна на плащане Payment Cancellation Request	79
5.7.	Искане за получаване на под-ресурсите при оторизирано анулиране.....	83
5.8.	Множествена ЗУИ авторизация при Плащания.....	84
5.9.	Особеност при инициране на плащания от много-валутна сметка	86
6.	Услуги за Информация по сметка	87
6.1.	Потоци на процеса за достъп до информация (Account Information Service Flows)....	89
6.1.1.	Последователност на процесите при подаване на Съгласие за достъп до информация за сметка.....	89
6.1.2.	Последователност на процесите при Предоставяне на данни за сметка.....	95
6.2.	Общ преглед на данните в услугата „Информация за сметка“.....	95
6.3.	Установяване на съгласие за Информация по сметка.....	100
6.3.1.	Заявка за установяване на съгласие	100
6.3.2.	Искане за състояние на заявката (Get Status Request)	108
6.3.3.	Заявка за съдържание на съгласието (Get Consent Request).....	109
6.3.4.	Множествено ЗУИ при Установяване на съгласие	111
6.4.	Изтриване на Съгласие за Информация за сметка.....	111
6.5.	Предоставяне на „Данни за сметка“ (Read Account Data Requests).....	112
6.5.1.	Предоставяне на списък от сметки (Read Account List).....	112
6.5.2.	Предоставяне на детайли за сметка (Read Account Details).....	115
6.5.3.	Предоставяне на баланс на сметка (Read Balance)	117
6.5.4.	Предоставяне на списък на транзакции от сметка (Read Transaction List)	119
6.5.5.	Предоставяне на детайли по транзакции от сметки (Read Transaction Details) .	125
6.6.	Предоставяне на „Данни за картова сметка“ (Read Card Account Data Requests)....	127
6.6.1.	Предоставяне на списък от картови сметки (Read Card Account List).....	127
6.6.2.	Предоставяне на детайли за картова сметка (Read Card Account Details)	128
6.6.3.	Предоставяне на баланс по картова сметка (Read Card Account Balance).....	130
6.6.4.	Предоставяне на списък от транзакции по картова сметка (Read Card Account Transaction List).....	131
7.	Общи процеси при използване на AIS и PIS услуги.....	135
7.1.	Стартиране на процеси по авторизация на заявка	135
7.2.	Процеси по обмен на данни с Ползвателя.....	140
7.2.1.	Обмен на данни за идентификация на Ползвателя	141
7.2.2.	Обмен на данните за автентикация на Ползвателя	144
7.2.3.	Обмен на данните при избор на метод за автентикация с Ползвателя.....	149
7.3.	Авторизация на транзакции (Transaction Authorization).....	153
7.4.	Получаване на авторизация за под-ресурс	155
7.5.	Проверка на ЗУИ статус	156

7.6.	Заявка за потвърждение.....	158
7.6.1.	Получаване на код за потвърждение при подхода на redirect ЗУИ	159
7.6.2.	Изисквания към HTTP заявка браузъра на Ползвателя.....	159
7.6.3.	Предварително условие за заявка за потвърждение	159
7.6.4.	Авторизиране на заявката за потвърждение	160
8.	Подписване на Кошница	163
8.1.	Създаване на заявка за подпис на кошница.....	163
8.2.	Получаване на заявка за подпис на кошница	167
8.3.	Заявка за статус на кошница за подпис	168
8.4.	Множествена ЗУИ при подпис на кошница	169
8.5.	Анулиране на кошница за подпис (Cancellation of Signing Baskets)	170
9.	Комбиниране на информационни и платежни услуги	172
10.	Потвърждение за наличност на средства по сметка	173
10.1.	Установяване на съгласие за Потвърждение за наличност на средства по сметка. 173	
10.1.1.	Общ преглед на данните в услугата „ Установяване на съгласие за Потвърждение за наличност на средства по сметка“	173
10.1.2.	Особеност при съгласие за Потвърждение за наличност по много-валутна сметка 173	
10.1.3.	Заявка за установяване на съгласие	173
10.1.4.	Искане за състояние на заявката (Get Status Request)	179
10.1.5.	Заявка за съдържание на съгласието (Get Consent Request).....	180
10.1.6.	Множествено ЗУИ при Установяване на съгласие за Потвърждение за наличност по много-валутна сметка	181
10.1.7.	Изтриване на Съгласие за Потвърждение за наличност	181
10.2.	Общ преглед на данните в услугата „Потвърждение за наличност на средства“	183
10.3.	Механизъм на Потвърждение за наличност на средства	184
11.	Структура на основни платежни продукти	185
11.1.	Единично плащане.....	185
11.1.1.	Структура в JSON формат.....	186
11.1.2.	Структура в XML ISO20022 код	190
11.2.	Периодично плащане / Плащане с бъдещ вальор	192
11.3.	Масово плащане	192
12.	Подпис (Signatures)	194
12.1.	Задължителна заглавка “Digest”	194
12.2.	Изисквания в заглавка “Signature”	194
13.	Изисквания при използване на OAuth2 метод на ЗУИ	198
13.1.	Заявка за авторизация (Authorization Request).....	198
13.2.	Отговор за авторизация (Authorization Response) се състои от следните данни.....	199
13.3.	Заявка за токън (Token Request).....	199
13.4.	Отговор от токън (Token response)	199

13.5.	Обновяване на тип разрешение с токън (Refresh Token Grant Type).....	200
13.6.	Заявки API (API request)	200
14.	Типове данни и конструкции (Complex Data Types and Code Lists)	201
14.1.	PSU Data.....	201
14.2.	TPP Message Information	201
14.3.	Amount	201
14.4.	Address.....	201
14.5.	Remittance.....	202
14.6.	Links	202
14.7.	href Type.....	206
14.8.	Authentication Object.....	206
14.9.	Authentication Type	207
14.10.	Challenge	207
14.11.	Message Code	208
14.11.1.	Service unspecific HTTP Error Codes.....	208
14.11.2.	PIS specific error codes	209
14.11.3.	AIS specific error codes	210
14.11.4.	PIIS specific error codes	211
14.11.5.	Signing Basket Specific Error Codes	211
14.12.	Error Information.....	211
14.13.	Transaction status	211
14.14.	Consent Status	212
14.15.	SCA Status	212
14.16.	Account Access	213
14.17.	Additional Information Access	213
14.18.	Account Reference	214
14.19.	Account Details.....	214
14.20.	Card Account Details.....	215
14.21.	Balance Type.....	217
14.22.	Balance.....	217
14.23.	Account Report.....	218
14.24.	Transactions	218
14.25.	Entry Details	220
14.26.	Structured Additional Information Data Type	221
14.27.	Standing Order Details Data Type	221
14.28.	Card Account Report	222
14.29.	Card Transactions	222
14.30.	Report Exchange Rate	223
14.31.	Payment Exchange Rate	223

14.32.	Geo Location	224
14.33.	Frequency Code	224
14.34.	Charge Bearer	224
14.35.	Other ISO-related basic Types	224
15.	Препратки (References).....	226

1. ВЪВЕДЕНИЕ

1.1. Предистория

С [PSD2] Европейският съюз публикува нова директива относно платежните услуги на вътрешния пазар. Освен другото [PSD2] съдържа разпоредби за нови услуги, които да бъдат управлявани от т.нар. Доставчици на Платежни Услуги от трети страни (ДПУ) от името на Ползвател на платежни услуги (PSU). Тези нови услуги са:

- Инициране на плащане (PIS) от ДПУ с роля на ДОСТАВЧИК НА ИНИЦИИРАНЕ НА ПЛАЩАНЕ, дефинирана в чл.66 на PSD2
- Информация по сметка (AIS) от ДПУ с роля на ДОСТАВЧИК НА ИНФОРМАЦИЯ за сметка, дефинирана в чл.67 на PSD2
- Потвърждение за наличност на средства по сметка (FCS) от ДПУ с роля на Доставчик на платежни инструменти и потвърждение за наличност на средства за транзакция от сметка (PIISP), дефинирана в чл.65 на PSD2

За да работи с новите услуги, ДПУ трябва да има достъп до сметка на Ползвателя. Този достъп обикновено се управлява от Доставчик на Платежни Услуги за Обслужване на Сметка (ДПУОС). Съгласно директивата, ДПУОС трябва да осигури интерфейс наречен „Достъп до сметка“ към неговите системи, които да бъдат използвани от ДПУ в обхвата регулиран от [PSD2].

Други изисквания за внедряването и използването на този интерфейс се определят от Технически Регулаторен Стандарт (RTS) от Европейския банков орган и се публикувани в Официален вестник на Европейската комисия на 13.03.2018.

1.2. История на документа

Версия	Описание на промените	Утвърждаване / Публикуване
1.0	- Решение за използване на документа NextGen PSD2 Implementation guide, като база за създаване. - Уточняване на обхвата и дефиниране на местните плащания със специфични характеристики - Описание на компонентите	Утвърдена от Работна група Предоставена за обсъждане на банките чрез АББ. 04.2018
1.1	- Конкретно описание на API компоненти, относно Плащания Достъп до информация по сметка Обработка на съгласия Методи на ЗУИ	Утвърдена от Работна група Предоставена за обсъждане на банките чрез АББ. Публикувана след одобрение на СД на БОРИКА 06.2018
1.2	Тази версия на документа представлява промяна на версия 1.1 като съдържа следните корекции в Секция 11.1.1. 1. Детайлите за плащане към бюджета в JSON формат се групират в един елемент: budgetPaymentDetails 2. Всички елементи за плащане към бюджета стават под-елементи в структурата на елемента budgetPaymentDetails 3. Елементът documentKind се преименува на regulatoryReportType, като съдържанието и структурата се запазват. 4. Елементът paymentType се преименува на serviceLevel, като съдържанието и структурата се запазват. 5. Корекция на примерите на заявки за плащане в с. 5.3.1 6. Преименуване на крайни точки: • BGN Budget Transfer в Domestic Budget Transfer BGN	Утвърдена от Работна група

	• <i>BGN Credit Transfer</i> в Domestic Credit Transfer BGN • <i>EUR Credit Transfer</i> в SEPA Credit Transfer 7. Промени в структурата на API Cross Border CT както следва: • Допълнение с код за валютен на плащането • Допълнение с полета за Име на банка на получател и Адрес на банка на получател в случаите, когато не е предоставен IBAN и SWIFT BIC в нареждането 8. Промяна на задължителност на поле Информация за превода. 9. Забележка относно дължината на поле Информация за превода в системата БИСЕРА 10. Атрибут cardNumber не може да се използва в заявката за Потвърждение за наличност по средства. 11. Атрибут PAN не може да се използва в заявките за Достъп до сметка. Препоръчва се използването на елемента maskedPan. 12. Промяна в имената на полета в структурата на плащане към бюджета, както следва: • taxId в taxPayerId • taxTr в taxPayerType <u>Всички следващи версии ще се тълкуват като допълнение на предшестващите, а не както в случая за промяна</u>	
1.3	Съдържа следните допълнения: 1. Добавя се описание на API за Плащане с бъдещ валютен (Future Dated Payments), Постоянно нареждане за периодично плащане (Standing Orders for Recurring/Periodic Payments) и Нареждане на масово плащане (Bulk Payment) 2. Добавя се множествена ЗУИ авторизация (за ЮЛ с повече от един подпис/авторизация) 3. Добавя се функция за Анулиране на плащане 4. Добавя се функция за Подписване на кошница (Signing Basket) с цел подпис/авторизация на множество плащане 5. Добавя се авторизацията на под-ресурсите Плащане/Кошница/Съгласие/Анулиране на плащане 6. Добавя се нов ресурс – Card Accounts и методи Read Card Account, Card Account Balances, Card Account Transactions 7. Добавят се нови HTTP хедъри, като например данни за приложението, което ДПУ използва за връзка с Ползвателя 8. Добавя се показване на имената на собственика на сметката в детайли за сметка чрез допълнителни полета в съгласието и детайлите за сметка 9. Включват се постоянни нареждания в списъка с трансакции по AIS 10. Актуализиране с поправките от Берлинската група a. Change Log V1.3 V1.3.4	Утвърдена от Работна група

	b. Change Log V1.3.4. V1.3.6 c. V1.3.6 Errata 20200327 11. Интегрират се допълнителните услуги a. известяване за промяна на състояние b. показване на имената на собственика на сметката и списък с постоянни нареждания c. съгласие при предоставяне на наличност 12. Добавят се препоръките за попълване на изброените полета в отговор на запитване за „Баланс“ и „Трансакции“ по сметка	
1.3.1	1. Разширяват се препоръките за попълване на изброените полета в отговор на запитване за „Баланс“ и „Трансакции“ по сметка a. Добавя се препоръка за идентификатор на сметка - 4.17.1 Идентификатор на сметка b. Добавя се препоръка за header параметър TPP-Redirect-URI - 4.17.2 TPP-Redirect-URI Header Parameter c. Добавят се препоръки при установяване на съгласие - 4.17.3 Установяване на съгласие d. Добавя се Дата на баланса (referenceDate) - 4.17.4 Предоставяне на баланс на сметка e. Добавят се препоръки и примери при списък с трансакции - 4.17.5 Предоставяне на списък на трансакции от сметка 2. Правят се задължителни полета a. transactionId в тип 14.24 Transactions 3. Актуализиране с поправките от Берлинската група a. Change Log V1.3.6 V1.3.8 b. Change Log V1.3.8 V1.3.9	Утвърдена от Работна група
1.3.2	1. Добавен е платежен продукт за незабавни плащания - instant-domestic-credit-transfers-bgn в: a. 5.3.1 Инициране на плащане в JSON кодиране b. 5.3.2 Инициране на плащане в XML съобщение pain.001 c. 5.3.3.1 Инициране на масово плащане (bulk payment) в JSON кодиране d. 5.3.3.2 Инициране на масово плащане (bulk payment) в XML кодиране e. 11.1 Единично плащане	Утвърдена от Работна група
1.3.3	1. Промяна в реквизитите на бюджетното плащане в лева (структурата на елемент budgetPaymentDetails) a. 11.1 Единично плащане 2. Дефинира на незабавен кредитен превод е лева, чрез платежен продукт domestic-credit-transfers-bgn и нова стойност BLNK за Service Level a. 11.1 Единично плащане 3. Добавен е платежен продукт за незабавни плащания в евро - instant-sepa-credit-transfers в: a. 5.3.1 Инициране на плащане в JSON кодиране b. 5.3.2 Инициране на плащане в XML съобщение pain.001	Утвърдена от Работна група

	с. 5.3.3.1 Инициране на масово плащане (bulk payment) в JSON кодиране d. 5.3.3.2 Инициране на масово плащане (bulk payment) в XML кодиране е. 11.1 Единично плащане	
1.3.4	1. Премахване на преводите в лева (продукти domestic-credit-transfers-bgn, domestic-budget-transfers-bgn и instant-domestic-credit-transfers-bgn) и замяната им със SEPA преводи (sepa-credit-transfers и instant-sepa-credit-transfers) а. 5.3. Заявка за инициране на плащане b. 5.3.1. Инициране на плащане в JSON кодиране с. 5.3.2. Инициране на плащане в XML съобщение pain.001 d. 11.1.Единично плащане 2. Добавяне на атрибути за идентификатор на наредителя и идентификатор на получателя при инициране на плащане а. 11.1.Единично плащане	Утвърдена от Работна група

1.3. Спецификация на интерфейса „Достъп до сметка“

Този документ е част от спецификацията, която дефинира стандарт за интерфейс „Достъп до сметка“ и постига оперативна съвместимост на интерфейсите на ДПУОС поне за основните услуги, определени от PSD2. На тази база ДПУОС може да използва този стандарт като основа за внедряването на интерфейс „Достъп до сметка“ в пълен обхват, за да бъде изцяло в съответствие с PSD2.

Интерфейсът е проектиран като B2B интерфейс между ДПУ сървър и ДПУОС сървър. На този етап в този документ е дефиниран протокол клиент-сървър, приемайки, че ДПУ е клиент, т.е. всички API повиквания се инициират от него. В бъдещите стъпки този протокол може да бъде разширен до протокол сървър-сървър, където и ДПУОС инициира API повиквания.

Рамката за оперативна съвместимост определя оперативните правила, изискванията към модела на данните и описанието на процесите при „Достъп до сметка“.

Този документ детайлизира стандарта за дефиниране на съобщения и подробни структури на данни от интерфейса Достъп до сметка. За спецификацията се различават два слоя:

- Транспортен слой и
- Приложен слой

В тази версия на документа за приложния слой ще бъдат описани само основните услуги. В бъдещите версии на тази рамка някои разширени услуги също ще станат част от стандарта, след като те са изяснени и пазарната нужда от тях вече е идентифицирана.

В документа с цел абстрактно описание на процесите се използват понятията Ресурс и Крайна точка, за които следва да се прилага следната интерпретация:

- Ресурс: Вид информация, която се изисква от ДПУ към ДПУОС или се генерира от ДПУОС и след това се транспортира към ДПУ
- Крайна точка: Конкретно посочен вид информация в рамките на ресурса, който се разменя в рамките на интерфейса за Достъп до сметка

Примери:

```
{ресурс/конкретен вид}
{payments/sepa-credit-transfers}
или
{consents/consent-ID}
```

2. Използване на символи и нотации

2.1. Основни и допълнителни символи

- Наборът от символи е кодиран с UTF 8;
- Спецификацията използва само основни типове данни "String", "Boolean", "ISODateTime", "ISODate", "UUID" and "Integer" (с дължина 32 бита) и ISO базирани списъци с кодове. За кодовете дефинирани по ISO, са дадени референции към съответния ISO стандарт в 14.34;
- Max35Text, Max70Text, Max140Text and Max500Text дефинират низове с максимална дължина от съответно 35, 70, 140 и 500 символа;
- ДПУОС задължително трябва да приемат текстове, които са съставени от следните символи (Базови):

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z

0 1 2 3 4 5 6 7 8 9

/ - ? : () . , ' +

Шпация (Space)

- Разрешено е ДПУОС да приемат и допълнителни буквени символи (кирилица) САМО КОГАТО те се съдържат в полета от тип TEXT (име, адрес, основание ...).

A B B Г Д Е Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ь Ю Я
а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ь ю я

- Позволено е ДПУОС да конвертират допълнителните символи (кирилица) към базовите символи (латински) с цел съобщенията да се приемат от чуждестранните платежни системи.

- Забранено е използването на допълнителните символи в маркерите (Tag), които се ползват за начало и край на елемента:

Пример:

Разрешено: <element>Адрес</element>

Забранено: <елемент>Адрес</елемент>

2.2. Нотации

2.2.1 Нотация при подаване на заявка

Параметрите на заявките от приложния програмен интерфейс (API), параметрите на заглавката на HTTP и параметрите от съдържанието на тялото се указват в Дефиниции както следва (в табличен вид):

Attribute	Type	Condition	Description
Attribute tag	Type of attribute	condition	Description of the semantic of the attribute and further conditions

Могат да бъдат зададени следните условия:

- Mandatory: Атрибутът се поддържа от ДПУОС и се използва от ДПУ.

- Conditional: Атрибутът се поддържа от ДПУОС и може да се използва само по начина описан в собствената му документация за поддръжка на интерфейса Достъп до сметка.
- Optional: Атрибутът се поддържа от ДПУОС, но използването му е по избор за ДПУ
- Optional if supported by API provider: Атрибутът може да се поддържа по желание на ДПУОС. Ако ДПУОС документира, че поддържа атрибута, използването му е по избор за ДПУ. Ако ДПУОС не поддържа атрибута, а ДПУ го използва в заявката, то тя ще бъде отхвърлена.

2.2.2 Нотация при отговор на заявка

Параметрите на заявките от приложния програмен интерфейс (API), параметрите на заглавката на HTTP и параметрите от съдържанието на тялото се указват в Дефиниции както следва (в табличен вид):

Attribute	Type	Condition	Description
Attribute tag	Type of attribute	condition	Description of the semantic of the attribute and further conditions

Могат да бъдат зададени следните условия:

- Mandatory: Атрибутът се поддържа от ДПУОС.
- Conditional: Атрибутът се поддържа от ДПУОС и може да се използва само по начина описан в собствената му документация за поддръжка на интерфейса Достъп до сметка.
- Optional: Атрибутът се поддържа по желание на ДПУОС

3. Транспортен слой

Комуникацията между ДПУ и ДПУОС винаги се гарантира чрез използване на TLS връзка с TLS версия 1.2 [[RFC 5246](#)] или по-висока. За избора на шифриращи пакети следва да се спазват препоръките на NIST за криптографска сила. ДПУОС може да прилага и други изисквания за шифриране, ако това се изисква от тяхната национална агенция за ИТ сигурност.

Тази TLS връзка се установява винаги от ДПУ. Не е необходимо да се създава нова TLS връзка за всяка транзакция, но ДПУОС може да прекрати съществуваща TLS връзка, ако това се изисква от настройките за сигурност.

Създадената TLS-връзка винаги включва удостоверяване на клиента (т.е. ДПУ). За това удостоверяване, ДПУ трябва да използва квалифициран сертификат за удостоверяване на уебсайтове. Този квалифициран сертификат трябва да бъде издаден от квалифициран доставчик на доверителни услуги съгласно регламента eIDAS [eIDAS]. Съдържанието на сертификата трябва да е съвместимо с изискванията на [EBA-RTS].

Сертификатът на ДПУ трябва да показва всички роли, които ДПУ има право да използва.

4. Приложен слой – Водещи принципи

4.1. Местоположение на параметрите

Интерфейсът ДОСТЪП ДО СМЕТКА се базира на подхода REST услуги. (Уеб услуги, които осигуряват оперативна съвместимост между компютърните системи в Интернет) [[RFC 2616](#)].

Този подход позволява транспортиране на параметрите на съобщения в различни нива:

- Ниво HTTP Header (заглавен ред)
- Ниво path (идентификация на ресурс или адрес) с допълнителни параметри в заявката
- Ниво HTTP Body (съдържание)

Параметрите на съдържанието в съответния HTTP Body ще бъдат кодирани в JSON или XML синтаксис. Синтаксис в XML се използва само когато заявката съдържа:

- Инициране на плащане въз основа на ISO20022 (съобщение pain.001) и съответния отговор за статус на плащането (съобщение pain.002) или
- Съобщение за информация на базата на информация по ISO20022 (съобщение camt.052, camt.053 или camt.054)

По изключение съобщенията за отговор може да съдържат формат на обикновен текст в съобщенията с информация за сметка, за да поддържат форматите на съобщения MT940, MT941 или MT942.

Параметри на съобщенията

4.1.1. Кодиране на параметрите в съобщенията на различните нива:

- Винаги с букви от латинската азбука
- На ниво HTTP Header: Винаги започва с главна буква (Spinal-case)
- На ниво path: Винаги се използват малки букви (spinal-case)
- На ниво HTTP Body, ако атрибута е в JSON [[RFC 7159](#)] формат параметъра винаги започва с малка буква, а след това е разрешено използване на единична главна буква (lowerCamelCase)
- На ниво HTTP Body, може да се използва и XML синтаксис съгласно ISO20022 стандарт

4.1.2. Прилагане на параметри за дефиниране на API:

4.1.2.1. На ниво path

Всички данни, които идентифицират ДПУ и адресират ресурс:

- Идентификация на доставчика,
- Идентификация на услугата,
- Идентификация на платежния продукт,
- Идентификация на подтипа на продукта за информация по сметка
- Идентификатор на вече създаден ресурс

4.1.2.2. На ниво HTTP Header

- Параметър за указване на синтаксиса в съдържанието JSON / XML
- Параметър съдържание на Сертификат и подпис. При поискване от ДПУОС, ДПУ трябва да подпише съобщенията за заявки. Подписът се включва в HTTP-

Header. Електронният подпис на ДПУ трябва да се основава на квалифициран сертификат за електронни печати. Това се отнася за случаите в които ДПУОС прецени, че идентификацията от Транспортния интерфейс не е достатъчна. Съгласно правилата на EBA-RTS, сертификатът на ДПУ трябва да показва всички роли, които ДПУ има право да използва.

- Параметър който съдържа данни за идентификация на Ползвателя. Данните, които се извличат от Интернет базираното приложение или от токъна за достъп (ID, IP Address, Token, GEO локация ...)
- Параметър на данни от протокола (пр. Време на постъпване на заявка, Идентификатор на Заявка)

4.1.2.3. Параметри на заявката:

Допълнителна информация, необходима за обработване на искането като адрес за управление на процеса или филтър за достъп до конкретна информация

4.1.2.4. На ниво HTTP Body

- Съдържанието на бизнес данни
- Данни за автентичността на Ползвателя (PSU)
- Информация за съобщения
- Хипервръзки за управление на процеса ДПУ – ДПУОС от край до край

Препоръчва се информацията от ниво Header или отделни части от нея да се съхранява при ДПУОС за допълнителни проверки и статистически цели на националния или европейски регулаторен орган.

4.2. Подписване на съобщения в приложния слой

При поискване от ДПУОС, ДПУ трябва да подпише съобщенията за заявките, които са изпратени. Изискването на ДПУОС трябва изрично да е посочено в неговата документация. По дефиниция подписът се включва като параметър в ниво HTTP-Header.

Електронният подпис на ДПУ трябва да се основава на квалифициран сертификат за електронни печати. Това квалифицирано удостоверение трябва да бъде издадено от квалифициран доставчик на доверителни услуги в съответствие с регламента eIDAS. Съдържанието на сертификата трябва да е в съответствие с изискванията на [EBA-RTS] Документацията за интерфейс Достъп до сметка, съвместим с PSD2, версия 1.0, публикувана на 08 февруари 2018 г.

Съгласно Регулаторния Технически Стандарт [EBA-RTS], сертификатът на ДПУ трябва да показва всички роли, които има право да използва.

Спецификацията на подписа в HTTP протокола и конкретно в частта HTTP Header унифицира използването на следните атрибути:

Attribute	Type	Condition	Description
Digest	String	Conditional	Is contained if and only if the "Signature" element is contained in the header of the request.
Signature	Section 12	Conditional	A signature of the request by the TPP on application level. This might be mandated by ASPSP.
TPP-Signature-Certificate	String	Conditional	The certificate used for signing the request, in base64 encoding. Must be contained if a signature is contained, see above.

Приложените дефиниции на тези атрибути няма да се повтарят в по-нататъшната спецификация за по-лесно четене на документа.

4.3. Допълнително използване на OAuth2 за удостоверяване или авторизация на PSU

API за Достъп до сметка ще позволява на ДПУОС да внедрява OAuth2 като метод за Управление на съгласието на Ползвател към ДПУ, за услуга Инициране на плащания и / или Информация по сметка. В този случай ДПУ ще бъде клиента, Ползвателят е собственик на ресурса, а ДПУОС ще бъдат ресурсният сървър в абстрактния модел OAuth2.

Тази спецификация поддържа два начина за интегриране на OAuth2. Първата възможност е удостоверяване на Ползвателя в предварителна стъпка, преобразувана в идентификационен токън за достъп, който ще бъде използван след това в интерфейса XS2A. Тази предварителна стъпка ще използва опциите за обработка на протокола OAuth2 без пренасочване към сървъра за удостоверяване. Това използване на OAuth2 ще бъде посочено в тази спецификация като "Обмен на данни с Ползвателя при OAuth2 метод на идентификация". Всяко ДПУОС, което прилага OAuth2 метод, трябва да укаже в своята документация всички допълнителни детайли на този интерфейс за Достъп до сметка.

Забележка: Когато се изпълнява OAuth като предварителната стъпка, изискванията за напр. регистрационни стъпки или липса на задължително използване на две SCA в конкретни сценарии само на PIS, както е дефинирано от [EBA OP2], трябва да бъдат разпознати от ASPSP.

Втората възможност за интегриране на OAuth2 е интеграцията като подход за Задълбочено Установяване на Идентичност (ЗУИ) чрез OAuth2, който да се използва за оторизиране при инициране на плащания и обработка на съгласия.

Когато се използва OAuth2, повикванията за „Достъп до сметка“ работят с токън, вместо да използват правата на Ползвателя в съгласието. Така се осигурява интеграция на съгласието за услугата и нейното придобиване:

За услугата PIS, OAuth2 ще бъде използвана интегрирано с придобиване на съгласие, като се изпълняват следните стъпки:

- 1) Данните за плащане от сметка се публикуват (post) в съответното съобщение за Инициране на плащане.
- 2) Протоколът OAuth2 се използва с цел "Авторизация" за придобиване на съгласие и разрешение за вида на плащането, по т.1.
- 3) След успешно оторизиране от страна на Ползвателя, съответното плащане автоматично се иницира от ДПУОС.

За услуга AIS, OAuth2 ще бъде използвана интегрирано с придобиване на Съгласие, като се изпълняват следните стъпки:

- 1.) Данните за достъп до информационните услуги (AIS) в Съгласието се публикуват (post) като крайна точка за Съгласие на приложния програмен интерфейс (API) XS2A.
- 2.) Протоколът OAuth2 се използва с цел "Авторизация" на Съгласието, в частта за услугите Достъп до информация по сметка.
- 3.) ДПУ може да използва получения токън от протокола OAuth2, за достъп до крайната точка (разрешените услуги за информация по сметка; за периода на валидност на разрешеното съгласие, респ. периода на валидност на токъна за технически достъп).

За Стъпка 2.) подробностите са описани в Раздел 13.

При използването на метод OAuth2, заявките на API интерфейса за Достъп до сметка се оторизират с данните от токъна, вместо с данни въведени от Ползвателя.

4.4. Структура на API в интерфейса за Достъп до сметка (XS2A Interface API Structure)

Интерфейсът за Достъп до сметка е ориентиран към достъп до ресурс (Съгласие, Плащане, Информация). ДПУ указва какъв конкретен ресурс изисква. За да получи ресурса, ДПУ трябва да се представи и да направи заявка за достъп към ДПУОС. ДПУ трябва да подготви структурата на своето API, така че да приеме отговора на ДПУОС и всички предоставени данни от него.

Заявката транспортира чрез HTTP протокол, параметри с различно съдържание

<HTTPS://{доставчик}/v1/{услуга}{?заявени-параметри}>

Съдържанието на конкретната услуга се указва с допълнителен параметър.

Където:

- доставчик – съдържателно име на приложението (пример: www.api.testbank.com)
- v1 – обозначава версията на интерфейса
- услуга – указва се вида на ресурса (съгласие, плащане, масово плащане, периодично плащане, подпис на кошница от плащания, информация за сметка, информация за карта, потвърждение за наличност по сметка) и разширение за вид и обхват на заявката (плащане / бюджетен превод или сметка / баланс по сметка)
- ?заявени-параметри – са параметри, които се използват като филтър при искане за достъп до ресурс
- параметри – указва съдържание на атрибути в JSON или XML формат. Кодирането в XML ISO20022 pain.001 е само когато заявка се изисква от ДПУОС за определен платежен продукт. Всички останали параметри се описват в JSON формат.

Структурата Заявка / Отговор може да се опише в следните категории

4.4.1. Path

Атрибут, който указва вида на ресурса

Пример: <https://api.testbank.com/v1/payments/sepa-credit-transfers>

или

Пример: <https://api.testbank.com/v1/consents/consent-ID>

4.4.2. Query parameter

Атрибути, които се добавя към path след знака „ ? “ като управляващи флагове на процеса или филтриращи атрибути на методите за достъп чрез GET

4.4.3. Header

Атрибути, кодирани в HTTP заглавието на заявката или отговора (HTTP Request / HTTP Response). Представяват данни за типа кодиране на информацията, Идентификация на ДПУ, Идентификация на Ползвателя, Точен час на подаване на заявката, код на резултат от обработка на заявката.

4.4.4. Body

- Заявка: Искане за изпълнение на функция, посочена или филтрирана с параметър

- Отговор на заявка: Атрибути, които съдържат отговор по определени правила в XML, JSON или текстов формат.
 - В XML формат се представят само съобщения от тип camt.052, camt.053, camt.054, pain.002. Съобщение pain.002 се изготвя само ако в първата стъпка съобщението от заявката е от тип pain.001.
 - Текстов формат се използва само в случаи на транспортиране на съобщения MT940, MT941 и MT942
 - При всички останали случаи отговорите са JSON кодирани
 - Доставка на ресурс от обхвата на ДОСТЪП ДО СМЕТКА може да съдържа и Хипервръзка за изпълнение на процес по идентификация или достъп до ресурс със значителен обем от информация.

Кодовете за HTTP отговор, които могат да се използват в този XS2A интерфейс, са посочени в раздел 14.11.

4.5. Много-валутна сметка

Дефиниция: Много-валутна сметка е съвкупност от различни под-сметки, които са адресират от един и същ идентификатор (като IBAN, напр.). Под-сметките са законово различни и всички се различават по тяхната валута, салда и транзакции. Идентификаторът на сметката като IBAN заедно с валута, винаги уникално адресира под-сметка на много-валутна сметка.

Тази спецификация поддържа адресиране на много-валутни сметки, както на агрегирано ниво, така и на ниво под-сметка. Атрибутът за код валута в съответната структура от данни "Account Reference" позволява изграждането на структури като:

```
{"iban": "DE40100100103307118608"}
```

или

```
{"iban": "DE40100100103307118608",  
  "currency": "EUR"}
```

Ако основната сметка е много-валутна сметка тогава:

- първото позоваване се отнася до адресиране към този IBAN за всички под-сметки към него;
- второто позоваване се отнася само за под-сметката във валута евро.

Тази спецификация на интерфейса се отнася за под-сметки на много-валутни сметки по същия начин, както при обикновени сметки. Това се отнася както за инициране на плащания, така и за услугите за информация по сметка.

Забележка: Продуктът с много-валутни сметки се използва на някои пазари в Европа, напр. в онлайн-банковите продукти на белгийския пазар. Поддръжката на тази функционалност в интерфейса API XS2A е приложима само на тези пазари

4.6. Авторизация като крайна точка в ресурс

С настоящата версия на този документ се въвежда нова крайна точка за авторизация на транзакции при услугите за инициране на плащане и установяване на съгласие. Тази функция се използва в случаите, които изискват авторизация от крайния Ползвател:

- Използване на ЗУИ с няколко нива, при които дадена транзакция се нуждае от разрешение от повече от един Ползвател, напр. в корпоративен контекст,
- Подписване на група транзакции с една ЗУИ авторизация, както се предлага в онлайн банкирането на повечето ДПУОС

- Подписване на група транзакции с няколко нива на ЗУИ, когато се изисква авторизация от повече от един Ползвател, напр. в корпоративен контекст.

Тази нова функционалност може да се прилага и в процеса на авторизация на индивидуални заявки, което е значима промяна в модела на версията поддържана до този момент. Досегашната функционалност за интеграция на процеса по авторизация в случаите на инициране на плащания или установяване на съгласие все още се поддържа.

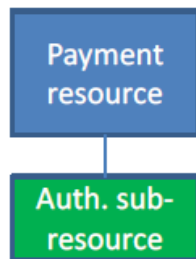
Процесът на авторизация се отделя от процеса на получаване на ресурси в резултат от подаването на заявки за плащане или установяване на съгласие. С други думи при заявка за Плащане като ресурс, за което се изискват n броя авторизации, ще се появява платежен ресурс за n броя авторизации като под-ресурси (SCA sub-resources).

Групирането на няколко транзакции за един общ процес на авторизация се поддържа като крайна точка за подписване на кошница. ***Това е допълнителна функция която може да бъде предложена от ДПУОС.***

Ако тази функция се предлага от ДПУОС, ДПУ може първо да подаде данни за плащане и съгласие, без да започне разрешението. Първа стъпка е групиране на свързаните ресурси за плащане и съгласие в кошница. Следващата стъпка е чрез използване на команда за подписване на кошници, като крайна точка. Така се стартира авторизация на съдържанието в кошницата.

Следващата картина предоставя общ преглед на абстрактния модел при различни сценарии:

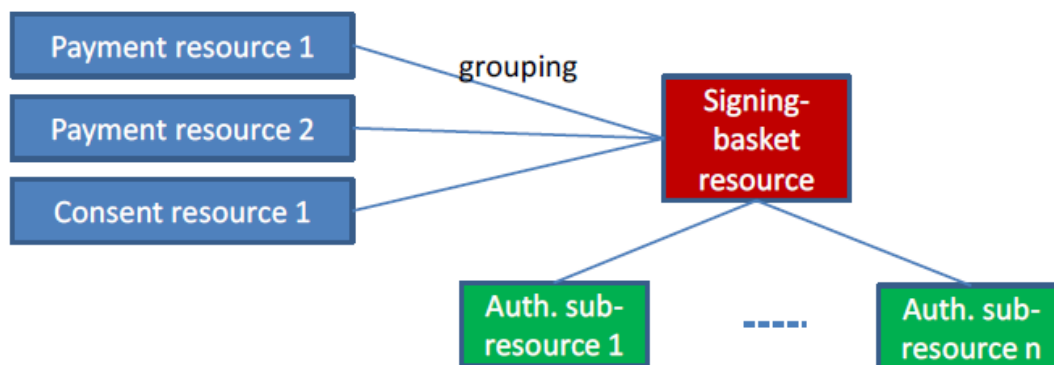
Модел на данни за еднократно плащане с една ЗУИ авторизация



Модел на данни за еднократно плащане с няколко ЗУИ авторизации



Модел на данните за упълномощаването на група транзакции с множество ЗУИ авторизации



Забележка: ДПУОС трябва да подготви подробно описание в своята документация за метода и ограниченията при групиране на плащания. Когато предлага функцията за кошница за подпис, ДПУОС може да ограничи групирането например:

- към всички видове плащания както са инициирани (с една или повече авторизация се подписва кошницата от всички наредени плащания без ограничения),
- за индивидуални плащания (пълно ограничение - всяко плащане ще се оторизира поотделно с един или няколко подписа),
- към един и същ вид плащане (ДПУОС групира в кошница само кредитни трансфери от един и същ тип и изисква един или няколко подписа за цялата кошница).

Забележка: На този етап стандартът не обхваща всички възможни случаи на групиране поради многобройните варианти и различна степен на сложност особено в корпоративен контекст. Съществуват различни политики относно сума, брой на подписи, ред за подписване и т.н.

Оптимизация на процеса за подаване на еднократни плащания

Общият модел, описан по-горе, изисква от ДПУ да стартира два под-процеса при инициране на плащане, създаване на кошница за подписване или подаване на съгласие. При инициране на плащане тип СЕПА Кредитен превод това би довело до заявка:

POST /payments/sepa-credit-transfers {payment data}

която генерира платежния ресурс и връща paymentId като идентификация на ресурсите.

След това започва процеса на упълномощаване, като създава под-ресурс за авторизация със заявка:

POST /payments/sepa-credit-transfers/paymentId/authorisations

Като след това се връща адрес на авторизация за този под-ресурс.

Прилагането на това изискване за всяка отделна авторизация за транзакции, напр. в подхода Redirect на ЗУИ би увеличил значително броя на API повикванията. Поради тази причина настоящата спецификация все още позволява на ДПУОС да създаде автоматично необходимия брой на адреси за авторизация и да даде достъп до тези под-ресурси на ДПУ, като върне съответните хипервръзки, описани в Раздел 4.12. Резултатът за статус на авторизацията се получава след командата:

GET /payments/sepa-credit-transfers /paymentId/authorisations/authorisationId

където ДПУОС имплицитно генерира ресурса за авторизация и идентификатора му.

4.7. Отмяна на плащане като крайна точка в ресурс

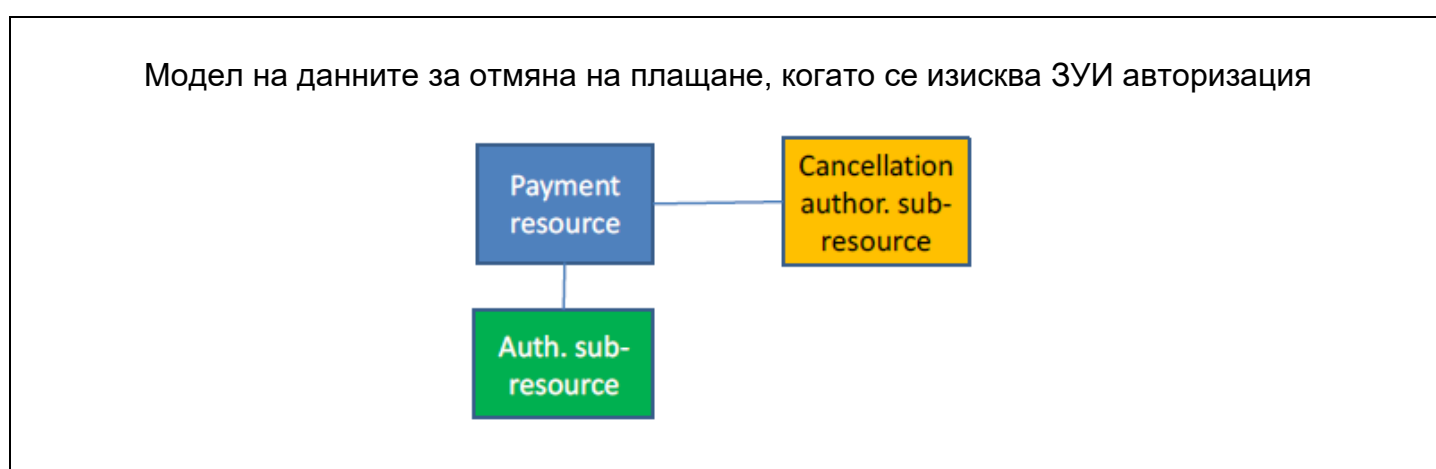
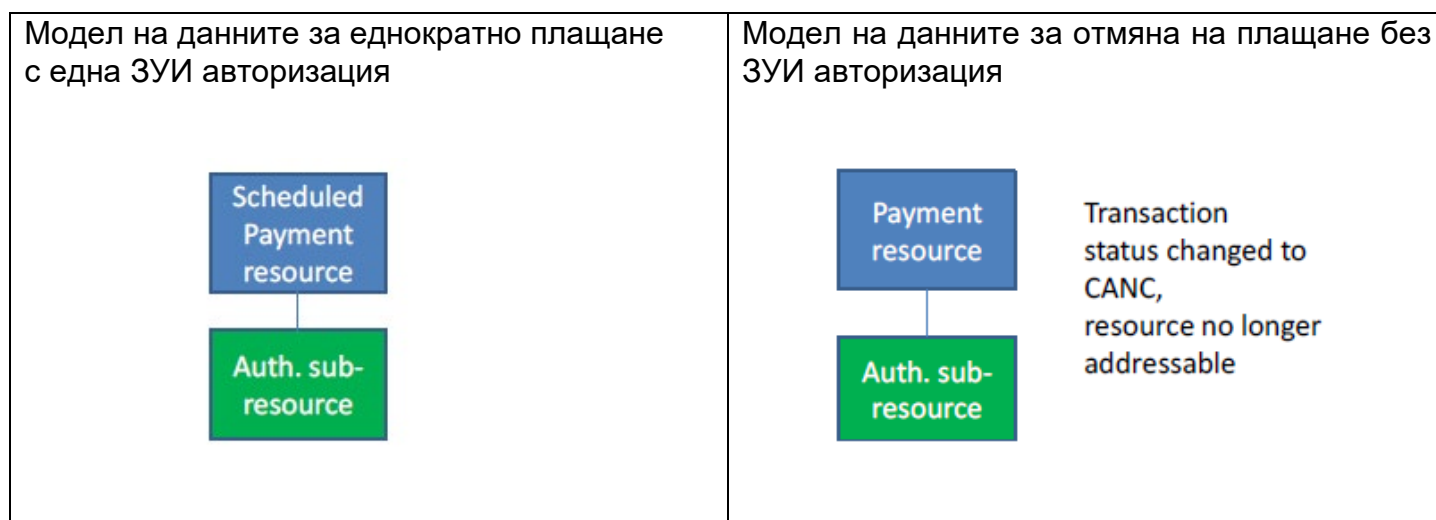
Условията за изтриване/оттегляне на Съгласие за Информационни услуги чрез ДПУ са описани в още в началната версия. Управлението на съгласието се обработва между ДПУ и Ползвателя и съгласието за достъп до информационни услуги може да бъде отделено, без да има страничен ефект върху изпълнението на транзакциите.

От тази версия спецификацията ще поддържа отмяна на инициирано плащане чрез ДПУ. Този процес е разделен на две стъпки:

1. ИЗТРИВАНЕ (DELETE) на съответния ресурс, когато не се изисква авторизация.
2. За стартиране на процеса по анулиране на плащане, ако се изисква авторизация:
Команда: POST payments/sepa-credit-transfers/paymentId/cancellation-authorizations

Втората стъпка може да бъде пропусната, когато ДПУОС не изисква изрична авторизация за анулиране. Необходимостта за авторизация на анулирането се съобщава чрез изпращане на съответни хипервръзки към ДПУ, ср. Раздел 4.12.

Подходът на анулиране чрез авторизация ще се управлява чрез под-ресурс разрешение за анулиране на плащане по аналогия с разрешенията за иницииране на плащане. Историята на използваните под-ресурсите при разрешение за иницииране на плащане не се променят през целия жизнен цикъл на плащането с цел да се запази историята му отначало докрай. Следните картинки показват промените на ниво ресурс при инициирано плащане:



Съответните оригинални под-ресурси за авторизация остават непроменени при всички случаи на отмяна на иницирирано плащане.

За транзакции, при които е необходима многостепенна ЗУИ авторизация за потвърждение, може да е необходима и многостепенна ЗУИ авторизация за анулиране. Ако политиката на ДПУОС изисква еквивалентност на разрешението, моделът за отмяна ще съдържа повече под-ресурси за отмяна.

4.8. Изисквания към контекстните данни на Ползвател

Следните елементи от данни препращат информация за Ползвател / ДПУ интерфейса и разширяват процедурите за управление на риска на ДПУОС. Настоятелно се препоръчва тези елементи на данни да се изпращат във всички съобщения за заявка в рамките на транзакцията за иницириране на плащане или за създаване на съгласие, т.е. потоци с включена PSU идентификация. По-нататъшните дефиниции на параметрите на заявката в съответните секции не повтарят дефиницията на тези елементи с цел по-добра четимост. Единственото изключение е, когато условия, различни от „незадължителни“, се прилагат за конкретни съобщения за заявка, напр. за IP адреса на PSU. Повече подробности са предоставени в прегледа на данните в Раздел 5.2 или Раздел 6.2.

Attribute	Format	Condition	Description
PSU-IP-Address	String	Optional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP.
PSU-IP-Port	String	Optional	The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available.
PSU-Accept	String	Optional	The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available.
PSU-Accept-Charset	String	Optional	see above
PSU-Accept-Encoding	String	Optional	see above
PSU-Accept-Language	String	Optional	see above
PSU-User-Agent	String	Optional	The forwarded Agent header field of the HTTP request between PSU and TPP, if available.
PSU-Http-Method	String	Optional	HTTP method used at the PSU – TPP interface, if available. Valid values are: • GET • POST • PUT • PATCH • DELETE
PSU-Device-ID	String	Optional	UUID (Universally Unique Identifier) for a device, which is used by the PSU, if available. UUID identifies either a device or a device dependant application installation. In case of an installation identification this ID need to be unaltered until removal from device.
PSU-Geo-Location	Geo Location	Optional	The forwarded Geo Location of the corresponding HTTP request between PSU and TPP if available.

Забележка: Информация за Ползвател / ДПУ интерфейса може да се използва от ДПУОС като входни данни за системите за откриване на измами и за управление на риска си. Някои ДПУОС използват тази информация и за да изключат някои методи за удостоверяване (например някои ДПУОС не позволяват получаване на OTP чрез SMS на същия смартфон, използван и за самата транзакция). В допълнение, ДПУОС може да се наложи да получава конкретна информация, свързана с устройството, за да може да поддържа оптимизирана процедура за пренасочване на приложение-към-приложение за TPP. Поради тези причини силно се препоръчва TPP да включва цялата тази информация в съответните съобщения за заявка. Липсващата информация може да доведе до оценка на потребителското устройство като неприложимо за метода за удостоверяване или до класификация на текущата транзакция

като „трансакция с по-висок риск“, напр. поради атаки свързани със сесията. По този начин вероятността за отхвърляне на тази трансакция поради резултат от откриване на измами и / или управление на риска може да бъде увеличена, вж. [XS2A-SecB] за подробности.

4.9. Изисквания за идентификация на ДПУ

[PSD2] задължава идентифицирането на ДПУ да е чрез eIDAS сертификати, свързани с PSD2. Специфичните сертификати, които ще се използват в контекста на PSD2, са посочени в [ETSI PSD2]. Изискванията, дефинирани в [XS2A-OR], изискват на ДПУ идентификация чрез QWAC и / или QSEAL сертификат, използван от ДПУ.

ДПУ е отбелязан в eIDAS сертификата със законното си име. И все пак ДПУ може да използва търговски наименования (марки) към Ползвателя, които силно се различават от законното му име. По този начин може да е от полза за ДПУ, ако ДПУОС е в състояние да използва същите търговски наименования на ДПУ спрямо Ползвателя във всички свързани с Ползвателя процеси като SCA. Конкретни наименования на търговската марка на ДПУ могат да бъдат въведени в полето за сертификат на организационната единица (маркирано с етикет „OU“). ДПУОС може да игнорира записи в това поле.

Пояснение: Използването на полето OU на сертификат от ДПУ ще доведе до използването на няколко сертификата, ако ДПУ възнамерява да използва различни търговски марки при работата си.

Забележка: Използването на повече от един сертификат от ДПУ, напр. поради различни записи в OU не означава, че управлението на съгласието третира тези различни сертификати като различни единици. По подразбиране законният собственик на сертификата е контрагент за управление на достъпа чрез съгласие, а не търговската марка, цитирана в полето на OU.

4.10. Изисквания към URIs на ДПУ

ДПУ може да предостави няколко URI на ДПУОС като параметри за следващи стъпки на протокола на взаимодействие. От съображения за сигурност трябва да се гарантира, че тези URI са защитени от eIDAS QWAC на ДПУ, използван за идентифициране на ДПУ. Прилага се следното:

URI, които се предоставят от ДПУ в TPP-Redirect-URI или TPP-Nok-Redirect-URI, трябва да съответстват на домейна, защитен от eIDAS QWAC сертификата на ДПУ в полето CN или SubjectAltName на сертификата. Моля, обърнете внимание, че в случай на example-TPP.com като въвеждане на сертификат TPP-Redirect-URI като

- www.example-TPP.com/xs2a-client/v1/ASPSIdentification/mytransaction-id или
- redirections.example-TPP.com/xs2a-client/v1/ASPSIdentification/mytransaction-id

биха били съвместими.

Дефинициите със заместващи символи се вземат предвид при проверките за съответствие от ДПУОС.

Пояснение за в бъдеще: ДПУОС в бъдеще могат да отхвърлят заявките, ако предоставените URI адреси не отговарят. Това все още не е валидно за текущата версия на спецификацията.

Пояснение за в бъдеще: Поради причини за миграция, тази спецификация дава мандат на ДПУ да поддържа TPP-Redirect-URI, използван във всички процеси на разрешаване за конкретна трансакция по време на жизнения цикъл на тази трансакция. Това може да бъде премахнато в следващата версия на спецификацията.

Пояснение за в бъдеще: Ограниченията за URI ще се прилагат за URI на ДПУ, използвани в бъдещи push услуги на ДПУОС.

4.11. Методи на достъп чрез API (API Access Methods)

Следващите таблици съдържат общ преглед на методите за достъп по HTTP, поддържани от крайните точки на приложния програмен интерфейс (API), и от ресурси, създадени чрез този API.

Приложният Програмен Интерфейс (API) изготвен от ДПУ трябва да поддържа стандартните методи за достъп съгласно HTTP протокола.

Метод POST – за създаване на ресурс. (Инициране на плащане; Предоставяне на съгласие)

Метод PUT - В случаи за установяване на идентичност на ползвателя при метод Embedded

Метод GET – за получаване на информация, свързана с услуга ДОСТЪП ДО СМЕТКА. Примерно при искане за резултат от заявка или искане за статус на плащане.

Метод DELETE – за изтриване на данни по конкретно съгласие за ДОСТЪП ДО СМЕТКА.

Освен това е дефинирано дали тази поддръжка на метода е задължителна или опционална за ДПУОС по тази спецификация.

Следва таблица с методите на достъп и управление на конкретни ресурси

4.11.1. Крайни точки за Разплащания

Endpoints/Resources	Method	Condition	Description
payments/{payment-product}	POST	Mandatory	Create a payment initiation resource addressable under {paymentId} with all data relevant for the corresponding payment product. This is the first step in the API to initiate the related payment. Section 5.3.1 and 5.3.2
payments/{payment-product}/{paymentId}	GET	Mandatory	Read the details of an initiated payment. Section 5.5
payments/{payment-product}/{paymentId}/status	GET	Mandatory	Read the transaction status of the payment. Section 5.4
bulk-payments/{payment-product}	POST	Optional	Create a bulk payment initiation resource addressable under {paymentId} with all data relevant for the corresponding payment product. This is the first step in the API to initiate the related bulk payment. Section 5.3.3
bulk-payments/{payment-product}/{paymentId}	GET	Mandatory	Read the details of an initiated bulk payment. Section 5.5
bulk-payments/{payment-product}/{paymentId}/status	GET	Mandatory	Read the transaction status of the bulk payment. Section 5.4
periodic-payments/{payment-product}	POST	Optional	Create a standing order initiation resource for recurrent i.e. periodic payments addressable under {paymentId} with all data relevant for the corresponding payment product and the execution of the standing order. This is the first step in the API to initiate the related recurring/periodic payment. Section 5.3.4
periodic-payments/{payment-product}/{paymentId}	GET	Mandatory	Read the details of an initiated standing order for recurring/periodic payments. Section 5.4
periodic-payments/{payment-product}/{paymentId}/status	GET	Mandatory	Read the transaction status of the standing order for recurring/periodic payments. Section 5.4
{payment-service}/{payment-product}/{paymentId}/authorisations	POST	Mandatory	Create an authorization sub-resource and start the authorization process, might in addition transmit authentication and authorization related data. This method is iterated n times for a n times SCA authorization in a corporate context, each creating an own authorization sub-endpoint for the corresponding PSU authorizing the transaction.

			The ASPSP might make the usage of this access method unnecessary in case of only one SCA process needed, since the related authorization resource might be automatically created by the ASPSP after the submission of the payment data with the first POST payments/{payment-product} call. Section 7.1
{payment-service}/{payment-product}/{paymentId}/authorisations	GET	Mandatory	Read a list of all authorization sub-resources Ids which have been created. Section 7.4
{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}	PUT	Mandatory for Embedded SCA Approach, Conditional for other approaches	Update data on the authorization resource if needed. It may authorize a payment within the Embedded SCA Approach where needed. Independently from the SCA Approach it supports e.g. the selection of the authentication method and a non-SCA PSU authentication. Section 7.2 and Section 7.3
{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}	GET	Mandatory	Read the SCA status of the authorization. Section 7.5
{payment-service}/{payment-product}/{paymentId}	DELETE	Optional	Cancels the addressed payment with resource identification paymentId if applicable to the payment-service, payment-product and received in product related timelines (e.g. before end of business day for scheduled payments of the last business day before the scheduled execution day). The response to this DELETE command will tell the TPP whether the - access method was rejected - access method was successful, or - access method is generally applicable, but further authorization processes are needed.
{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations	POST	Optional	Starts the authorization of the cancellation of the addressed payment with resource identification paymentId if mandated by the ASPSP (i.e. the DELETE access method is not sufficient) and if applicable to the payment-service, and received in product related timelines (e.g. before end of business day for scheduled payments of the last business day before the scheduled execution day). Section 7.1
{payment-service}{payment-product}/{paymentId}/cancellation-authorisations	GET	Optional	Retrieve a list of all created cancellation authorization sub-resources. If the POST command on this endpoint is supported, then also this GET method needs to be supported. Section 5.7
{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}	PUT	Mandatory for Embedded SCA Approach, Conditional for other approaches	Update data on the cancellation authorization resource if needed. It may authorize a cancellation of the payment within the Embedded SCA Approach where needed. Independently from the SCA Approach it supports e.g. the selection of the authentication method and a non-SCA PSU authentication. Section 7.2 and Section 7.3
{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}	GET	Mandatory	Read the SCA status of the cancellation authorization. Section 7.5

4.11.2. Крайни точки за Информация по сметка

Endpoints/Resources	Method	Condition	Description
accounts	GET	Mandatory	Read all identifiers of the accounts, to which an account access has been granted to through the /consents endpoint by the PSU. In addition, relevant information about the accounts and hyperlinks to corresponding account information resources are provided if a related consent has been already granted. - Remark: Note that the /consents endpoint optionally offers to grant an access on all available payment accounts of a PSU. In this case, this endpoint will deliver the information about all available payment accounts of the PSU at this ASPSP. Section 6.6.1
accounts/?withBalance	GET	Optional	Read the identifiers of the available payment account together with booking balance information, depending on the consent granted. Section 6.6.1
accounts/{account-id}	GET	Mandatory	Give detailed information about the addressed account. Section 6.6.2
accounts/{account-id}/?withBalance	GET	Optional	Give detailed information about the addressed account together with balance information. Section 6.6.2
accounts/{account-id}/balances	GET	Mandatory	Give detailed balance information about the addressed account. Section 6.6.3
accounts/{account-id}/transactions	GET	Mandatory	Read transaction reports or transaction lists of a given account, depending on the steering parameter "bookingStatus" For a given account, additional parameters are e.g. the attributes "dateFrom" and "dateTo". The ASPSP might add balance information, if transaction lists without balances are not supported. Section 6.6.4
accounts/{account-id}/transactions/?withBalance	GET	Optional	Read transaction reports or transaction lists of a given account, depending on the steering parameter "bookingStatus" together with balances. Section 6.6.4
accounts/{account-id}/transactions/{transaction-id}	GET	Optional	Read transaction details of an addressed transaction. Section 6.6.5

Забележка: Имайте предвид, че параметрите {account-id} могат да бъдат маркирани от ДПУОС така, че реалните номера на сметки, като IBAN или PAN, да не са част от дефинициите на API за целите на защитата на данните. Тази токънизация се управлява от ДПУОС.

4.11.3. Крайна точка за картова сметка

Тази крайна точка доставя информация за сметката, свързана с кредитна карта, където сметката се използва за съгласуване на транзакциите с кредитни карти на Ползвателя. Тази крайна точка не е пряко свързана с кредитните карти като такива, а с финансовата сметка зад съответните карти.

Endpoints/Resources	Method	Condition	Description
---------------------	--------	-----------	-------------

card-accounts	GET	Optional	Read all identifiers of the card accounts, to which an account access has been granted to through the /consents endpoint by the PSU. In addition, relevant information about the card accounts and hyperlinks to corresponding account information resources are provided if a related consent has been already granted. Section 6.7.1
card-accounts/{account-id}	GET	Optional	Give detailed information about the addressed card account. Section 6.7.2
card-accounts/{account-id}/balances	GET	Optional	Give detailed balance information about the addressed card account. Section 6.7.3
card-accounts/{account-id}/transactions	GET	Mandatory	Read transaction reports or transaction lists related to a given card account For a given card account, additional parameters are e.g. the attributes "dateFrom" and "dateTo". Section 6.7.4

Забележка: Имайте предвид, че параметрите {card-account-id} могат да бъдат маркирани от ДПУОС така, че реалните номера на сметки, като IBAN или PAN, да не са част от дефинициите на API за целите на защитата на данните. Тази токенизация се управлява от ДПУОС

4.11.4. Крайна точка за съгласие

Endpoints/Resources	Method	Condition	Description
consents	POST	Mandatory	Create a consent resource, defining access rights to dedicated accounts of a given PSU-ID. These accounts are addressed explicitly in the method as parameters as a core function. Section 6.4.1
consents	POST	Optional	As an option, an ASPSP might optionally accept a specific access right on the access on all psd2 related services for all available accounts. As another option an ASPSP might optionally also accept a command, where only access rights are inserted without mentioning the addressed account. The relation to accounts is then handled afterwards between PSU and ASPSP. This option is supported only within the Decoupled, OAuth2 or Re-direct SCA Approach. As a last option, an ASPSP might in addition accept a command with access rights - to see the list of available payment accounts or - to see the list of available payment accounts with balances. Section 6.4.1
consents/{consentId}	GET	Mandatory	Reads the exact definition of the given consent resource {consentId} including the validity status. Section 6.4.3
consents/{consentId}	DELETE	Mandatory	Delete the addressed consent. Section 6.5
consents/{consentId}/status	GET	Mandatory	Read the authentication status of the addressed consent resource. Section 6.4.2
consents/{consentId}/authorisations	POST	Mandatory	Create an authorization sub-resource and start the authorization process, might in addition transmit authentication and authorization related data. The ASPSP might make the usage of this access method unnecessary, since the related

			authorization resource will be automatically created by the ASPSP after the submission of the consent data with the first POST consents call. Section 7.1
consents/{consentId}/authorisations	GET	Mandatory	Read a list of all authorisation sub-resources IDs which have been created. Section 7.4
consents/{consentId}/authorisations/{authorisationId}	PUT	Mandatory for Embedded SCA Approach, conditional for other SCA approaches	Update data on the authorization resource if needed. It may authorize a consent within the Embedded SCA Approach where needed. Independently from the SCA Approach it supports e.g. the selection of the authentication method and a non-SCA PSU authentication. Section 7.2 and Section 7.3
consents/{consentId}/authorisations/{authorisationId}	GET	Mandatory	Read the SCA status of the authorization. Section 7.5

4.11.5. Крайна точка за съгласие за Потвърждение на наличност на средства по сметка

Endpoints/Resources	Method	Condition	Description
consents/confirmation-of-funds	POST	Optional	Create a consent resource to register a TPP for the confirmation of funds service for a given account by a PSU for a given PSU ID. Section 10.2
consents/confirmation-of-funds/{consentId}	GET	Mandatory	Reads the exact definition of the given consent resource {consentId} including the validity status. Section
	DELETE	Mandatory	Terminate the addressed consent. Section
consents/confirmation-of-funds/{consentId}/status	GET	Mandatory	Read the consent status of the addressed consent resource. Section
consents/confirmation-of-funds/{consentId}/authorisations	POST	Mandatory	Create an authorisation sub-resource and start the authorisation process, might in addition transmit authentication and authorisation related data. The ASPSP might make the usage of this access method unnecessary, since the related authorisation resource will be automatically created by the ASPSP after the submission of the consent data with the first POST consents call. Cp. [XS2A-IG]
consents/confirmation-of-funds/{consentId}/authorisations/{authorisationId}	PUT	Mandatory for Embedded SCA Approach, Conditional for other approaches	Update data on the authorisation resource if needed. It may authorise a consent within the Embedded SCA Approach where needed. Independently from the SCA Approach it supports e.g. the selection of the authentication method and a non-SCA PSU authentication. Cp. [XS2A-IG]
consents/confirmation-of-funds/{consentId}/authorisations/{authorisationId}	GET	Mandatory	Read the SCA status of the authorisation. Cp. [XS2A-IG]

4.11.6. Крайна точка за подписване на кошница

Endpoints/Resources	Method	Condition	Description
signing-baskets	POST	Optional	Create a signing basket resource for authorizing several transactions with one SCA method. The resource identifications of these transactions are contained in the payload of this access method. Section 8.1
signing-baskets/{basketId}	GET	Optional	Retrieve the signing basket content. Section 8.2
signing-baskets/{basketId}/status	GET	Optional	By ERRATA 07.02.2019
signing-baskets/{basketId}	DELETE	Mandatory	Delete the signing basket structure as long as no authorization has yet been applied. The underlying transactions are not affected by this deletion. Section 8.4
signing-baskets/{basketId}/authorisations	POST	Mandatory	Create an authorization sub-resource and start the authorization process, might in addition transmit authentication and authorization related data. The ASPSP might make the usage of this access method unnecessary, since the related authorization resource will be automatically created by the ASPSP after the submission of the basket data with the first POST consents call. Section 7.1
signing-baskets/{basketId}/authorisations/{authorisationId}	PUT	Mandatory for Embedded SCA Approach, conditional for other SCA approaches	Update data on the authorization resource if needed. It may authorize all transactions in the addressed signing basket within the Embedded SCA Approach where needed. Independently from the SCA Approach it supports e.g. the selection of the authentication method and a non-SCA PSU authentication. Section 7.2 and Section 7.3
signing-baskets/{basketId}/authorisations/{authorisationId}	GET	Mandatory	Read the SCA status of the authorization. Section 7.5

4.11.7. Крайна точка за потвърждение на наличност по сметка

Endpoints/Resources	Method	Condition	Description
funds-confirmations	POST	Mandatory	Checks whether a specific amount is available at point of time of the request on an account linked to a given tuple card issuer(TPP)/card number, or addressed by IBAN and TPP respectively. Section 10.2

Забележка: Методите PUT HTTP могат да бъдат адаптирани към техническите PATCH методи в бъдеща версия на спецификацията. Съответното решение ще се отрази в настоящите пазарни практики и работата по ISO TC68 / SC9 / WG2 за Финансовите API услуги.

4.12. HTTP Response Codes and Additional Error Information

Трябва да се прави разлика между отговорите на ниво HTTP и отговорите на ниво Response Body. Кодът за отговор на ниво HTTP протокол, съобщава за успешно или неуспешно приемане на заявка от ДПУ. Статусът на искането за плащане или съгласие обикновено се връща като HTTP код 200 (успешна) независимо дали действителното плащане от съобщението

или съгласието е успешно завършено или не. Кодовете за отговор на HTTP 4XX трябва да се дават само ако настоящата заявка не може да бъде изпълнена.

На ниво Response Body се предоставят отговори, свързани с успешното изпълнение или доставка на ресурса.

Следва Таблица с кодовете и отговорите на ниво HTTP:

Status code	Description
200 OK	PUT, GET Response Codes This return code is permitted when the request is repeated due to a time-out. The response in that might be either a 200 or 201 code depending on the ASPSP implementation. The POST for a Funds request will also return 200 since it does not create a new resource. DELETE Response Code where a payment resource has been cancelled successfully and no further cancellation authorization is required.
201 Created	POST Response code where Payment Initiation or Consent Request was correctly performed.
202 Accepted	DELETE response code, where a payment resource can be cancelled in general, but where a cancellation authorization is needed in addition.
204 No Content	DELETE Response code where a consent resource was successfully deleted. The code indicates that the request was performed, but no content is returned.
400 Bad Request	Validation error occurred. This code will cover malformed syntax in request or incorrect data in payload.
401 Unauthorized	The TPP or the PSU is not correctly authorized to perform the request. Retry the request with correct authentication information.
403 Forbidden	Returned if the resource that was referenced in the path exists but cannot be accessed by the TPP or the PSU. This code should only be used for non-sensitive id references as it will reveal that the resource exists even though it cannot be accessed.
404 Not found	Returned if the resource that was referenced in the path does not exist or cannot be referenced by the TPP or the PSU. When in doubt if a specific id in the path is sensitive or not, use http code 404 instead of 403.
405 Method Not Allowed	This code is only sent when the http method (PUT, POST, DELETE, GET etc) is not supported on a specific endpoint. It has nothing to do with the consent, payment or account information data model. DELETE Response code in case of cancellation of a payment initiation, where the payment initiation cannot be cancelled due to legal or other operational reasons
406 Not Acceptable	The ASPSP cannot generate the content that the TPP specified in the Accept header.
408 Request Timeout	The sever is still working correctly, but an individual request has timed out.
409 Conflict	The request could not be completed due to a conflict with the current state of the target resource.
415 Unsupported Media Type	The TPP has supplied a media type which the ASPSP does not support.
429 Too Many Requests	The TPP has exceeded the number of requests allowed by the consent or by the RTS.
500 Internal Server Error	Internal server error occurred.
503 Service Unavailable	The ASPSP server is currently unavailable. Generally, this is a temporary state.

4.13. Допълнителна информация за грешки

За да се постигне по-добра четимост, основната част на документа описва отговорите само в случай на положителен резултат от обработката. Следващият раздел дава конкретни правила за случай на отрицателен резултат от обработката.

4.13.1. Header

Като цяло, едни и същи правила относно наличието на заглавни елементи се прилагат и за положителни, и за отрицателни отговори. Изключение се прави за случаите, когато е възникнала грешка преди самата обработка. Примери за такива случаи на грешки са общи грешки на сървъра (обикновено с 50x http код за отговор) и - в зависимост от изпълнението - валидиране на сертификата. В тези случаи на грешка ДПУОС може да пропусне посочените заглавни елементи. Когато обаче вече е проведена функционална обработка, ДПУОС все още се изисква да включва задължителните (и ако е приложимо условните) заглавни елементи също в отрицателен отговор.

4.13.2. Body

Всички описания на елементите на тялото в документа се прилагат само за случаи с положителен отговор. Съответните атрибути също трябва да бъдат предоставени в тялото, където е възможно и приложимо. Освен това API трябва да предлага допълнителна информация за грешки, както е описано в раздел 4.13.3, когато API сървърът е технически в състояние да я предостави.

4.13.3. Допълнителна информация за грешки

Ако е необходимо, ДПУОС може да съобщи на ДПУ допълнителна информация за грешка в диалога "заявка / отговор" в резултат на който се получават кодовете за отговор HTTP 4xx или 5xx. Тази спецификация предлага две възможности за ДПУОС - да предават само основната или основната заедно с допълнителната информация за грешки. ДПУОС може да избере едно от решенията. Имайте предвид, че допълнителната информация за грешка е детайлният код за грешка, който обогатява информацията на основния тип "Код на съобщението", както е дефиниран в раздел 14.11.

В случаите, когато няма дефиниран основен код за грешка в отговора по HTTP response code в Раздел 14.11, не може да се използва и допълнителна информация за грешка.

4.13.3.1. Специфична допълнителна информация за грешки по NextGenPSD2

Спецификацията по NextGenPSD2 предлага собствен начин за транспортиране на допълнителна информация за грешки. В нея, допълнителната информация за грешка се изпраща до ДПУ с помощта на елемент от данни tppMessageInformation и атрибут "category" със стойност "ERROR". Атрибутът "code" показва грешката, ср. Раздел 14.11 и, ако е приложимо, пътя на елемента на съобщението за заявка, който провокира това съобщение за грешка. Освен това се предлага поле в свободен текст, за описание на грешката или действията, които трябва да бъдат предприети от ДПУ.

Този елемент на грешка може да бъде вграден във всички съобщения на базата на JSON от интерфейса Достъп до сметка. Ако към ДПУ бъде изпратена информация за грешка, състоянието на транзакцията винаги е "Отхвърлена".

Пример 1: (Access token not correct)

```
{ "tppMessages": [ {  
  "category": "ERROR",  
  "code": "TOKEN_INVALID",
```

```

        "text": "additional text information of the ASPSP up to 512
characters"
    } ]
}

```

В допълнение съобщението за отговор може да съдържа секция `_links`, съдържаща хипервръзка, за да съобщи на ДПУ следващата стъпка, с цел да избегне следващи грешки. Раздел 4.12. Това се отнася особено за случаите на грешки при автентикация на Ползвателя, когато може да се наложи повторно въвеждане на данните за авторизация чрез ДПУ.

Пример 2: (Password incorrect)

```

{"tppMessages": [{
  "category": "ERROR",
  "code": "PSU_CREDENTIALS_INVALID",
  "text": "additional text information of the ASPSP up to 512 characters"
}],
 "_links": {
  "updatePsuAuthentication": {"href": "/v1/payments/sepa-credit-
transfers/1234-wertiq-983/authorisations/123auth456"}
}
}

```

4.13.3.2. Стандартизирана допълнителна информация за грешки

В [RFC 7807](#) е описано стандартно определение на информацията за грешки. По-долу са дефинирани изисквания за това как да се използва тази стандартизирана информация за грешки в контекста на интерфейса NextGenPSD2 XS2A.

Response Code

Отговорите за грешки на ниво HTTP от типове 4xx или 5xx са дефинирани в раздел 4.9.

Response Header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	The string application/problem + json is used

Response Body

Attribute	Type	Condition	Description
type	Max70Text	Mandatory	A URI reference [RFC3986] that identifies the problem type. Remark For Future: These URI will be provided by NextGenPSD2 in future.
title	Max70Text	Optional	Short human readable description of error type. Could be in local language. To be provided by ASPSPs.
detail	Max500Text	Optional	Detailed human readable text specific to this instance of the error. XPath might be used to point to the issue generating the error in addition. Remark for Future: In future, a dedicated field might be introduced for the XPath.
code	Message Code	Mandatory	Message code to explain the nature of the underlying error.

additionalErrors	Array of Error Information	Optional	Might be used if more than one error is to be communicated
_links	Links	Optional	Should refer to next steps if the problem can be resolved e.g. for re-submission of credentials.

Пример:

HTTP/1.1 401 Unauthorized

Content-Type: application/problem+json

Content-Language: en

```
{
  "type": "https://berlingroup.com/error-codes/TOKEN_INVALID",
  "title": "The OAuth2 token is associated to the TPP but is not valid for the addressed service/resource.",
  "detail": "additional text information of the ASPSP up to 512 characters ",
  "code": "TOKEN_INVALID",
  "additionalErrors": [ {
    "title": "The PSU-Corporate-ID cannot be matched by the addressed ASPSP.",
    "detail": "additional text information of the ASPSP up to 512 characters",
    "code": "CORPORATE_ID_INVALID"
  }, ... ],
  "_links": { }
}
```

4.14. Информация за статус

4.14.1. Информация за статус при услуга за инициране на плащане

Системите от типа backend на ДПУОС за плащания, поддържат статуса на транзакцията, който е дефиниран в стандарт ISO20022 и се разглежда в тази спецификация като елемент от данни "transactionStatus". ДПУОС ще доставя този статус във всички съобщения за отговор след като е бил създаден ресурс за инициране на плащане и ако съответното заявено съобщение е правилно форматирано и няма друга тежка грешка при обработката.

Статусът на транзакцията при инициране на плащане се променя по време на процеса на инициране, в зависимост от резултата при под-стъпки като проверки на формати, проверки на SCA, проверки на сметка, свързани със съгласието или свободната наличност, или в зависимост от началото на процесите за подготовка на деня.

В края на платежния процес състоянието на транзакцията в подсистемата на ДПУОС е "RJCT", което означава "Отхвърлено" или "ACSC", което означава "AcceptedSettlementCompleted". В зависимост от процеса на осчетоводяване на ДПУОС, риска от действителното плащане, състоянието на финансовата сметка на сметката на Ползвателя или датата и часа на инициране, последният статус може да бъде достигнат след определен период и след като процесът на започване на плащането е бил такъв финализиран. Следователно, информацията за статус в процеса на обработка на иницираното плащане може да се раздели на следните кодове:

- "PDNG", който означава "предстоящ" се използва от ДПУОС за да информира ДПУ относно факта, че плащането не е достигнало базовите проверки;
- "RCVD", който означава "Received" се използва от ДПУОС за да информира ДПУ относно факта, че плащането е достигнало до базовите проверки;

- "ACTC" обозначава "Accepted Technical Validation", с което се потвърждава идентификацията на Ползвателя, и успешната валидация на синтаксиса и семантиката за иницирираното плащане;
- "ACWC" което означава "AcceptedWithChanges", при което проверките за автентикация, синтактични и семантични (продуктови) записи са успешни и ДПУОС информира ДПУ, че някои промени са били приложени при започването на плащането, напр. на заявената дата на изпълнение;
- "ACCP", има значение "Accepted Customer Profile", с което се потвърждава успешна проверка на рисковия профил на Ползвателя;
- "ACFC", което означава "AcceptedFundsChecked", по сметката на Ползвателя наличността на средствата е проверена положително;
- "ACSP", със значение "Accepted Settlement in Process", когато плащането е насочено към платежна система, с очакване на резултат от сетълмента;
- "ACSC", се използва при стандартни плащания отново със значение "Accepted Settlement Completed", което информира за успешен край на плащането от страна на дебитора;
- "ACCC", се използва само при незабавни плащания със значение "Accepted Settlement Completed", което информира за успешен край на плащането от страна на кредитора;
- "RJCT", което означава "Отхвърлено";
- "PART", се използва при иницириране на масово плащане със значение „PartiallyAccepted“, което информира, че всички задължителни авторизации са преминали, но не всички плащания са приети поради други причини.

ДПУ може да поиска чрез заявка към ДПУОС да се информира за състоянието на техническия процес на ЗУИ като част от процеса на иницириране на плащането. Използва се съобщението GET SCA Status Response Message. Отговорът за статуса на идентификацията се предоставя чрез елемента за данни "scaStatus".

При проверка за наличност, спецификацията предоставя незадължителен елемент

```
"fundsAvailable": true/false
```

Който може да се използва заедно с кодовете "ACTC", "ACWC" и "ACCP" в съобщението за отговор на състоянието. Чрез него се указва, че проверката на средствата е била обработена с посочения резултат. Това е един и същ елемент от данните, използван в заявката за потвърждаване на средствата, и може да бъде използван от ДПУОС, за да информира ДПУ за наличността на средства, съгласно изискванията на [EBA-RTS].

Дори ако проверката на средствата е положителна, плащането може да бъде отхвърлено на по-късна фаза поради други причини.

Пример 1: Минала е техническа валидация и положителна проверка за наличност

```
{"transactionStatus": "ACTC",  
  "fundsAvailable": true}
```

В случай, че няма налични средства, плащането може все още да не бъде отхвърлено поради практиката на ДПУОС и че ще чака ликвидност за определен период от време.

Пример 2: Проверен е клиентския профил и по сметката няма достатъчно наличност, но плащането все още не е отхвърлено.

```
{"transactionStatus": "ACCP",  
  "fundsAvailable": false}
```

Плащане с бъдеща дата и периодичните плащания са двата вида плащания, които не се изпълняват директно след инициирането. За двата вида плащания ДПУОС може да има намалена или никаква проверка на потребителския профил или наличността на средства, поради факта, че действителните плащания се извършват по-късно. Крайният статус по време на процеса на иницииране на плащането е "ACTC" или "ACCP" в зависимост от процедурите на ДПУОС в своите онлайн канали. Елементът за данни за наличните средства "fundsAvailable" също може да се съдържа в случай, че е извършена проверка на наличността на средствата при започването на плащането.

Статус за отменено плащане - След успешно анулиране на инициирано плащане, съответният статус на транзакцията приема стойност "CANC". Този статус на транзакцията ще се връща, докато отмененият ресурс за иницииране на плащането е адресируем.

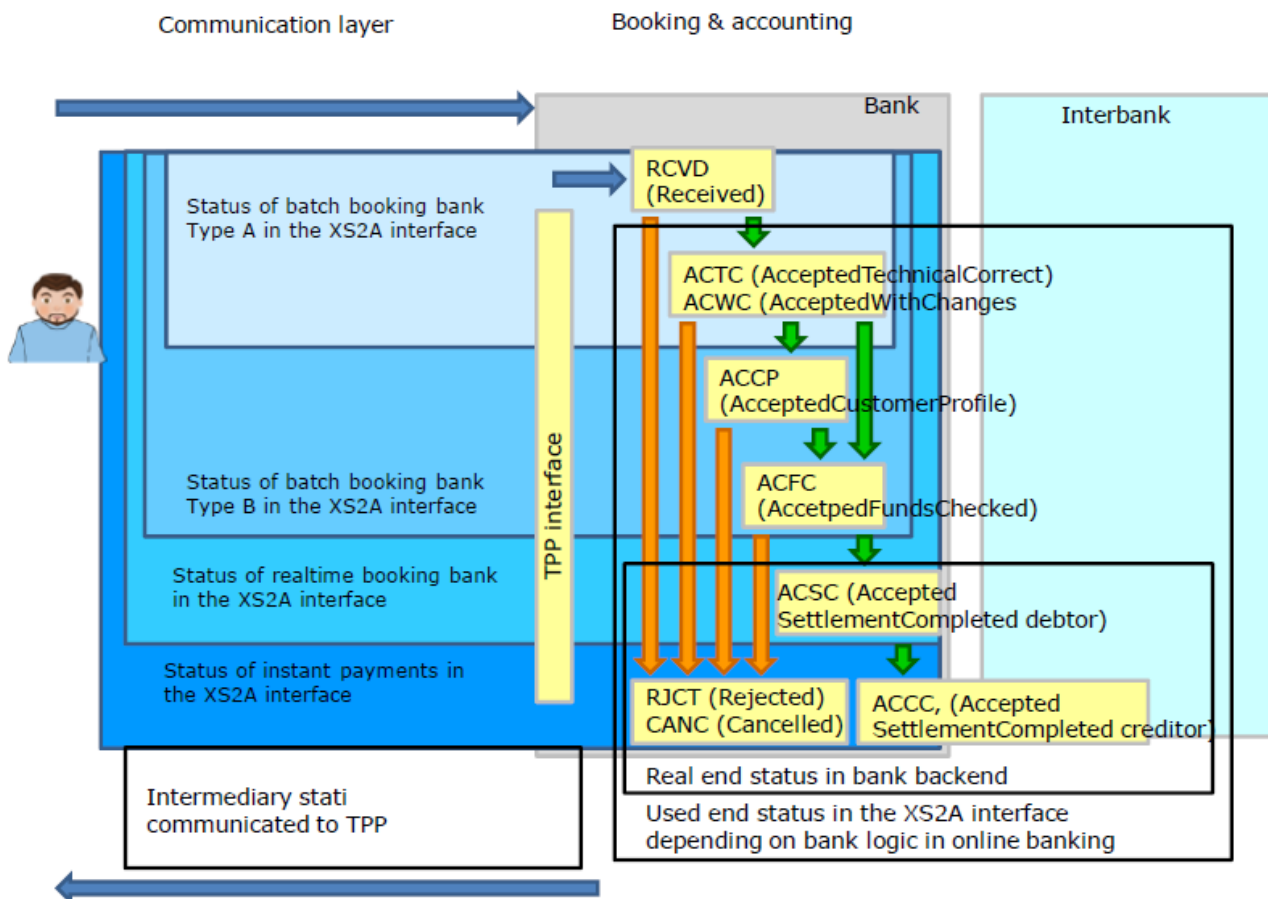
Забележка: Този код все още не е част от кодовете за състоянието на транзакциите по ISO20022. Берлинската група ще внесе съответно искане за промяна.

Статус за частично оторизирано плащане в процеса на множествена ЗУИ – Въвежда се допълнителен статус "PATC" за "Partially Accepted Technical Correct". Инициирано плащане, което е оторизирано поне от един Ползвател, но все още не е окончателно оторизирано от всички изискуеми Ползватели.

Общ модел на Информация за статус

Следващата картинка предоставя общия модел за трансформацията на съобщението през различните статуси в неговия жизнен цикъл:

Statuses according applied checks



4.14.2. Информация за статус при услуга за Информация по сметка като процес от предоставяне на съгласие

Услугите за Информация по сметка представляват ресурси, описани в съгласието на ползвателя пред ДПУОС. В процеса на Установяване на съгласие, статусът на ресурсите в съгласието може да се променя. За разлика от процеса на инициране на плащане, при проверка на ресурса за съгласие е необходимо само ЗУИ и няма обратна връзка с backend приложенията на ДПУОС. Елементът за данни за статуса на съгласието се дефинира като "consentStatus".

Във фазата Установяване на съгласие, за елемента „consentStatus“ се поддържат кодовете "received", "rejected" и "valid". Те се отнасят за цялото съгласие.

След успешно оторизиране на съгласие от страна на Ползвателя, отделните ресурси в съгласието може да променят статуса си по време на жизнения цикъл, за което се поддържат следните кодове:

- "expired": Съгласието е изтекло (например след 90 дни).
- "revokedByPsu": Съгласието е отменено от Ползвателя
- "terminatedByTpp": ДПУ е прекратил съгласието

ДПУ може да изтегли тези статуси в съобщение чрез GET Status Response.

В процеса на установяване на съгласие ДПУОС информира ДПУ за състоянието на техническия процес на ЗУИ в рамките на съобщението GET SCA Status Response Message. За тази цел се използва елементът за данни "scaStatus".

4.15. Хипервръзки за управление на API процеси

Интерфейсът за Достъп до сметка изисква при услугите за Инициране на плащане и Информация за сметката да се направят няколко заявки от ДПУ към ДПУОС. След искането за Инициране на плащане и Искането за съгласие за информация за сметка при ДПУОС се генерира съответния вид ресурс. След това ДПУОС предоставя този ресурс на ДПУ, а в частта Location Header на отговора може да се съдържа хипервръзка към създадения ресурс.

При отговор на искане и на всички следващи заявки в рамките на услугите, ДПУОС може да вгради хипервръзка заедно с "маркер" за нейната семантиката. Тази хипервръзка може да бъде или относителна връзка, (с цел да се спести място, напр. с "/ v1 / payments / sepa-credit-transfers" или може да бъде глобална връзка – от вида:

```
https://www.testbank.com/psd2/v1/payments/sepa-credit-transfers/asdf-asdf-asdf-1234.
```

Глобалните връзки може да са необходими при някои обстоятелства, напр. пренасочване. Маркерът на хипервръзката транспортира функционалността на ресурса, адресиран от връзката, напр. "redirect".

Хипервръзките за управление се транспортират в елемента за данни "_links". Той може да съдържа една или няколко хипервръзки:

```
Пример: "_links": {  
    "redirect": "https://www.testbank.com/asdfasdfasdf",  
    "self": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"  
}
```

Списък на хипервръзките е дефиниран в Секция 14.6

Следва таблица със съдържанието на хипервръзките за управление, както и допълнителни елементи на данните, които се транспортират в контекста на съответната хипервръзка. Допълнителни връзки могат да бъдат добавени от приложенията на ДПУОС. Препоръчва се ДПУОС да опишат в документацията си използването на повече хипервръзки, за да не бъдат игнорирани от ДПУ.

Hyperlink	Additional Link Related Data	Description
startAuthorisationWith PsuAuthentication	(challengeData)	The link to an endpoint where the authorization of a transaction or of a transaction cancellation shall be started, where PSU authentication data shall be uploaded with the corresponding call. Remark: In rare cases the ASPSP will ask only for some dedicated ciphers of the passwords. This information is then transported to the TPP by using the "challenge" data element, normally used only in SCA context.
startAuthorisationWith EncryptedPsuAuthentication	(challengeData)	Same as startAuthorisationWith PsuAuthentication, but password is encrypted on application layer when uploaded.
updatePsuAuthentication	(challengeData)	The link to the payment initiation/consent resource, which needs to be updated by a PSU password and eventually the PSU identification if not delivered yet. Remark: In rare cases the ASPSP will ask only for some dedicated ciphers of the passwords. This information is then transported to the TPP by using the "challenge" data element, normally used only in SCA context.
updateEncryptedPsu Authentication	(challengeData)	Same as updatePsuAuthentication, but password is encrypted on application layer when uploaded.

startAuthorisationWith AuthenticationMethodSelection	scaMethods	This is a link to and endpoint where the authorization of a transaction or of a transaction cancellation shall be started, where the selected SCA method shall be uploaded with the corresponding call.
selectAuthenticationMethod	scaMethods	This is a link to a resource, where the TPP can select the applicable strong customer authentication methods for the PSU, if there were several available authentication methods.
authoriseTransaction	challengeData, chosenScaMethod	A link to the resource, where a "Transaction Authorization Request" can be sent to. This request transports the result of the SCA method performed by the customer, generating a response to the challenge data.
startAuthorisationWith TransactionAuthorisation	challengeData, chosenSCAMethod	A link to an endpoint, where an authorization of a transaction or a cancellation can be started, and where the response data for the challenge is uploaded in the same call for the transaction authorization or transaction cancellation at the same time in the Embedded SCA Approach.

4.16. Разширяване на атрибутите за данни

ДПУОС може да добавя и други атрибути за данни към съобщенията за отговор. Такива разширения трябва да бъдат документирани в документацията на ДПУОС за неговия интерфейс Достъп до сметка. Тези атрибути на данни могат да бъдат игнорирани от ДПУ или могат да бъдат интерпретирани, само както е определено от документацията на ДПУОС.

ДПУОС може да добави допълнителни незадължителни атрибути за данни, които да бъдат подадени, напр. за създаване на допълнителни услуги. Освен това, ДПУОС може да поиска от ДПУ да подаде данни за обработка на собствен тип данни (Proprietary Data). Това изискване трябва да се публикува от ДПУОС в документацията му.

Забележка: Преди да се дефинират допълнителни атрибути, от ДПУОС се изисква да представи тяхното описание на работната група NextGen в Берлинската група, където ще бъде взето решение за стандартизиран подход за съответните атрибути на данни.

4.17. Попълване на атрибутите за данни

За да предостави качествена услуга на своите Ползватели чрез ДПУ и да е в синхрон със становище на Европейския Банков Орган (ЕБО) относно пречките при предоставяне на услуги от трети страни съгласно PSD2, ДПУОС трябва да изпълни следните препоръки, които се отнасят и за предишни версии на този стандарт:

4.17.1. Идентификатор на сметка

Когато сметката има IBAN изражение, тогава да се подава тази стойност в полето iban като идентификатор на сметката в типа Account Reference или Account Details.

4.17.2. TPP-Redirect-URI Header Parameter

Да взема под внимание параметъра TPP-Redirect-URI, когато е подаден от ДПУ и след потвърждаване на съгласието от Ползвателя при Redirect метод, да го препраща на адреса от този параметър. За това има становище ЕВА/ОР/2020/10 на ЕБО от 04.06.2020 г – 16. (ii).

4.17.3. Установяване на съгласие

Да приема заявки за създаване на съгласие, в които не е попълнен IBAN на сметки, т.е. под-атрибути "сметки", "салда" и "транзакции", които да съдържат само празен масив или където се използват под-атрибути "availableAccounts", "availableAccountsWithBalance", или "allPsd2" - всички със стойност "allAccounts" или "allAccountsWithOwnerName", описани в Раздел 6.3.1.2 Искане за установяване на съгласие към списък от сметки или без посочена сметка. Така се премахва пречката за необходимостта от ръчно въвеждане на IBAN от Ползвателя, за която има становище ЕВА/ОР/2020/10 на ЕБО от 04.06.2020 г - Account selection.

4.17.4. Предоставяне на баланс на сметка

Да попълва в отговорите на AIS заявки изброените полета:

- Текущо разполагаемо салдо (balanceType="interimAvailable");

- Дата на баланса (referenceDate).

4.17.5. Предоставяне на списък на трансакции от сметка

Да попълва в отговорите на AIS заявки изброените полета:

- Списък с баланси по сметката (balances) – когато е използван параметъра withBalances и заявеният период е минал, ДПУОС трябва да връща масив от баланси по сметката и този масив да съдържа начален (openingBooked) и краен (closingBooked) баланс за периода на заявката за списък с трансакции;
- Уникален идентификатор на ресурса на трансакцията в ДПУОС (transactionId);
- Account на титуляря на сметката (creditorAccount или debtorAccount) - в стандарта няма изрична индикация за посоката на движение на средства в една трансакция, затова да се използват полетата creditorAccount или debtorAccount. Когато трансакцията е дебитна, се попълва creditorAccount на кореспондента, където е наличен и задължително debtorAccount на титуляря, а когато трансакцията е кредитна, се попълва debtorAccount на кореспондента, където е наличен и задължително creditorAccount на титуляря;
- Account на кореспондента (creditorAccount или debtorAccount), където е наличен;
- Име на кореспондента (или creditorName, или debtorName);
- Дата (bookingDate);
- Вальор (valueDate);
- Основание (remittanceInformationUnstructured).

Примери за трансакции по сметката на титуляря DE67100100101306118605:

- кредитен превод по сметката на титуляря

```
{
  "transactionId": "9577805583",
  "entryReference": "1234567 002",
  "debtorName": "Ivan Ivanov",
  "debtorAccount": {
    "iban": "BG80UNCR70001623981166"
  },
  "creditorAccount": {
    "iban": "DE67100100101306118605"
  },
  "transactionAmount": {
    "currency": "EUR",
    "amount": "2205.67"
  },
  "bookingDate": "2020-10-31",
  "valueDate": "2020-11-01",
  "remittanceInformationUnstructured": "credit transfer"
}
```

- такса – попълнени са:

- creditorName - отсрещната страна, взета такса от сметката на титуляря за превод;
- в debtorAccount е посочена сметката на титуляря, защото трансакцията е дебитна.

```
{
  "entryReference": "1234567",
  "creditorName": "Deutsche Bank",
  "debtorAccount": {
    "iban": "DE67100100101306118605"
  },
  "transactionAmount": {
    "currency": "EUR",
    "amount": "1.67"
  },
  "bookingDate": "2020-10-25",
  "valueDate": "2020-10-26",
  "remittanceInformationUnstructured": "Credit transfer fee"
}
```

- лихва – попълнени са:

- debtorName - отсрещната страна, начислена лихва по сметката на титуляря;

- в creditorAccount е посочена сметката на титуляря, защото трансакцията е кредитна.

```
{
  "entryReference": "1234567 001",
  "debtorName": "Deutsche Bank",
  "creditorAccount": {
    "iban": "DE67100100101306118605"
  },
  "transactionAmount": {
    "currency": "EUR",
    "amount": "2.67"
  },
  "bookingDate": "2020-10-31",
  "valueDate": "2020-11-01",
  "remittanceInformationUnstructured": "Monthly interest"
}
```

- сторно на кредитна операция

```
{
  "transactionId": "3",
  "bookingDate": "2021-01-01",
  "valueDate": "2021-01-01",
  "transactionAmount": {
    "currency": "EUR",
    "amount": "-4.50"
  },
  "debtorAccount": {
    "iban": "DE67100100101306118605",
    "currency": "EUR"
  },
  "remittanceInformationUnstructured": "Incorrect invoice"
}
```

- сторно на дебитна операция

```
{
  "transactionId": "4",
  "bookingDate": "2021-01-01",
  "valueDate": "2021-01-01",
  "transactionAmount": {
    "currency": "EUR",
    "amount": "-4.50"
  },
  "creditorAccount": {
    "iban": "DE67100100101306118605",
    "currency": "EUR"
  },
  "remittanceInformationUnstructured": "Incorrect invoice"
}
```

4.18. Пример

В описания по-долу пример са включени сценариите за подаване на заявка от ДПУ и отговорите от ДПУОС.

Request

- ДПУ изпраща заявка от своето API за изпълнение на плащане от вид SEPA кредитен трансфер
- Следва информация за кодирането и формат на съобщението (JSON)
- Информация за идентификация на трансакцията и идентификационен номер на заявката издадена от ДПУ
- Информация за Ползвателя, IP-address, местоположение и технически параметри
- Дата и час на подаване на заявката
- Детайли за плащането в упоменатия по-горе формат JSON

```
POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Encoding: gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-GEO-Location: GEO:52.506931;13.144558
PSU-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 06 Aug 2017 15:02:37 GMT
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "debtorAccount": {"iban": "DE2310010010123456789"},
  "creditorName": "Merchant123",
  "creditorAccount": {"iban": "DE23100120020123456789"},
  "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

Response in case of a redirect

- ДПУОС връща отговор на ДПУ за успешно приета заявка на ниво HTTP
- Връща отговор, за статуса на заявката за плащане - получено успешно
- Предава информация за идентификационен номер на плащането
- Подава информация към ДПУ за redirect хипервръзка чрез която Ползвателя следва да потвърди своята идентичност
- Информация за хипервръзка (линк към началната точка на заявката) от която Ползвателя на API на ДПУ може да поиска статус на плащането по неговия идентификационен номер след ЗУИ

Response

HTTP/1.x 201 Created

Response Body

```
{
  "transactionStatus": "Received",
  "paymentId": "1234-wertiq-983",
  "_links": {
    "redirect": "https://www.testbank.com/asdfasdfasdf",
    "self": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"
  }
}
```

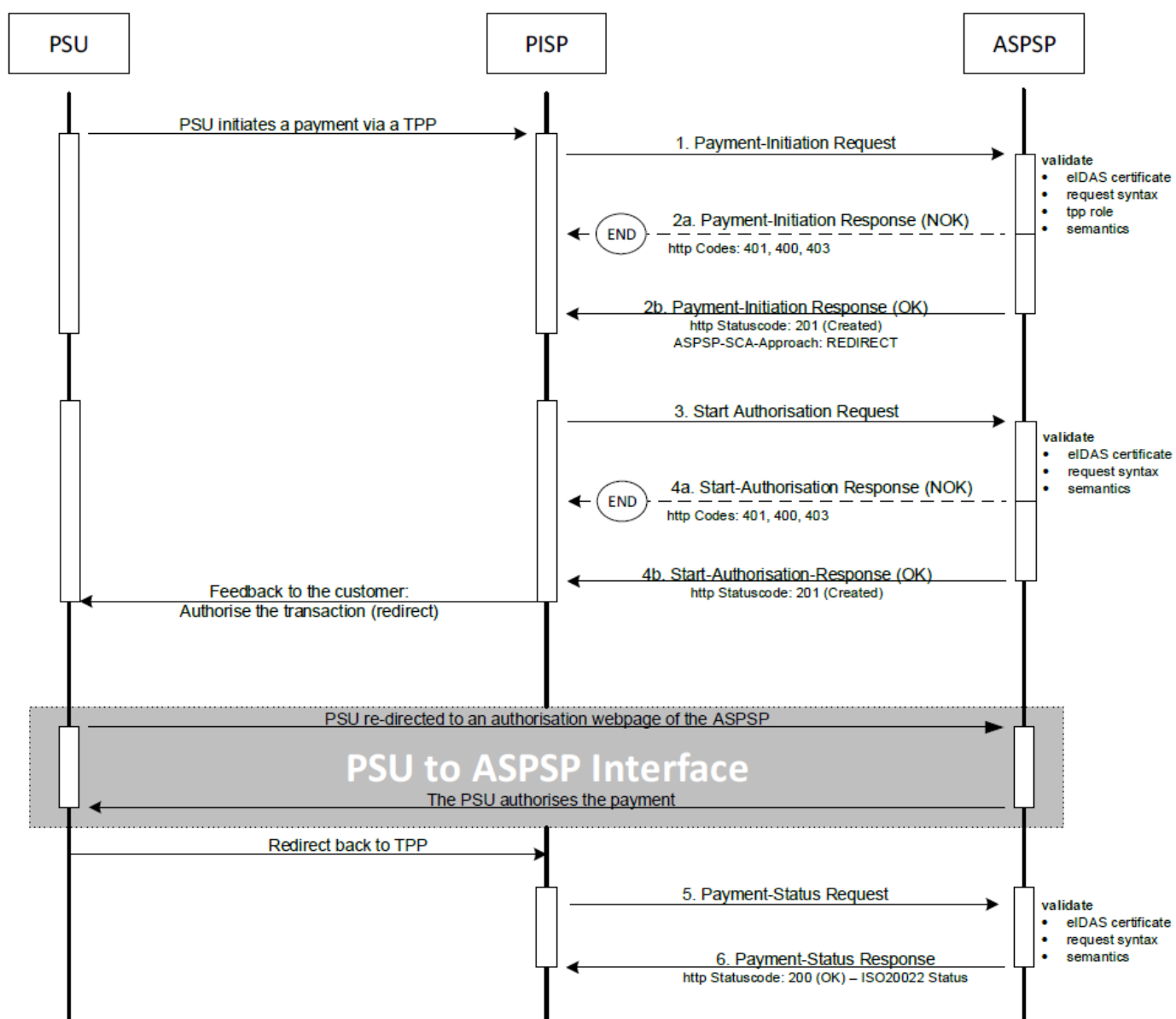
5. Услуга за инициране на плащане

5.1. Процес на Инициране на плащане

Дизайнът на приложния програмен интерфейс (API) се различава при различните подходи на ЗУИ (Embedded, Redirect, OAuth2 или Decoupled). Процесът на инициране на плащания зависи в голяма степен от подхода на ЗУИ, прилаган от ДПУОС. Най-сложен е процеса при прилагане на Embedded подход, който освен всичко се разделя на различни методи за удостоверяване, налични за Ползвателя. По-долу се представя общ преглед на различни сценарии за API.

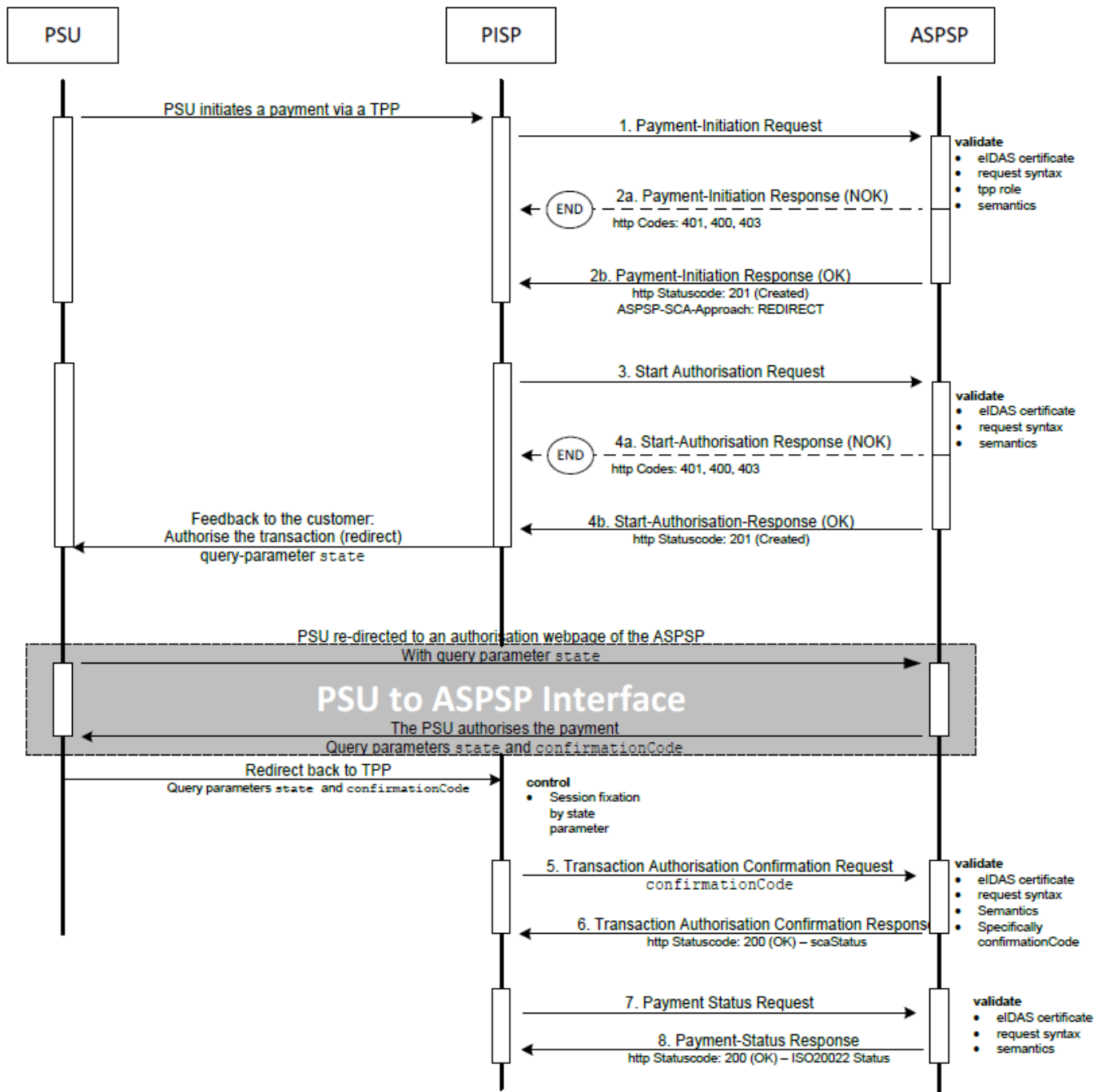
5.1.1. Redirect подход на ЗУИ – с изрично стартиране на авторизация

Ако ДПУОС поддържа подхода Redirect ЗУИ, потокът от съобщения в услугата за инициране на плащания е прост. Първо се изпраща заявка за инициране на плащането, а след това се пуска изрично искане от ДПУ за старт на авторизацията. Това е последвано от пренасочване към сайта за упълномощаване на ДПУОС. ДПУ може да поиска информация за статуса на заявката след като сесията бъде върната към неговата система.



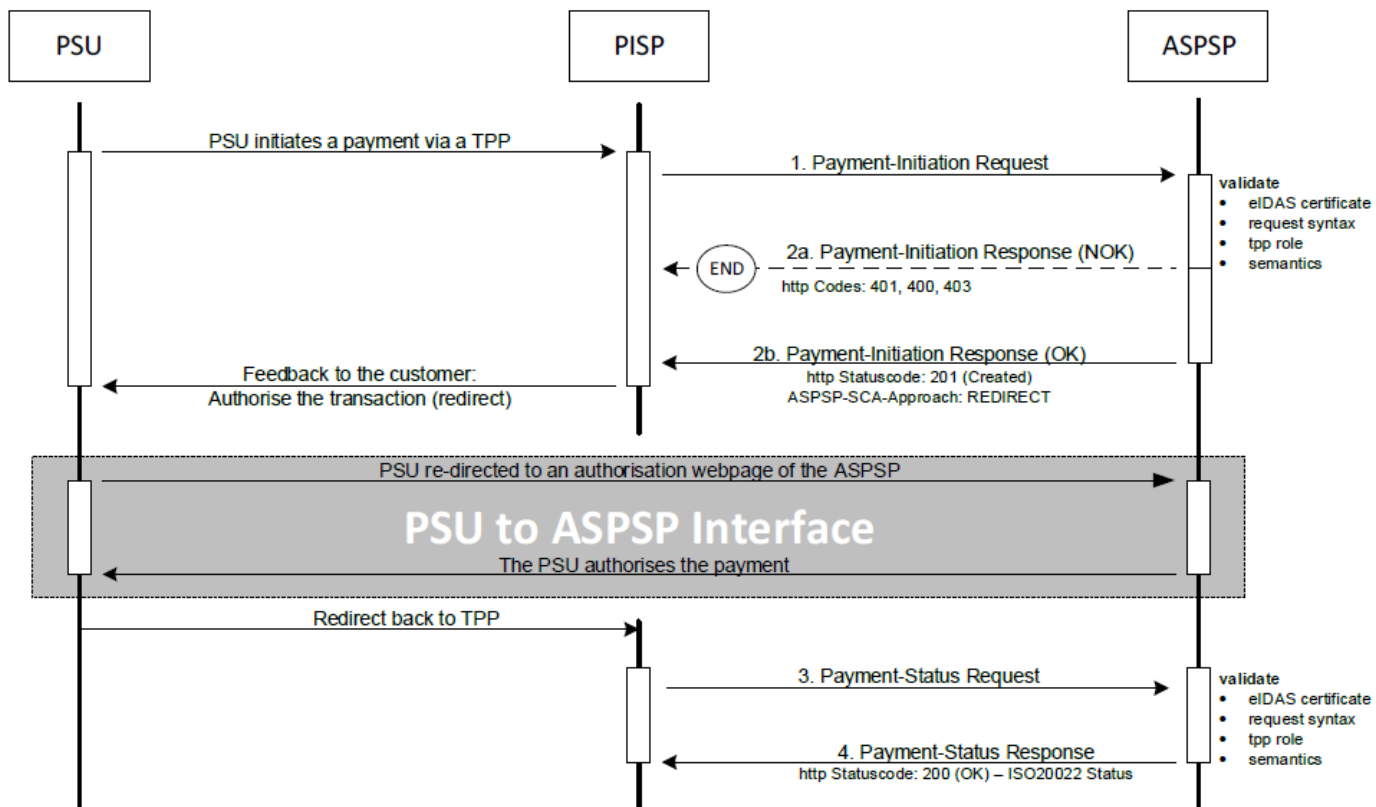
5.1.2. Redirect подход на ЗУИ – с изрично стартиране на авторизация с код за потвърждаване

В допълнение към горния сценарий, може да бъде поискана от ДПУОС заявка за потвърждение на авторизацията от ДПУ, след като сесията се пренасочва към системата на ДПУ и след контрола на ДПУ върху нея. В крайна сметка може да е необходима заявка за състояние на плащане от ДПУ за проверка на точното състояние на иницирираното на плащане.



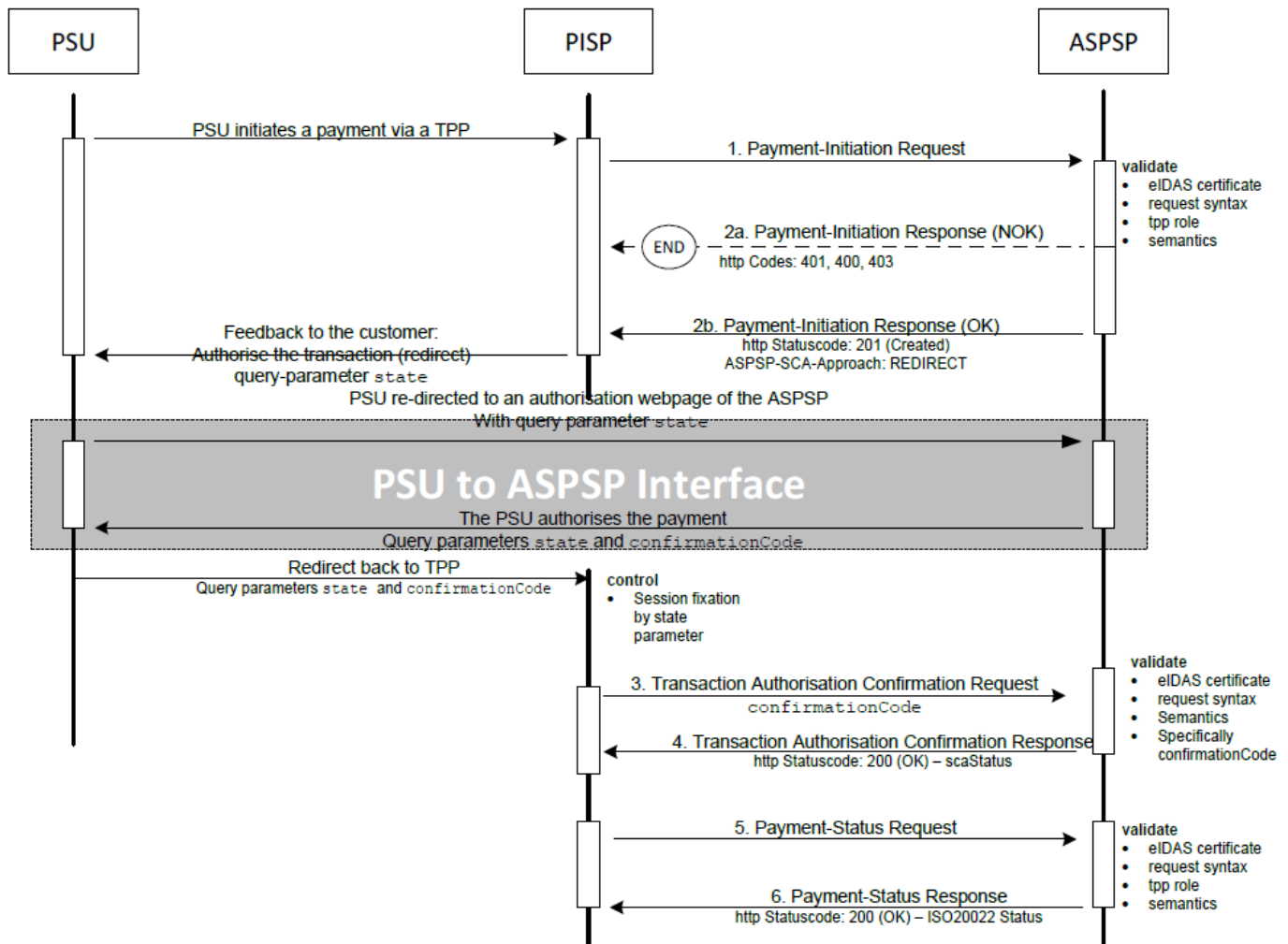
5.1.3. Redirect подход на ЗУИ – автоматично стартиране

Този подход е описан и в първата версия на стандарта преди да са въведени под-ресурсите за авторизация. Ако ДПУОС поддържа подхода Redirect ЗУИ, а след приемане на иницириращата заявка за плащане, Ползвателя автоматично се пренасочва към сайта за упълномощаване от ДПУОС. Заявката за статус може да бъде поискана от ДПУ, след като сесията бъде пренасочена обратно към системата на ДПУ.



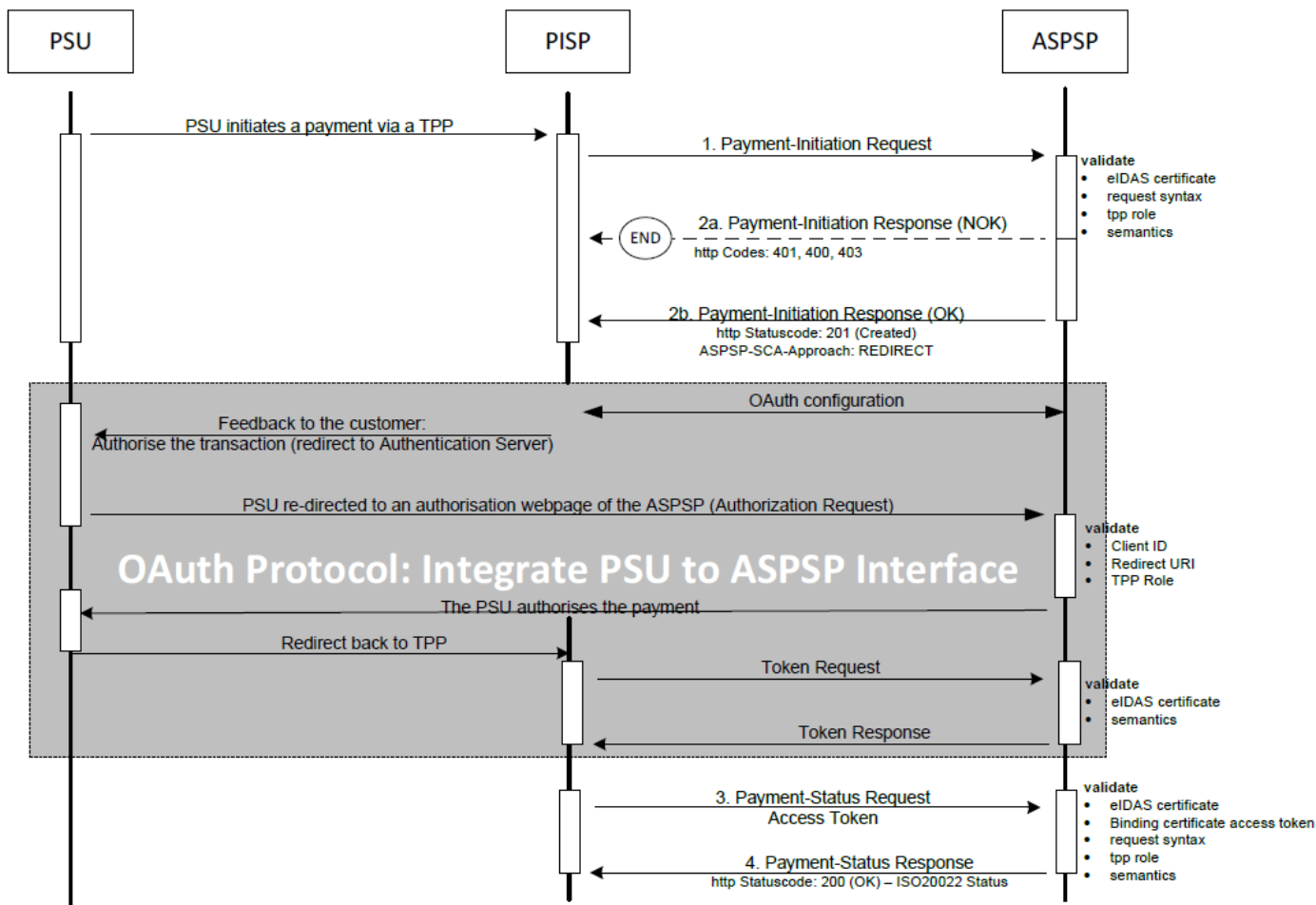
5.1.4. Redirect подход на ЗУИ – автоматично стартиране с код за потвърждаване

В допълнение към горния сценарий, може да бъде поискана от ДПУОС заявка за потвърждение на авторизацията от ДПУ, след като сесията се пренасочва към системата на ДПУ и след контрола на ДПУ върху нея. В крайна сметка може да е необходима заявка за състояние на плащане от ДПУ за проверка на точното състояние на иницирираното на плащане.



5.1.5. OAuth2 подход на ЗУИ – автоматично стартиране

Ако ДПУОС поддържа OAuth2 ЗУИ подход, потокът е много подобен на подхода за Redirect с автоматично пренасочване. Вместо да пренасочва към сървър за удостоверяване на ЗУИ, протоколът OAuth2 (който се поддържа от ДПУОС) се използва директно за процеса на авторизиране на транзакции.

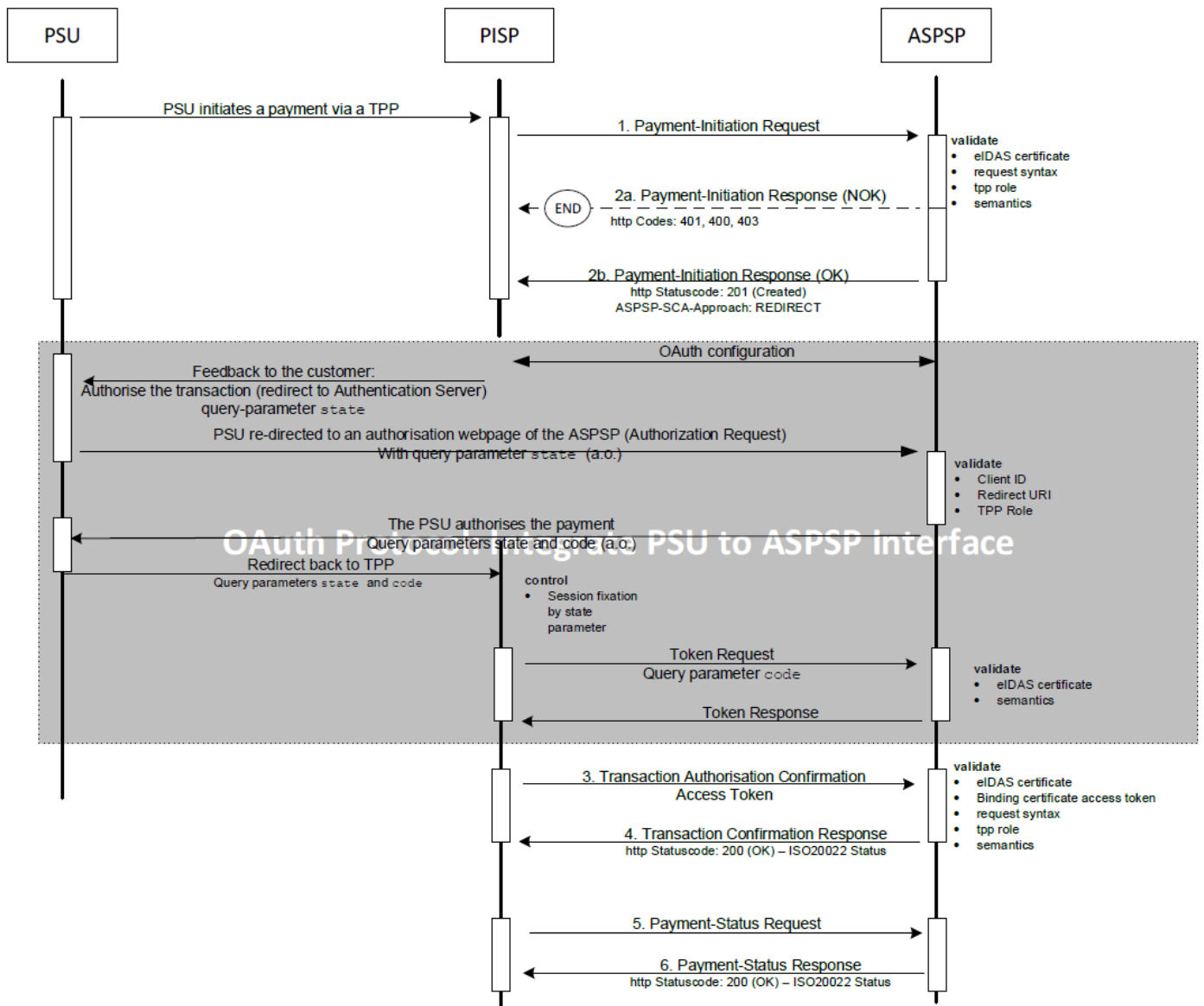


Подходът на OAuth2 ЗУИ с изрично стартиране на процеса на авторизиране е аналогичен.

5.1.6. OAuth2 подход на ЗУИ – автоматично стартиране с код за потвърждаване

В допълнение към горния сценарий, може да бъде поискана от ДПУОС заявка за потвърждение на авторизацията от ДПУ, след като сесията се пренасочва към системата на ДПУ и след контрола на ДПУ върху нея. В крайна сметка може да е необходима заявка за състояние на плащане от ДПУ за проверка на точното състояние на иницирираното на плащане.

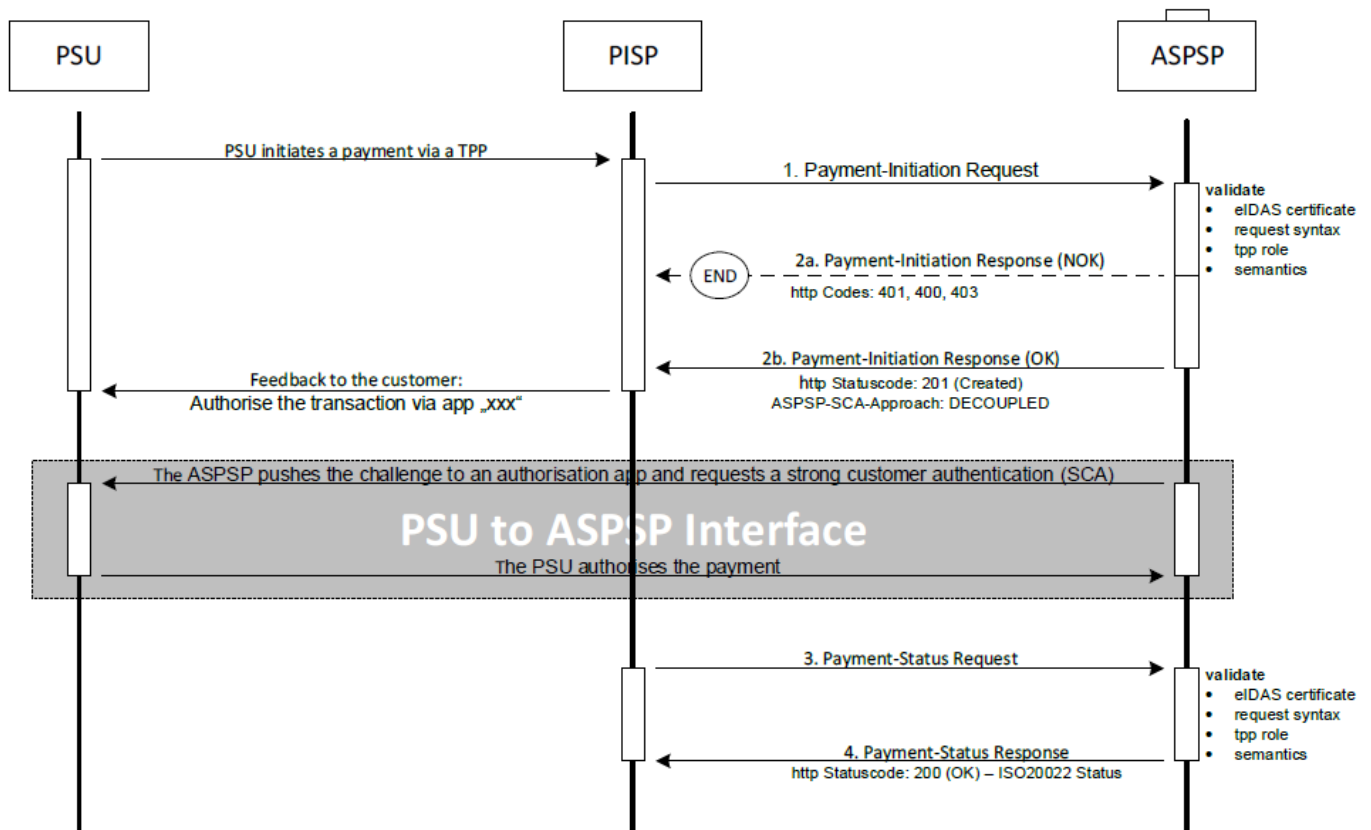
Подходът на OAuth2 ЗУИ с изрично стартиране на процеса на авторизиране със стъпка за потвърждаване на транзакцията е аналогичен.



5.1.7. Decoupled подход на ЗУИ

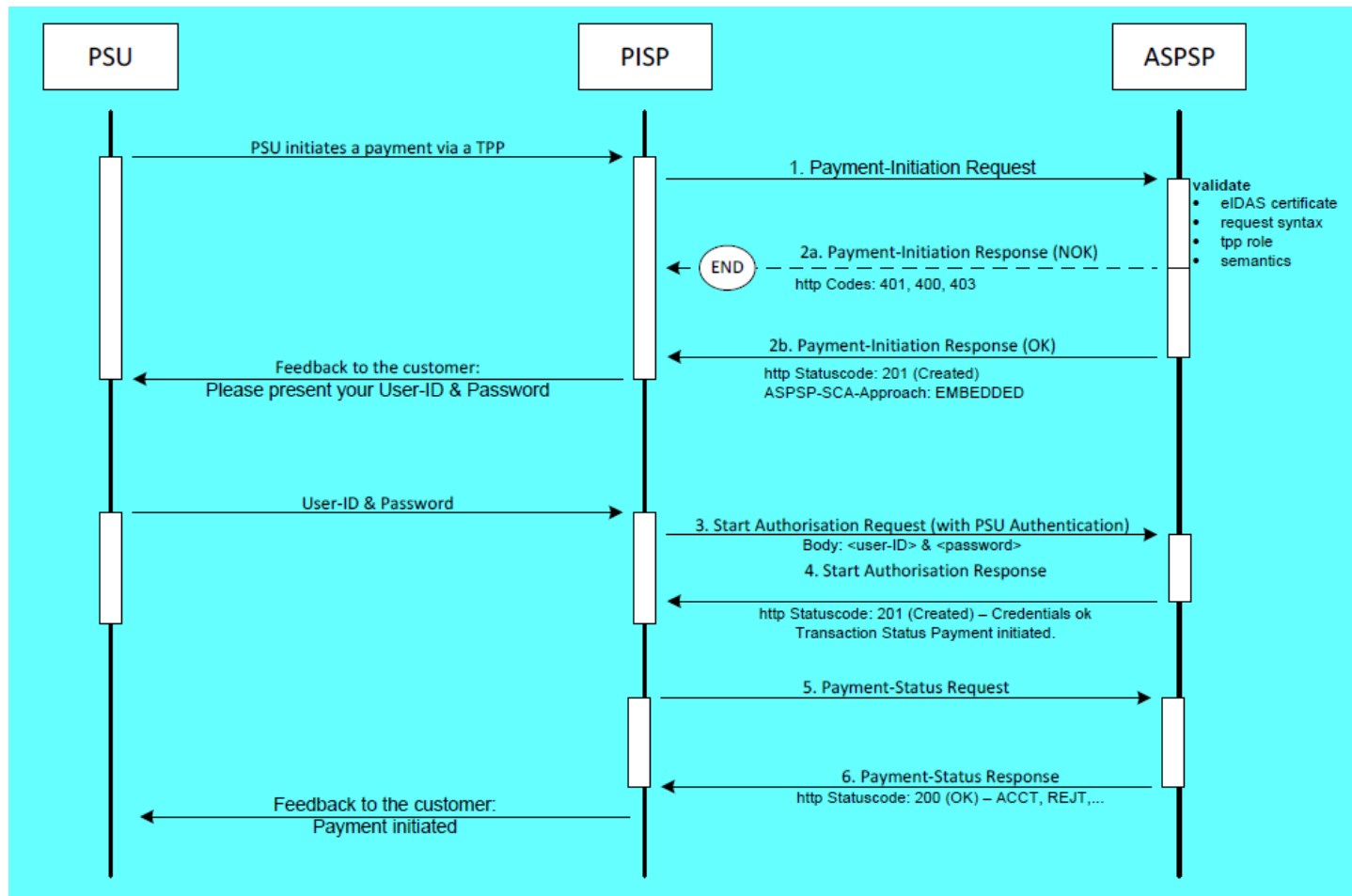
Потокият на транзакцията в Отделен ЗУИ подход е подобен на подхода за Redirect ЗУИ с автоматично стартиране. Разликата е, че ДПУОС изисква от Ползвателя да упълномощи плащането чрез специално мобилно приложение или друго приложение или устройство, което е независимо от интерфейса за онлайн банкиране. ДПУОС иска от ДПУ да уведоми Ползвателя на услугата за това удостоверяване чрез изпращане на съответното съобщение като "Моля, използвайте приложението си xxx, за да удостоверите плащането".

След процеса на ЗУИ между ДПУОС и Ползвателя, ДПУ трябва да поиска резултата от транзакцията.



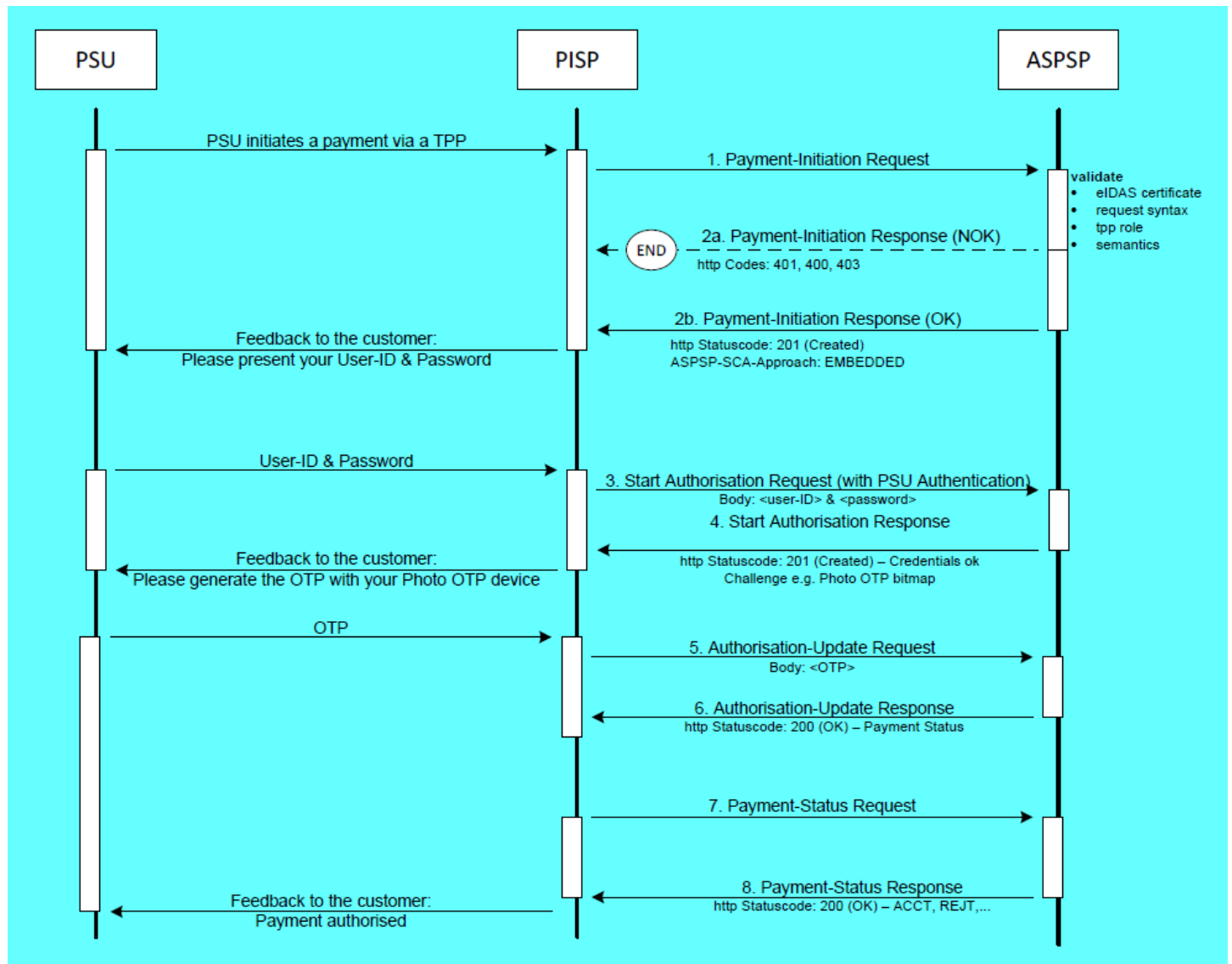
5.1.8. Embedded подход без ЗУИ (към сигурен получател)

При всеки случай на Embedded подход, Ползвателя трябва да се идентифицира с първи фактор преди да се приложи метод на ЗУИ чрез ДПУ към ДПУОС. Когато платежното инициране е прието без ЗУИ метод (например кредитора е в списъка за освобождаване от ЗУИ), Ползвателя предостави идентификацията си (user name) чрез ДПУ към ДПУОС и напр. парола или OTP.



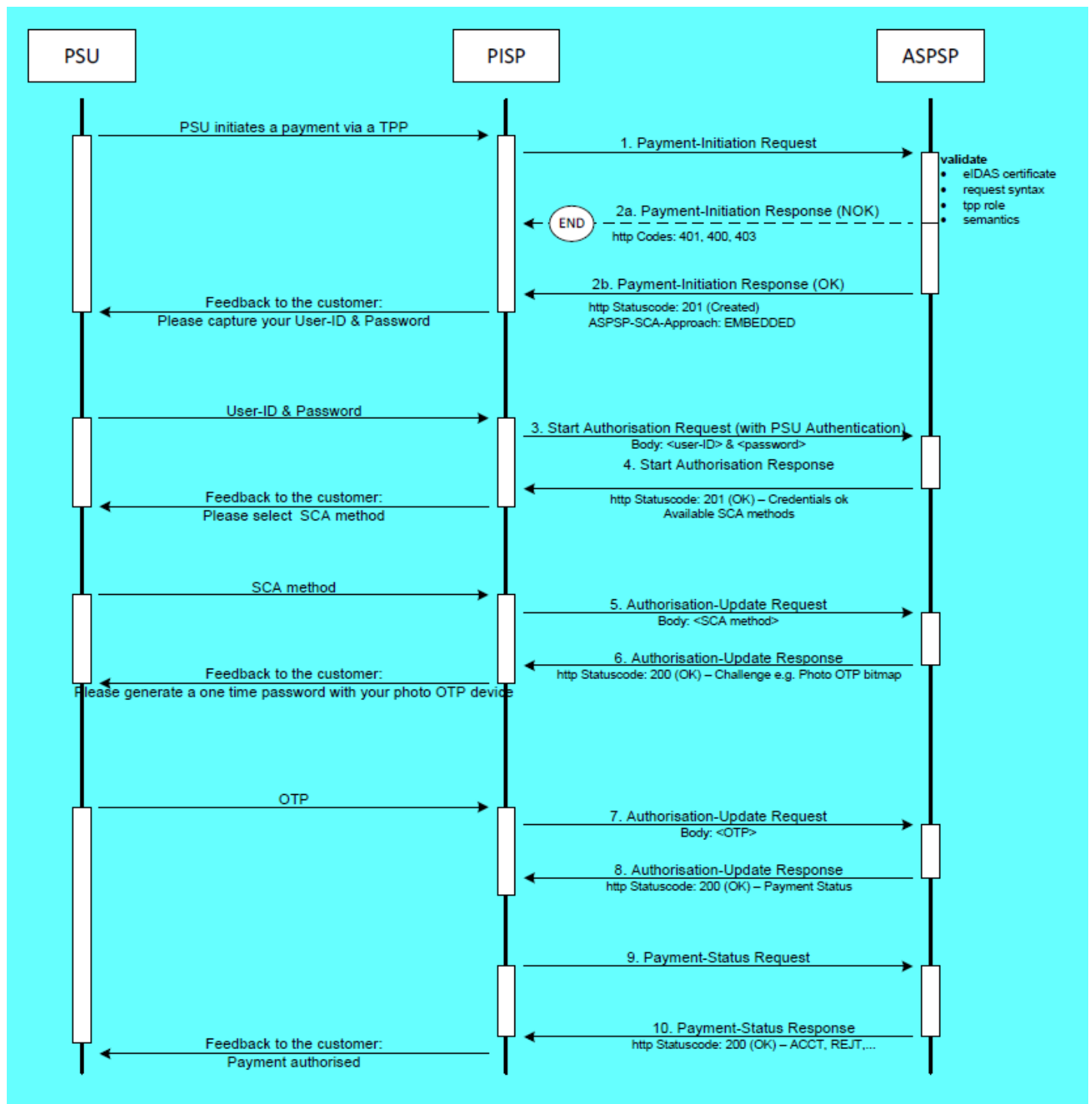
5.1.9. Embedded подход при единствен метод на ЗУИ

В случай, че е налице само един ЗУИ метод, към "процеса" се добавя "заявка за разрешаване на транзакция", където ДПУ предава данните за удостоверяване на клиента, напр. OTP с включено динамично свързване с данните за транзакцията.



5.1.10. Embedded подход чрез избор на метод за ЗУИ

Ако ДПУОС поддържа няколко ЗУИ метода при този процес се предлага избор на ЗУИ метод за Ползвателя. ДПУОС първо предава наличните методи на ДПУ. ДПУ може да ги филтрира, ако не може да поддържа технически всички методи за удостоверяване. След това наличните методи се представят на Ползвателя за избор.



5.1.11. Комбинация от потоци със смесени ЗУИ подходи

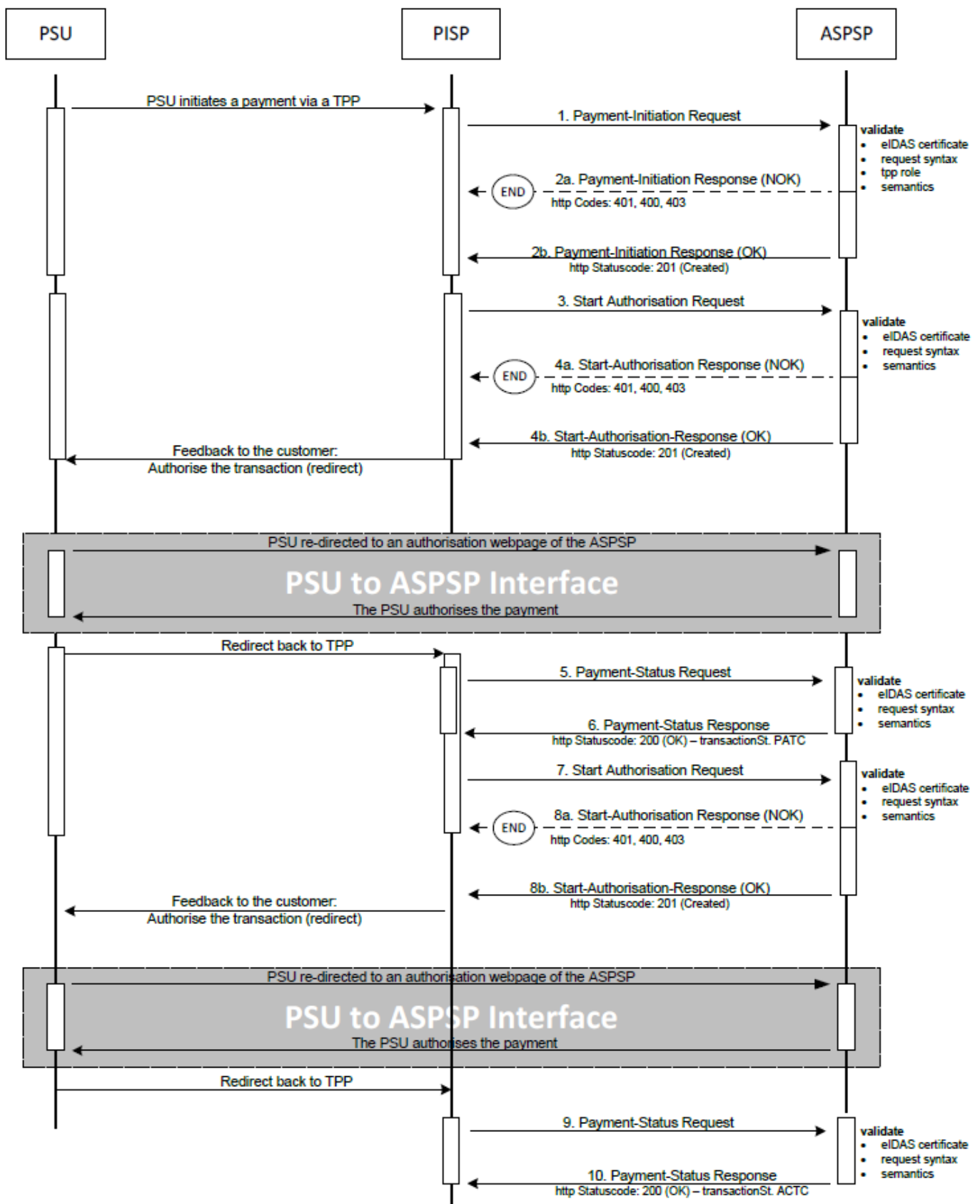
В случай, че ДПУОС поддържа няколко подхода на ЗУИ то трябва първо да предложи SCA методите на разположение за Ползвателя. След избора на Ползвателя за ЗУИ подход ДПУОС прилага съответната схема за "Redirect", "Decoupled", "Embedded".

Ако ДПУОС поддържа за Ползвателя най-малко „decoupled” ЗУИ метод и в същото време поне един ЗУИ метод, който не е „decoupled”, тогава горните потоци могат да бъдат смесени както следва:

- В случай, че ДПУОС стартира потока на инициране на плащането с redirect, Ползвателя може да избере в сайта за удостоверяване на ДПУОС метода за decoupled удостоверяване. Това е прозрачно за ДПУ и няма влияние върху потоците, дефинирани по-горе.
- В случай, че ДПУОС стартира потока за инициране на плащането с embedded ЗУИ подход, ДПУОС ще предостави списък на наличните методи за ЗУИ към Ползвателя чрез ДПУ. Ако Ползвателя избере метод за удостоверяване, който изисква DECOUPLED ЗУИ подход, тогава ДПУОС се разклонява в потока на транзакциите за DECOUPLED подход, както е показано по-горе: ДПУОС ще върне съответния HTTP ДПУОС - ЗУИ подход със стойност "DECOUPLED" и текущото състояние на започването на плащането, напр "ACTC" за коректни технически проверки, но за по-нататъшни действия ще върне хипервръзка "self" или "status". За да получи окончателния статус на транзакцията, следващото искане на ДПУ трябва да бъде заявката за статус GET.
- В случай, че ДПУОС трябва да реши между подхода "Decoupled" и "Redirect" ЗУИ, ДПУОС също може първо да предложи ЗУИ методите на разположение на Ползвателя и след това да се разклонява в подхода "Decoupled" или "Redirect" съгласно избора му.

5.1.12. Множествена ЗУИ авторизация: Пример за подхода с Redirect ЗУИ

Множествената ЗУИ авторизация поддържа разрешението за плащане от няколко Ползватели, напр. разрешение на принципа 4 очи. Множествена ЗУИ авторизация винаги се обработва с изрично стартиране на авторизация. По-долу е показан потокът за оторизиране на принципа 4 очи, при който и двете ЗУИ авторизации се извършват чрез Redirect.



Забележка: Този поток не зависи от метода на ЗУИ. Множествените авторизации по ЗУИ се извършват, като се използва n пъти заявката за старт за n пъти ЗУИ, където съответният метод на ЗУИ е представен като Redirect ЗУИ. Тези ЗУИ процеси също могат да се генерират едновременно от ДПУОС с цел да се спестят API извиквания.

5.2. Обзор на данните за услугата за инициране на плащания

Следната таблица дефинира техническото описание на абстрактния модел на данни, определен в правилата за услугата Инициране на плащане. Колоните дават общ поглед върху API протоколите, както следва:

- Колоната "Data element" използва абстрактните елементи на данни, по [XS2A OR], за да достави връзката към правилата и дефинициите на роли в този документ.
- Колоната Attribute encoding дава определението за действително кодиране в API XS2A, както е дефинирано в този документ.
- Колоните "Location" определят кога съответните елементи на данните се транспортират като параметри на HTTP на ниво path, header или body и са взети от сертификатите eIDAS. Моля, обърнете внимание, че елементите от данни, свързани със сертификат за удостоверяване на уеб сайт, не са елементи на действителното обаждаване от API. Те са посочени тук, тъй като са задължителни в обработката на бекенда и могат да бъдат транспортирани от крайната точка на API към приложението на ДПУОС. Моля, обърнете внимание, че за разлика от това данните за удостоверенията за електронния печат могат да бъдат транспортирани в специално заглавие на полето HTTP.
- Колона "Usage" дава общ преглед на използването на елементи от данни в различните услуги и API повиквания. В [XS2A OR] обажданията XS2A се описват като абстрактни API повиквания. Тези обаждания ще бъдат технически реализирани като команди HTTPS POST, PUT и GET. Обажданията се разделят на следните обаждания за Инициране на плащане:
 - Заявката за инициране е първата стъпка в приложния програмен интерфейс (API) за всяка транзакция в рамките на услугата Плащане. Това повикване генерира съответния ресурс. Инициализирането на плащанията може да обхване еднократно плащане, групови плащания и периодични плащания.
 - Повикването за актуализация на данни е повикване при което ДПУ трябва да добави данни, свързани с идентификация на Ползвателя и след което се трябва да се върне към първото обаждаване. Такова повикване може да се повтори няколко пъти (особено при ЗУИ метод Embedded).
 - Искането за разрешение се използва само при метод Embedded, за да се разреши транзакцията в случай на необходимост от второ удостоверяване на фактора.
 - Заявката за състояние се използва в случаите след успешно изпълнение на ЗУИ и ДПУ се нуждае от по-късна информация за резултата.

Използва се следното използване на съкращения в колоните " Location и Usage "

x: Този елемент от данните се транспортира на съответното ниво.

m: Задължително

o: Незадължително за използване от ДПУ

c: Условно. Условието се определя от ДПУОС и трябва да е описано в адресираните на приложния програмен интерфейс (API) състояния.

Следващата таблица не само определя изискванията към съобщенията за заявки, но и изисквания за елементите на данните в съобщенията за отговори. Тези изисквания се

прилагат само в случай на код за HTTP отговор 2xx. В случай на HTTP отговор код 4xx или 5xx изисквания, се прилагат определените в раздел 4.8.

Забележка: Повечето технически функции като GET ... / {paymentId} и GET ... / {authorisationId} и заявката за анулиране не са обхванати от тази таблица.

	Data element	Attribute encoding	Location					Usage							
			Path	Query P.	Header	Body	Certificate	Init Req.	Init Resp.	Upd. Req.	Upd. Resp.	Auth. Req.	Auth Resp.	Stat. Req.	Stat. Resp.
REQUEST PART (TPP)	TPP Registration Number						x	m		m		m		m	
	TPP Name						x	m		m		m		m	
	TPP Roles						x	m		m		m		m	
	TPP National Competent Authority						x	m		m		m		m	
	Resource ID		x							m		m		m	
	Payment Product	payment-product	x					m		m		m		m	
	Request Identification	X-Request-ID			x			m	m	m	m	m	m	m	m
	Access Token (from optional OAuth2)	Authorization			x			c		c		c		c	
	Further signature related data	Digest			x			c		c		c		c	
	TPP Signing Certificate	TPP-Signature-Certificate			x			c		c		c		c	
	TPP Electronic Signature	Signature			x			c		c		c		c	
	Transaction Status	transactionStatus				x			m		m		m		m
	Funds Availability Flag	fundsAvailable				x									c
	PSU Message Information	psuMessage				x			o		o		o		o
	TPP Message Information	tppMessages				x			o		o		o		o
	PSU Identification	PSU-ID			x			c		c					
	PSU Identification Type	PSU-ID-Type			x			c		c					
	Corporate Identification	PSU-Corporate-ID			x			c		c		c		c	
	Corporate ID Type	PSU-Corporate-ID-Type			x			c		c		c		c	
	PSU Password	psuData.password				x				c					
	IP Address PSU	PSU-IP-Address			x			m		o		o		o	
	IP Port PSU	PSU-IP-Port			x			o		o		o		o	
	PSU User Agent	PSU-User-Agent			x			o		o		o		o	
	GEO Information	PSU-Geo-Location			x			o		o		o		o	
	Further PSU related Information	PSU-Accept			x			o		o		o		o	
		PSU-Accept-Charset			x			o		o		o		o	
		PSU-Accept-Encoding			x			o		o		o		o	
		PSU-Accept-Language			x			o		o		o		o	
		PSU-Http-Method			x			o		o		o		o	
		PSU-Device-ID			x			o		o		o		o	
	Redirect Preference	TPP-Redirect-Preferred			x			o							
	Decoupled Preference	TPP-Decoupled-Preferred			x			o							
	Redirect URI TPP	TPP-Redirect-URI			x			c							
		TPP-Nok-Redirect_URI			x			o							
	Authorization Preference	TPP-Explicit-Authorisation-Preferred			x			o							
	Rejection Preference	TPP-Rejection-NoFunds-Preferred			x			o							
	TPP Notification URI	TPP-Notification-URI			x			o							
	TPP Notification Content Preference	TPP-Notification-Content-Preferred			x			o							
	TPP Brand Information	TPP-Brand-Logging-Information			x			o							
	PSU Password	psuData.password				x				c					

	Chosen SCA Method	chosenScaMethod				x				c										
	SCA Challenge Data	challengeData				x				c		c								
	PSU Authentication Data	scaAuthenticationData				x							m							
Response (ASPSP)	Request Identification	X-Request-ID				x			m	m	m	m	m	m	m	m	m	m	m	m
	ASPSP-SCA-Approach	ASPSP-SCA-Approach				x				o		o								
	Available SCA method	scaMethods				x				c		c								
	Resource ID	paymentId				x			m											
	Transaction Fees	transactionFees				x				o										
	Transaction Fee Indicator	transactionFeeIndicator				x				o										
	Transaction Status	transactionStatus				x			m			m		m		m				m
	PSU Message Information	psuMessage				x				o		o				o				o
	TPP Message Information	tppMessages				x				o		o				o				o
	SCA Challenge Data	challengeData				x				c		c								
	Redirect URL ASPSP	_links.scaRedirect				x				c										

Повикванията в интерфейс за Достъп до сметка, които представляват съобщения, ще бъдат дефинирани в следващите раздели.

Забележка: Маркерът "Timestamp" за заявка на всяко повикване се съдържа в задължителния формат на HTTP header "Date". Този маркер не се съдържа в таблиците с данни по-долу, тъй като това е задължително поле за HTTP header и с цел да се избегнат конфликти с други процедури за спецификация.

IP адрес / порт и допълнителна информация, свързана с Ползвателя.

Следните елементи от данните от горната таблица препращат информация за интерфейса Ползвател / ДПУ и подобряват процедурите за управление на риска на ДПУОС. Препоръчително е тези елементи от данни да присъстват във всички съобщения за заявки в рамките на потока от транзакции за инициране на плащания. По-надолу в табличен вид е предоставена допълнителна информация (описание) за параметрите на заявката и дефиницията на тези елементи. Като изключение в описанието за IP адреса на PSU е "незадължително", но при заявка за инициране на плащане се прилага "задължително".

Attribute	Format	Condition	Description
PSU-IP-Address	String	Optional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP.
PSU-IP-Port	String	Optional	The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available.
PSU-Accept	String	Optional	The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available.
PSU-Accept-Charset	String	Optional	see above
PSU-Accept-Encoding	String	Optional	see above
PSU-Accept-Language	String	Optional	see above
PSU-User-Agent	String	Optional	The forwarded Agent header field of the HTTP request between PSU and TPP, if available.
PSU-Http-Method	String	Optional	HTTP method used at the PSU – TPP interface, if available.

			Valid values are: · GET · POST · PUT · PATCH · DELETE
PSU-Device-ID	String	Optional	UUID (Universally Unique Identifier) for a device, which is used by the PSU, if available. UUID identifies either a device or a device dependent application installation. In case of an installation identification this ID need to be unaltered until removal from device.
PSU-Geo-Location	Geo Location	Optional	The forwarded Geo Location of the corresponding HTTP request between PSU and TPP if available.

5.3. Заявка за инициране на плащане

Стандартът включва спецификите на плащанията в национална валута, както и кредитните трансфери в чуждестранна валута.

A. Разплащанията в национална валута са обособени в две категории:

- SEPA Кредитен превод, включително и към бюджетен разпоредител
- SEPA Незабавен кредитен превод

Стандартът поддържа и атрибут за избор на RTGS платежна система за кредитен превод – TARGET.

B. Кредитен трансфер в чуждестранна валута:

- Кредитен превод в чуждестранна валута (Non SEPA)

C. Ограничения за размера на сумата при инициране на превод

Съгласно действащата регулация, при нареждане на превод за сума над 15,000 евро се изисква подаване на декларация за произход на паричните средства. В тази връзка ДПУОС (банка) има правото да откаже изпълнението на превод за сума над 15,000 евро или нейната равностойност в чужда валута, тъй като на този етап в Стандарта не се поддържа метод за прилагане на декларация към превод

5.3.1. Инициране на плащане в JSON кодиране

Повикване – POST /v1/payments/{payment-product}
/ ДПУ създава и изпраща заявка за инициране на плащане към ДПУОС /

Path

Attribute	Type	Description
payment-product	String	The addressed payment product endpoint, e.g. for SEPA Credit Transfers (SCT). The default list of products supported in this standard is: • sepa-credit-transfers • cross-border-transfers • instant-sepa-credit-transfers The ASPSP will publish which of the payment products/endpoints will be supported.

Query Parameter

Няма Query Parameter

Request Header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	application/json
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party. This is the unique ID of TPP for the payment initiation regarding PSD2 article 46b, 47 and EBA RTS article 29.
PSU-ID	String	Conditional	Client ID of the PSU in the ASPSP client interface. Might be mandated in the ASPSP's documentation. It might be contained even if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in an preceding AIS service in the same session. In this case the ASPSP might check whether PSU-ID and token match, according to ASPSP documentation.
PSU-ID-Type	String	Conditional	Type of the PSU-ID, needed in scenarios where PSUs have several PSU-IDs as access possibility. In this case, the mean and use is then defined in the ASPSP's documentation.
PSU-Corporate-ID	String	Conditional	Identification of a Corporate in the Online Channels Might be mandated in the ASPSP's documentation. Only used in a corporate context.
PSU-Corporate-ID-Type	String	Conditional	This is describing the type of the identification needed by the ASPSP to identify the PSU-Corporate-ID content. Mean and use is defined in the ASPSP's documentation. Only used in a corporate context.
Authorization	String	Conditional	Bearer Token. Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in an preceding AIS service in the same session.
Consent-ID	String	Optional	This data element may be contained, if the payment initiation transaction is part of a session, i.e. combined AIS/PIS service. This then contains the "consentId" of the related AIS consent, which was performed prior to this payment initiation.
PSU-IP-Address	String	Mandatory	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. If not available, the TPP shall use the IP Address used by the TPP when submitting this request.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", "URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandated for the Redirect SCA Approach, specifically when TPP-Redirect-Preferred equals "true". This entry is not mandated in the integrated OAuth case, since the redirect URI is transported during the OAuth protocol. If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU.

Attribute	Type	Condition	Description
			If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Rejection-NoFunds-Preferred	Boolean	Optional	"If it equals "true" then the TPP prefers a rejection of the payment initiation in case the ASPSP is providing an integrated confirmation of funds request and the result of this is that not sufficient funds are available. If it equals "false" then the TPP prefers that the ASPSP is dealing with the payment initiation like in the ASPSPs online channel, potentially waiting for a certain time period for funds to arrive to initiate the payment.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandatory for the SCA OAuth Approach.
TPP-Nok-Redirect-URI	String	Optional	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method. This might be ignored by the ASPSP.
TPP-Explicit-Authorisation-Preferred	Boolean	Optional	If it equals "true", the TPP prefers to start the authorisation process separately, e.g. because of the usage of a signing basket. This preference might be ignored by the ASPSP, if a signing basket is not supported as functionality. If it equals "false" or if the parameter is not used, there is no preference of the TPP. This especially indicates that the TPP assumes a direct authorisation of the transaction in the next step, without using a signing basket.
TPP-Rejection-NoFunds-Preferred	Boolean	Optional	If it equals "true" then the TPP prefers a rejection of the payment initiation in case the ASPSP is providing an integrated confirmation of funds request and the result of this is that not sufficient funds are available. If it equals "false" then the TPP prefers that the ASPSP is dealing with the payment initiation like in the ASPSPs online channel, potentially waiting for a certain time period for funds to arrive to initiate the payment. This parameter may be ignored by the ASPSP.
TPP-Notification-URI	String	Optional	URI for the Endpoint of the TPP-API to which the status of the payment initiation should be sent. This header field may be ignored by the ASPSP, cp. also the extended service definition in [XS2A-RSNS].
TPP-Notification-Content-Preferred	String	Optional	The string has the form status=X1, ..., Xn where Xi is one of the constants SCA, PROCESS, LAST and where constants are not repeated. The usage of the constants supports the following semantics: SCA: A notification on every change of the scaStatus attribute for all related authorisation processes is preferred by the TPP. PROCESS: A notification on all changes of consentStatus or transactionStatus attributes is preferred by the TPP. LAST: Only a notification on the last consentStatus or transactionStatus as available in the XS2A interface is preferred by the TPP. This header field may be ignored, if the ASPSP does not support resource notification services for the related TPP.

Attribute	Type	Condition	Description
TPP-Brand-Logging-Information	String	Optional	This header might be used by TPPs to inform the ASPSP about the brand used by the TPP towards the PSU. This information is meant for logging entries to enhance communication between ASPSP and PSU or ASPSP and TPP. This header might be ignored by the ASPSP.

Request Body

Данните, които трябва да бъдат транспортирани в заявката, зависят от избраната крайна точка (разплащателен продукт) за приложния програмен интерфейс (API). В **Раздел 11** на този документ са предоставени Стандартните и Допълнителните дефиниции необходими за покриване на изискванията на местните особености на пазара. По-нататъшни определения също може да бъдат добавени при възникване на нови специфики за общността или ДПУОС.

Response Header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource (if created)
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	This data element must be contained, if the SCA Approach is already fixed. Possible values are: - EMBEDDED - DECOUPLED - REDIRECT The OAuth SCA approach will be subsumed by REDIRECT..
ASPSP-Notification-Support	Boolean	Conditional	true if the ASPSP supports resource status notification services. false if the ASPSP supports resource status notification in general, but not for the current request. Not used, if resource status notification services are generally not supported by the ASPSP. Shall be supported if the ASPSP supports resource status notification services, see more details in the extended service definition [XS2A-RSNS].
ASPSP-Notification-Content	String	Conditional	The string has the form status=X1, ..., Xn where Xi is one of the constants SCA, PROCESS, LAST and where constants are not repeated. The usage of the constants supports the following semantics: SCA: Notification on every change of the scaStatus attribute for all related authorisation processes is provided by the ASPSP for the related resource. PROCESS: Notification on all changes of consentStatus or transactionStatus attributes is provided by the ASPSP for the related resource. LAST: Notification on the last consentStatus or transactionStatus as available in the XS2A interface is provided by the ASPSP for the related resource. This field must be provided if the ASPSP-Notification-Support =true. The ASPSP might consider the notification content as preferred by the TPP, but can also respond independently of the preferred request.

Полето "Location" се използва като връзка към създадения ресурс. Няма други специфични изисквания.

Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	The values defined in Section 14.13 Transaction status might be used.
paymentId	String	Mandatory	resource identification of the generated payment initiation resource.
transactionFees	Amount	Optional	Might be used by the ASPSP to transport the total transaction fee relevant for the underlying payments. This field includes the entry of the currencyConversionFees if applicable.
currencyConversionFees	Amount	Optional	Might be used by the ASPSP to transport specific currency conversion fees related to the initiated credit transfer.
estimatedTotalAmount	Amount	Optional	The amount which is estimated to be debited from the debtor account
estimatedInterbankSettlementAmount	Amount	Optional	The estimated amount to be transferred to the payee.
transactionFeeIndicator	Boolean	Optional	If equals "true", the transaction will involve specific transaction cost as shown by the ASPSP in their public price list or as agreed between ASPSP and PSU. If equals "false" or is not used, the transaction will not involve additional specific transaction costs to the PSU unless the fee amount is given specifically in the data elements transactionFees and/or currencyConversionFees.
scaMethods	Array of authentication objects	Conditional	This data element might be contained, if SCA is required and if the PSU has a choice between different authentication methods. Depending on the risk management of the ASPSP this choice might be offered before or after the PSU has been identified with the first relevant factor, or if an access token is transported. If this data element is contained, then there is also an hyperlink of type "selectAuthenticationMethods" contained in the response body. These methods shall be presented towards the PSU for selection by the TPP.
chosenScaMethod	Authentication object	Conditional	This data element is only contained in the response if the APSPS has chosen the Embedded SCA Approach, if the PSU is already identified e.g. with the first relevant factor or alternatively an access token, if SCA is required and if the authentication method is implicitly selected.

Attribute	Type	Condition	Description
challengeData	Challenge	Conditional	It is contained in addition to the data element "chosenScaMethod" if challenge data is needed for SCA.
			In rare cases this attribute is also used in the context of the "updatePsuAuthentication" link.
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Type of links admitted in this response, (further links might be added for ASPSP defined extensions): "scaRedirect": In case of an SCA Redirect Approach, the ASPSP is transmitting the link to which to redirect the PSU browser.
			"scaOAuth": In case of a SCA OAuth2 Approach, the ASPSP is transmitting the URI where the configuration of the Authorisation Server can be retrieved. The configuration follows the OAuth 2.0 Authorisation Server Metadata specification.
			"confirmation": Might be added by the ASPSP if either the "scaRedirect" or "scaOAuth" hyperlink is returned in the same response message. This hyperlink defines the URL to the resource which needs to be updated with ❑ a confirmation code as retrieved after the plain redirect authentication process with the ASPSP authentication server or ❑ an access token as retrieved by submitting an authorization code after the integrated OAuth based authentication process with the ASPSP authentication server.
			"startAuthorisation": In case, where an explicit start of the transaction authorisation is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded).
			"startAuthorisationWithPsuIdentification": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU identification data.
			"startAuthorisationWithPsuAuthentication": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU authentication data.

Attribute	Type	Condition	Description
			"startAuthorisationWithAuthentication MethodSelection": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while selecting the authentication method. This link is contained under exactly the same conditions as the data element "scaMethods"
			"startAuthorisationWithTransactionAuthorisation": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while authorising the transaction e.g. by uploading an OTP received by SMS.
			"self": The link to the payment initiation resource created by this request. This link can be used to retrieve the resource data. "status": The link to retrieve the transaction status of the payment initiation.
			"scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource. This link is only contained, if an authorisation sub-resource has been already created.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU
tppMessages	Array of Message	Optional	Messages to the TPP on operational issues.

Example – Примери

1. SEPA credit transfer (with SEPA Service level marker)

Request

POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Encoding : gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-GEO-Location: GEO:52.506931;13.144558
PSU-USER-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 28 Jan 2018 16:42:37 GMT

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "paymentType": {"ServiceLevel" : "SEPA"},
  "chargeBearer": "SLEV",
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "DE23100120020123456789"},
  "remittanceInformationUnstructured": "Information for Merchant and payment "
}
```

Response in case of decoupled approach

HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: DECOUPLED
Date: Sun, 28 Jan 2018 16:42:37 GMT
Location: https://www.testbank.com/psd2/v1/payments/sepa-credit-transfers/1234-wertiq-983
Content-Type: application/json

```
{
  "transactionStatus": "RCVD",
  "paymentId": "1234-wertiq-983",
  "_links": {
    "updatePsuIdentification": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"},
    "self": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"}
  }
}
```

Response in case of decoupled approach with explicit start of authorization needed (will be done with the update PSU identification function)

HTTP/1.x 201 Created

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: DECOUPLED

Date: Sun, 28 Jan 2018 16:42:37 GMT

Location: <https://www.testbank.com/psd2/v1/payments/sepa-credit-transfers/1234-wertiq-983>

Content-Type: application/json

```
{
  "transactionStatus": "RCVD",
  "paymentId": "1234-wertiq-983",
  "_links": {
    "startAuthorisationWithPsuIdentification": {
      "href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations",
      "self": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"}
    }
  }
}
```

Response in case of embedded approach with explicit start of authorization

HTTP/1.x 201 Created

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: EMBEDDED

Date: Sun, 28 Jan 2018 16:42:37 GMT

Location: <https://www.testbank.com/psd2/v1/payments/1234-wertiq-983>

Content-Type: application/json

```
{
  "transactionStatus": "RCVD",
  "paymentId": "1234-wertiq-983",
  "_links": {
    "startAuthenticationWithPsuAuthentication": {
      "href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983 /authorisations",
      "self": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"}
    }
  }
}
```

2. SEPA credit transfer (budget transfer)

Request

POST <https://api.testbank.com/v1/payments/sepa-credit-transfers>

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

PSU-IP-Address: 192.168.8.78

PSU-GEO-Location: GEO:52.506931;13.144558

PSU- User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

Date: Sun, 28 Jan 2018 16:47:37 GMT

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "paymentType": {"ServiceLevel": "SEPA"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver TD NRA SOFIA",
  "creditorAccount": {"iban": "BG47BNBG96668123456789"},
  "ultimateDebtor": "EGN-9904281234-110000",
  "remittanceInformationUnstructured": "Tax payment ZDDFL info"
}
```

Response in case of an OAuth2 SCA response approach with implicitly creating an authorization sub-resource

HTTP/1.x 201 Created

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 28 Jan 2018 16:47:37 GMT

Location: <https://www.testbank.com/psd2/v1/payments/sepa-credit-transfers/1234-wertiq-983>

Content-Type: application/json

```
{
  "transactionStatus": "RCVD",
  "paymentId": "1234-wertiq-983",
  "_links": {
    "scaOAuth": {"href": "https://www.testbank.com/oauth/.well-known/oauth-authorization-server"},
    "self": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983"},
    "status": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983/status"},
    "scaStatus": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations/123auth456"}
  }
}
```

3. SEPA credit transfer (instant transfer)

Request

POST <https://api.testbank.com/v1/payments/sepa-credit-transfers>

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

PSU-IP-Address: 192.168.8.78

PSU-GEO-Location: GEO:52.506931;13.144558

PSU- User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

Date: Sun, 28 Jan 2018 16:47:37 GMT

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "paymentType": {"ServiceLevel": "INST"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "DE23100120020123456789"},
  "remittanceInformationUnstructured": "Information for Merchant and payment "
}
```

Response in case of an OAuth2 SCA response approach with implicitly creating an authorization sub-resource

HTTP/1.x 201 Created

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 28 Jan 2018 16:47:37 GMT

Location:https://www.testbank.com/psd2/v1/payments/sepa-credit-transfers/1234-wertiq-983
Content-Type: application/json
{
 "transactionStatus": "RCVD",
 "paymentId": "1234-wertiq-983",
 "_links": {
 "scaOAuth":{"href": "<https://www.testbank.com/oauth/.well-known/oauth-authorization-server>"},
 "self": {"href":"/v1/payments/sepa-credit-transfers/1234-wertiq-983"},
 "status":{"href":"/v1/payments/sepa-credit-transfers/1234-wertiq-983/status"},
 "scaStatus":{"href":"/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations/123auth456"}
 }
}

4. Cross border credit transfer

Request

POST https://api.testbank.com/v1/payments/cross-border-transfers
Content-Encoding: gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-GEO-Location: GEO:52.506931;13.144558
PSU-USER-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 28 Jan 2018 16:52:37 GMT

Request Body

```
{  
  "instructedAmount": {"currency": "USD", "amount": "123.50"},  
  "chargeBearer": "SHAR",  
  "debtorAccount": {"iban": "BG94BANK12341234567890"},  
  "creditorName": "Receiver Merchant123",  
  "creditorAccount": {"iban": "TR73TURKBANK000000001234567890"},  
  "creditorAddress": {"country": "TR", "city": "Istanbul", "street": "Main Street 25"},  
  "remittanceInformationUnstructured": "Information for Merchant and payment"  
}
```

Response in case of embedded approach

HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: EMBEDDED
Date: Sun, 28 Jan 2018 16:52:37 GMT
Location: https://www.testbank.com/psd2/v1/payments/cross-border-transfers/1234-wertiq-983
Content-Type: application/json
{
 "transactionStatus": "RCVD",
 "paymentId": "1234-wertiq-983",
 "_links": {
 "updatePsuAuthentication":
 {"href": "/v1/payments/cross-border-transfers/1234-wertiq-983"},
 "self":{"href":"/v1/payments/cross-border-transfers/1234-wertiq-983"}
 }
}

5. Instant SEPA credit transfer

Request

POST https://api.testbank.com/v1/payments/instant-sepa-credit-transfers
Content-Encoding: gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-GEO-Location: GEO:52.506931;13.144558
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 28 Jan 2018 16:45:37 GMT

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "BG96BGBK43210123456789"},
  "remittanceInformationUnstructured": "Information for Merchant and payment"
}
```

5.3.2. Инициране на плащане в XML съобщение pain.001

Повикване – POST /v1/payments/{payment-product}
/ ДПУ създава и изпраща заявка за инициране на плащане към ДПУОС /

Path

Attribute	Type	Description
Payment-product	String	The addressed payment product endpoint. The default list of products supported in this standard is: • pain.001-sepa-credit-transfers • pain.001-cross-border-transfers • pain.001-instant-sepa-credit-transfers The ASPSP will publish which of the payment products/endpoints will be supported.

Query Parameter - Същите стойности като в секция 5.3.1.

Request Header - Има разлика в стойността на атрибута Content-Type, който указва XML кодиране. Останалите стойности са същите както в секция 5.3.1.

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	application/xml

Request Body – Структурата на pain.001, която отговаря на избрания продукт. XML схемата е указана в Секция 11.1.2.

Response - Същите стойности като в секция 5.3.1.

Example – SEPA credit transfer (budget transfer)

Request

POST https://api.testbank.com/v1/payments/pain.001-sepa-credit-transfers
Content-Encoding : gzip
Content-Type: application/xml
X-Request-ID: "123e4567-e89b-12d3-a456-426655440000"

PSU-IP-Address: "192.168.8.78"

PSU-Agent: "Chrome_v12"

Request Body

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.001.001.08">
  <CstmrCdtTrfInitn>
    <GrpHdr>
      <MsgId>ACT/180128/BUDG002</MsgId>
      <CreDtTm>2018-01-28T14:07:00</CreDtTm>
      <NbOfTxs>1</NbOfTxs>
      <CtrlSum>256</CtrlSum>
      <InitgPty>
        <Nm>ИМЕ НА ИНИЦИАТОР НА ПЛАЩАНЕ</Nm>
        <PstlAdr>
          <StrtNm>ул. Св. София 6</StrtNm>
          <PstCd>1000</PstCd>
          <TwnNm>Sofia</TwnNm>
          <Ctry>BG</Ctry>
        </PstlAdr>
        <Id><PrvtId>1234567890</PrvtId></Id>
      </InitgPty>
    </GrpHdr>
    <PmtInf>
      <PmtInfId>ADE/0012345678</PmtInfId>
      <PmtMtd>TRF</PmtMtd>
      <BtchBookg>false</BtchBookg>
      <PmtTpInf><CtgyPurp><Cd>GOVT</Cd></CtgyPurp></PmtTpInf>
      <Dbtr>
        <Nm>ИМЕ НА НАРЕДИТЕЛ</Nm>
        <PstlAdr><PstCd>1000</PstCd><TwnNm>София</TwnNm><Ctry>BG</Ctry>
        </PstlAdr>
        <Id><PrvtId>1234567890</PrvtId></Id>
      </Dbtr>
      <DbtrAcct><Id> <IBAN>BG68BANK91231098765432</IBAN></Id></DbtrAcct>
      <DbtrAgt><FinInstnId><BICFI>BANKBGSF</BICFI></FinInstnId></DbtrAgt>
      <CdtTrfTxInf>
        <PmtId><InstrId>ACT/180128/BUDG002/01</InstrId></PmtId>
        <Amt>
          <InstdAmt Ccy="EUR">256</InstdAmt>
        </Amt>
        <CdtrAgt><FinInstnId><BICFI>BUDGBGSF</BICFI></FinInstnId></CdtrAgt>
        <Cdtr>
          <Nm>ТД на НАП СОФИЯ Офис СЕРДИКА</Nm>
          <PstlAdr><TwnNm>София</TwnNm><Ctry>BG</Ctry></PstlAdr>
        </Cdtr>
        <CdtrAcct><Id><IBAN>BG52BUDG96618188843800</IBAN></Id></CdtrAcct>
        <Tax>
          <Dbtr>
            <TaxId>1234567890</TaxId>
            <TaxTp>EGN</TaxTp>
            <Authstn><Nm>ИМЕ НА ЗАДЪЛЖЕНО ЛИЦЕ</Nm></Authstn>
          </Dbtr>
          <TtlTaxAmt Ccy="EUR">256</TtlTaxAmt>
          <Rcrd>
            <Ctgy>110000</Ctgy>
          </Rcrd>
        </Tax>
      </CdtTrfTxInf>
    </PmtInf>
  </CstmrCdtTrfInitn>
</Document>
```

Response in case of a redirect

Header Response in JSON encoding as example in Section 5.3.1

Response Body

```
{
  "transactionStatus": "Received",
  "paymentId": "1234-wertiq-983",
  "_links": {
```

```

"redirect": "https://www.testbank.com/asdfasdfasdf",
"self": "/v1/payments/pain.001-sepa-credit-transfers/1234-wertiq-983"
}
}

```

Response in case of an OAuth2 response

Header Response in JSON encoding as example in Section 5.3.1

Response Body

```

{
"transactionStatus": "Received",
"paymentId": "1234-wertiq-983",
"_links": {
"oAuth": "https://www.testbank.com/oauth/.well-known/oauth-authorization-server",
"self": "/v1/payments/pain.001-sepa-credit-transfers/1234-wertiq-983"
}
}

```

Response in case of decoupled approach

Header Response in JSON encoding as example in Section 5.3.1

Response Body

```

{
"transactionStatus": "Received",
"paymentId": "1234-wertiq-983",
"_links": {
"updatePsuIdentification": "/v1/payments/pain.001-sepa-credit-transfers/1234-wertiq-983",
"self": "/v1/payments/pain.001-sepa-credit-transfers/1234-wertiq-983"
}
}

```

Response in case of embedded approach

Header Response in JSON encoding as example in Section 5.3.1

Response Body

```

{
"transactionStatus": "Received",
"paymentId": "1234-wertiq-983",
"_links": {
"updatePsuAuthentication": "/v1/payments/pain.001-sepa-credit-transfers/1234-wertiq-983"
}
}

```

5.3.3. Инициране на масово плащане (bulk payment)

Тази функционалност е незадължителна за ДПУОС. Тя може да бъде предложена от в JSON или XML моделиране на данните за плащане.

5.3.3.1. Инициране на масово плащане (bulk payment) в JSON кодиране

Повикване – POST /v1/bulk-payments/{payment-product}
/ ДПУ създава и изпраща заявка за инициране на масово плащане към ДПУОС /

Path

Attribute	Type	Description
Payment-product	String	The addressed payment product endpoint. The default list of products supported in this standard is: - sepa-credit-transfers - instant-sepa-credit-transfers The ASPSP will publish which of the payment products/endpoints will be supported.

Query Parameter - Същите стойности като в секция 5.3.1.

Request Header – Стойностите са същите както в секция 5.3.1.

Request Body – Дефиницията за масово СЕПА плащане се съдържа в Секция 11.3.

Response – Дефиницията на отговора е аналогична с инициране на единично плащане като в секция 5.3.1.

5.3.3.2. *Инициране на масово плащане (bulk payment) в XML кодиране*

Повикване – POST /v1/bulk-payments/{payment-product}
/ ДПУ създава и изпраща заявка за инициране на масово плащане към ДПУОС /

Path

Attribute	Type	Description
Payment-product	String	The addressed payment product endpoint. The default list of products supported in this standard is: • pain.001-sepa-credit-transfers • pain.001-instant-sepa-credit-transfers The ASPSP will publish which of the payment products/endpoints will be supported.

Query Parameter - Същите стойности като в секция 5.3.2.

Request Header – Стойностите са същите както в секция 5.3.2.

Request Body – Структурата на pain.001, която кореспондира с посочения платежен продукт.

Response – Дефиницията на отговора е аналогична с инициране на единично плащане в XML като в секция 5.3.2.

5.3.4. Инициране на нареждане за периодично плащане

Функцията за периодични плащания се разглежда в настоящата спецификация като специфична заявка за „Постоянно нареждане“: ДПУ подава искане за повтарящо се плащане. В заявката се съдържат данни за Начална дата, Честота и условно Крайна дата. След като бъде оторизирано от Ползвателя, плащането ще се извършва от ДПУОС, ако е възможно, на базата на това "Постоянно нареждане", представена от ДПУ. Не е необходима допълнителна дейност по ДПУ.

Това плащане се нарича периодично плащане в този контекст, за да се разграничи от други повтарящи се видове плащане, когато трети страни иницират една и съща сума за един и същ бенефициент за транзакции с кредитна карта или директни дебити за заплащане на стоки или услуги. Последните видове плащания не са част от този интерфейс.

5.3.4.1. *JSON кодиране на Постоянно нареждане за периодично плащане*

Повикване: POST /v1/periodic-payments/{payment-product}

Path Parameter - Използва се един и същ параметър за определяне на вид плащане като периодичното плащане, както е посочено в раздел 5.3.1.

Query Parameter - Същите стойности като в секция 5.3.1.

Request Header – Стойностите са същите както в секция 5.3.1.

Request Body – Може да се използва всеки tag на основното плащане, определен в раздел 11.1.1. В допълнение се използват следните маркери:

Tag	Type	Usage	Description
startDate	ISODate	Mandatory	The first applicable day of execution starting from this date is the first payment.
executionRule	String	Optional	The "following" or "preceding" supported as values. This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday. The payment is then executed either the "preceding" or the "following" working day. ASPSP might reject the request due to the communicated value, if rules in Online-Banking are not supporting this execution rule.
endDate	ISODate	Optional	The last applicable day of executionIf not given, it is an infinite standing order.
frequency	Frequency Code	Mandatory	The frequency of the recurring payment resulting from this standing order.
dayOfExecution	Max2Text	Conditional	"31" is ultimo. The format is following the regular expression \d{1,2}. Example: „1“addresses the first day. The date is referring to the time zone of the ASPSP.

Response: Форматът на отговора за инициране на плащането съответно. последващият процес на оторизиране на транзакции за постоянни поръчки с данни за плащане, базирани на JSON, е аналогичен на съответния отговор за инициране на единично плащане, респ. последващия процес на оторизиране на транзакции за еднократно плащане, съдържащо данни за плащане, базирани на JSON.

Пример:

```
POST https://v1/periodic-payments/sepa-credit-transfers
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101
Firefox/54.0
Date: Sun, 06 Aug 2017 15:02:37 GMT
{
  "instructedAmount": {"currency": "EUR", "amount": "123"},
  "debtorAccount": {"iban": "DE40100100103307118608"},
  "creditorName": "Merchant123",
  "creditorAccount": {"iban": "DE23100120020123456789"},
  "remittanceInformationUnstructured": "Information Number Abonnement",
  "startDate": "2018-03-01",
  "executionRule": "preceding",
  "frequency": "Monthly",
  "dayOfExecution": "01"
}
```

5.3.4.2. XML кодиране на Постоянно нареждане за периодично плащане

В предложението на Берлинската група, постоянните данни за управление на плащането са JSON базирани, докато съответните данни за плащане се основават на XML синтаксис. По тази причина заявката за инициране на постоянно нареждане се определя като HTTP multipart съобщение и не се поддържа.

5.4. Заявка за статус на Транзакция за Плащане

С това съобщение ДПУ генерира заявка за проверка на статуса на транзакцията при ДПУОС.

Call:

GET /v1/{payment-service}/{payment-product}/{paymentId}/status

Path parameter

Attribute	Type	Description
payment-service	String	Payment product of the related payment. The possible values are “payments”, “bulk-payments” and “periodic-payments”
paymentId	String	Resource Identification of the related payment

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current PIS transaction.
Accept	String	Optional	The TPP can indicate the formats of status reports supported together with a prioritisation following the HTTP header definition. The formats supported by this specification are • xml • JSON If only one format is supported by the TPP, which is not supported by the ASPSP this can lead to a rejection of the request.

Query Parameters

No specific query parameters defined.

Request Body

No body.

5.4.1. Отговор за статус на Плащане иницирано в JSON формат

С това съобщение ДПУОС връща към ДПУ информация за състоянието на транзакцията. В случай, че вече изпратеното искане за инициране на плащане е JSON кодирано, състоянието се връща също въз основа на JSON формат.

Response Code

The HTTP response code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body in Case of JSON based endpoint

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	In case where the Payment Initiation Request was JSON encoded as defined in Section 5.3.1., the status is returned in this JSON based encoding.
fundsAvailable	Boolean	Condition	This data element is contained, if supported by the ASPSP, if a funds check has been performed and if the transactionStatus is "ACTC", "ACWC" or "ACCP".
psuMessage	Max500Text	Optional	
_links	Links	Optional	Should refer to next steps if the problem can be resolved via the interface e.g. for re-submission of credentials.
tppMessages	Array of TPP Message Information	Optional	Messages to the TPP on operational issues.

Example for JSON based endpoint

Request

```
GET https://api.testbank.com/v1/payments/sepa-credit-transfers/1234-wertiq-983/status
Accept:application/json
X-Request-ID:99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date Sun, 28 Jan 2018 16:54:07 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID:99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date Sun, 28 Jan 2018 16:54:07 GMT
Content-Type application/json
{
  "transactionStatus": "ACCP",
  "fundsAvailable": true
}
```

5.4.2. Отговор за статус на Плащане иницирано в XML формат

С това съобщение ДПУОС връща към ДПУ информация за състоянието на транзакцията. Когато заявката за плащане е предоставена чрез XML pain.001 съобщение, отговорът за състоянието на транзакцията следва да се предостави в структурата на XML pain.002 съобщение.

Example for XML based endpoint

Request

```
GET https://api.testbank.com/v1/payments/pain.001-sepa-credit-transfers/1234-wertiq-983/status
Accept: application/xml
```

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:04:07 GMT

Response

HTTP/1.x 200 Ok

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 06 Aug 2017 15:05:08 GMT

Content-Type: application/xml

```
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.002.001.03">
  <CstmrPmtStsRpt>
    <GrpHdr>
      <MsgId>4572457256725689726906</MsgId>
      <CreDtTm>2017-08-05T20:24:56.021Z</CreDtTm>
      <DbtrAgt><FinInstnId><BIC>ABCDEFF</BIC></FinInstnId></DbtrAgt>
      <CdtrAgt><FinInstnId><BIC>DCBADEFF</BIC></FinInstnId></CdtrAgt>
    </GrpHdr>
    <OrgnlGrpInfAndSts>
      <OrgnlMsgId>MIPI-123456789RI-123456789</OrgnlMsgId>
      <OrgnlMsgNmId>pain.001.001.03</OrgnlMsgNmId>
      <OrgnlCreDtTm>2017-08-05T20:23:34.000Z</OrgnlCreDtTm>
      <OrgnlNbOfTxes>1</OrgnlNbOfTxes>
      <OrgnlCtrlSum>123</OrgnlCtrlSum>
      <GrpSts>ACCT</GrpSts>
    </OrgnlGrpInfAndSts>
    <OrgnlPmtInfAndSts>
      <OrgnlPmtInfId>BIPI-123456789RI-123456789</OrgnlPmtInfId>
      <OrgnlNbOfTxes>1</OrgnlNbOfTxes>
      <OrgnlCtrlSum>123</OrgnlCtrlSum>
      <PmtInfSts>ACCT</PmtInfSts>
    </OrgnlPmtInfAndSts>
  </CstmrPmtStsRpt>
</Document>
```

5.5. Отговор на искане за плащане Get Payment Request

GET /v1/{[payment-service](#)}/{[payment-product](#)}/{[paymentId](#)}

Връща съдържанието на платежно нареждане.

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the payment under paymentId has been initiated.
paymentId	String	ID of the corresponding payment initiation object as returned by an Payment Initiation Request

Query Parameters

No specific query parameter.

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Attribute	Type	Condition	Description
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current PIS transaction.

Request Body

No request body.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Code

The HTTP response code equals 200.

Response Body

Тялото на отговора зависи от параметъра {payment-service}. То съдържа адресирания платежен ресурс в ДПУОС, с възможни промени на оригиналните данни.

За базираните в JSON {payment-services} данните за съобщението може да съдържат и допълнителна информация напр. с допълнение на данните за статуса.

В допълнение, платежният ресурс може да съдържа полето debtorName, дори ако не е предоставено от ДПУ. Това дава възможност на ДПУОС да транспортира името на собственика на сметката до PISP в случай, че е необходима регулаторна необходимост и ако не е предоставена по други начини, като Списък на наличните сметки или общи AIS услуги за AISP.

За базираните в XML {payment-services} се връща pain.001. В случай на подадено периодично плащане във формат pain.001, може да се върне като HTTP multipart съобщение.

Във всички случаи ДПУОС може да върне различни данни от съдържанието на оригинално подадените елементи, ако се налага преформатиране на съдържанието, напр. заявените дати за изпълнение при периодично плащане или промяна на азбучни символи в информацията.

Забележка: Освен това ресурсът за плащане може да съдържа полето debtorName, дори ако то не е предоставено от ДПУ. Това дава възможност на ASPSP да транспортира името на собственика на акаунта до PISP в случай, че е предвидена регулаторната необходимост и ако не е предоставена по друг начин, като например списък на наличните сметки или общи AIS услуги за AISP.

Забележка: Съгласно точка 40 от [EBA-OP2] ресурсът за плащане трябва да съдържа сметката на длъжника, след като плащането е иницирано успешно, дори ако то не е било предоставено от ДПУ в рамките на първоначалното извикване.

5.6. Искане за отмяна на плащане Payment Cancellation Request

CALL

DELETE /v1/{payment-service}/{payment-product}/{paymentId}

То иницира анулиране на плащане. В зависимост от платежната услуга, платежния продукт и политиката за изпълнение на ДПУОС, това повикване на ДПУ може да е достатъчно за да се отмени плащането. Ако разрешението за анулиране на плащането е упълномощено от

ASPSP, съответната хипервръзка ще се съдържа в съобщението за отговор. ръща съдържанието на платежно нареждане.

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId	String	Resource Identification of the related payment.

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current PIS transaction.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a redirect over an embedded SCA approach. If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Decoupled-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a decoupled SCA approach. If it equals "false", the TPP prefers not to use the decoupled approach for SCA. The ASPSP will then choose between the embedded or the redirect SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the parameter TPP-Redirect-Preferred and the SCA method chosen by the TPP/PSU. The parameter might be ignored by the ASPSP. If both parameters TPP-Redirect-Preferred and TPP-Decoupled-Preferred are present and true, the request is still not rejected, but it is up to the ASPSP, which approach will actually be used. RFU: TPP-Redirect-Preferred and TPP-Decoupled-Preferred will be revised in future versions, maybe merged. Currently kept separate for downward compatibility.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandated for the Redirect SCA Approach, specifically when TPP-Redirect-Preferred equals "true". See Section 4.10 for further requirements on this header. It is recommended to always use this header field. Remark for Future: This field might be changed to mandatory in the next version of the specification.
TPP-Nok-Redirect-URI	String	Optional	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method. This might be ignored by the ASPSP. See Section 4.10 for further requirements on this header.
TPP-Explicit-Authorisation-Preferred	Boolean	Optional	If it equals "true", the TPP prefers to start the authorisation process separately, e.g. because of the usage of a signing basket. This preference might be ignored by the ASPSP, if a signing basket is not supported as functionality. If it equals "false" or if the parameter is not used, there is no preference of the TPP. This especially indicates that the TPP assumes a direct authorisation of the transaction in the next step, without using a signing basket.

Query Parameters

No specific query parameter.

Request Body

No request body.

Response Code

Ако DELETE е достатъчно за анулиране на плащането: HTTP отговор 204.

Ако DELETE не е достатъчна за анулиране на плащането, тъй като е необходимо разрешение чрез ЗУИ метод за анулирането от Ползвателя: HTTP отговор код 202.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	Transaction Status of the payment resource
scaMethods	Array of authentication objects	Conditional	This data element might be contained, if SCA is required and if the PSU has a choice between different authentication methods. Depending on the risk management of the ASPSP this choice might be offered before or after the PSU has been identified with the first relevant factor, or if an access token is transported. If this data element is contained, then there is also an hyperlink of type "selectAuthenticationMethods" contained in the response body. These methods shall be presented towards the PSU for selection by the TPP.
chosenScaMethod	Authentication object	Conditional	This data element is only contained in the response if the APSPS has chosen the Embedded SCA Approach, if the PSU is already identified e.g. with the first relevant factor or alternatively an access token, if SCA is required and if the authentication method is implicitly selected.
challengeData	Challenge	Conditional	It is contained in addition to the data element "chosenScaMethod" if challenge data is needed for SCA.
			In rare cases this attribute is also used in the context of the "updatePsuAuthentication" link.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandated for the Redirect SCA Approach, specifically when TPP-Redirect-Preferred equals "true". If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU.

Attribute	Type	Condition	Description
			If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Rejection-NoFunds-Preferred	Boolean	Optional	"If it equals "true" then the TPP prefers a rejection of the payment initiation in case the ASPSP is providing an integrated confirmation of funds request and the result of this is that not sufficient funds are available. If it equals "false" then the TPP prefers that the ASPSP is dealing with the payment initiation like in the ASPSPs online channel, potentially waiting for a certain time period for funds to arrive to initiate the payment.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandatory for the SCA OAuth Approach.
TPP-Explicit-Authorisation-Preferred	Boolean	Optional	If it equals "true", the TPP prefers to start the authorisation process separately, e.g. because of the usage of a signing basket. This preference might be ignored by the ASPSP, if a signing basket is not supported as functionality. If it equals "false" or if the parameter is not used, there is no preference of the TPP. This especially indicates that the TPP assumes a direct authorisation of the transaction in the next step, without using a signing basket.
_links	Links	Conditional	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Type of links admitted in this response, (further links might be added for ASPSP defined extensions):
			"startAuthorisation": In case, where an explicit start of the transaction authorisation is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded).
			"startAuthorisationWithPsuIdentification": In case where a PSU Identification needs to be updated when starting the cancellation authorisation: The link to the cancellation-authorisations end-point, where the cancellation sub-resource has to be generated while uploading the PSU identification data.
			"startAuthorisationWithPsuAuthentication": In case of a yet to be created authorisation sub-resource: The link to the cancellation-authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU authentication data.
			"startAuthorisationWithEncryptedPsuAuthentication": Same as startAuthorisationWithPsuAuthentication where the authentication data need to be encrypted on application layer in uploading.
			"startAuthorisationWithAuthentication MethodSelection": The link to the authorisation end-point, where the cancellation-authorisation sub-resource has to be generated while selecting the authentication method. This link is contained under exactly the same conditions as the data element "scaMethods".

Пример в случай, че процесът DELETE като такъв е достатъчен за анулиране на плащането

Request

DELETE https://api.testbank.com/v1/payments/sepa-credit-transfers/123456scheduled789
Content-Type application/json
X-Request-ID 99391c7e-ad88-49ec-a2ad-99ddcb1f7769
Date Sun, 13 Aug 2017 17:05:37 GMT

Response

HTTP/1.x 204
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7769
Date: Sun, 13 Aug 2017 17:05:38 GMT

Пример в случай, че процесът DELETE изисква ЗУИ авторизация от Ползвателя

Request

DELETE https://api.testbank.com/v1/payments/sepa-credit-transfers/123456scheduled789
Content-Type application/json
X-Request-ID 99391c7e-ad88-49ec-a2ad-99ddcb1f7769
Date Sun, 13 Aug 2017 17:05:37 GMT

Response

HTTP/1.x 202
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7769
Date: Sun, 13 Aug 2017 17:05:38 GMT
{
 "transactionStatus": "ACTC",
 "_links": {
 "self": {"href": "/v1/payments/sepa-credit-transfers/123456scheduled789"},
 "status": {"href": "/v1/payments/sepa-credit-transfers/123456scheduled789/status"},
 "startAuthorisation": {"href": "/v1/payments/sepa-credit-transfers/123456scheduled789/cancellation-authorisations"}
 }
}

5.7. Искане за получаване на под-ресурсите при оторизирано анулиране

CALL

GET/v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations

Ще предостави масив от идентификатори за всички генерирани под-ресурси на оторизираното анулиране.

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are "payments", "bulk-payments" and "periodic-payments"
payment-product	String	The payment product, under which the paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId	String	Resource Identification of the related payment.

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current PIS transaction.

Query Parameters

No specific query parameter.

Request Body

No request body.

Response Code

HTTP отговор 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
authorisationIds	Array of String	Mandatory	An array of all authorisationIds connected to this payment resource.

Пример:

Request

```
GET https://api.testbank.com/v1/payments/sepa-credit-transfers/1234-wertiq-983/cancellation-authorisations
Accept: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7723
Date: Sun, 06 Aug 2017 15:04:07 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7723
Date: Sun, 06 Aug 2017 15:04:08 GMT
Content-Type: application/json
{
  "authorisationIds": ["123auth456"]
}
```

5.8. Множествена ЗУИ авторизация при Плащания

Заявките за инициране на плащания, дефинирани в този раздел, са независими от необходимостта от единична или множествена обработка на ЗУИ, т.е. независимо от броя на

разрешенията, необходими за извършване на плащанията. Съобщенията за отговор, дефинирани по-горе в този раздел, са специфични за единична ЗУИ авторизация.

За започване на плащане с множествена ЗУИ авторизация, тази спецификация изисква изрично стартиране на разрешението. Когато се изисква множествена ЗУИ авторизация, връзките като "scaRedirect" или "scaOAuth", не могат да се съдържат в отговора на Искане за инициране на плащане. В отговора на Искането също така не се поддържат и други действия, като избора на ЗУИ.

В тези случаи най-напред трябва да се генерира под-ресурс за авторизация чрез link: "startAuthorisation".

Отговор на съобщения за инициране на плащания с множествена ЗУИ авторизация

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	The values defined in Section 14.22 might be used.
paymentId	String	Mandatory	resource identification of the generated payment initiation resource.
transactionFees	Amount	Optional	Can be used by the ASPSP to transport transaction fees relevant for the underlying payments.
transactionFee Indicator	Boolean	Optional	If equals "true", the transaction will involve specific transaction cost as shown by the ASPSP in their public price list or as agreed between ASPSP and PSU. If equals "false", the transaction will not involve additional specific transaction costs to the PSU.
_links	Links	Mandatory	"startAuthorisation": In case, where an explicit start of the transaction authorisation is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded).
			"startAuthorisationWithPsuIdentification": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU identification data.
			"startAuthorisationWithPsuAuthentication": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU authentication data.
			"startAuthorisationWithEncryptedPsuAuthentication": The link to the authorisation end-point, where an authorisation sub-resource has to be generated while uploading the encrypted PSU authentication data.
			"self": The link to the payment initiation resource created by this request. This link can be used to retrieve the resource data. "status": The link to retrieve the transaction status of the payment initiation.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU
tpmMessages	Array of Message	Optional	Messages to the TPP on operational issues.

Забележка: За разлика от потока при Инициране на плащане с една ЗУИ авторизация, процесите за оптимизация с автоматично генериране на авторизация не се поддържат за

множествената ЗУИ авторизация. За да се осъществи процеса на авторизация от различни Ползватели за едно и също плащане се изисква изрично стартиране на процеса по авторизация. Единствените хипервръзки за управление, които се връщат на ДПУ след започване на плащанията, са хипервръзки от тип "**startAuthorisation**", с искане за задължителна допълнителна информация, която се предоставя със заявката за стартиране на авторизацията. Команди за избор на метод (SCA method) или OTP отговор, са неприложими при множествена авторизация.

5.9. Особеност при инициране на плащания от много-валутна сметка

Данните за плащанията, съдържащи се в Request body, могат да се отнасят и до под-сметки, които се предоставят в конкретни валути, т.е. по дефиницията на много-валутни сметки в раздел 4.5. Това е независимо от кодирането в JSON или XML.

6. Услуги за Информация по сметка

Тази спецификация предвижда различни видове услуги за информация по сметки:

- Списък на наличните сметки;
- Детайли за конкретна сметка (включително салда, ако е приложимо);
- Баланс по конкретна сметка;
- Списък на транзакции по конкретна сметка, включително салда, ако е приложимо
- Предоставяне на детайли по транзакция от сметки.

По този начин дефинирането на списъка с налични и достъпни сметки е както следва:

Определение: Списък с **наличните** сметки в ДПУОС, свързан с Ползвателя, е списък на сметките на Ползвателя, които са отворени за достъп чрез интерфейс Достъп до сметка съгласно определението за платежни сметки, предоставено от [PSD2].

Определение: Списък с **достъпни** сметки в ДПУОС, е набор от сметки свързани с предоставено съгласие на Ползвателя за достъп до поне една от дефинираните типове услуги.

Забележка: Искането за четене на данни за списъка с наличните сметки и данните за конкретна сметка е синтактично идентично. Разликата е само в основния ресурс за съгласие, посочен чрез HTTP параметъра "Consent-Id".

Пример:

ДПУОС поддържа IBAN1 и IBAN2 на Ползвателя. Ползвателят предоставя на ДПУ съгласието за достъп до транзакции и салда по IBAN1. В този случай наличните сметки са IBAN1 и IBAN2, списъкът с достъпни сметки се състои само от IBAN1.

Установяване на съгласие и Предоставяне на данни за сметка

В рамките на тази спецификация услугата за Информация по сметка е разделена на две фази:

- **Установяване на съгласие за информация за сметка**

В рамките на този етап от услугата за информация по сметка, доставчикът на услуги дава съгласието си на AISP за

- Вида на предоставената услуга за информация по сметка
- Честота на услугата за информация по сметка, т.е. еднократен или повтарящ се достъп, и
- Продължителността на съгласието в дни или максималния срок, предложен от ДПУОС и по избор честотата на повтарящата се заявка. (трябва да се прави разлика между честота на услуга и честота на заявка)

Като последна стъпка съгласието се оторизира от Ползвателя към ДПУОС чрез ЗУИ метод, съгласно изискванията на Делегирания документ [EBA-RTS].

Резултатът от тази фаза е ресурс „Съгласие“. В рамките на фазата този ресурс се съхранява при ДПУОС. ДПУ може да изтегли Съгласието като обект чрез подаване на метод GET за този ресурс. Този обект съдържа подробните Права за достъп, Идентификатор на съгласието и предоставя Псевдоними на сметките, като част от услугата за достъп до тях.

Забележка: Установяването на съгласие за AIS е една транзакция, следваща правилата за Достъп до сметка, която създава Съгласие и идентификационен номер на Съгласието. По този начин всички съобщения ще използват един и същ идентификатор в елемента Идентификационен номер на Съгласие при ДПУ-транзакция.

- **Предоставяне на данни за сметка**

В рамките на тази фаза ДПУ (AISP) получава достъп до данните за сметката, както е определено в съгласието на Ползвателя на услуги. Заявката за Предоставяне на данни се отнася до съответния ресурс в съгласието, като използва горепосочената връзка към този ресурс (Правила за достъп, Идентификатор на съгласие, псевдоними и т.н.).

Заявката за Предоставяне на данни по сметка трябва да съдържа:

- Типът на банковите сметки, до които трябва да получи достъп,
- Идентификацията на адресираната сметка, където е приложимо,
- Дали Ползвателя директно е инициирал заявката в реално време,
- Дали балансите трябва да се предоставят допълнително, когато е приложимо,
- В случай на отчети за транзакции като допълнителна информация за сметка:
 - Идентификатор на адресираната сметка
 - Периода на отчета
 - Предпочитаните формати на отчетите за транзакциите
 - В допълнение, по избор делта-флаг, показващ искане само за допълнителните данни спрямо данните от последната заявка.

При Предоставяне на данни за сметка, обичайните банкови сметки и (кредитните) картови сметки се разделят на отделни крайни точки, тъй като данните обикновено са в различни модули от системата на ДПУОС.

В случай на еднократно съгласие достъпът може да бъде отказан от ДПУОС, ако ДПУ като (AISP) иска повече от един път данните или ако валидността на съгласието е изтекла, напр. след 20 минути от финализирането на механизма за съгласие.

Предоставянето на данни може да бъде отказано и в случай, че типът на услугата Информация за сметка не отговаря на услуга от Съгласието или ако действителният достъп не съвпада със съгласуваната продължителността или честотата.

Ако съгласието на Ползвателя е за достъп до списък със сметки, ДПУОС поддържа честотата и правото на достъпа за всяка една сметка поотделно.

Забележка: В случай на голям обем от транзакции с данни, съгласно интерфейса Достъп до сметка, това са собствени транзакции, така че идентификатора на транзакциите (transaction-id) ще се използва многократно при странициране на информацията за Списък на транзакции / Извлечение от сметка.

Модели за съгласие

Тази спецификация поддържа три различни модела на съгласие:

- Подробно съгласие

Управлението на съгласието се обработва между ДПУ и Ползвателя. След това ДПУ предоставя информацията за подробно съгласие - идентификация на ползвателя, услугите и номерата на сметките, които са засегнати - до ДПУОС за авторизация от страна на ползвателя. ДПУОС показва данните за съгласието на ползвателя при извършване на ЗУИ.

- Глобално съгласие

Управлението на съгласието се обработва между ДПУ и Ползвателя. След това ДПУ предоставя информацията за глобално съгласие, която е само идентификация на ползвателя към ДПУОС за авторизация от ползвателя. ДПУОС показва само общия достъп до сметката на ползвателя при извършване на ЗУИ.

- Предложено от банката съгласие

ДПУ иска от ДПУОС да извърши Управлението на съгласието. ДПУОС може да поиска от ползвателя подробно съгласие или просто да получи глобално съгласие за всички услуги „Информация за сметка“. Това се разрешава от ползвателя чрез ЗУИ. Информацията за подробно съгласие може да бъде извлечена от ДПУ в следваща стъпка, като се прочете съответното съгласие.

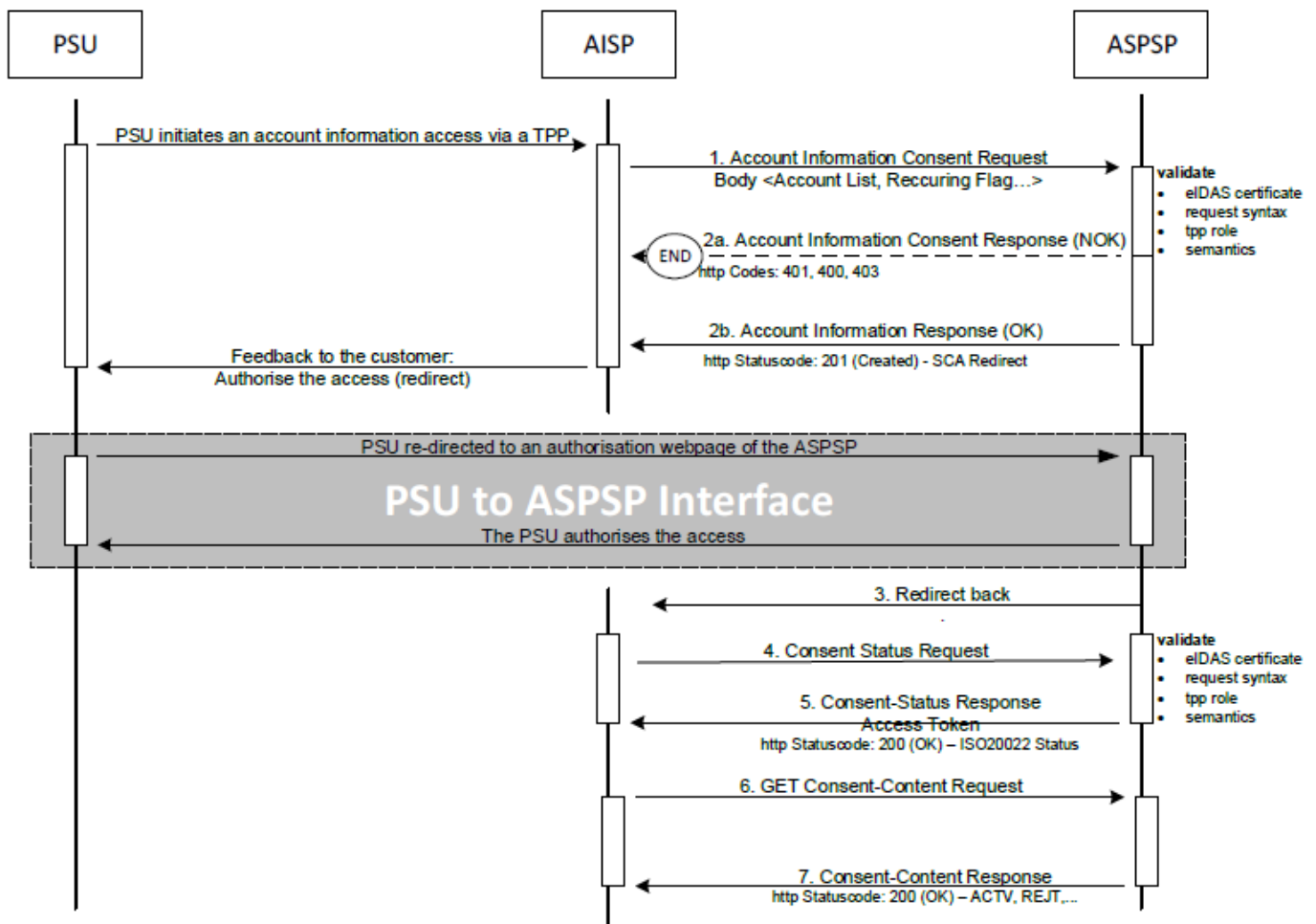
6.1. Потоци на процеса за достъп до информация (Account Information Service Flows)

Както в секцията за инициране на плащане, трябва да се има в предвид, че следните потоци не обхващат всички възможни варианти и са само примерни схеми.

6.1.1. Последователност на процесите при подаване на Съгласие за достъп до информация за сметка

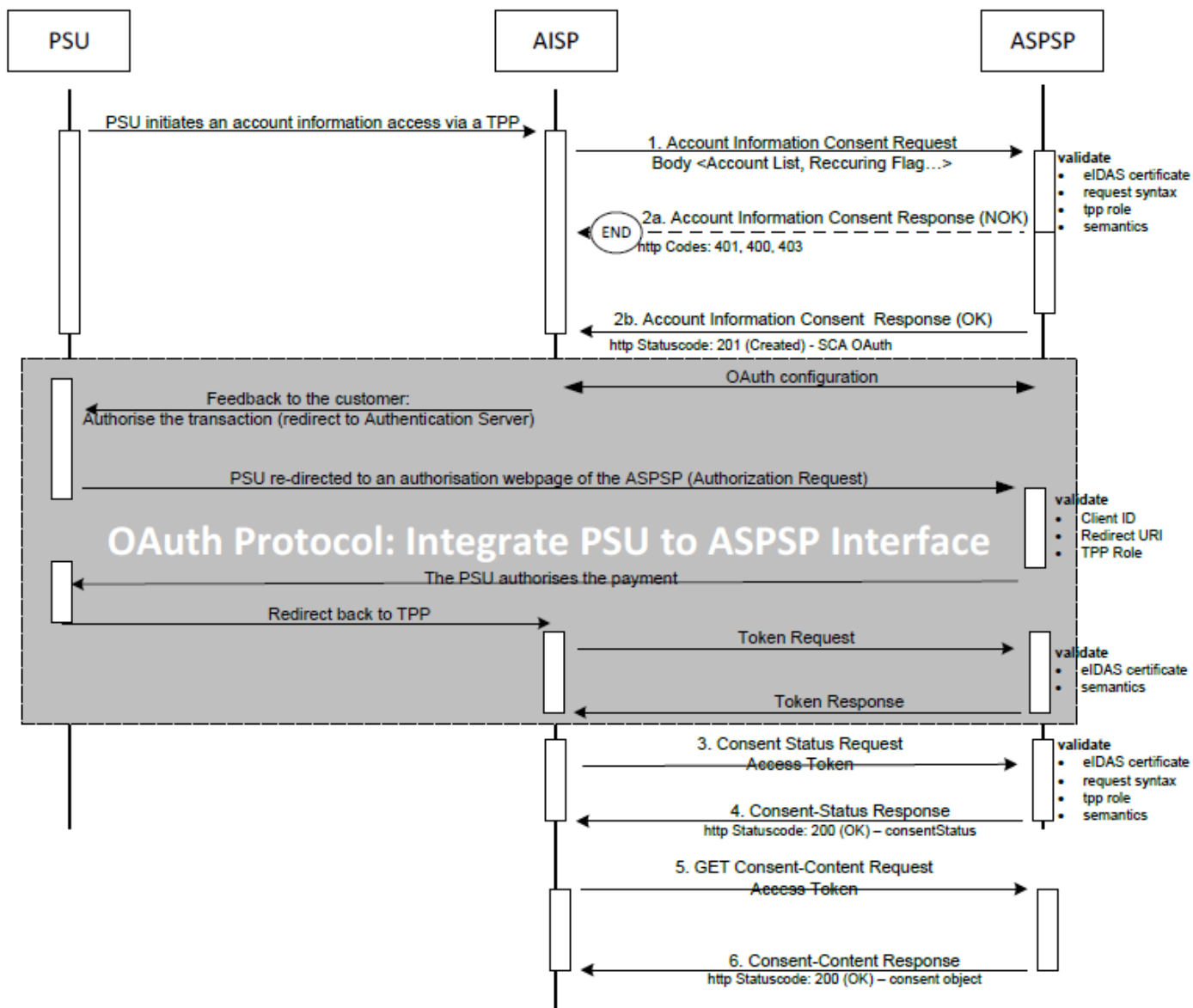
Redirect подход на ЗУИ

Ако ДПУОС поддържа подхода "Redirect ЗУИ", потокът от съобщения в под-услугата "Съгласие за информация за сметка" е прост. Искането за съгласие за информация по сметка е последвано от пренасочване към сайта за разрешение на ДПУОС. Заявката за статус или съдържание на създадения ресурс за съгласие може да бъде поискана от ДПУ, след като сесията бъде пренасочена обратно към системата на ДПУ.



OAuth2 подход на ЗУИ

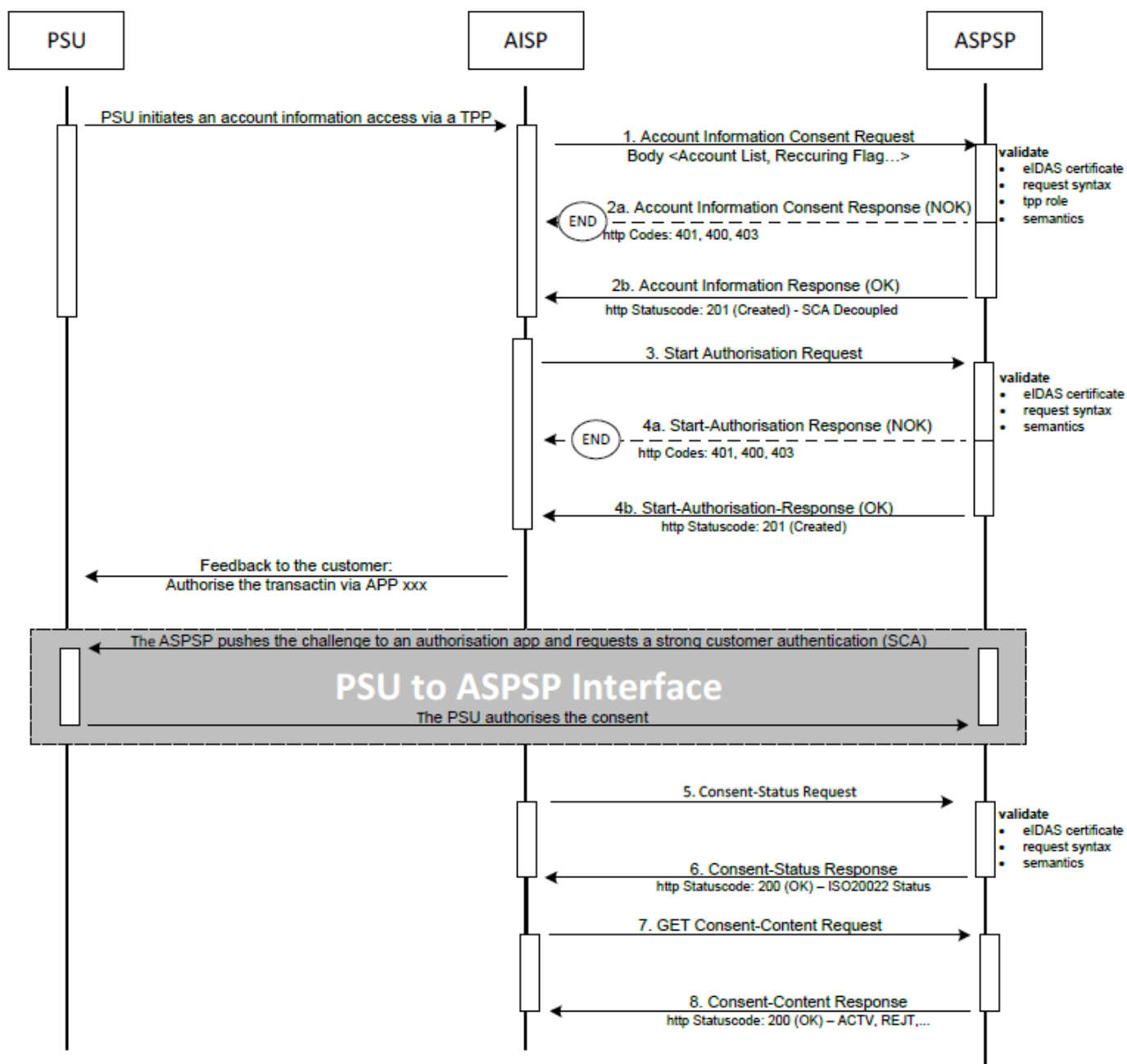
Ако ДПУОС поддържа OAuth2 ЗУИ подход, потокът е много подобен на подхода за Redirect. Вместо да пренасочва към сървър за удостоверяване на ЗУИ, протоколът OAuth2 (който се поддържа от ДПУОС) се използва директно за процеса на упълномощаване на транзакции.



Decoupled подход на ЗУИ

Потокът на транзакцията в Отделен ЗУИ подход е подобен на подхода Redirect ЗУИ. Разликата е, че ДПУОС изисква от Ползвателя да упълномощи съгласието за достъп до информация чрез специално мобилно приложение или друго приложение или устройство, което е независимо от интерфейса за онлайн банкиране. ДПУОС иска от ДПУ да уведоми Ползвателя на услугата за това удостоверяване чрез изпращане на съответното съобщение като "Моля, използвайте приложението си xxx, за да удостоверите достъпа до сметките".

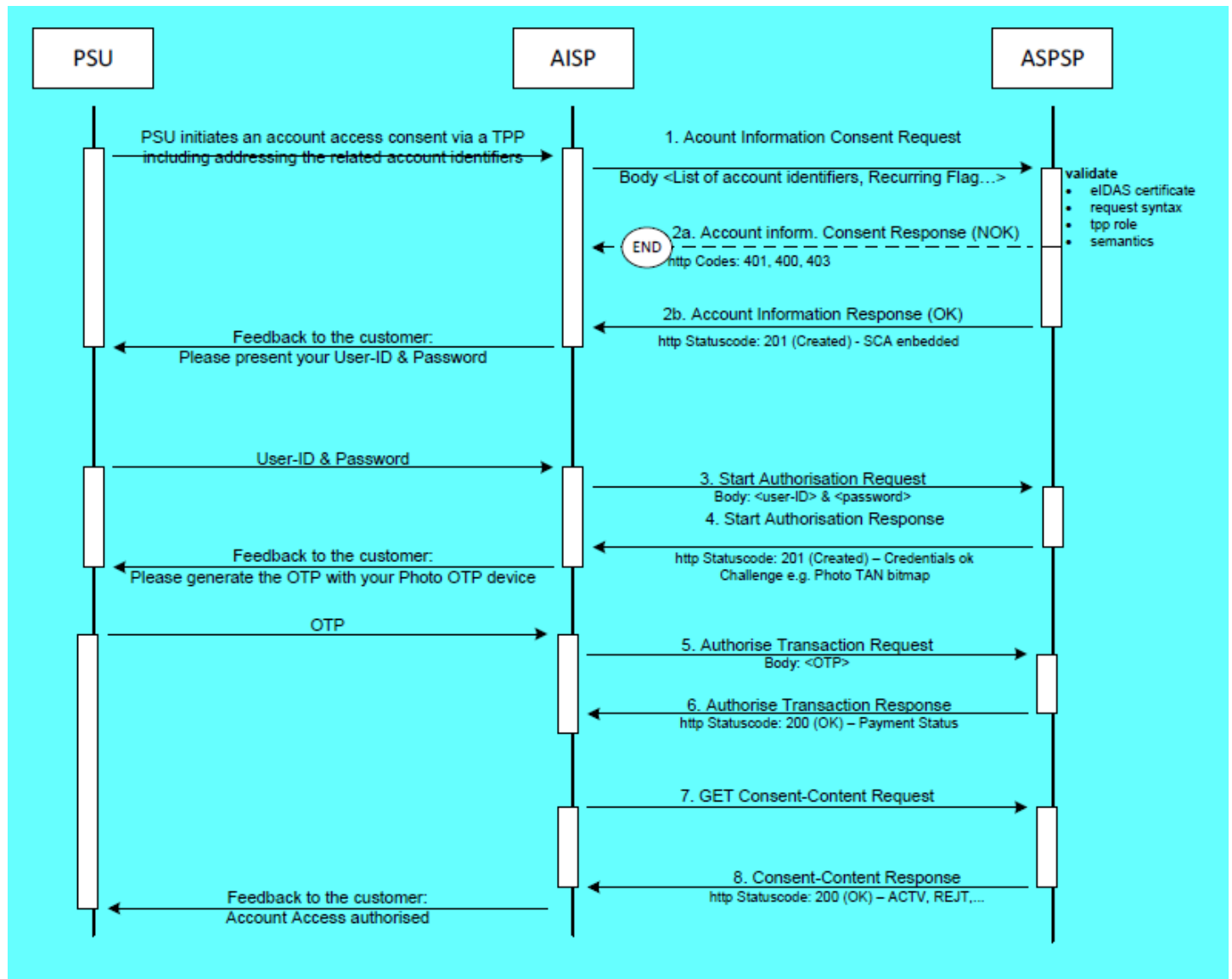
След процеса на ЗУИ между ДПУОС и Ползвателя, ДПУ трябва да поиска резултата от транзакцията.



Embedded подход при единствен метод на ЗУИ

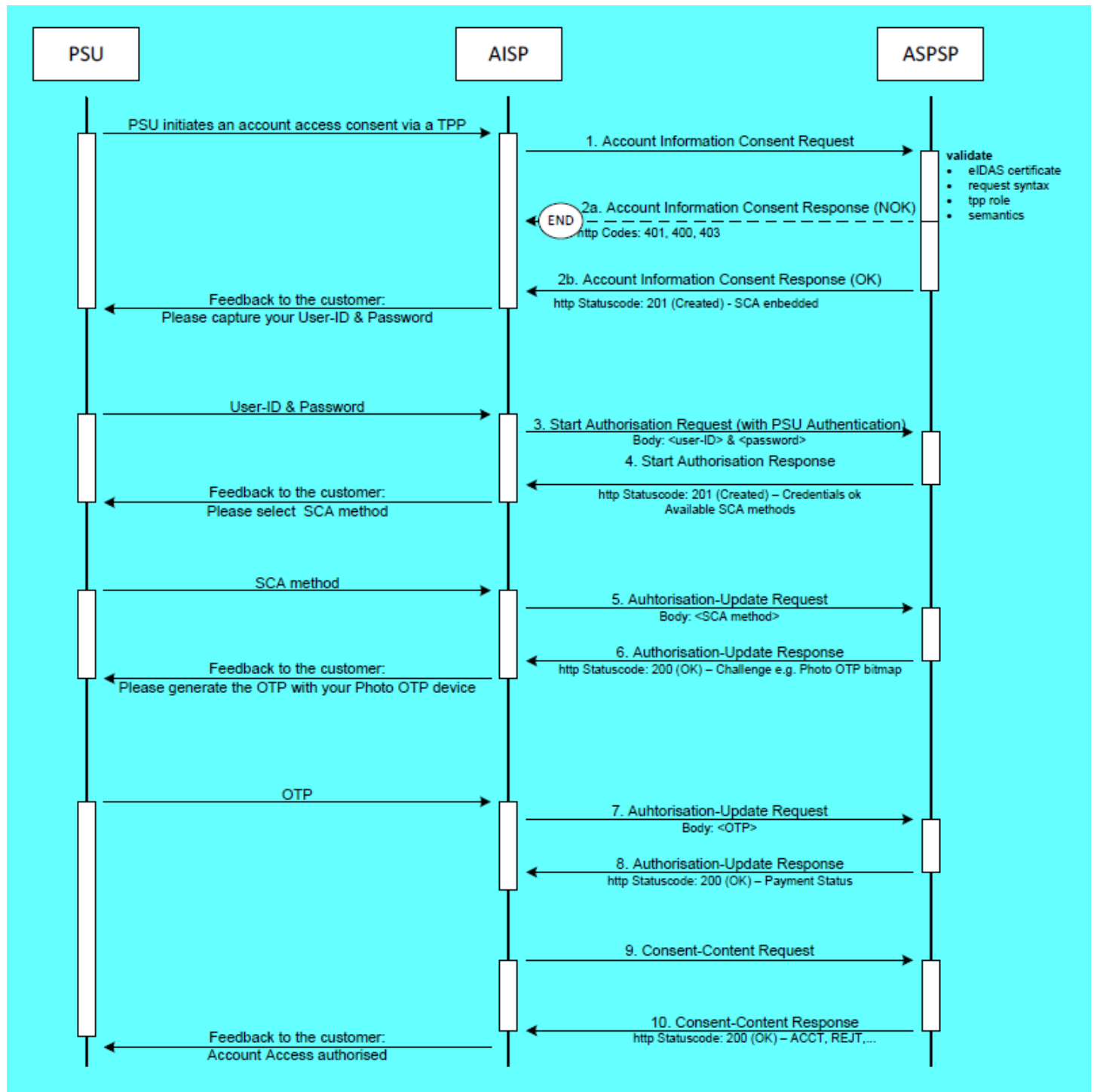
По-долу са показани няколко примерни потока, в които ДПУОС е избрал да обработва чрез Embedded метод на ЗУИ одобрение на съгласието чрез интерфейса ДПУ – ДПУОС. Във всеки случай, Ползвателя обикновено ще трябва да се идентифицира с първия фактор, още преди ДПУ да има подробности за наличните сметки или за метода на ЗУИ.

Когато ДПУОС поддържа само един технически метод на ЗУИ, след одобрението на първия фактор, към потока се добавя "Заявка за разрешаване на транзакция". След това ДПУ предава данните за удостоверяване на клиента, напр. OTP с включено динамично свързване с данните за транзакцията (втори фактор).



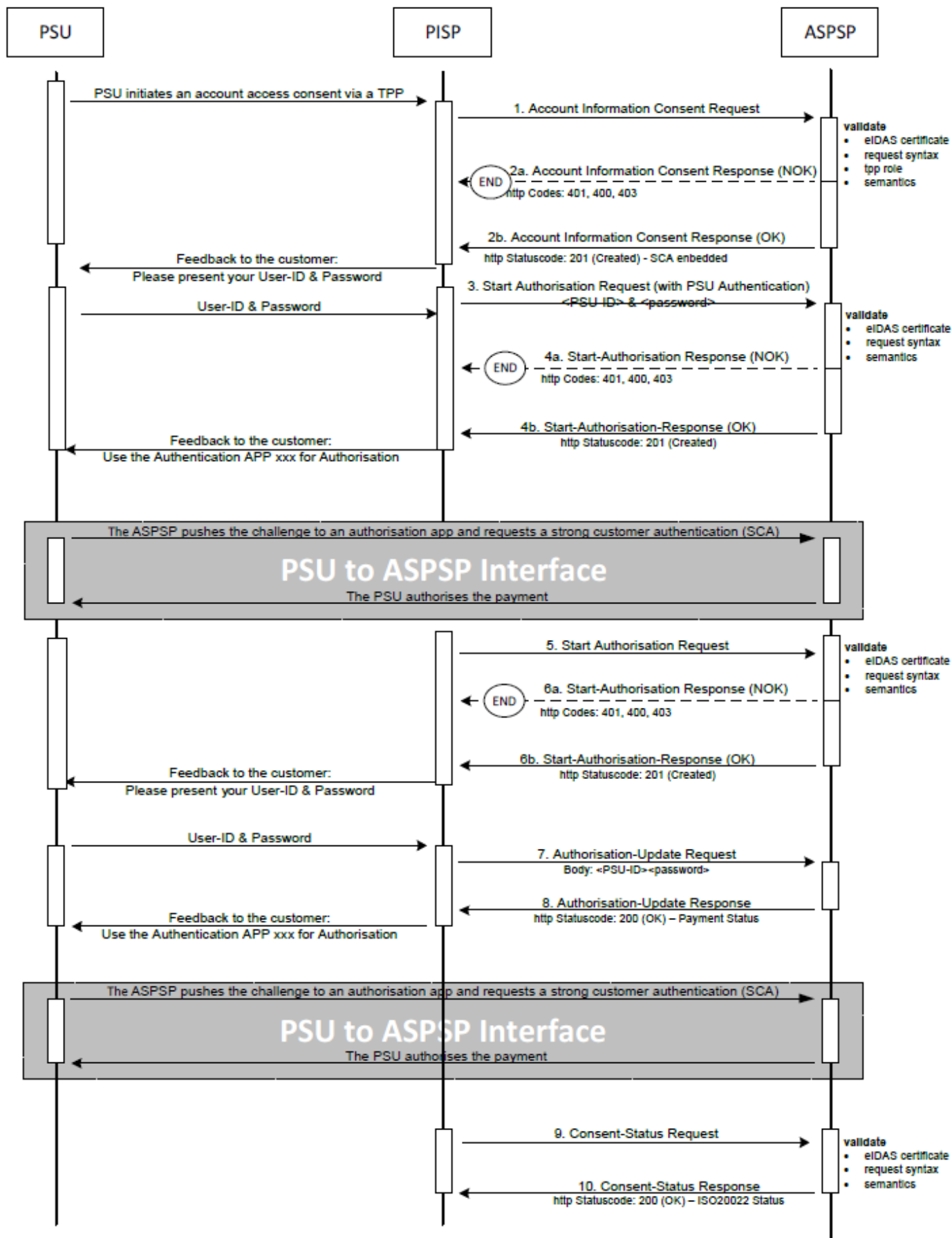
Embedded подход чрез избор на метод за ЗУИ

След одобрението на първия фактор, ако ДПУОС поддържа няколко ЗУИ метода за упълномощаване на процеса, се предлага избор на ЗУИ метод за Ползвателя. ДПУОС предлага наличните методи на ДПУ. ДПУ може да ги филтрира, до броя на техническите методи за удостоверяване, които може да поддържа. След това наличните методи се представят на Ползвателя за избор. Процесът завършва след успешна идентификация на втория фактор избран от Ползвателя и предоставен от ДПУ към ДПУОС.



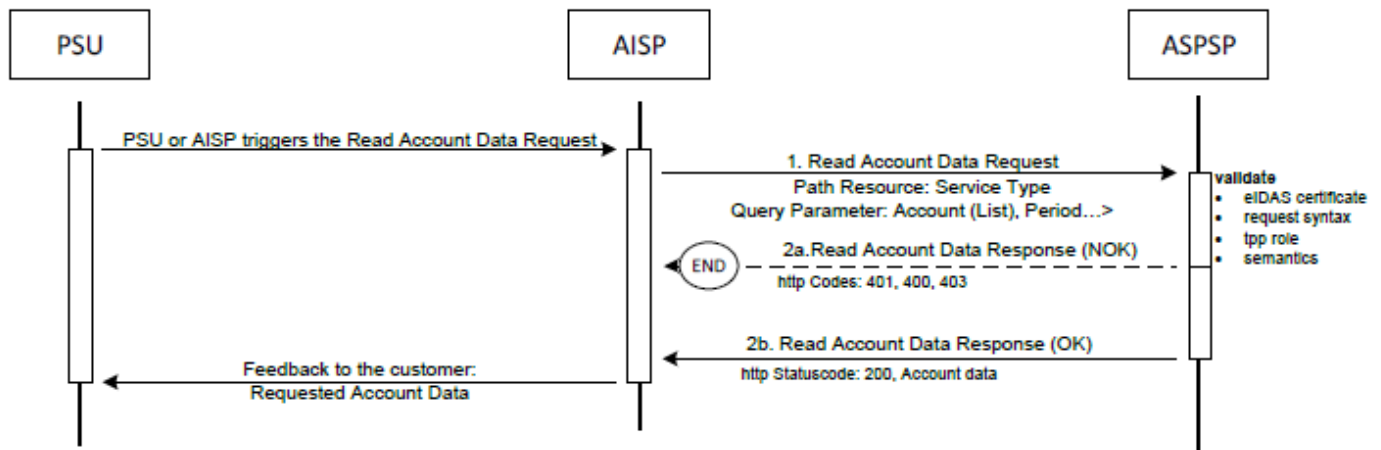
Decoupled подход чрез Multilevel ЗУИ

Многостепенният ЗУИ поток за заявките за установяване на съгласие следват точно същият модел като при иницирирането на плащане, вж. Раздел 5.1.12.



6.1.2. Последователност на процесите при Предоставяне на данни за сметка

Потокът "Предоставяне на данни за сметка" е независим от потока за управление на съгласието. Това е прост процес на заявка / отговор, както следва:



6.2. Общ преглед на данните в услугата „Информация за сметка“ (Data Overview Account Information Service)

Следната таблица дефинира техническото описание на абстрактния модел на данни, определен в правилата за услугата Информация за сметка. Колоните дават общ поглед върху API протоколите, както следва:

- Колоната "Data element" използва абстрактните елементи на данни, по [XS2A OR], за да достави връзката към правилата и дефинициите на роли в този документ.
- Колоната Attribute encoding дава определението за действително кодиране в API XS2A, както е дефинирано в този документ.
- Колоните "Location" определят кога съответните елементи на данните се транспортират като параметри на HTTP на ниво path, header или body и са взети от сертификатите eIDAS.
- Колона "Usage" дава общ преглед на използването на елементи от данни в различните услуги и API повиквания. По правило, повикванията за Достъп до сметка се описват като абстрактни API повиквания. Тези повиквания се реализират технически като команди HTTPS POST, PUT, GET и DELETE. Повикванията са изброени както следва:

- **Създаване на искане за съгласие**, което е първото повикване за приложния програмен интерфейс (API) за всяка транзакция в услугата „Информация за сметка“.
- **Повикването за актуализация на данни** е повикване при което ДПУ трябва да добави данни, свързани с идентификация на Ползвателя и след което се трябва да се върне към първото обаждане. Такова повикване може да се повтори няколко пъти (особено при ЗУИ метод Embedded).
- **Искането за авторизация** се използва само при метод Embedded, за да се разреши транзакцията в случай на необходимост от удостоверяване чрез втори фактор.
- **Искането за Предоставяне на данни** е искането за извличане на данните за сметка, които се адресират до различни крайни точки с различни параметри.

- **Заявката за състояние** се използва в случаите след успешно изпълнение на ЗУИ и ДПУ се нуждае от по-късна информация за резултата.

Използва се следното използване на съкращения в колоните " Location и Usage "

x: Този елемент от данните се транспортира на съответното ниво.

m: Задължително

o: Незадължително за използване от ДПУ

c: Условно. Условието е описано в адресираните при приложния програмнен интерфейс (API) състояния, определени от ДПУОС.

Следващата таблица дефинира не само изискванията към съобщенията за заявки, но и изисквания за елементите на данните за съобщенията за отговор. Тези изисквания се прилагат само в случай на код за HTTP отговор 2xx. В случай на HTTP отговор код 4xx или 5xx се прилагат изисквания, както е определено в раздел 4.6.

Пример: В случай на съобщение за установяване на съгласие и когато ресурсът за съгласие е създаден успешно отговорът е с код 2xx. Ако не може да бъде върната информация, свързана с ресурсите, то кодът за HTTP отговор е равен на 4xx или 5xx.

	Data element	Attribute encoding	Location					Usage									
REQUEST PART (TPP)			Path	Query Parameter.	Header	Body	Certificate	Establ. Cons. Req.	Establ. Cons. resp.	Upd. Data Req.	Upd. Data Resp	Auth. Req.	Auth Resp.	Status Req.	Status Resp.	Read Data Req.	Read Data Resp
	Provider Identification		x					m		m		m		m		m	
	Resource ID	consentId				x			m								
	Resource ID[1]		x							m		m		m			
	TPP Registration Number						x	m		m		m		m		m	
	TPP Name						x	m		m		m		m		m	
	TPP Role						x	m		m		m		m		m	
	TPP National Competent Authority						x	m		m		m		m		m	
	Resource-ID[2]	Consent-ID			x											m	
	Access Token (from optional OAuth2)	Authorization			x			c		c		c		c		c	
	TPP Signing Certificate Data	TPP-Signature-Certificate			x			c		c		c		c		c	
	TPP Signing Electronic Signature	Signature			x			c		c		c		c		c	
	Further signature related data	Digest			x			c		c		c		c		c	
	PSU Identification	PSU-ID			x			c		c							
	PSU Identification Type	PSU-ID-Type			x			c		c							
	Corporate Identification	PSU-Corporate-ID			x			c		c		c		c			
	Corporate Type	PSU-Corporate-ID-Type			x			c		c		c		c			
	IP Address PSU	PSU-IP-Address			x			m		o		o		o		c	
	PSU IP Port	PSU-IP-Port			x			o		o		o		o		o	
	Further PSU related Information	PSU-Accept			x			o		o		o		o		o	
		PSU-Accept-Charset			x			o		o		o		o		o	
		PSU-Accept-Encoding			x			o		o		o		o		o	
		PSU-Accept-Language			x			o		o		o		o		o	
	PSU-Http-Method			x			o		o		o		o		o		

		PSU-Device-ID			x					o		o		o		o			
	PSU User Agent	PSU-User-Agent			x					o		o		o		o			
	GEO Information	PSU-Geo-Location			x					o		o		o		o			
	Redirect URL TPP	TPP-Redirect-URI			x					c									
	Decoupled Preference	TPP-Decoupled-Preferred			x					o									
	Authorisation Preference	TPP-Explicit-Authorisation-Preferred			x					o									
	TPP Notification URI	TPP-Notification-URI			x					o									
	TPP Notification Content Preference	TPP-Notification-Content-Preferred			x					o									
	TPP Brand Information	TPP-Brand-Logging-Information			x					o									
	PSU Password	psuData.password				x						c							
	PSU Authentication Data	psuData.authentication				x								m					
	PSU Account	account				x												c	
	PSU Account List	access				x			m										
	Validity Period	validUntil				x			m										
	Frequency	frequencyPerDay				x			m										
	Recurring Indicator	recurringIndicator				x			m									c	
	Combined service	combinedServiceIndicator				x			m										
	Redirect Preference	TPP-Redirect-Preferred			x				o										
	Date From	dateFrom		x														c	
	Date To	dateTo		x														c	
Response (ASPSP)	Transaction From	entryReferenceFrom		x														o	
	Booking Status	bookingStatus		x														o	
	Delta Indicator	deltaList		x														o	
	With Balance Flag	withBalance		x														o	
	Request Identification	X-Request-ID			x				m	m	m	m	m	m	m	m	m	m	m
	ASPSP-SCA-Approach	ASPSP-SCA-Approach			x					c		c							
	Resource ID	consentId				x			m										
	Transaction Status	consentStatus				x			m		m		m		m				
	PSU Message Information	psuMessage				x			o		o		o		o		o		
	TPP Message Information	tppMessages				x			o		o		o		o		o		
	SCA Status	scaStatus				x									o				
	SCA Challenge Data	challengeData				x			c		c								
	Redirect URL ASPSP	_links.scaRedirect				x			c										

[1] Please note that the Resource ID is transported in the path after the generation of the consent resource. This is then a path parameter without an explicit encoding of the attribute name.

[2] Please note that the consent identification is addressed by different syntax depending of where it is transported.

Забележка: Горната таблица се отнася до "Заявка за Съгласие за информация по сметка", отнасяща се до конкретни сметки, Секция 6.3.1.1.

Повиквания от интерфейса за Достъп до сметка, които представляват съобщения, определени в Искането за съгласие за плащане, ще бъдат дефинирани в следващите раздели.

Забележка: Услугите на AIS и PIS споделят някои под-процеси, които са описани в Раздел 7. Това се отнася за всички дефиниции от тип Заявка / Отговор на данни за Ползвателя, както и за дефиниции за Заявка / Отговор за авторизация на транзакции.

IP адрес / порт и допълнителна информация, свързана с Ползвателя.

Следните данни за елементи от горната таблица препращат информация за интерфейса Ползвател / ДПУ и подобряват процедурите за управление на риска на ДПУОС. Препоръчително е тези елементи от данни да присъстват във всички съобщения за заявки в рамките на потока от транзакции Установяване на съгласие и Предоставяне на данни по сметка. По-надолу в табличен вид е предоставена допълнителна информация с описание за параметрите на заявката и дефиницията на тези елементи. Като изключение описанието за IP-адреса на PSU е "незадължително", но при Установяване на съгласие е "задължително".

Attribute	Format	Condition	Description
PSU-IP-Address	String	Optional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP.
PSU-IP-Port	String	Optional	The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available.
PSU-Accept	String	Optional	The forwarded IP Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available.
PSU-Accept-Charset	String	Optional	see above
PSU-Accept-Encoding	String	Optional	see above
PSU-Accept-Language	String	Optional	see above
PSU-User-Agent	String	Optional	The forwarded Agent header field of the HTTP request between PSU and TPP, if available.
PSU-Http-Method	String	Optional	HTTP method used at the PSU – TPP interface, if available. Valid values are: • GET • POST • PUT • PATCH • DELETE
PSU-Device-ID	String	Optional	UUID (Universally Unique Identifier) for a device, which is used by the PSU, if available. UUID identifies either a device or a device dependant application installation. In case of an installation identification this ID need to be unaltered until removal from device.
PSU-Geo-Location	Geo Location	Optional	The forwarded Geo Location of the corresponding HTTP request between PSU and TPP if available.

Много-валутни Сметки (Multicurrency Accounts)

Определение: Много-валутна сметка е съвкупност от различни под-сметки, които са адресират от един и същ идентификатор (като IBAN, напр.). Под-сметките са законово различни и всички се различават по тяхната валута, салда и транзакции. Идентификаторът на сметката като IBAN заедно с валута, винаги уникално адресира под-сметка на много-валутна сметка.

Тази спецификация поддържа адресиране на много-валутни сметки, както на агрегирано ниво, така и на ниво под-сметка. Атрибутът за код валута в съответната структура от данни "Account Reference" позволява изграждането на структури като:

```
{"iban": "DE40100100103307118608"}
```

или

```
{"iban": "DE40100100103307118608",  
  "currency": "EUR"}
```

Ако основната сметка е много-валутна сметка тогава:

- първото позоваване се отнася до адресиране към този IBAN за всички под-сметки към него;
- второто позоваване се отнася само за под-сметката за валута евро.

Тази спецификация на интерфейса действа по под-сметки на сметка с няколко валути по същия начин, както при обикновени сметки.

Методите за достъп до много-валутни сметки се различават в интерфейса поради факта, че се адресира колекция от сметки. По-долу разликите са описани на абстрактно ниво:

Много-валутни сметки при подаване на съгласие

Много-валутните сметки се адресират само чрез използване на идентификатора на външната сметка при подаване на съгласие, без да се посочва валута. Искането на съгласие за извличане на данни от тип „Информация за сметка“ на много-валутни сметки предполага получаването на информация за всички под-сметки.

Много-валутни сметки при Информация за сметка или Детайли за сметка

ДПУОС ще реши в изпълнението си дали да предостави достъп до данни за много-валутна сметка с агрегация на външно ниво, на външно ниво и под-сметка или само на ниво под-сметка.

Много-валутни сметки при информация с баланс

Последицата от тази функция е, че се връща масив от салда от всички под-сметки, ако на ниво агрегиране се адресира много-валутна сметка. Валутата на съответната под-сметка имплицитно се предоставя като валута на елемента balanceAmount в баланса.

Много-валутни сметки при информация за транзакции

В следствие на тази функция, списъкът на транзакциите ще съдържа всички транзакции на всички под-сметки, ако на ниво агрегиране е адресирано много-валутна сметка. В този случай платежните транзакции, съдържащи се в отчета, могат да имат различни валути на транзакциите.

6.3. Установяване на съгласие за Информация по сметка (Establish Account Information Consent)

В този раздел са дефинирани процесите в интерфейса за установяване на съгласие за Информация по сметка.

6.3.1. Заявка за установяване на съгласие

validUntil

6.3.1.1. *Искане за установяване на съгласие към определена сметка*

Повикване

POST /v1/consents

Създава Съгласие за Информация за сметка в ДПУОС относно достъпа до конкретно посочените сметки в заявката.

При подаване на искане за съгласие, където "повтарящ се индикатор" има стойност "true" и ако вече съществува предварително съгласие за повтарящ се достъп до информацията за сметката, тогава предишното съгласие автоматично изтича веднага след като искането за ново съгласие е упълномощено от Ползвателя.

Ако за предишното съгласие "повтарящ се индикатор" има стойност "false", не се изискват никакви действия по него, защото се счита, че вече е изтекло.

Query parameters

Няма Query parameters

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
PSU-ID	String	Conditional	Client ID of the PSU in the ASPSP client interface. Might be mandated in the ASPSP's documentation. It might be contained even if an OAuth2 based authentication was performed in a pre-step In this case the ASPSP might check whether PSU-ID and token match, according to ASPSP documentation.
PSU-ID-Type	String	Conditional	Type of the PSU-ID, needed in scenarios where PSUs have several PSU-IDs as access possibility.
PSU-Corporate-ID	String	Conditional	Might be mandated in the ASPSP's documentation. Only used in a corporate context.
PSU-Corporate-ID-Type	String	Conditional	Might be mandated in the ASPSPs documentation. Only used in a corporate context.
PSU-IP-Address	String	Mandatory	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. If not available, the TPP shall use the IP Address used by the TPP when submitting this request.
Authorization	String	Conditional	If OAuth2 has been chosen as pre-step to authenticate the PSU.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a redirect over an embedded SCA approach. If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach,

Attribute	Type	Condition	Description
			depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Decoupled-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a decoupled SCA approach. If it equals "false", the TPP prefers not to use the decoupled approach for SCA. The ASPSP will then choose between the embedded or the redirect SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the parameter TPP-Redirect-Preferred and the SCA method chosen by the TPP/PSU. The parameter might be ignored by the ASPSP. If both parameters TPP-Redirect-Preferred and TPP-Decoupled-Preferred are present and true, the request is still not rejected, but it is up to the ASPSP, which approach will actually be used. RFU: TPP-Redirect-Preferred and TPP-Decoupled-Preferred will be revised in future versions, maybe merged. Currently kept separate for downward compatibility.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandatory for the SCA OAuth Approach.
TPP-Nok-Redirect-URI	String	Optional	
TPP-Explicit-Authorisation-Preferred	Boolean	Optional	If it equals "true", the TPP prefers to start the authorisation process separately, e.g. because of the usage of a signing basket. This preference might be ignored by the ASPSP, if a signing basket is not supported as functionality. If it equals "false" or if the parameter is not used, there is no preference of the TPP. This especially indicates that the TPP assumes a direct authorisation.
TPP-Notification-URI	String	Optional	URI for the Endpoint of the TPP-API to which the status of the consent should be sent. This header field may by ignored by the ASPSP, cp. also the extended service definition in [XS2A-RSNS].
TPP-Notification-Content-Preferred	String	Optional	The string has the form status=X1, ..., Xn where Xi is one of the constants SCA, PROCESS, LAST and where constants are not repeated. The usage of the constants supports the following semantics: SCA: A notification on every change of the scaStatus attribute for all related authorisation processes is preferred by the TPP. PROCESS: A notification on all changes of consentStatus or transactionStatus attributes is preferred by the TPP. LAST: Only a notification on the last consentStatus or transactionStatus as available in the XS2A interface is preferred by the TPP. This header field may be ignored, if the ASPSP does not support resource notification services for the related TPP.
TPP-Brand-Logging-Information	String	Optional	This header might be used by TPPs to inform the ASPSP about the brand used by the TPP towards the PSU. This information is meant for logging entries to enhance communication between ASPSP and PSU or ASPSP and TPP. The ASPSP might ignore this field.

Request body

Attribute	Type	Condition	Description
access	Account Access	Mandatory	Requested access services.
recurringIndicator	Boolean	Mandatory	"true", if the consent is for recurring access to the account data "false", if the consent is for one access to the account data
validUntil	ISODate	Mandatory	This parameter is requesting a valid until date, including this date for the requested consent. The content is the local ASPSP date in ISODate Format, e.g. 2017-10-30. Future dates might get adjusted by ASPSP. If a maximal available date is requested, a date in far future is to be used: "9999-12-31". In both cases, the consent object to be retrieved by the GET Consent Request will contain the adjusted date.
frequencyPerDay	Integer	Mandatory	This field indicates the requested maximum frequency for an access without PSU involvement per day. For a one-off access, this attribute is set to 1." The frequency needs to be greater equal to one. If not otherwise agreed bilaterally between TPP and ASPSP, the frequency is less equal to 4. Remark for Future: Additional conditions might be added later to deal with the situation where the PSU is consenting towards the TPP for account access only where the PSU is actively asking.
combinedService Indicator	Boolean	Mandatory	If "true" indicates that a payment initiation service will be addressed in the same "session", cp. Section 9 Комбиниране на информационни и платежни услуги.

Забележка: Всички позволени атрибути „access“ („accounts“, „balances“ и „transactions“), използвани в това съобщение, не трябва да съдържат празен масив от справки за сметки, а да посочват сметките, за които се изисква вид на достъп. Имайте предвид, че правото за достъп до „transactions“ или „balances“ по подразбиране поддържа и достъпа до списък от "сметки" без те да са посочени.

Атрибутът „additionalInformation“ в „access“ съдържа допълнителни под-атрибути. Атрибутът additionalInformation може да се използва само заедно с един от основните атрибути за „access“, вижте по-горе. Няма изискване за свързаните под-атрибути на „additionalInformation“ да носят и непразни атрибути, където е приложимо. В случай на празен масив в такъв под-атрибут, смисълът е, че ДПУ иска допълнителна информация за всички акаунти, адресирани в поне един от основните атрибути за достъп.

Дори ако ДПУОС не изисква изрично съгласие за допълнителна информация (additionalInformation), напр. името на собственика на акаунта, ДПУОС трябва да игнорира разширението на искането за съгласие на ДПУ, т.е. да не отхвърля свързаната заявка за съгласие. Това важи и в случай, че заявеният достъп не се предлага (напр. име на собственика на акаунта).

Тази спецификация задължава ДПУОС да поддържа всички заявки за съгласие по POST за конкретни сметки, т.е. POST заявки с гореспоменатите под-атрибути, които съдържат

най-малко един допълнителен атрибут, който носи масив с препратки към сметки. За този тип заявка за съгласие се изисква ЗУИ подход.

По желание, ДПУОС може да поддържа и искания за съгласие, където гореспоменатите под-атрибути "сметки", "салда" и "транзакции" съдържат само празен масив или където се използват под-атрибути "availableAccounts", "availableAccountsWithBalance" или "allPsd2" - всички със стойност "allAccounts" или "allAccountsWithOwnerName", описани в Раздел 6.3.1.2.

Response Code

HTTP Response Code equals 201.

Response header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource.
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPS-SCA-Approach	String	Conditional	Possible values are: • EMBEDDED • DECOUPLED • REDIRECT OAuth will be subsumed by the constant value REDIRECT

Response body

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	authentication status of the consent
consentId	String	Conditional	Identification of the consent resource as it is used in the API structure Shall be contained, if a consent resource was generated.
scaMethods	Array of Authentication Objects	Conditional	This data element might be contained, if SCA is required and if the PSU has a choice between different authentication methods. Depending on the risk management of the ASPSP this choice might be offered before or after the PSU has been identified with the first relevant factor, or if an access token is transported. If this data element is contained, then there is also a hyperlink of type "selectAuthenticationMethods" contained in the response body. These methods shall be presented towards the PSU for selection by the TPP.
chosenSca Method	Authentication Object	Conditional	This data element is only contained in the response if the APSPS has chosen the Embedded SCA Approach, if the PSU is already identified with the first relevant factor or alternatively an access token, if SCA is required and if the authentication method is implicitly selected.
challengeData	Challenge	Conditional	It is contained in addition to the data element chosenScaMethod if challenge data is needed for SCA.
			In rare cases this attribute is also used in the context of the updatePsuAuthentication link.

Attribute	Type	Condition	Description
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. Type of links admitted in this response (which might be extended by single ASPSPs as indicated in its XS2A documentation): "scaRedirect": In case of an SCA Redirect Approach, the ASPSP is transmitting the link to which to redirect the PSU browser. "scaOAuth": In case of an OAuth2 based Redirect Approach, the ASPSP is transmitting the link where the configuration of the OAuth2 Server is defined. "startAuthorisation": In case, where an explicit start of the transaction authorisation is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded). "startAuthorisationWithPsuIdentification": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU identification data. "startAuthorisationWithPsuAuthentication": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU authentication data. "startAuthorisationWithEncryptedPsu Authentication": The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the encrypted PSU authentication data. "startAuthorisationWithAuthentication MethodSelection": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while selecting the authentication method. This link is contained under exactly the same conditions as the data element "scaMethods". "startAuthorisationWithTransactionAuthorisation": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while authorising the transaction e.g. by uploading an OTP received by SMS. "self": The link to the Establish Account Information Consent resource created by this request. This link can be used to retrieve the resource data. "status": The link to retrieve the transaction status of the account information consent. "scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource. This link is only contained, if an authorisation sub-resource has been already created.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU, e.g. in a Decoupled SCA Approach

Example

Request

POST <https://api.testbank.com/v1/consents>
Content-Encoding: gzip

Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7756
PSU-IP-Address: 192.168.8.78
PSU-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 06 Aug 2017 15:05:37 GMT
{
 "access":
 {"balances":
 [{"iban": "DE2310010010123456789"}],
 [{"iban": "DE2310010010123456790"},
 "currency": "USD"},
 [{"iban": "DE2310010010123456788"}]},
 "transactions":
 [{"iban": "DE2310010010123456789"},
 {"maskedPan": "123456xxxxxx1234"}]},
 "recurringIndicator": "true",
 "validUntil": "2017-11-01",
 "frequencyPerDay" : 4
 }
}

Response in case of a redirect

HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPS-SCA-Approach: REDIRECT
Location: "v1/consents/1234-werti-983"
Content-Type: application/json
{
 "consentStatus": "received",
 "consentId": "1234-werti-983",
 "_links": {
 "scaRedirect": {"href": "https://www.testbank.com/authentication/1234-werti-983"}
 }
}

Response in case of the OAuth2 approach

HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPS-SCA-Approach: REDIRECT
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v1/consents/1234-werti-983"
Content-Type: application/json
{
 "consentStatus": "received",
 "consentId": "1234-werti-983",
 "_links": {
 "self": {"href": "/v1/consents/1234-werti-983"}
 }
}

Response in case of the Decoupled approach

HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPS-SCA-Approach: DECOUPLED
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v1/consents/1234-werti-983"

Content-Type: application/json

```
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "updatePsuIdentification": {"href": "/v1/consents/1234-wertiq-983"}
  }
}
```

Response in case of the Embedded approach

HTTP/1.x 201 Created

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: EMBEDDED

Date: Sun, 06 Aug 2017 15:05:47 GMT

Location: "v1/consents/1234-wertiq-983"

Content-Type: application/json

```
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "updatePsuAuthentication": {"href": "/v1/consents/1234-wertiq-983"}
  }
}
```

6.3.1.2. *Искане за установяване на съгласие към списък от сметки или без посочена сметка*

Искане за съгласие до списък от наличните сметки

Тази функция се поддържа по същия начин както искането за съгласие към конкретна сметка. Единствената разлика е, че повикването съдържа под-атрибута "налични сметки" в атрибута "достъп" със стойност "всички сметки".

В този случай обаждането създава ресурс за съгласие за информация за сметка в ДПУОС за връщане на списък с всички налични сметки. За този тип заявка за съгласие се изисква ЗУИ подход.

Искане за съгласие без посочване на сметки

Тази функция се поддържа по същия начин както искането за съгласие към конкретна сметка. Единствената разлика е, че повикването съдържа под-атрибут "сметки", "баланси" и / или "транзакции" в атрибута "достъп" с празен масив.

След това ДПУОС се договаря двустранно директно със ДПУ за кои сметки ще бъде се поддържа съгласие за достъп. Резултатът може да бъде извлечен от ДПУ, като се използва методът за заявка за съгласие GET, Раздел 6.4.3. За тази функция подход Embedded ЗУИ не се поддържа.

Искане за съгласие за достъп до всички сметки за всички AIS, определени от PSD2

Тази функция се поддържа по същия начин както искането за съгласие към конкретна сметка. Единствената разлика е, че повикването съдържа под-атрибут "allPsd2" в атрибута "access" със стойността "all-accounts".

Ако тази функция се поддържа, тя ще означава съгласие по всички налични сметки на Ползвателя за всички информационни услуги за сметки, свързани с PSD2. За този тип заявка за съгласие се изисква ЗУИ подход.

Example Consent on Account List of Available Accounts

Request

```
POST https://api.testbank.com/v1/consents
Content-Encoding : gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7756
PSU-IP-Address: 192.168.8.78
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101
Firefox/54.0
Date: Sun, 06 Aug 2017 15:05:37 GMT
```

```
{"access":
  {"availableAccounts": "allAccounts"},
  "recurringIndicator": "false",
  "validUntil": "2017-08-06",
  "frequencyPerDay": 1
}
```

Example Consent without dedicated Account

Request

```
POST https://api.testbank.com/v1/consents
```

Content-Encoding gzip
Content-Type application/json
X-Request-ID 99391c7e-ad88-49ec-a2ad-99ddcb1f7756
PSU-IP-Address 192.168.8.78
PSU-User-Agent Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date Sun, 06 Aug 2017 15:05:37 GMT

```
{"access":  
  {"balances": [],  
   "transactions": []},  
  "recurringIndicator": "true",  
  "validUntil": "2017-11-01",  
  "frequencyPerDay": 4  
}
```

6.3.2. Искане за състояние на заявката (Get Status Request)

Повикване

GET/v1/consents/ {consentId}/status

Използва се за проверка на състоянието на Съгласието за информация за сметка

Path:

Attribute	Type	Description
consentId	String	The consent identification assigned to the created resource.

Query parameters

Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Digest	cp. Section Error! Reference source not found.	Conditional	Is contained if and only if the "Signature" element is contained in the header of the request.
Signature	cp. Section Error! Reference source not found.	Conditional	A signature of the request by the TPP on application level. This might be mandated by ASPSP.
TPP-Signature-Certificate	String	Conditional	The certificate used for signing the request, in base64 encoding. It shall be contained if a signature is used, see above.

Request Body

Няма

Response Header

Attribute	Type	Condition	Description
-----------	------	-----------	-------------

X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
--------------	------	-----------	---

Response Body

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	This is the overall lifecycle status of the consent.
psuMessage	Max500Text	Optional	

Example

Request

```
GET https://api.testbank.com/v1/consents/qwer3456tzui7890/status
Content-Encoding : gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101
Firefox/54.0
Date: Sun, 06 Aug 2017 15:05:46 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{
  "consentStatus": "valid",
}
```

6.3.3. Заявка за съдържание на съгласието (Get Consent Request)

Повикване

```
GET/v1/consents/{consentId}
```

Връща съдържанието на съгласие по информация за сметка. Така се подават данните към ДПУ, когато съгласието е директно управлявано между ДПУОС и Ползвателя, напр. в Redirect ЗУИ подход.

Path:

Attribute	Type	Description
consentId	String	ID of the corresponding consent object as returned by an Account Information Consent Request

Query parameters - Няма

Request header - Както по-горе в 6.4.2.

Request body - Няма

Response header - Както по-горе в 6.4.2.

Response body

Attribute	Type	Condition	Description
Access	Account Access	Mandatory	
recurringIndicator	Boolean	Mandatory	
validUntil	ISODate	Mandatory	
frequencyPerDay	Integer	Mandatory	
lastActionDate	ISODate	Mandatory	This date is containing the date of the last action on the consent object either through the XS2A interface or the PSU/ASPSP interface having an impact on the status.
consentStatus	Consent Statusxxx	Mandatory	The status of the consent resource.
_links	Links	Optional	Type of links recommended for this response is "account" and/or "cardAccount", depending on the nature of the consent.

Example

Request

GET <https://api.testbank.com/v1/consents/qwer3456tzui7890?>

Response

```
HTTP/1.x 200 Ok
X-Request-ID:          99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date:                  Sun, 06 Aug 2017 15:05:47 GMT
Content-Type:          application/json
{
  "access":
    {
      "balances":
        [{"iban": "DE2310010010123456789"}]
      "transactions":
        [{"iban": "DE2310010010123456789"},
          {"pan": "123456xxxxxx3457"}]
    }
  "recurringIndicator": "true",
  "validUntil": "2017-11-01",
  "frequencyPerDay": 4,
  "consentStatus": "valid",
  "_links": {"account": {"href": "/v1/accounts"}}
}
```

Забележка: Тази спецификация не поддържа подробни примери за връзки към всички крайни точки на услугата на Информация за сметка. Ако се посочи като крайна точка „сметка“, ДПУОС може да предостави подробна информация, включително хипервръзките, напр. за салдата или транзакциите по сметката. Също така, ако ДПУОС предоставя още хипервръзки, те следва да бъдат описани в документацията API ДПУОС „Достъп до сметка“.

6.3.4. Множествено ЗУИ при Установяване на съгласие

Съобщенията за установяване на съгласие за информация по сметка, са независими от необходимостта от един или няколко процеса на ЗУИ, т.е. независимо от броя на авторизациите, необходими за установяване на съгласието. Обратно, съобщенията за отговор при установяване на съгласието за информация по сметка, дефинирани по-горе в този раздел, са специфична за обработката в едно ЗУИ. По-долу се обяснени различни изисквания при отговора на установяване на съгласие за информация.

За да се установи съгласието за информация по сметка с множествоно ЗУИ, по тази спецификация изисква изрично (explicit) стартиране на авторизацията, т.е. връзките, пряко свързани с обработката на ЗУИ като "scaRedirect" или "scaOAuth", не могат да се съдържат в съобщението за отговор на заявка за установяване на съгласие за информация за сметка, когато са необходими няколко разрешения. Също така, ако са необходими данни за следващото действие, всички стартирания на множеството разрешения са напълно равни. В тези случаи най-напред трябва да се генерира под-ресурс за авторизация чрез link "startAuthorisation".

Response Body for Establish Account Information Messages with Multilevel SCA

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	The values defined in Section 14.14 might be used.
consentId	String	Mandatory	Resource identification of the generated initiated resource.
_links	Links	Mandatory	"startAuthorisation": In case, where an explicit start of the transaction authorisation is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded). "startAuthorisationWithPsuIdentification": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU identification data. "startAuthorisationWithPsuAuthentication": The link to the authorisation end-point, where an authorisation sub-resource has to be generated while uploading the PSU authentication data. "self": The link to the consent resource created by this request. This link can be used to retrieve the resource data. "status": The link to retrieve the status of the consent.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU
tppMessage	Array of TPP Message Information	Optional	Messages to the TPP on operational issues.

Забележка: Процесите с имплицитно генериране на под-ресурси за авторизация не поддържат от множествона ЗУИ. В тези случаи единствените хипервръзки, които се връщат на ДПУ след започване на установяването на съгласие, е хипервръзка за "startAuthorisation", като в допълнение има информация за задължителните данни, които да бъдат качени със заявката за стартиране на авторизацията (PSU Identification или PSU Authentication data)).

6.4. Изтриване на Съгласие за Информация за сметка (Delete an Account Information Consent Object)

TPP може да изтрие обекта „Съгласие за информация за сметка“, при необходимост, чрез следното повикване:

Повикване

DELETE /v1/consents/{consentId}

Изтрива Съгласието с подаден идентификатор

Path:

Attribute	Type	Description
consentId	String	Contains the resource-ID of the consent to be deleted.

Query parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based SCA was performed in the corresponding consent transaction or if OAuth2 has been used in a pre-step.

Request body - Няма

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body - Няма

Example

Request

DELETE https://api.testbank.com/v1/consents/qwer3456tzui7890
Content-Encoding gzip
Content-Type application/json
X-Request-ID 99391c7e-ad88-49ec-a2ad-99ddcb1f7757
Date Sun, 13 Aug 2017 17:05:37 GMT

Response

HTTP/1.x 204 No Content
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757
Date: Sun, 06 Aug 2017 15:05:47 GMT

6.5. Предоставяне на „Данни за сметка“ (Read Account Data Requests)

6.5.1. Предоставяне на списък от сметки (Read Account List)

Повикване

GET /v1/accounts/{query-parameters}

Предоставя списък от сметки, (при поискване заедно с баланса по тях). Предполага се, че съгласието на Ползвателя за този достъп вече е дадено и се съхранява в системата на ДПУОС. Посоченият списък от сметки се филтрира чрез идентификационен номер на Ползвателя и на съхраненото съгласие, адресирано в consentId, или в съответния достъп на OAuth2 токън.

Забележка: Ако съгласието се дава само за показване на списъка с наличните сметки (права за достъп "налични сметки", раздел 6.3.1.2), тогава се показват много по-малко подробности. По-конкретно, хипервръзките към салдата или крайната точка на транзакциите не трябва да се доставят.

Забележка: Ако детайлите, предоставени с това повикване не са достатъчни, или правата за достъп "сметки", "салда", "транзакции" или "allPsd2" не са достатъчни, тогава може да се изтеглят повече подробности чрез адресиране на крайната точка /accounts/{account-id}, ср. Раздел 6.6.2. (Детайли за сметка)

Query parameters

Attribute	Type	Condition	Description
withBalance	Boolean	Optional	If contained, this function reads the list of accessible payment accounts including the booking balance, if granted by the PSU in the related consent and available by the ASPSP. This parameter might be ignored by the ASPSP.

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Shall be contained since "Establish Consent Transaction" was performed via this API before.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."

Request body

Няма

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
accounts	Array of Account Details	Mandatory	

Example

Отговор в случай на дадено съгласие за два различни IBAN-а с различен достъп (първият с баланс и транзакции, вторият само с баланс)

Response

```
{
  "accounts": [
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
      "iban": "DE2310010010123456789",
      "currency": "EUR",
      "product": "Girokonto",
      "cashAccountType": "CACC",
      "name": "Main Account",
      "_links": {
        "balances": {
          "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances"
        },
        "transactions": {
          "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/transactions"
        }
      }
    },
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e81g",
      "iban": "DE2310010010123456788",
      "currency": "USD",
      "product": "Fremdwährungskonto",
      "cashAccountType": "CACC",
      "name": "US Dollar Account",
      "_links": {
        "balances": {
          "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/balances"
        }
      }
    }
  ]
}
```

Отговор в случай на дадено съгласие за транзакции и салда в много-валутна сметка, която има две под-сметки с валута EUR и USD и където ДПУОС дава достъп до данните само на ниво под-сметка:

Response

```
{
  "accounts": [
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
      "iban": "DE2310010010123456788",
      "currency": "EUR",
      "product": "Girokonto",
      "cashAccountType": "CACC",
      "name": "Main Account",
      "_links": {
        "balances": {
          "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances"
        },
        "transactions": {
          "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/transactions"
        }
      }
    },
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e81g",
      "iban": "DE2310010010123456788",
      "currency": "USD",
      "product": "Fremdwährungskonto",
      "cashAccountType": "CACC",
      "name": "US Dollar Account",
      "_links": {
        "balances": {
          "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/balances"
        }
      }
    }
  ]
}
```

```

        "transactions": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/transactions"}}
    }
}

```

Отговор в случай на дадено съгласие за салда и транзакции в много-валутна сметка, която има две под-сметки с валута EUR и USD и където ДПУОС предоставя достъп до данни на ниво агрегация и на ниво под-сметка.

Response

```

{"accounts":
  [
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
      "iban": "DE2310010010123456788",
      "currency": "XXX",
      "product": "Multi currency account",
      "cashAccountType": "CACC",
      "name": "Aggregation Account",
      "_links": {
        "balances": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e333/balances"},
        "transactions": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e333/transactions"}}
    },
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
      "iban": "DE2310010010123456788",
      "currency": "EUR",
      "product": "Girokonto",
      "cashAccountType": "CACC",
      "name": "Main Account",
      "_links": {
        "balances": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances"},
        "transactions": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/transactions"}}
    },
    {
      "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e81g",
      "iban": "DE2310010010123456788",
      "currency": "USD",
      "product": "Fremdwährungskonto",
      "cashAccountType": "CACC",
      "name": "US Dollar Account",
      "_links": {
        "balances": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/balances"},
        "transactions": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/transactions"}}
    }
  ]
}

```

6.5.2. Предоставяне на детайли за сметка (Read Account Details)

Повикване

GET /v1/accounts/{account-id} {query-parameters}

Предоставя детайли за конкретна сметка (с баланс, когато е поискано). Предполага се, че съгласието на Ползвателя с този достъп вече е дадено и се съхранява в системата ДПУОС. Посочените детайли за тази сметка зависят от параметрите на съхраняваното съгласие, адресирано от consentId, или съответното обозначение за достъп OAuth2.

Забележка: Идентификаторът на сметката може да представлява много-валутна сметка. В този случай кода за валута е посочен като "XXX".

Query parameters

Attribute	Type	Condition	Description
withBalance	Boolean	Optional	If contained, this function reads the details of the addressed account including the booking balance, if granted by the PSU's consent and if supported by ASPSP. This data element might be ignored by the ASPSP.

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.

Request Body

Няма

Response Code

HTTP Response Code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
account	Account Details	Mandatory	

Example

Отговор в случай на дадено съгласие за стандартна сметка

Response

```
{ "account":  
  { "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",  
    "iban": "FR7612345987650123456789014",  
    "currency": "EUR",  
    "ownerName": "Heike Mustermann",  
    "product": "Girokonto",  
    "cashAccountType": "CACC",  
    "name": "Main Account",  
    "_links": {  
      "balances": { "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances" },  
      "transactions": { "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/transactions" }  
    }  
  }  
}
```

Отговор в случай на дадено съгласие за много-валутна сметка

Response

```
{ "account":  
  { "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",  
    "iban": "FR7612345987650123456789014",  
    "currency": "XXX",  
    "ownerName": "Heike Mustermann",  
    "product": "Multicurrency Account",  
    "cashAccountType": "CACC",  
    "name": "Aggregation Account",  
    "_links": {  
      "balances": { "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances" },  
      "transactions": { "href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/transactions" }  
    }  
  }  
}
```

6.5.3. Предоставяне на баланс на сметка (Read Balance)

Повикване

GET /v1/accounts/{account-id}/balances

Предоставя детайли за конкретна сметка с баланс. Сметката е адресирана с accountId.

Забележка: Стойността accountId (идентификационен номер на сметка) може да се извлече след повикването за "Предоставяне на Списък на сметките", Раздел 6.6.1.

Идентификаторът accountId е валиден за целия жизнен цикъл на дадено съгласие.

Path parameters

Attribute	Type	Description
account-id	String	This identification is denoting the addressed account. The account-id is retrieved by using a "Read Account List" call. The account-id is the

		"resourceId" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent.
--	--	--

Query parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.

Request body - Няма

Response Code

HTTP Response Code equals 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
account	Account Reference	optional	Identifier of the addressed account. Remark for Future: It is recommended to use this data element. The condition might change to "mandatory" in a next version of the specification.
balances	Array of Balance	Mandatory	A list of balances regarding this account, e.g. the current balance, the last booked balance.

Example

Отговор в случай на съгласие за стандартна сметка

Response

```
{
  "account": {"iban": "FR7612345987650123456789014"},
  "balances":
    [{"balanceType": "closingBooked",
      "balanceAmount": {"currency": "EUR", "amount": "500.00"},
      "referenceDate": "2017-10-25"
    },
    {"balanceType": "expected",
      "balanceAmount": {"currency": "EUR", "amount": "900.00"},
    }
  ]
}
```

```

    "lastChangeDateTime": "2017-10-25T15:30:35.035Z"
  }]
}

```

Отговор в случай на много-валутна сметка с една под-сметка в EUR и една в USD, където ДПУОС е доставя link към крайната точка (салдото) по отношение на обобщената много-валутна сметка.

Response

```

{
  "balances":
    [{ "balanceType": "closingBooked",
      "balanceAmount": { "currency": "EUR", "amount": "500.00" },
      "referenceDate": "2017-10-25"
    },
    { "balanceType": "expected",
      "balanceAmount": { "currency": "EUR", "amount": "900.00" },
      "lastChangeDateTime": "2017-10-25T15:30:35.035Z"
    },
    { "balanceType": "closingBooked",
      "balanceAmount": { "currency": "USD", "amount": "350.00" },
      "referenceDate": "2017-10-25"
    },
    { "balanceType": "expected",
      "balanceAmount": { "currency": "USD", "amount": "350.00" },
      "lastChangeDateTime": "2017-10-24T14:30:21Z"
    }
  ]
}

```

Отговор в случай на стандартна сметка, при която съответните салда показват текущото салдо за текущото време:

Response

```

{
  "balances": [
    {
      "balanceType": "interimBooked",
      "balanceAmount": { "currency": "EUR", "amount": "1000.00" }
    },
    {
      "balanceType": "interimAvailable",
      "balanceAmount": { "currency": "EUR", "amount": "300.00" }
    },
    {
      "balanceType": "interimAvailable",
      "creditLimitIncluded": true,
      "balanceAmount": { "currency": "EUR", "amount": "5300.00" }
    }
  ]
}

```

6.5.4. Предоставяне на списък на транзакции от сметка (Read Transaction List)

Повикване

GET /v1/accounts/{account-id}/ transactions{query-parameters}

Предоставя списък на транзакциите по конкретна сметка, съгласно критерий посочен като параметър. Сметката е адресирана с accountId.

Забележка: Стойността accountId (идентификационен номер на сметка) може да се извлече след повикването за "Предоставяне на Списък от сметки", Раздел 6.6.1.

Забележка: Моля, имайте предвид, че PATH може да е вече предоставен в отговора на повикването "Предоставяне на Списък от сметки" в под-атрибут "_links".

Забележка: В случай на използване на странициране, повикването на връзка за страница следва същите изисквания, както при това повикване, като към PATH се добавя и параметър за страница.

Path

Attribute	Type	Description
account-id	String	This identification is denoting the addressed account. The account-id is retrieved by using a "Read Account List" call. The account-id is the "id" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent.

Query parameters

Attribute	Type	Condition	Description
dateFrom	ISODate	Conditional	Starting date (inclusive the date dateFrom) of the transaction list, mandated if no delta access is required. For booked transactions, the relevant date is the booking date. For pending transactions, the relevant date is the entry date, which may not be transparent neither in this API nor other channels of the ASPSP.
dateTo	ISODate	Optional	End date (inclusive the data dateTo) of the transaction list, default is „now“ if not given. For booked transactions, the relevant date is the booking date. For pending transactions, the relevant date is the entry date, which may not be transparent neither in this API nor other channels of the ASPSP.
entryReferenceFrom	String	Optional if supported by API provider	This data attribute is indicating that the AISP is in favour to get all transactions after the transaction with identification entryReferenceFrom alternatively to the above defined period. This is a implementation of a delta access. If this data element is contained, the entries "dateFrom" and "dateTo" might be ignored by the ASPSP if a delta report is supported.
bookingStatus	String	Mandatory	Permitted codes are "booked", "pending", "both", "information" and "all". "booked" shall be supported by the ASPSP. "booked" shall be supported by the ASPSP. To support the "pending" and "both" feature is optional for the ASPSP, Error code if not supported in the online banking frontend. If supported, "both" means to request transaction reports of transaction of bookingStatus either "pending" or "booked".

Attribute	Type	Condition	Description
			To support the "information" feature is optional for the ASPSP. Currently the booking status "information" only covers standing orders. Error code if not supported. To support the "all" feature is optional for the ASPSP, Error code if not supported. If supported, "all" means to request transaction reports of transaction of any bookingStatus ("pending", "booked" or "information").
deltaList	Boolean	Optional if supported by API provider	This data attribute is indicating that the AISP is in favour to get all transactions after the last report access for this PSU on the addressed account. This is another implementation of a delta access-report. This delta indicator might be rejected by the ASPSP if this function is not supported. If this data element is contained, the entries "dateFrom" and "dateTo" might be ignored by the ASPSP if a delta report is supported.
withBalance	Boolean	Optional	If contained, this function reads the list of transactions including the booking balance, if granted by the PSU in the related consent and available by the ASPSP. This parameter might be ignored by the ASPSP.

Забележка: В случай на bookingStatus е равно на "information", параметрите на заявката dateFrom, dateTo, withBalance, deltaList и entryReferenceFrom ще бъдат игнорирани и няма да имат ефект върху резултата.

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."

Attribute	Type	Condition	Description
Accept	String	Optional	The TPP can indicate the formats of account reports supported together with a prioritisation following the HTTP header definition. The formats supported by this specification are • xml • JSON • text Remark: in the next version of the specification. This shall enable the TPP to address different camt.05x versions or different MT94x versions in a corporate context. The TPP then could e.g. say: "I prefer MT942, but take MT940 if MT942 is not available."

Забележка: Берлинската група възнамерява да внедри записи в атрибута "асепт" за формати camt.05x и MT94x. Тези стойности ще бъдат добавени към тази спецификация възможно най-скоро.

Request Body

Няма

Response code

HTTP Response Code equals 200.

Response header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	Possible values are: • application/json • application/xml • plain/text
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

В случай, че ДПУОС връща структурата на camt.05x XML, отговорът се състои или от съобщение тип camt.052 или camt.053. Camt.052 може да включва чакащи плащания, които все още не са осчетоводени. ДПУОС ще взема своето решение за това, кое съобщение и формат да приложи, въз основа на избраните параметри и по-специално от избраните дати по отношение на периода на заявката.

В случай, че ДПУОС връща MT94x съдържание, отговорът се състои от съобщение във формат MT940 или MT942 в текстова структура. MT942 може да включва предстоящи плащания, които все още не са осчетоводени. ДПУОС ще вземе решение за формата въз основа на избраните параметри, по-специално за избраните дати в периода на заявката.

Отговорът JSON формат е определен, както следва:

Attribute	Type	Condition	Description
account	Account Reference	optional	Identifier of the addressed account. Remark for Future: It is recommended to use this data element. The condition might change to "mandatory" in a next version of the specification.
transactions	Account Report	Optional	JSON based account report. This account report contains transactions resulting from the query parameters.
balances	Array of Balance	Optional	A list of balances regarding this account, which might be restricted to the current balance.
_links	Links	Optional	A list of hyperlinks to be recognised by the TPP. Type of links admitted in this response: "download": a link to a resource, where the transaction report might be downloaded from in case where transaction reports have a huge size. Remark: This feature shall only be used where camt-data is requested which has a huge size.

Example

Request

GET https://api.testbank.com/v1/accounts/qwer3456tzui7890/transactions?dateFrom=2017-07-01&dateTo=2017-07-30&bookingStatus=both

Accept: application/json, plain/text;q=0.9, application/xml;q=0.8

Response - Отговор в JSON формат при съгласие за стандартна сметка

HTTP/1.x 200 Ok

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757

Date: Sun, 06 Aug 2017 15:05:47 GMT

Content-Type: application/json

```
{
  "account": {
    "iban": "DE2310010010123456788"
  },
  "transactions": {
    "booked": [
      {
        "transactionId": "1234567",
        "creditorName": "John Miles",
        "creditorAccount": {
          "iban": "DE67100100101306118605"
        },
        "transactionAmount": {
          "currency": "EUR",
          "amount": "256.67"
        },
        "bookingDate": "2017-10-25",
        "valueDate": "2017-10-26",
        "remittanceInformationUnstructured": "Example 1"
      },
      {
        "transactionId": "1234568",
        "debtorName": "Paul Simpson",
        "debtorAccount": {
          "iban": "NL76RABO0359400371"
        },
        "transactionAmount": {
          "currency": "EUR",
          "amount": "343.01"
        },
        "bookingDate": "2017-10-25",
        "valueDate": "2017-10-26",
        "remittanceInformationUnstructured": "Example 2"
      }
    ],
    "pending": [
      {
        "transactionId": "1234569",
        "creditorName": "Claude Renault",
        "creditorAccount": {
          "iban": "FR7612345987650123456789014"
        },

```

```

        "transactionAmount": {"currency": "EUR", "amount": "-100.03"},
        "valueDate": "2017-10-26",
        "remittanceInformationUnstructured": "Example 3"
    }
  ],
  {
    "_links": {
      "account": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f"}
    }
  }
}

```

Response - Отговор в случай на много голям обем данни за изтегляне

HTTP/1.x 204 No Content

X-Request-ID:99391c7e-ad88-49ec-a2ad-99ddcb1f7757

Date: Sun, 06 Aug 2017 15:05:47 GMT

```

{
  "_links":{"download":{"href":"www.test-api.com/xs2a/v1/accounts/1234567890/transactions/download/"}
}
}

```

Response - Отговор в JSON формат за достъп до много-валутна сметка на ниво агрегиране:

HTTP/1.x 204 No Content

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757

Date: Sun, 06 Aug 2017 15:05:47 GMT

```

{"account": {"iban": "DE40100100103307118608"},
 "transactions":
  {"booked":
    [{
      "transactionId": "1234567",
      "creditorName": "John Miles",
      "creditorAccount": {"iban": "DE67100100101306118605"},
      "transactionAmount": {"currency": "EUR", "amount": "-256.67"},
      "bookingDate": "2017-10-25",
      "valueDate": "2017-10-26",
      "remittanceInformationUnstructured": "Example 1"
    },{
      "transactionId": "1234568",
      "debtorName": "Paul Simpson",
      "debtorAccount": {"iban": "NL76RABO0359400371"},
      "transactionAmount": {"currency": "EUR", "amount": "343.01"},
      "bookingDate": "2017-10-25",
      "valueDate": "2017-10-26",
      "remittanceInformationUnstructured": "Example 2"
    },{
      "transactionId": "1234569",
      "debtorName": "Pepe Martin",
      "debtorAccount": {"iban": "SE9412309876543211234567"},
      "transactionAmount": {"currency": "USD", "amount": "100"},
      "bookingDate": "2017-10-25",
      "valueDate": "2017-10-26",
      "remittanceInformationUnstructured": "Example 3"
    }
  ],
  {"pending":
    [{
      "transactionId": "1234570",
      "creditorName": "Claude Renault",
      "creditorAccount": {"iban": "FR7612345987650123456789014"},
      "transactionAmount": {"currency": "EUR", "amount": "-100.03"},
      "valueDate": "2017-10-26",
      "remittanceInformationUnstructured": "Example 4"
    }
  ]
}
}

```

```
{ "_links":  
  {"account": {"href": "/v1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f"}}  
}
```

6.5.5. Предоставяне на детайли по транзакции от сметки (Read Transaction Details)

Повикване

GET /v1/accounts/{account-id}/transactions/{transactionId}

Чете данните за конкретна транзакция, адресирана чрез "transactionId" в дадена сметка, адресирана от "account-id". Това повикване изисква отговора за детайлите по транзакция да е само в JSON формат.

Забележка: Моля, обърнете внимание, че PATH може да е вече подробно представен от съответното вписване на отговора на повикването "Прочетете списъка с транзакции" в под-поле _links.

Path Parameters

Attribute	Type	Description
account-id	String	This identification is denoting the addressed account, where the transaction has been performed.
transactionId	String	This identification is given by the attribute resourceId of the corresponding entry of a transaction list.

Query Parameters

No Query Parameters

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.

Request Body

No request body.

Response Code

HTTP Response Code equals 200.

Response Header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	Possible values are: application/json

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
transactionsDetails	Transactions	Optional	

Example Request

GET <https://api.testbank.com/v1/accounts/qwer3456tzui7890/transactions/{1234567}/details>

Response

HTTP/1.x 200 Ok

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757

Date: Sun, 06 Aug 2017 15:05:47 GMT

Content-Type: application/json

```
{
  "transactionsDetails": {
    "transactionId": "1234567",
    "creditorName": "John Miles",
    "creditorAccount": {"iban": "DE67100100101306118605"},
    "mandateId": "Mandate-2018-04-20-1234",
    "transactionAmount": {"currency": "EUR", "amount": "-256.67"},
    "bookingDate": "2017-10-25",
    "valueDate": "2017-10-26",
    "remittanceInformationUnstructured": "Example 1"
    "bankTransactionCode": "PMNT-RDDT-ESDD",
  }
}
```

Забележка: В този пример, типична допълнителна подробност за дадена транзакция са детайлите за SEPA mandate в получено плащане по SEPA Direct Debit.

6.6. Предоставяне на „Данни за картова сметка“ (Read Card Account Data Requests)

6.6.1. Предоставяне на списък от картови сметки (Read Card Account List)

Повикване

GET /v1/card-accounts

Предоставя списък от картови сметки с допълнителна информация (напр. заедно с баланса по тях). Предполага се, че съгласието на Ползвателя за този достъп вече е дадено и се съхранява в системата на ДПУОС. Посоченият списък от картови сметки се филтрира чрез идентификационен номер на Ползвателя и на съхраненото съгласие, адресирано в consentId, или в съответния достъп на OAuth2 токън.

Query parameters

Не се поддържат

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Identification of the corresponding consent as granted by the PSU.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."

Request header

Няма

Response Code

HTTP Response Code equals 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
cardAccounts	Array of Card Account Details	Mandatory	

Example

Response body

```
{
  "cardAccounts": [
    {
      "resourceId": "3d9a81b3-a47d-4130-8765-a9c0ff861b99",
      "maskedPan": "525412*****3241",
      "currency": "EUR",
      "name": "Main",
      "product": "Basic Credit",
      "status": "enabled",
      "creditLimit": { "currency": "EUR", "amount": "15000"},
      "balances": [
        {
          "balanceType": "interimBooked",
          "balanceAmount": { "currency": "EUR", "amount": "14355.78"}
        }, {
          "balanceType": "nonInvoiced",
          "balanceAmount": { "currency": "EUR", "amount": "4175.86"}
        }
      ],
      "_links": {
        "transactions": { "href": "/v1/card-accounts/3d9a81b3-a47d-4130-8765-a9c0ff861b99/transactions"}
      }
    }
  ]
}
```

6.6.2. Предоставяне на детайли за картова сметка (Read Card Account Details)

Повикване

GET /v1/card-accounts/{account-id}

Предоставя детайли за конкретна картова сметка. Предполага се, че съгласието на Ползвателя с този достъп вече е дадено и се съхранява в системата ДПУОС. Достъпът до детайли за сметка се указва чрез идентификационен номер на Ползвателя и на съхраненото съгласие, адресирано в consentId, или в съответния достъп на OAuth2 токън

Query parameters

Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Identification of the access consent as granted by the PSU.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.

Attribute	Type	Condition	Description
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."

Request Body

Няма

Response Code

HTTP Response Code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
cardAccount	Card Account Details	Mandatory	

Example

Response

```
{
  "cardAccount": {
    "resourceId": "3d9a81b3-a47d-4130-8765-a9c0ff861b99",
    "maskedPan": "525412*****3241",
    "currency": "EUR",
    "debitAccounting": true,
    "name": "Main",
    "product": "Basic Credit",
    "status": "enabled",
    "creditLimit": { "currency": "EUR", "amount": "15000"},
    "balances": [
      {
        "balanceType": "interimBooked",
        "balanceAmount": { "currency": "EUR", "amount": "14355.78"}
      }, {
        "balanceType": "nonInvoiced",
        "balanceAmount": { "currency": "EUR", "amount": "4175.86"}
      }
    ],
    "_links": {
      "transactions": { "href": "/v1/card-accounts/3d9a81b3-a47d-4130-8765-a9c0ff861b99/transactions" }
    }
  }
}
```

6.6.3. Предоставяне на баланс по картова сметка (Read Card Account Balance)

Повикване

GET /v1/card-accounts/{account-id}/balances

Предоставя детайли за конкретна картова сметка с баланс. Сметката е адресирана с accountId.

Забележка: Стойността accountId (идентификационен номер на сметка) може да се извлече след повикването за "Предоставяне на Списък на картови сметки", Раздел 6.7.1.

Идентификаторът accountId е валиден за целия жизнен цикъл на дадено съгласие.

Path parameters

Attribute	Type	Description
account-id	String	This identification is denoting the addressed card account. The account-id is retrieved by using a "Read Account List" call. The account-id is the "resourceId" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent.

Query parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Identification of the corresponding consent as granted by the PSU.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."

Request body - Няма

Response Code

HTTP Response Code equals 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
cardAccount	Account Reference	optional	Identifier of the addressed account. Remark for Future: It is recommended to use this data element. The condition might change to "mandatory" in a next version of the specification.
debitAccounting	Boolean	Optional	If true, the amounts of debits on the reports are quoted positive with the related consequence for balances. If false, the amount of debits on the reports are quoted negative.
balances	Array of Balance	Mandatory	A list of balances regarding this card account, e.g. the current balance, the last booked balance.

Example

Response

```
{
  "cardAccount": {"maskedPan": "525412*****3241"},
  "debitAccounting": true,
  "balances": [
    {
      "balanceType": "interimBooked",
      "balanceAmount": { "currency": "EUR", "amount": "14355.78" }
    }, {
      "balanceType": "nonInvoiced",
      "balanceAmount": { "currency": "EUR", "amount": "4175.86" }
    } ]
}
```

6.6.4. Предоставяне на списък от транзакции по картова сметка (Read Card Account Transaction List)

Повикване

GET /v1/card-accounts/{account-id}/transactions{query-parameters}

Предоставя списък на транзакциите по конкретна картова сметка, съгласно критерий посочен като параметър. Сметката е адресирана с accountId.

Забележка: Стойността accountId (идентификационен номер на сметка) може да се извлече след повикването за "Предоставяне на Списък от картови сметки", Раздел 6.7.1.

Забележка: Моля, имайте предвид, че PATH може да е вече предоставен в отговора на повикването "Предоставяне на Списък от картови сметки" в под-атрибут "_links".

Path

Attribute	Type	Description
account-id	String	This identification is denoting the addressed card account. The account-id is retrieved by using a "Read Card Account List" call. The account-id is the "id" attribute of the account structure. Its value is constant at least throughout the lifecycle of a given consent..

Query parameters

Attribute	Type	Condition	Description
dateFrom	ISODate	Conditional	Starting date (inclusive the date dateFrom) of the transaction list, mandated if no delta access is required
dateTo	ISODate	Optional	End date (inclusive the data dateTo) of the transaction list, default is „now“ if not given.
bookingStatus	String	Mandatory	Permitted codes are "booked", "pending", "both" and "information" "booked" shall be supported by the ASPSP. To support the "pending" and "both" feature is optional for the ASPSP, Error code if not supported in the online banking frontend. To support the "information" feature is optional for the ASPSP. Currently the booking status “information” only covers standing orders. Error code if not supported.
deltaList	Boolean	Optional if supported by API provider	This data attribute is indicating that the AISP is in favour to get all transactions after the last report access for this PSU on the addressed account. This is another implementation of a delta access-report. This delta indicator might be rejected by the ASPSP if this function is not supported. If this data element is contained, the entries "dateFrom" and "dateTo" might be ignored by the ASPSP if a delta report is supported.

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	String	Mandatory	Identification of the consent for this access as granted by the PSU.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the related consent authorisation.
PSU-IP-Address	String	Conditional	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."

Забележка: Берлинската група възнамерява да внедри записи в атрибута "асерт" за формати samt.05x и MT94x. Тези стойности ще бъдат добавени към тази спецификация възможно най-скоро.

Request Body

Няма

Response code

HTTP Response Code equals 200.

Response header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	Possible values are: • application/json • application/xml • plain/text
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
cardAccount	Account Reference	optional	Identifier of the addressed card account. Remark for Future: It is recommended to use this data element. The condition might change to "mandatory" in a next version of the specification.
debitAccounting	Boolean	Optional	If true, the amounts of debits on the reports are quoted positive with the related consequence for balances. If false, the amount of debits on the reports are quoted negative.
cardTransactions	Card Account Report	Optional	JSON based account report.
balances	Array of Balance	Optional	A list of balances regarding this account, which might be restricted to the current balance.
_links	Links	Optional	A list of hyperlinks to be recognised by the TPP. Type of links admitted in this response: "download": a link to a resource, where the transaction report might be downloaded from in case where transaction reports have a huge size.

Example

Request

GET <https://api.testbank.com/v1/card-accounts/3d9a81b3-a47d-4130-8765-a9c0ff861b99/transactions?dateFrom=2017-10-01&dateTo=2017-10-30>
Accept: application/json, plain/text;q=0.9, application/xml;q=0.8
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Response - Отговор в JSON формат при съгласие за стандартна сметка

HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{
 "cardAccount": {
 "maskedPan": "525412*****3241"

```

},
"debitAccounting": true,
"cardTransactions": {
  "booked": [
    {
      "cardTransactionId": "201710020036959",
      "transactionAmount": { "currency": "EUR", "amount": "256.67" },
      "transactionDate": "2017-10-25",
      "bookingDate": "2017-10-26",
      "originalAmount": { "currency": "SEK", "amount": "2499" },
      "cardAcceptorAddress": {
        "city" : "STOCKHOLM",
        "country" : "SE"
      },
      "maskedPan": "525412*****3241",
      "proprietaryBankTransactionCode" : "PURCHASE",
      "invoiced": false,
      "transactionDetails": "WIFIMARKET.SE"
    }, {
      "cardTransactionId": "201710020091863",
      "transactionAmount": { "currency": "EUR", "amount": "10.72" },
      "transactionDate": "2017-10-25",
      "bookingDate": "2017-10-26",
      "originalAmount": { "currency": "SEK", "amount": "99" },
      "cardAcceptorAddress": {
        "city" : "STOCKHOLM",
        "country" : "SE"
      },
      "maskedPan": "525412*****8999",
      "proprietaryBankTransactionCode" : "PURCHASE",
      "invoiced": false,
      "transactionDetails": "ICA SUPERMARKET SKOGHA"
    }
  ],
  "pending": [ ],
  "_links": {
    "cardAccount": { "href": "/v1/card-accounts/3d9a81b3-a47d-4130-8765-a9c0ff861b99" }
  }
}
}

```

7. Общи процеси при използване на AIS и PIS услуги

Тази секция предоставя информация за процесите с които Ползвателя на услуги от интерфейса Достъп до сметка предоставя своята идентичност и начините с които потвърждава своето съгласие за изпълнение на превод или достъп до информация пред ДПУОС чрез API на ДПУ.

Процесите по

- Стартиране на авторизация
- Идентификацията на Ползвателя
- Потвърждение на данните на Ползвателя
- Изрична авторизацията на транзакциите чрез използване на ЗУИ

са много сходни в услугите PIS и AIS. По-надолу са описани API повикванията, за прилагане на тези процеси, независимо от услугата / крайната точка.

За повече яснота, крайните точки винаги посочват конкретна услуга:

- Инициране на плащане,
- Отмяна на плащане
- Подпис на кошница
- Информация за сметка.

Тези процеси обикновено се използват след хипервръзка доставена от ДПУОС. Структурата на всички параметри в "header / body" на Искането и "header / body" на Отговора са еднакви. По-надолу се дефинира начина на използване на процесите.

7.1. Стартиране на процеси по авторизация на заявка

Процесът Старт на авторизация се използва при създаване на нов под-ресурс или за анулиране на такъв. Той се прилага в следните сценарии:

- ДПУОС е посочила с хипервръзка "startAuthorisation" в предхождащия отговор за инициране на плащането, че ДПУ изрично стартира процеса на упълномощаване. Връзката "startAuthorisation" пренася допълнителна информация за данните, които трябва да бъдат качени, когато се използват формите:

- "startAuthorisationWithPseudIdentification",
- "startAuthorisationWithPseudAuthentication",
- "startAuthorisationWithEncryptedPseudAuthentication",
- "startAuthorisationWithAuthenticationMethodSelection"

- ДПУОС е посочил с хипервръзка "startAuthorisation" в предупредителния отговор за отмяна на плащането, че ДПУ изрично стартира процеса на упълномощаване. Връзката "startAuthorisation" пренася допълнителна информация за данните, които трябва да бъдат качени, когато се използват формите посочени по-горе.

- Когато се изисква множествена авторизация за изпълнение на съответното иницирано плащането

- Когато за съответното искане за анулиране на плащане се изисква множествена ЗУИ авторизация

- При авторизация на кошница от плащания

Повикване в контекста на Искане за инициране на плащане

POST /v1/{payment-service}/{payment-product}/{paymentId}/authorisations

Повикване в контекста на Искане за отмяна на плащане

POST /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations

Повикване в контекста на искане за съгласие за информация по сметка

POST /v1/consents/{consentId}/authorisations

Повикване в контекста на авторизация и подписване на кошницата

POST /v1/signing-baskets/{basketId}/authorisations

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
PSU-ID	String	Optional	Client ID of the PSU in the ASPSP client interface. Shall be transmitted if this Request is indicated by "startAuthorisationWithPsuIdentification" or "startAuthorisationWithPsuAuthentication" or "startAuthorisationWithEncryptedPsuAuthentication" and this field has not yet been transmitted before.
PSU-ID-Type	String	Optional	Type of the PSU-ID, needed in scenarios where PSUs have several PSU-IDs as access possibility. Shall be transmitted if this Request is indicated by "startAuthorisationWithPsuIdentification" or "startAuthorisationWithPsuAuthentication" or "startAuthorisationWithEncryptedPsuAuthentication" and this field has not yet been transmitted before.
PSU-Corporate-ID	String	Optional	Identification of a Corporate in the Online Channels. Shall be transmitted if this Request is indicated by "startAuthorisationWithPsuIdentification" or "startAuthorisationWithPsuAuthentication" or "startAuthorisationWithEncryptedPsuAuthentication" and this field has not yet been transmitted before and only where generally needed in a corporate context.

Attribute	Type	Condition	Description
PSU-Corporate-ID-Type	String	Optional	This is describing the type of the identification needed by the ASPSP to identify the PSU-Corporate-ID content. Shall be transmitted if this Request is indicated by "startAuthorisationWithPsuIdentification" or "startAuthorisationWithPsuAuthentication" or "startAuthorisationWithEncryptedPsuAuthentication" and this field has not yet been transmitted before. Mean and use is defined in the ASPSP's documentation. Only used in a corporate context.
Authorization	String	Conditional	Bearer Token. Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in an preceding AIS service in the same session.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandated for the Redirect SCA Approach, specifically when TPP-Redirect-Preferred equals "true". If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Decoupled-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a decoupled SCA approach. If it equals "false", the TPP prefers not to use the decoupled approach for SCA. The ASPSP will then choose between the embedded or the redirect SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the parameter TPP-Redirect-Preferred and the SCA method chosen by the TPP/PSU. The parameter might be ignored by the ASPSP. If both parameters TPP-Redirect-Preferred and TPP-Decoupled-Preferred are present and true, the request is still not rejected, but it is up to the ASPSP, which approach will actually be used. RFU: TPP-Redirect-Preferred and TPP-Decoupled-Preferred will be revised in future versions, maybe merged. Currently kept separate for downward compatibility.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandatory for the SCA OAuth Approach.
TPP-Nok-Redirect-URI	String	Optional	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method. This might be ignored by the ASPSP.

Request Body - Няма

Response Code

HTTP response code equals 201.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	Possible values are: • EMBEDDED • DECOUPLED • REDIRECT OAuth will be subsumed by the value REDIRECT

Response Body

Attribute	Type	Condition	Description
transactionFees	Amount	Optional	Might be used by the ASPSP to transport the total transaction fee relevant for the underlying payments. This field includes the entry of the currencyConversionFees if applicable.
currencyConversionFees	Amount	Optional	Might be used by the ASPSP to transport specific currency conversion fees related to the initiated credit transfer.
estimatedTotalAmount	Amount	Optional	The amount which is estimated to be debted from the debtor account. Note: This amount includes fees.
estimatedInterbankSettlementAmount	Amount	Optional	The estimated amount to be transferred to the payee.
scaStatus	SCA Status	Mandatory	A definition of the provided SCA method is contained, if only one authentication method is available, and if the Embedded SCA approach is chosen by the ASPSP.
authorisationId	String	Mandatory	Unique resource identification of the created authorisation sub-resource.
scaMethods	Array of authentication objects	Conditional	This data element might be contained, if SCA is required and if the PSU has a choice between different authentication methods. Depending on the risk management of the ASPSP this choice might be offered before or after the PSU has been identified with the first relevant factor, or if an access token is transported. If this data element is contained, then there is also an hyperlink of type "selectAuthenticationMethod" contained in the response body. These methods shall be presented towards the PSU for selection by the TPP.
chosenSca Method	Authentication object	Conditional	This data element is only contained in the response if the APSPS has chosen the Embedded SCA Approach, if the PSU is already identified e.g. with the first relevant factor or alternatively an access token, if SCA is required and if the authentication method is implicitly selected.
challengeData	Challenge	Conditional	It is contained in addition to the data element "chosenScaMethod" if challenge data is needed for SCA. In rare cases this attribute is also used in the context of the "updatePsuAuthentication" link.
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP.

Attribute	Type	Condition	Description
			Type of links admitted in this response, (further links might be added for ASPSP defined extensions):
			"scaRedirect": In case of an SCA Redirect Approach, the ASPSP is transmitting the link to which to redirect the PSU browser.
			"scaOAuth": In case of a SCA OAuth2 Approach, the ASPSP is transmitting the URI where the configuration of the Authorisation Server can be retrieved. The configuration follows the OAuth 2.0 Authorisation Server Metadata specification.
			"confirmation": Might be added by the ASPSP if either the "scaRedirect" or "scaOAuth" hyperlink is returned in the same response message. This hyperlink defines the URL to the resource which needs to be updated with a confirmation code as retrieved after the plain redirect authentication process with the ASPSP authentication server or an access token as retrieved by submitting an authorization code after the integrated OAuth based authentication process with the ASPSP authentication server.
			"updatePsuIdentification": The link to the authorisation or cancellation authorisation sub-resource, where PSU identification data needs to be uploaded.
			"updatePsuAuthentication": The link to the authorisation or cancellation authorisation sub-resource, where PSU authentication data needs to be uploaded.
			"updateEncryptedPsuAuthentication": The link to the authorisation or cancellation authorisation sub-resource, where encrypted PSU authentication data needs to be uploaded
			"selectAuthenticationMethod": The link to the authorisation or cancellation authorisation sub-resource, where the selected authentication method needs to be uploaded. This link is contained under exactly the same conditions as the data element "scaMethods"
			"authoriseTransaction": The link to the authorisation or cancellation authorisation sub-resource, where the authorisation data has to be uploaded, e.g. the TOP received by SMS.
			"scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource.
psuMessage	Max500Text	Optional	

Example

Request

POST <https://api.testbank.com/v1/payments/sepa-credit-transfers/qwer3456tzui7890/authorisations>
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

PSU-ID: PSU-1234

Response

HTTP/1.x 201 CREATED

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: DECOUPLED

Date: Sun, 06 Aug 2017 15:05:47 GMT

Content-Type: application/json

```
{
  "scaStatus": "received",
  "psuMessage": "Please use your Bank App for transaction Authorisation.",
  "_links": {
    "scaStatus": { "href": "/v1/payments/sepa-credit-transfers/qwer3456tzui7890/authorisations/123auth456" }
  }
}
```

HTTP/1.x 201 CREATED

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

ASPSP-SCA-Approach: DECOUPLED

Date: Sun, 06 Aug 2017 15:05:47 GMT

Location: https://www.testbank.com/psd2/v1/payments/sepa-credit-transfers/qwer3456tzui7890/123auth456

Content-Type: application/json

```
{
  "scaStatus": "received",
  "authorisationId": "123auth456",
  "psuMessage": "Please use your BankApp for transaction Authorisation.",
  "_links": {
    "scaStatus": { "href": "/v1/payments/sepa-credit-transfers/qwer3456tzui7890/authorisations/123auth456" }
  }
}
```

Забележка: Ако се използват хипервръзки в следващите разширени форми, се прилагат допълнителни условия за параметрите, посочени по-долу:

- "startAuthorisationWithPsuIdentification": Секция 7.2.1
- "startAuthorisationWithPsuAuthentication": Секция 7.2.2
- "startAuthorisationWithEncryptedPsuAuthentication": Секция 7.2.2
- "startAuthrosiationWithAuthenticationMethodSelection": Секция 7.2.3.

Разликата в повикванията е само дали да се използва команда POST, за да се създаде под-ресурса за авторизация и да се актуализират данните едновременно или да се използва командата PUT, за да се актуализират посочените данни към вече създаден под-ресурс.

7.2. Процеси по обмен на данни с Ползвателя

Възможни са няколко вида заявки при обмен на данните с Ползвателя, в зависимост от подхода на ЗУИ:

- При Redirect подход: В конкретна заявка се обменят данни за избор на ЗУИ подход
- При Decoupled подход: Специфична обмяна на данни за Ползвателя, приложима само при:

- Добавяне на идентификацията на Ползвателя за услугата, ако не е предоставена в Заявката за инициране на плащане или Искането за съгласие за информация или ако не се използва OAuth2 токън за достъп
- При избор на метод за ЗУИ
- При Embedded подход: Обменът на данни с Ползвателя относно:
 - Добавяне на идентификация като първи фактор за удостоверяване Ползвателя
 - Избор на метод за ЗУИ

Подходът на ЗУИ може да зависи от избрания метод на ЗУИ. Това е причината при всички подходи на ЗУИ да се предлага обмен на данни с Ползвателя – Избор на метод за ЗУИ. Този избор се предлага на Ползвателя, само когато ДПУОС поддържа повече от един метод на ЗУИ.

Различните искания за обмяна на данни с Ползвателя са описани в подточките:

7.2.1. Обмен на данни за идентификация на Ползвателя

(Update PSU Data -Identification) чрез Decoupled метод на ЗУИ

Това повикване се използва от ДПУ, когато след началното повикване е получен отговор от тип "updatePsuIdentification".

- Повикване в случай на искане за инициране на плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}

- Повикване в случай на искане за отмяна на плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}

- Повикване в случай на искане за съгласие за информация за сметка

PUT /v1/consents/{consentId}/authorisations/{authorisationId}

- Повикване в случай на авторизация на кошница от плащания

PUT /v1/signing-baskets/{basketId}/authorisations/{authorisationId}

Path

Attribute	Type	Description
payment-service	String	The possible values are "payments", "bulk-payments" and "periodic-payments"
payment-product	String	The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.
authorisationId	String	Resource identification of the related Payment Initiation, Signing Basket or Consent authorization sub-resource.
authorisationId	String	Resource identification of the related Payment Cancellation authorization sub-resource

Query Parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
PSU-ID	String	Conditional	Contained if not yet contained in a preceding request, and mandated by the ASPSP in the related response
PSU-ID-Type	String	Conditional	Type of the PSU-ID, needed in scenarios where PSUs have several PSU-IDs as access possibility.
PSU-Corporate-ID	String	Conditional	Contained if not yet contained in the first request, and mandated by the ASPSP in the related response. This field is relevant only in a corporate context.
PSU-Corporate-ID-Type	String	Conditional	Might be mandated by the ASPSP in addition if the PSU-Corporate-ID is contained.

Request body - Няма

Response Code

HTTP response code is 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	Possible values are: • EMBEDDED • DECOUPLED • REDIRECT OAuth will be subsumed by the value REDIRECT
scaMethods	Array of authentication objects	Conditional	Might be contained, if several authentication methods are available. (name, type)

Response body

Attribute	Type	Condition	Description
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Type of links admitted in this response, (further links might be added for ASPSP defined extensions): "scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource.
			"selectAuthenticationMethod": This is a link to a resource, where the TPP can select the applicable second factor authentication methods for the PSU, if there are several available authentication methods and if the PSU is already sufficiently authenticated.. If this link is contained, then there is also the data element "scaMethods" contained in the response body
scaStatus	SCA Status	Mandatory	
transactionFees	Amount	Optional	Might be used by the ASPSP to transport the total transaction fee relevant for the underlying payments. This field includes the entry of the currencyConversionFees if applicable.
currencyConversionFees	Amount	Optional	Might be used by the ASPSP to transport specific currency conversion fees related to the initiated credit transfer.
estimatedTotalAmount	Amount	Optional	The amount which is estimated to be debted from the debtor account
estimatedInterbankSettlementAmount	Amount	Optional	The estimated amount to be transferred to the payee.

Attribute	Type	Condition	Description
transactionFeeIndicator	Boolean	Optional	If equals "true", the transaction will involve specific transaction cost as shown by the ASPSP in their public price list or as agreed between ASPSP and PSU. If equals "false" or is not used, the transaction will not involve additional specific transaction costs to the PSU unless the fee amount is given specifically in the data elements transactionFees and/or currencyConversionFees.
psuMessage	Max500Text	Optional	

Example

Request

PUT <https://api.testbank.com/v1/payments/sepa-credit-transfer/qwer3456tzui7890>
 authorisations/123auth456
 X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
 PSU-ID: PSU-1234

Response

HTTP/1.x 200 OK
 X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
 ASPSP-SCA-Approach: DECOUPLED
 Date: Sun, 06 Aug 2017 15:05:47 GMT
 Content-Type: application/json
 {
 "scaStatus": "psuIdentified",
 "psuMessage": "Please use your BankApp for transaction Authorisation.",
 "_links": {
 "scaStatus": { "href": "/v1/payments/sepa-credit-transfers/qwer3456tzui7890/authorisations/123auth456" }
 }
 }

7.2.2. Обмен на данните за автентикация на Ползвателя

(Update PSU Data Authentication) чрез методи на ЗУИ Decoupled или Embedded

Това повикване се използва от ДПУ, когато след началното повикване е получен отговор от тип "updatePsuAuthenication" или „updateEncryptedPsuAuthenication“ т.е. ДПУОС изисква удостоверение от Ползвателя.

- Повикване в случай на искане за инициране на плащане

PUT /v1/{payment-service}/{paymentId}/{payment-product}/authorisations/{authorisationId}

След искане от ДПУОС се удостоверяват данните на Ползвателя в процеса на инициране на плащане

- Повикване в случай на искане за отмяна на плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}

- Повикване в случай на искане за съгласие за информация за сметка

PUT /v1/consents/{consentId}/authorisations/{authorisationId}

След искане от ДПУОС се удостоверяват и актуализират данните на Ползвателя в базата за съгласие по услугите „Информация за сметка“.

- Повикване в случай на авторизация на кошница от плащания

PUT /v1/signing-baskets/{basketId}/authorisations/{authorisationId}

Path

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.
authorisationId	String	Resource identification of the related Payment Initiation, Signing Basket or Consent authorization sub-resource.
authorisationId	String	Resource identification of the related Payment Cancellation authorization sub-resource

Query Parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
PSU-ID	String	Conditional	Contained if not yet contained in a preceding request, and mandated by the ASPSP in the related response
PSU-ID-Type	String	Conditional	Contained if not yet contained in a preceding request, and mandated by the ASPSP in the related response
PSU-Corporate-ID	String	Conditional	Contained if not yet contained in a preceding request, and mandated by the ASPSP in the related response. This field is relevant only in a corporate context.
PSU-Corporate-ID-Type	String	Conditional	Contained if not yet contained in a preceding request, and mandated by the ASPSP documentation. Might be mandated by the ASPSP in addition if the PSU-Corporate-ID is contained.

Request body

Attribute	Type	Condition	Description
psuData	PSU Data	Mandatory	The password, encryptedPassword, additionalPassword, or additionalEncryptedPassword subfield is used, depending whether the password or the additional password needs to be sent and depending on encryption requirements of the ASPSP

Attribute	Type	Condition	Description
			as indicated in the corresponding hyperlink contained in the preceding response message of the ASPSP. Remark for Future: More details on the encrypted password transport will be published by a future bulletin.

Response Code

HTTP response code is 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	Possible values are: • EMBEDDED • DECOUPLED • REDIRECT OAuth will be subsumed by the value REDIRECT

Response body

Attribute	Type	Condition	Description
chosenScaMethod	Authentication object	Conditional	A definition of the provided SCA method is contained, if only one authentication method is available, and if the Embedded SCA approach is chosen by the ASPSP.
challengeData	Challenge	Conditional	Challenge data might be contained, if only one authentication method is available.
scaMethods	Array of authentication objects	Conditional	Might be contained, if several authentication methods are available. (name, type)

Attribute	Type	Condition	Description
_links	Links	Conditional	A list of hyperlinks to be recognised by the TPP. Might be contained, if several authentication methods are available for the PSU. Type of links admitted in this response: "updateAdditionalPsuAuthentication" The link to the payment initiation or account information resource, which needs to be updated by an additional PSU password. This link is only contained in rare cases, where such additional passwords are needed for PSU authentications. "updateAdditionalEncryptedPsuAuthentication" The link to the payment initiation or account information resource, which needs to be updated by an additional encrypted PSU password. This link is only contained in rare cases, where such additional passwords are needed for PSU authentications. "selectAuthenticationMethod": This is a link to a resource, where the TPP can select the applicable second factor authentication methods for the PSU, if there were several available authentication methods. This link is only contained, if the PSU is already identified or authenticated with the first relevant factor or alternatively an access token, if SCA is required and if the PSU has a choice between different authentication methods. If this link is contained, then there is also the data element "scaMethods" contained in the response body.
			"authoriseTransaction": The link to the resource, where the "Transaction Authorisation Request" is sent to. This is the link to the resource which will authorise the transaction by checking the SCA authentication data within the Embedded SCA approach.
			"scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource.
scaStatus	SCA Status	Mandatory	

Attribute	Type	Condition	Description
transactionFees	Amount	Optional	Might be used by the ASPSP to transport the total transaction fee relevant for the underlying payments. This field includes the entry of the currencyConversionFees if applicable.
currencyConversionFees	Amount	Optional	Might be used by the ASPSP to transport specific currency conversion fees related to the initiated credit transfer.
estimatedTotalAmount	Amount	Optional	The amount which is estimated to be debted from the debtor account
estimatedInterbankSettlementAmount	Amount	Optional	The estimated amount to be transferred to the payee.
transactionFeeIndicator	Boolean	Optional	If equals "true", the transaction will involve specific transaction cost as shown by the ASPSP in their public price list or as agreed between ASPSP and PSU. If equals "false" or is not used, the transaction will not involve additional specific transaction costs to the PSU unless the fee amount is given specifically in the data elements transactionFees and/or currencyConversionFees.
psuMessage	Max500Text	Optional	

ЗАБЕЛЕЖКА: При грешна парола ДПУ трябва да поиска от Ползвателя да въведе отново паролата. Ново-въведената парола трябва да бъде обновена по същия път. Препоръчва се ДПУОС да информира ДПУ за това чрез добавяне на секция `_links` в допълнителната информация за грешка и представяне на съответната `updatePsuAuthentication` или `updateEncryptedPsuAuthentication` хипервръзка.

Example

Request in case of Embedded Approach

```
PUT https://api.testbank.com/v1/payments/sepa-credit-transfers/qwer3456tzui7890/
authorisations/123auth456
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-ID: PSU-1234
{
  "psuData": {
    "password": "start12"
  }
}
```

Response in case of the Embedded Approach

```
HTTP/1.x 200 OK
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: EMBEDDED
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{ "scaStatus": "psuAuthenticated",
  "_links":{
```

```
"authoriseTransaction": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations/123auth456"}
}
```

7.2.3. Обмен на данните при избор на метод за автентикация с Ползвателя (Update PSU Data - Select Authentication Method)

Това повикване се използва от ДПУ, когато след началното повикване ДПУОС е върнал отговор от тип "selectAuthenticationMethod" т.е. ДПУОС поддържа няколко метода за удостоверяване на Ползвателя.

- Повикване в случай на искане за инициране на плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}

Актуализира данните за инициране на плащания чрез данни за Ползвателя, ако това се изисква от ДПУОС.

- Повикване в случай на искане за отмяна на плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}

- Повикване в случай на искане за съгласие за информация за сметка

PUT /v1/consents/{consentId}/authorisations/{authorisationId}

След искане от ДПУОС се актуализират авторизационните данни на Ползвателя в базата за съгласие по услугите „Информация за сметка“.

- Повикване в случай на авторизация на кошница от плащания

PUT /v1/signing-baskets/{basketId}/authorisations/{authorisationId}

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are "payments", "bulk-payments" and "periodic-payments"
payment-product	String	Only in case of an Update Data Request in a Payment Initiation context. The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.
authorisationId	String	Resource identification of the related Payment Initiation, Signing Basket or Consent authorization sub-resource.
authorisationId	String	Resource identification of the related Payment Cancellation authorization sub-resource

Query Parameters - Няма

Response Code

HTTP response code is 200.

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Request body

Attribute	Type	Condition	Description
authentication MethodId	String	Mandatory	The authentication method ID as provided by the ASPSP.

Response Code

HTTP response code equals 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	Possible values are: • EMBEDDED • DECOUPLED • REDIRECT OAuth will be subsumed by the value REDIRECT

Response body

Attribute	Type	Condition	Description
chosenSca Method	Authentication object	Conditional	A definition of the provided SCA method is contained, if only one authentication method is available, and if the Embedded SCA approach is chosen by the ASPSP.
challengeData	Challenge	Conditional	Challenge data might be contained, if only one authentication method is available.

Attribute	Type	Condition	Description
_links	Links	Conditional	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Remark: This method can be applied before or after PSU identification. This leads to many possible hyperlink responses. Type of links admitted in this response, (further links might be added for ASPSP defined extensions): "scaRedirect": In case of an SCA Redirect Approach, the ASPSP is transmitting the link to which to redirect the PSU browser.
			"scaOAuth": In case of a SCA OAuth2 Approach, the ASPSP is transmitting the URI where the configuration of the Authorisation Server can be retrieved. The configuration follows the OAuth 2.0 Authorisation Server Metadata specification.
			"confirmation": Might be added by the ASPSP if either the "scaRedirect" or "scaOAuth" hyperlink is returned in the same response message. This hyperlink defines the URL to the resource which needs to be updated with • a confirmation code as retrieved after the plain redirect authentication process with the ASPSP authentication server or • an access token as retrieved by submitting an authorization code after the integrated OAuth based authentication process with the ASPSP authentication server.
			"updatePsuIdentification": The link to the authorisation or cancellation authorisation sub-resource, where PSU identification data needs to be uploaded.

Attribute	Type	Condition	Description
			"updatePsuAuthentication": The link to the authorisation or cancellation authorisation sub-resource, where PSU authentication data needs to be uploaded.
			"updateEncryptedPsuAuthentication": The link to the authorisation or cancellation authorisation sub-resource, where encrypted PSU authentication data needs to be uploaded.
			"authoriseTransaction": The link to the authorisation or cancellation authorisation sub-resource, where the authorisation data has to be uploaded, e.g. the TOP received by SMS.
			"scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource.
scaStatus	SCA Status	Mandatory	
transactionFees	Amount	Optional	Might be used by the ASPSP to transport the total transaction fee relevant for the underlying payments. This field includes the entry of the currencyConversionFees if applicable.
currencyConversionFees	Amount	Optional	Might be used by the ASPSP to transport specific currency conversion fees related to the initiated credit transfer.
estimatedTotalAmount	Amount	Optional	The amount which is estimated to be debted from the debtor account
estimatedInterbankSettlementAmount	Amount	Optional	The estimated amount to be transferred to the payee.
transactionFeeIndicator	Boolean	Optional	If equals "true", the transaction will involve specific transaction cost as shown by the ASPSP in their public price list or as agreed between ASPSP and PSU. If equals "false" or is not used, the transaction will not involve additional specific transaction costs to the PSU unless the fee amount is given specifically in the data elements transactionFees and/or currencyConversionFees.
psuMessage	Max500Text	Optional	

Example

Request in case of Embedded Approach

```
PUT https://api.testbank.com/v1/payments/sepa-credit-transfers/qwer3456tzui7890/
authorisations/123auth456
X-Request-ID: asdfoeljkasdfoelkjasdf-123479093
{
    authenticationMethodId: "myAuthenticationID"
}
```

Response in case of the Embedded Approach

```
HTTP/1.x 200 OK
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: EMBEDDED
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{
    "scaStatus": "scaMethodSelected",
    "chosenScaMethod": {
        "authenticationType": "SMS_OTP",
        "authenticationMethodId": "myAuthenticationID"},
    "challengeData": {
        "otpMaxLength": "6",
        "otpFormat": "integer"},
    "_links": {
        "authoriseTransaction": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-
983/authorisations /123auth456"}
    }
}
```

7.3. Авторизация на транзакции (Transaction Authorization)

Тази секция описва процеса на авторизация на транзакция, който се използва само при Embedded метод на ЗУИ.

- Повикване в случай на искане за инициране на плащане

```
PUT /v1/payments/{payment-product}/{paymentId}/authorisations/{authorisationId}
    Подава данни за разплащане, които подлежат на ЗУИ авторизация от ДПУОС
```

- Повикване в случай на искане за отмяна на плащане

```
PUT /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-
authorisations/{authorisationId}
```

- Повикване в случай на искане за съгласие за информация за сметка

```
PUT /v1/consents/{consentId}/authorisations/{authorisationId}
```

- Повикване в случай на авторизация на кошница от плащания

```
PUT /v1/signing-baskets/{basketId}/authorisations/{authorisationId}
```

Path

Attribute	Type	Description
payment-product	String	The related payment product of the payment initiation to be authorized.

paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.
authorisationId	String	Resource identification of the related Payment Initiation, Signing Basket or Consent authorization sub-resource.
authorisationId	String	Resource identification of the related Payment Cancellation authorization sub-resource

Query Parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if the optional Oauth Pre-Step was performed.

Request body

Attribute	Type	Condition	Description
scaAuthenticationData	String	Mandatory	SCA authentication data, depending on the chosen authentication method. If the data is binary, then it is base64 encoded.

Response Code

HTTP response code is 200.

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
scaStatus	SCA Status	Mandatory	

ЗАБЕЛЕЖКА: В случай на некоректни scaAuthenticationData, ДПУ трябва да поиска от Ползвателя да въведе отново данните за удостоверяване, като повтори първо метода ЗУИ. В зависимост от изпълнението на съответния метод на ЗУИ, ДПУ се нуждае:

- или да възобнови процеса на пълно оторизиране, като генерира нов под-ресурс за авторизация, напр. в случай на SMS OTP,
- или да изпрати ново-генерирани данни за удостоверяване от клиентско устройство, по същия начин, както първия път, напр. в случай на CHIP OTP.

ДПУОС информира ДПУ за това чрез добавяне на секция `_links` в допълнителната информация за грешка и предоставяне на съответната хипервръзка `startAuthorisation` или `transactionAuthorisation`.

Example

Request

```
PUT https://api.testbank.com/v1/payments/sepa-credit-transfers/qwer3456tzui7890/
authorisations/ 123auth456
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
{
  "scaAuthenticationData": "123456"
}
```

Response in case of the embedded approach

Response Code 200

Response body

```
{
  "scaStatus": "finalised",
  "_links":{
    "scaStatus": {"href":"/v1/payments/sepa-credit-transfers/qwer3456tzui7890/
authorisations/123auth456"}
  }
}
```

7.4. Получаване на авторизация за под-ресурс

Следващите команди се използват за да се предостави масив от идентификатори на ресурса и на всички генерирани под-ресурси за авторизация.

Повикване в контекста на Искане за инициране на плащане

GET /v1/{payment-service}/{payment-product}/{paymentId}/authorisations

Повикване в контекста на искане за съгласие за информация по сметка

GET /v1/consents/{consentId}/authorisations

Повикване в контекста на авторизация и подписване на кошницата

GET /v1/signing-baskets/{basketId}/authorisations

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current PIS transaction.

Request Body - Няма

Response Code

HTTP response code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
authorisationIds	Array of String	Mandatory	An array of all authorisationIds connected to this payment, signing basket or consent resource.

Example

Request

```
GET https://api.testbank.com/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations
Accept: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7723
Date: Sun, 06 Aug 2017 15:04:07 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7723
Date: Sun, 06 Aug 2017 15:04:08 GMT
Content-Type: application/json
{
  "authorisationIds": ["123auth456"]
}
```

7.5. Проверка на ЗУИ статус

Следващите команди се използват за проверка на статуса на оторизирания ресурс.

Повикване в контекста на Искане за инициране на плащане

GET /v1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}

Повикване в контекста на Искане за отмяна на плащане

GET/v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}

Повикване в контекста на искане за съгласие за информация по сметка

GET /v1/consents/{consentId}/authorisations/{authorisationId}

Повикване в контекста на авторизация и подписване на кошницата

GET /v1/signing-baskets/{basketId}/authorisations/{authorisationId}

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.
authorisationId	String	Resource identification of the related Payment Initiation, Signing Basket or Consent authorization sub-resource.
authorisationId	String	Resource identification of the related Payment Cancellation authorization sub-resource

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current PIS transaction.

Request Body - Няма

Response Code

HTTP response code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
scaStatus	SCA Status	Mandatory	This data element is containing information about the status of the SCA method applied.
_links	Links	Optional	Should refer to next steps if the problem can be resolved via the interface e.g. for re-submission of credentials.
tppMessages	Array of TPP Message Information	Optional	Messages to the TPP on operational issues.

Example

Request

```
GET https://api.testbank.com/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations/123auth456
Accept: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:04:07 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:04:08 GMT
Content-Type: application/json
{
  "scaStatus": "finalised"
}
```

7.6. Заявка за потвърждение

Тази заявка се използва, когато в предходния отговор се съдържа хипервръзката от тип „confirmation“ и ако е приложен redirect метод за авторизация. Преди заявката да бъде изпратена от ДПУ, трябва да се извлече код за авторизация, съответно и код за потвърждение, от ДПУ след обработката на ЗУИ при пренасочване към сървър за авторизация на ДПУОС.

В случай на интегрирания подход на OAuth ЗУИ, цялостната процедура за успешно получаване на код за авторизация и токен за достъп е описана в раздел 13.

В случай на подход на redirect ЗУИ, процедурата за извличане на кода за авторизация е описана в следващите подраздели. Действителното съобщение за заявка за потвърждение е описано в раздел 7.6.4, както за интегрирания подход на OAuth2 ЗУИ, така и за подхода за redirect ЗУИ.

7.6.1. Получаване на код за потвърждение при подхода на redirect ЗУИ

ДПУ трябва да фиксира сесията на Ползвателя в брауъра на ДПУ с nonce, където част от него е уникален "state" параметър.

При подготовката на изпращане на заявката за авторизация, ДПУ трябва

- да създайте XSRF токен за еднократна употреба, който ще бъде предаден на ДПУОС в параметъра "state" и,
- да обвържете тази стойност с текущата сесия в потребителския агент.

Забележка: В случай на интегрирания подход на OAuth ЗУИ, ДПУ трябва да генерира допълнително „nonce“ за параметъра за предизвикателство. Това също трябва да бъде обвързано със сесията на потребителския агент.

7.6.2. Изисквания към HTTP заявка брауъра на Ползвателя

ДПУ трябва да препрати „state“ параметъра като параметър на заявката към Ползвателя, което ще доведе до GET HTTP заявка от брауъра на Ползвателя, както се изисква, както следва:

Параметър на заявката за авторизация на Ползвателя (GET заявка)

Attribute	Type	Condition	Description
state	string	mandated	state parameter as defined by the TPP as a unique parameter and bound to the PSU/TPP session.

Example

GET ASPSP-Redirect-URI?state=1234567er

След провеждането на автентификацията на клиента на сървъра на ДПУОС, ДПУОС отговаря със същия "state" параметър и уникален код за потвърждение, свързан с ресурса на авторизация като параметри на заявката. „confirmationCode“ ще се съдържа само ако ЗУИ е успешно изпълнено.

Параметър на заявката за авторизация на Ползвателя (Отговор на GET заявка)

Attribute	Type	Condition	Description
state	string	mandated	state parameter as used in the corresponding request.
code	string	conditional	unique authorisation code of the ASPSP, bound to the related transaction, in case of Integrated OAuth SCA Approach.
confirmationCode	string	conditional	unique authorisation code of the ASPSP, bound to the related transaction, in case of Redirect SCA Approach.

Example in case of Redirect SCA Approach

http 302?state=1234567er&confirmationCode=2256ffgh

7.6.3. Предварително условие за заявка за потвърждение

Когато получи на GET заявка от брауъра на Ползвателя, ДПУ трябва да провери, дали „state“ параметъра е свързан с текущата сесия. Стойността на „state“ е свързана с текущата сесия в потребителския агент. Ако проверката е положителна, тогава ДПУ последващо обработва

- в контекста на интегрирания OAuth ЗУИ подход с извличане на access Bearer токен, както е описано в раздел 13 на този документ, и след това продължава, както е описано в раздел 7.6.4.
- в контекста на подхода на redirect ЗУИ директно, както е описано в раздел 7.6.4.

Ако проверката не успее, транзакцията трябва да бъде спряна от ДПУ.

7.6.4. Авторизиране на заявката за потвърждение

Извикване в контекста на заявка за инициране на плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}

Обновява данните на под-ресурса за авторизация на иницирано плащане на сървъра по авторизационен код, ако се изисква от ДПУОС.

Извикване в контекста на заявка за отмяна на иницирано плащане

PUT /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}

Обновява данните на под-ресурса за отмяна на иницирано плащане на сървъра по авторизационен код, ако се изисква от ДПУОС.

Извикване в контекста на заявка за създаване на съгласие

PUT /v1/consents/{consentId}/authorisations/{authorisationId}

Обновява данните на съгласието за информация по сметка на сървъра по авторизационен код, ако се изисква от ДПУОС.

Извикване в контекста на заявка за множествена авторизация при плащане

PUT /v1/signing-baskets/{basketId}/authorisations/{authorisationId}

Обновява данните на кошницата с подписи на сървъра по авторизационен код, ако се изисква от ДПУОС.

Path Parameters

Attribute	Type	Description
payment-service	String	The possible values are “payments”, “bulk-payments” and “periodic-payments”
payment-product	String	The payment product, under which the payment under paymentId has been initiated. It shall be checked by the ASPSP, if the payment-product is matching the payment initiation addressed by paymentId.
paymentId, basketId or consentId	String	Resource identification of the related payment initiation, signing basket or consent resource.
authorisationId	String	Resource identification of the related Payment Initiation, Signing Basket or Consent authorisation sub-resource.
authorisationId	String	Resource identification of the related Payment Cancellation authorisation sub-resource

Query Parameters

No specific query parameters.

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Authorization Bearer Token as retrieved by the TPP in case the integrated OAuthSCA Approach as described in Section 13.

Request Body

Attribute	Type	Condition	Description
confirmationCode	String	Conditional	Confirmation Code as retrieved by the TPP from the redirect based SCA process as described in Section 7.6.1 ff.

Response Code

HTTP response code is 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
scaStatus	SCA Status	Mandatory	Value "finalised" if the transaction authorisation and confirmation was successful. Value "failed" if the transaction authorisation or confirmation was not successful.
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Type of links admitted in this response, (further links might be added for ASPSP defined extensions): "status": The link to retrieve the status of the corresponding transaction resource.
psuMessage	Max512Text	Optional	

Example for integrated OAuth solution

Request

PUT https://api.testbank.com/v1/payments/sepa-credit-transfers/qwer3456tzui7890/authorisations/123auth456

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Authorization: Bearer 1234567

Response

HTTP/1.x 200 OK

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 06 Aug 2017 15:05:47 GMT

Content-Type: application/json

```
{
  "scaStatus": "finalised",
  "_links": {
    "status": { "href": "/v1/payments/sepa-credit-transfers/qwer3456tzui7890/status" }
  }
}
```

Example for redirect solution

Request

PUT https://api.testbank.com/v1/payments/sepa-credit-transfers/qwer3456tzui7890/authorisations/123auth456

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

{ "confirmationCode": "2256ffgh" }

Response

HTTP/1.x 200 OK

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 06 Aug 2017 15:05:47 GMT

Content-Type: application/json

```
{
  "scaStatus": "finalised",
  "_links": {
    "status": { "href": "/v1/payments/sepa-credit-transfers/qwer3456tzui7890/status" }
  }
}
```

8. Подписване на Кошница

8.1. Създаване на заявка за подпис на кошница

Създаване на кошница за подпис

POST /v1/signing-baskets/

Path Parameters - Няма

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
Content-Type	String	Mandatory	application/json
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
PSU-ID	String	Conditional	Client ID of the PSU in the ASPSP client interface. Might be mandated in the ASPSP's documentation. It might be contained, even if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in an preceding AIS service in the same session. In this case the ASPSP might check whether PSU-ID and token match, according to ASPSP documentation.
PSU-ID-Type	String	Conditional	Type of the PSU-ID, needed in scenarios where PSUs have several PSU-IDs as access possibility. In this case, the mean and use is then defined in the ASPSP's documentation.
PSU-Corporate-ID	String	Conditional	Identification of a Corporate in the Online Channels Might be mandated in the ASPSP's documentation. Only used in a corporate context.
PSU-Corporate-ID-Type	String	Conditional	This is describing the type of the identification needed by the ASPSP to identify the PSU-Corporate-ID content. Mean and use is defined in the ASPSP's documentation. Only used in a corporate context.
Authorization	String	Conditional	Bearer Token. Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in an preceding AIS service in the same session.
Consent-ID	String	Optional	This data element may be contained, if the signing basket transaction is part of a session, i.e. combined AIS/PIS service. This then contains the "consentId" of the related AIS one off consent, which was performed prior to this bulk signing.
PSU-IP-Address	String	Mandatory	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. If not available, the TPP shall use the IP Address used by the TPP when submitting this request.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a redirect over an embedded SCA approach. If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or

Attribute	Type	Condition	Description
			the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Decoupled-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a decoupled SCA approach. If it equals "false", the TPP prefers not to use the decoupled approach for SCA. The ASPSP will then choose between the embedded or the redirect SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the parameter TPP-Redirect-Preferred and the SCA method chosen by the TPP/PSU. The parameter might be ignored by the ASPSP. If both parameters TPP-Redirect-Preferred and TPP-Decoupled-Preferred are present and true, the request is still not rejected, but it is up to the ASPSP, which approach will actually be used. RFU: TPP-Redirect-Preferred and TPP-Decoupled-Preferred will be revised in future versions, maybe merged. Currently kept separate for downward compatibility.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandated for the Redirect SCA Approach (including OAuth2 SCA approach), specifically when TPP-Redirect-Preferred equals "true". It is recommended to always use this header field.
TPP-Nok-Redirect-URI	String	Optional	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method. This might be ignored by the ASPSP.
TPP-Explicit-Authorisation-Preferred	Boolean	Optional	Must equal "true", if contained. Remark: No optimisation processes for creating authorisation resources for signing baskets implicitly, since anyhow several calls have been submitted.

Request Body

Attribute	Type	Condition	Description
paymentIds	Array of String	Optional	An array of paymentIds. Array may not be empty.
consentIds	Array of String	Optional	An array of consentIds. Array may not be empty.

Response Code

The HTTP response code equals 201.

Response Header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource (if created)
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	This data element must be contained, if the SCA Approach is already fixed. Possible values are:

Attribute	Type	Condition	Description
			- EMBEDDED - DECOUPLED - REDIRECT The OAuth SCA approach will be subsumed by REDIRECT.

Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	The nonpayment related values defined in Section 14.23 might be used like RCVD, ACTC, CANC or RJCT
basketId	String	Mandatory	resource identification of the generated signing basket resource.
scaMethods	Array of authentication objects	Conditional	This data element might be contained, if SCA is required and if the PSU has a choice between different authentication methods. Depending on the risk management of the ASPSP this choice might be offered before or after the PSU has been identified with the first relevant factor, or if an access token is transported. If this data element is contained, then there is also an hyperlink of type "startAuthorisationWithAuthenticationMethodSelection" contained in the response body. These methods shall be presented towards the PSU for selection by the TPP.
chosenScaMethod	Authentication object	Conditional	This data element is only contained in the response if the APSPS has chosen the Embedded SCA Approach, if the PSU is already identified e.g. with the first relevant factor or alternatively an access token, if SCA is required and if the authentication method is implicitly selected.
challengeData	Challenge	Conditional	It is contained in addition to the data element "chosenScaMethod" if challenge data is needed for SCA. In rare cases this attribute is also used in the context of the "startAuthorisationWithPsuAuthentication" link.
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Type of links admitted in this response, (further links might be added for ASPSP defined extensions):
			"startAuthorisation": In case, where an explicit start of the transaction authorization is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded).
			"startAuthorisationWithPsuIdentification": The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the PSU identification data.
			"startAuthorisationWithPsuAuthentication":

Attribute	Type	Condition	Description
			The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the PSU authentication data.
			"startAuthorisationWithEncryptedPsuAuthentication": The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the encrypted PSU authentication data.
			"startAuthorisationWithAuthentication MethodSelection": The link to the authorization end-point, where the authorization sub-resource has to be generated while selecting the authentication method. This link is contained under exactly the same conditions as the data element "scaMethods"
			"startAuthorisationWithTransactionAuthorisation": The link to the authorization end-point, where the authorization sub-resource has to be generated while authorizing the transaction e.g. by uploading an OTP received by SMS.
			"self": The link to the payment initiation resource created by this request. This link can be used to retrieve the resource data.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU
tppMessages	Array of TPP Message Information	Optional	Messages to the TPP on operational issues.

Example

Request

```
POST https://api.testbank.com/v1/signing-baskets
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-GEO-Location: GEO:52.506931;13.144558
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 06 Aug 2017 15:02:37 GMT
{
  "paymentIds": ["123qwerty456789", "12345qwerty7899"]
}
```

Response *(always with explicit authorization start)*

```
HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: REDIRECT
Date: Sun, 06 Aug 2017 15:02:42 GMT
Location: https://www.testbank.com/psd2/v1/signing-baskets/1234-basket-567
Content-Type: application/json
{
  "transactionStatus": "RCVD",
  "basketId": "1234-basket-567",
  "_links": {
    "self": {"href": "/v1/signing-baskets/1234-basket-567"},
    "status": {"href": "/v1/signing-baskets/1234-basket-567/status"},
    "startAuthorisation": {
      "href": "/v1/signing-baskets/1234-basket-567/authorisations"
    }
  }
}
```

}

8.2. Получаване на заявка за подпис на кошница

Повикване:

GET /v1/signing-baskets/{basketId}

Изисква да се върне описание на съдържанието в кошницата

Path Parameters - Няма

Attribute	Type	Description
basketId	String	ID of the corresponding signing basket object.

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current signing basket transaction.

Request body - Няма

Response Code

The HTTP response code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
payments	array of paymentId	Optional	payment initiations which shall be authorised through this signing basket.
consents	array of consentId	Optional	consent objects which shall be authorised through this signing basket.
transactionStatus	Transaction Status	Mandatory	Only the not explicitly payment related codes like RCVD, PATC, ACTC, RJCT are used. For a list of all transactionStatus codes permitted for signing baskets, cp. Section 8.3.
_links	Links	Optional	The ASPSP might integrate hyperlinks to indicate next (authorisation) steps to be taken. Type of links admitted in

Attribute	Type	Condition	Description
			this response, (further links might be added for ASPSP defined extensions):

Example

Request

```
GET https://api.testbank.com/v1/signing-baskets/1234-basket-567
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:05:46 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{
  "payments": ["1234pay567", "1234pay568", "1234pay888"],
  "transactionStatus": "ACTC"
}
```

8.3. Заявка за статус на кошница за подпис

Повикване:

```
GET /v1/signing-baskets/{basketId}/status
```

Изисква да се върне статуса на кошницата

Path Parameters

Attribute	Type	Description
basketId	String	ID of the corresponding signing basket object.

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current signing basket transaction.

Request Body - Няма

Response Code

The HTTP response code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	Only the codes RCVD, ACTC, PATC, CANC or RJCT are supported for signing baskets. For a list of all transactionStatus codes permitted for signing baskets, cp. Section 8.3.

Example

Request

GET <https://api.testbank.com/v1/signing-baskets/1234-basket-567/status>

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 06 Aug 2017 15:05:49 GMT

Response

HTTP/1.x 200 Ok

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 06 Aug 2017 15:05:51 GMT

Content-Type: application/json

```
{
  "transactionStatus": "ACTC"
}
```

8.4. Множествена ЗУИ при подпис на кошница

Заявката за създаване на кошницата за подпис, определена по-горе, е независима от необходимостта от обработка на една или повече нива на ЗУИ т.е. независимо от броя на авторизациите, необходими за изпълнението на всички транзакции, съдържащи се в кошницата.

Отговорът за създаване на кошница за подпис с едно ниво на ЗУИ беше дефиниран по-горе в този раздел. По-долу е обяснен процеса при множествена ЗУИ в съобщението "Създаване на кошница за подпис".

Изборът на ЗУИ метод не се поддържа чрез хипервръзка в отговора. Стартът на множествена авторизация за всички методи е еднакъв. В този случай най-напред трябва да се генерира под-ресурс за авторизация, следван от връзката "startAuthorisation".

Response body при Множествена ЗУИ

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	The non payment related values defined in Section 14.23 might be used like RCVD, ACTC, PATC, CANC or RJCT
basketId	String	Mandatory	Resource identification of the generated signing basket resource.
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. The actual hyperlinks used in the response depend on the dynamical decisions of the ASPSP when processing the request. Remark: All links can be relative or full links, to be decided by the ASPSP. Type of links admitted in this response, (further links might be added for ASPSP defined extensions):
			"startAuthorisation": In case, where an explicit start of the transaction authorization is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded).
			"startAuthorisationWithPsuIdentification": The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the PSU identification data.
			"startAuthorisationWithPsuAuthentication": The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the PSU authentication data.
			"startAuthorisationWithEncryptedPsuAuthentication": The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the encrypted PSU authentication data.
			"self": The link to the payment initiation resource created by this request. This link can be used to retrieve the resource data.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU
tppMessages	Array of TPP Message Information	Optional	Messages to the TPP on operational issues.

8.5. Анулиране на кошница за подпис (Cancellation of Signing Baskets)

Анулирането на кошницата за подпис е разрешено докато няма (или има частична) авторизация за кошницата за подписване.

Повикване:

DELETE /v1/signing-baskets/{basketId}

Изтрива създадена кошница за подпис, докато не е оторизирана

Path Parameters - Няма

Attribute	Type	Description
-----------	------	-------------

basketId	String	ID of the corresponding signing basket object to be deleted.
----------	--------	--

Query Parameters - Няма

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based SCA has been used in a pre-step.

Request body - Няма

Response Code

The HTTP response code is 204 in case of successful deletion.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body - Няма

Example

Request

```
DELETE https://api.testbank.com/v1/signing-baskets/qwer3456tzui9876
X-Request-ID 99391c7e-ad88-49ec-a2ad-99ddcb1f7757
Date Sun, 13 Aug 2017 17:05:37 GMT
```

Response

```
HTTP/1.x 204 No Content
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757
Date: Sun, 13 Aug 2017 17:05:38 GMT
```

9. Комбиниране на информационни и платежни услуги

(Combination of AIS and PIS Services)

Изпълнението на сесиите в смисъла на комбинация от AIS и PIS услуги е незадължителна характеристика на този интерфейс. В случай, че ДПУОС поддържа тази функционалност, то трябва да даде ясна информация за това чрез своята PSD2 документация.

Тази функция може да е от значение, когато са необходими информационни услуги за сметка в рамките на инициране на плащания, особено за банките които използват пакетни обработки (batch booking). В този случай е необходимо съгласие за достъп до съответната информация за профила, вж. Раздел 6.4. Съответният метод GET за четене на данните в профила използва параметъра Header "Consent-ID".

ДПУ може да използва като параметър идентификационния номер на съгласието в метода POST при прилагане на искането за инициране на плащане (Раздел 5.3.). Предпоставка за използване на идентификационния номер на съгласието в последващото искане за инициране на плащане е, че е зададен флаг "combinedServiceIndicator" в искането за съгласие за информация за сметка, Раздел 6.3.1.

Използването на "Consent-ID" в последващото Инициране на плащане след това ще доведе до това, че няма да се поиска отново първи фактор за удостоверяване. Така че ДПУОС няма отново да предостави връзка за удостоверяване на Ползвателя. В случай на освобождаване от ЗУИ за съответното плащане, това може да доведе до ситуация, при която не е необходимо допълнително удостоверяване на Ползвателя - плащането ще бъде извършено без допълнително потвърждение.

В случай на освобождаване от ЗУИ за съответното плащане (изключения по смисъла на Директивата), плащането ще бъде изпълнено без по-нататъшно потвърждение.

В случай на метод OAuth2, съответните достъпи чрез токън трябва да поддържат аналогично тази функция.

10. Потвърждение за наличност на средства по сметка

10.1. Установяване на съгласие за Потвърждение за наличност на средства по сметка

Процесът за установяване на съгласие за Потвърждаване за наличност на средства по сметка е същият, както при установяване на съгласие за Информация по сметка.

Установяването на това съгласие не е задължително да се предоставя от XS2A интерфейса според Article 65 (b), [PSD2], защото то също може да функция на онлайн банкирането или дори хартиено базиран процес. Допълнителната услуга описана тук предлага установяване на съгласие за Потвърждение за наличност на средства като част от XS2A интерфейса.

Първо се установява съгласие като Ползвателя дава съгласие на ДПУОС да предостави на ДПУ (PIISP) достъп до конкретна сметка.

След това съгласието се авторизира/подписва през ДПУОС чрез ЗУИ.

Резултатът от процеса е ресурс на съгласието. Адрес на ресурса е върнат на ДПУ и то може да го достъпва чрез GET заявка. Обектът на съгласието съдържа детайли за сметката, валидност и Consent-ID.

Създаденото съгласие може да се използва имплицитно или експлицитно:

- Ако API-то funds-confirmations не поддържа Consent-ID, тогава съответното за Ползвателя съгласие се проверява вътрешно в ДПУОС;
- Ако ДПУОС предоставя API за съгласие за Потвърждение за наличност, тогава Consent-ID се предава в поле на HTTP хедъра.

10.1.1. Общ преглед на данните в услугата „Установяване на съгласие за Потвърждение за наличност на средства по сметка“

Използва се същия модел на данни, описан в услугата „Информация по сметка“.

10.1.2. Особеност при съгласие за Потвърждение за наличност по много-валутна сметка

Съгласието съдържа сметка, за която то е дадено. Валутата на сметката е незадължително поле в обекта за сметка.

В случай на много-валутна сметка се има предвид, че е адресирана сметката с валутата по подразбиране, ако не е указана валута в заявката на ДПУ. Сметката с валутата по подразбиране се определя от ДПУОС.

10.1.3. Заявка за установяване на съгласие

Повикване

POST /v2/consents/confirmation-of-funds

Създава Съгласие в ДПУОС относно Потвърждение за наличност до конкретно посочената сметка в заявката.

Няма странични ефекти

За разлика от установяване на съгласие за Информация по сметка, няма странични ефекти при установяване на съгласие за Потвърждение за наличност.

Query parameters

Няма Query parameters

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
PSU-ID	String	Conditional	Client ID of the PSU in the ASPSP client interface. Might be mandated in the ASPSP's documentation. It might be contained even if an OAuth2 based authentication was performed in a pre-step In this case the ASPSP might check whether PSU-ID and token match, according to ASPSP documentation.
PSU-ID-Type	String	Conditional	Type of the PSU-ID, needed in scenarios where PSUs have several PSU-IDs as access possibility.
PSU-Corporate-ID	String	Conditional	Might be mandated in the ASPSP's documentation. Only used in a corporate context.
PSU-Corporate-ID-Type	String	Conditional	Might be mandated in the ASPSPs documentation. Only used in a corporate context.
PSU-IP-Address	String	Mandatory	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. If not available, the TPP shall use the IP Address used by the TPP when submitting this request.
Authorization	String	Conditional	If OAuth2 has been chosen as pre-step to authenticate the PSU.
TPP-Redirect-Preferred	Boolean	Optional	If it equals "true", the TPP prefers a redirect over an embedded SCA approach. If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU.
TPP-Redirect-URI	String	Conditional	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandatory for the SCA OAuth Approach.
TPP-Nok-Redirect-URI	String	Optional	
TPP-Explicit-Authorisation-Preferred	Boolean	Optional	If it equals "true", the TPP prefers to start the authorisation process separately, e.g. because of the usage of a signing basket. This preference might be ignored by the ASPSP, if a signing basket is not supported as functionality. If it equals "false" or if the parameter is not used, there is no preference of the TPP. This especially indicates that the TPP assumes a direct authorisation.
TPP-Notification-URI	String	Optional	URI for the Endpoint of the TPP-API to which the status of the consent should be sent. This header field may by ignored by the ASPSP, cp. also the extended service definition in [XS2A-RSNS].

Attribute	Type	Condition	Description
TPP-Notification-Content-Preferred	String	Optional	The string has the form status=X1, ..., Xn where Xi is one of the constants SCA, PROCESS, LAST and where constants are not repeated. The usage of the constants supports the following semantics: SCA: A notification on every change of the scaStatus attribute for all related authorisation processes is preferred by the TPP. PROCESS: A notification on all changes of consentStatus or transactionStatus attributes is preferred by the TPP. LAST: Only a notification on the last consentStatus or transactionStatus as available in the XS2A interface is preferred by the TPP. This header field may be ignored, if the ASPSP does not support resource notification services for the related TPP.
TPP-Brand-Logging-Information	String	Optional	This header might be used by TPPs to inform the ASPSP about the brand used by the TPP towards the PSU. This information is meant for logging entries to enhance communication between ASPSP and PSU or ASPSP and TPP. The ASPSP might ignore this field.

Request body

Attribute	Type	Condition	Description
access	Account Access	Mandatory	Requested access services.
cardNumber	Max35Text	Optional	Card Number of the card issued by the PIISP. Should be delivered if available.
cardExpiryDate	ISODate	Optional	Expiry date of the card issued by the PIISP
cardInformation	Max140Text	Optional	Additional explanation for the card product.

Response Code

HTTP Response Code equals 201.

Response Header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource.
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-SCA-Approach	String	Conditional	Possible values are: - EMBEDDED - DECOUPLED - REDIRECT OAuth will be subsumed by the constant value REDIRECT

Response body

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	authentication status of the consent

Attribute	Type	Condition	Description
consentId	String	Conditional	Identification of the consent resource as it is used in the API structure Shall be contained, if a consent resource was generated.
scaMethods	Array of Authentication Objects	Conditional	This data element might be contained, if SCA is required and if the PSU has a choice between different authentication methods. Depending on the risk management of the ASPSP this choice might be offered before or after the PSU has been identified with the first relevant factor, or if an access token is transported. If this data element is contained, then there is also a hyperlink of type "selectAuthenticationMethods" contained in the response body. These methods shall be presented towards the PSU for selection by the TPP.
chosenSca Method	Authentication Object	Conditional	This data element is only contained in the response if the APSPS has chosen the Embedded SCA Approach, if the PSU is already identified with the first relevant factor or alternatively an access token, if SCA is required and if the authentication method is implicitly selected.
challengeData	Challenge	Conditional	It is contained in addition to the data element chosenScaMethod if challenge data is needed for SCA.
			In rare cases this attribute is also used in the context of the updatePsuAuthentication link.
_links	Links	Mandatory	A list of hyperlinks to be recognised by the TPP. Type of links admitted in this response (which might be extended by single ASPSPs as indicated in its XS2A documentation): "scaRedirect" : In case of an SCA Redirect Approach, the ASPSP is transmitting the link to which to redirect the PSU browser. "scaOAuth" : In case of an OAuth2 based Redirect Approach, the ASPSP is transmitting the link where the configuration of the OAuth2 Server is defined. "startAuthorisation" : In case, where an explicit start of the transaction authorisation is needed, but no more data needs to be updated (no authentication method to be selected, no PSU identification nor PSU authentication data to be uploaded). "startAuthorisationWithPsuIdentification" : The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU identification data. "startAuthorisationWithPsuAuthentication" : The link to the authorisation end-point, where the authorisation sub-resource has to be generated while uploading the PSU authentication data. "startAuthorisationWithEncryptedPsu Authentication" : The link to the authorization end-point, where the authorization sub-resource has to be generated while uploading the encrypted PSU authentication data. "startAuthorisationWithAuthentication MethodSelection" : The link to the authorisation end-point, where the authorisation sub-resource has to be generated while selecting the

Attribute	Type	Condition	Description
			authentication method. This link is contained under exactly the same conditions as the data element "scaMethods". "startAuthorisationWithTransactionAuthorisation": The link to the authorisation end-point, where the authorisation sub-resource has to be generated while authorising the transaction e.g. by uploading an OTP received by SMS. "self": The link to the Establish Account Information Consent resource created by this request. This link can be used to retrieve the resource data. "status": The link to retrieve the transaction status of the account information consent. "scaStatus": The link to retrieve the scaStatus of the corresponding authorisation sub-resource. This link is only contained, if an authorisation sub-resource has been already created.
psuMessage	Max500Text	Optional	Text to be displayed to the PSU, e.g. in a Decoupled SCA Approach

Example

Request

```
POST https://api.testbank.com/v2/consents/confirmation-of-funds
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7756
PSU-IP-Address: 192.168.8.78
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101
Firefox/54.0
Date: Sun, 06 Aug 2017 15:05:37 GMT
{
  "account":
  { "iban": "DE40100100103307118608" },
  "cardNumber": "1234567891234",
  "cardExpiryDate": "2020-12-31",
  "cardInformation": "MyMerchant Loyalty Card",
  "registrationInformation": "Your contract Number 1234 with MyMerchant is completed
with the registration with your bank."
}
```

Response in case of a redirect

```
HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: REDIRECT
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v2/consents/confirmation-of-funds/1234-wertiq-983"
Content-Type: application/json
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "scaRedirect": {"href": "https://www.testbank.com/authentication/1234-wertiq-983"},
    "status": {"href": "/v2/consents/confirmation-of-funds/1234-wertiq-983/status"},
    "scaStatus": {"href": "v2/consents/confirmation-of-funds/1234-wertiq-983/
authorisations/123auth567"}
  }
}
```

Response in case of a redirect with a dedicated start of the authorisation process

```
HTTP/1.x 201 Created
```

```
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: REDIRECT
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v2/consents/confirmation-of-funds/1234-wertiq-983"
Content-Type: application/json
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "startAuthorisation": { "href": "v2/consents/confirmation-of-funds/1234-wertiq-983/authorisations" }
  }
}
```

Response in case of the OAuth2 approach with an implicit generated authorisation resource

```
HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: REDIRECT
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v2/consents/confirmation-of-funds/1234-wertiq-983"
Content-Type: application/json
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "self": { "href": "/v2/consents/confirmation-of-funds/1234-wertiq-983",
    "scaStatus": { "href": "v2/consents/confirmation-of-funds/1234-wertiq-983/authorisations/123auth567" },
    "scaOAuth": { "href": "https://www.testbank.com/oauth/.well-known/oauth-authorization-server" }
  }
}
```

Response in case of the decoupled approach

```
HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: DECOUPLED
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v2/consents/confirmation-of-funds/1234-wertiq-983"
Content-Type: application/json
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "startAuthorisationWithPsuIdentification": { "href": "/v2/consents/confirmation-of-funds/1234-wertiq-983/authorisations" }
  }
}
```

Response in case of the embedded approach

```
HTTP/1.x 201 Created
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-SCA-Approach: EMBEDDED
Date: Sun, 06 Aug 2017 15:05:47 GMT
Location: "v2/consents/confirmation-of-funds/1234-wertiq-983"
Content-Type: application/json
{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "startAuthorisationWithPsuAuthentication": { "href": "/v2/consents/confirmation-of-funds/1234-wertiq-983/authorisations" }
  }
}
```

10.1.4. Искане за състояние на заявката (Get Status Request)

Повикване

GET /v2/consents/confirmation-of-funds/{consentId}/status

Използва се за проверка на състоянието на съгласието за Потвърждение на наличност.

Path Parameters:

Attribute	Type	Description
consentId	String	The consent identification assigned to the created resource.

Query parameters

Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based SCA was performed in the corresponding consent transaction or if OAuth2 has been used in a pre-step.

Request Body

Няма

Response Code

HTTP Response Code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
consentStatus	Consent Status	Mandatory	This is the overall lifecycle status of the consent.

Example

Request

```
GET https://api.testbank.com/v2/consents/confirmation-of-funds/qwer3456tzui7890/status
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
Date: Sun, 06 Aug 2017 15:05:46 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{
  "consentStatus": "valid"
}
```

10.1.5. Заявка за съдържание на съгласието (Get Consent Request)

Повикване

GET /v2/consents/confirmation-of-funds/{consentId}

Връща съдържанието на съгласие по Потвърждение за наличност. Така се подават данните към ДПУ, когато съгласието е директно управлявано между ДПУОС и Ползвателя, напр. в Redirect ЗУИ подход.

Path Parameters:

Attribute	Type	Description
consentId	String	ID of the corresponding consent object as returned by an Account Information Consent Request

Query parameters

Няма

Request header

Същите както при раздел 10.1.4

Request Body

Няма

Response Code

HTTP Response Code equals 200.

Response Header

Същите както при раздел 10.1.4

Response Body

Attribute	Type	Condition	Description
account	Account Reference	Mandatory	Account, where the confirmation of funds service is aimed to be submitted to.
cardNumber	Max35Text	Optional	Card Number of the card issued by the PIISP. Should be delivered if available.
cardExpiryDate	ISODate	Optional	Expiry date of the card issued by the PIISP
cardInformation	Max140Text	Optional	Additional explanation for the card product.
registrationInformation	Max140Text	Optional	Additional registration information.
consentStatus	Consent Status	Mandatory	The status of the consent resource.

Example

Request

GET https://api.testbank.com/v2/consents/confirmation-of-funds/qwer3456tzui7890

Response

```
HTTP/1.x 200 Ok
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:05:47 GMT
Content-Type: application/json
{
  "account":
  { "iban": "DE40100100103307118608" },
  "cardNumber": "1234567891234",
  "cardExpiryDate": "2020-12-31",
  "cardInformation": "MyMerchant Loyalty Card",
  "consentStatus": "valid"
}
```

10.1.6. Множествено ЗУИ при Установяване на съгласие за Потвърждение за наличност по много-валутна сметка

Използва се същия множествен ЗУИ, описан в услугата „Информация по сметка“.

10.1.7. Изтриване на Съгласие за Потвърждение за наличност

TPP може да изтрие съгласието за Потвърждение за наличност при необходимост, чрез следното повикване:

Повикване

DELETE /v2/consents/confirmation-of-funds/{consentId}

Path Parameters:

Attribute	Type	Description
consentId	String	Contains the resource-ID of the consent to be deleted.

Query parameters

Няма

Request header

Същите както при раздел 10.1.4

Request Body

Няма

Response Code

The HTTP response code equals 204 for a successful cancellation.

Response Header

Същите както при раздел 10.1.4

Response Body

Няма

Example

Request

DELETE <https://api.testbank.com/v2/consents/confirmation-of-funds/qwer3456tzui7890>

X-Request-ID 99391c7e-ad88-49ec-a2ad-99ddcb1f7757

Date Sun, 13 Aug 2017 17:05:37 GMT

Response

HTTP/1.x 204 No Content

X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7757

Date: Sun, 06 Aug 2017 15:05:47 GMT

10.2. Общ преглед на данните в услугата „Потвърждение за наличност на средства“

Следната таблица дефинира техническото описание на абстрактния модел на данни, определен в [XS2A OR] за услугата за инициране на плащания. Колоните дават общ поглед върху API протоколите, както следва:

- Колоната "Data element" използва абстрактните елементи на данни, за да достави връзката към правилата и дефинициите на роли.
- Колоната Attribute encoding дава определението за действително кодиране в API XS2A, както е дефинирано в този документ.
- Колоните "Location" определят кога съответните елементи на данните се транспортират като параметри на HTTP на ниво path, header или body и са взети от сертификатите eIDAS.
- Колоната "Usage" дава общ преглед на използването на елементи от данни в различните услуги и API повиквания. В [XS2A OR] обажданията XS2A се описват като абстрактни API повиквания. Тези обаждания ще бъдат технически реализирани като команда HTTPS POST. Обажданията формират повикване за:
 - Заявка за потвърждение (Confirmation Request), която е единствено API повикване в рамките на услугата Потвърждение за наличност на средства.

Използва се следното използване на съкращения в колоните "Location и Usage "

x: Този елемент от данните се транспортира на съответното ниво.

m: Задължително

o: Незадължително за използване от ДПУ

c: Условно. Условието е описано в адресираните при приложния програмен интерфейс (API) за случаи, определени от ДПУОС.

	Data element	Attribute encoding	Location				Usage	
			Path	Header	Body	Web Site Certificate	Conf. Request	Conf. Response
REQUEST PART (TPP)	Provider Identification		x				m	
	Consent-ID			x			c	
	TPP Registration Number					x	m	
	TPP Name					x	m	
	TPP Role					x	m	
	TPP National Competent Authority					x	m	
	Request Identification	X-Request-ID		x			m	m
	TPP Certificate Data	TPP-Signature-Certificate		x			c	
	Further signature related data	Digest		x			c	
	TPP Electronic Signature	Signature		x			c	
	Card Number	cardNumber			x		o	
	Account Number	account			x		m	
	Name Payee	payee			x		o	
	Transaction Amount	instructedAmount			x		m	
Response (ASP)	Request Identification	X-Request-ID		x			m	m

	TPP Message Information	tppMessages			x			o
--	-------------------------	-------------	--	--	---	--	--	---

10.3. Механизъм на Потвърждение за наличност на средства

Повикване

POST /v1/funds-confirmations

Създава заявка за потвърждение на средства в ДПУОС.

Query Parameters - Няма

Request header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Consent-ID	string	Conditional	Shall be provided if the consent of the PSU has been provided through the consent process as defined in [XS2A-COFC]. Otherwise not used.
Digest	cp. Section Error! Reference source not found.	Conditional	Is contained if and only if the "Signature" element is contained in the header of the request.
Signature	cp Section Error! Reference source not found.	Conditional	A signature of the request by the TPP on application level. This might be mandated by ASPSP.
TPP-Signature-Certificate	String	Conditional	The certificate used for signing the request, In base64 encoding.
Authorization	String	Optional	This field might be used in case where a consent was agreed between ASPSP and PSU through an OAuth2 based protocol, facilitated by the TPP.

Request body

Attribute	Type	Condition	Description
cardNumber	String	n.a	The request might be rejected If present.
account	Account Reference	Mandatory	PSU's account number.
payee	Max70Text	Optional	The merchant where the card is accepted as an information to the PSU.
instructedAmount	Amount	Mandatory	Transaction amount to be checked within the funds check mechanism.

Response code

The HTTP response code equals 200

Response header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response body

Attribute	Type	Condition	Description
fundsAvailable	Boolean	Mandatory	Equals "true" if sufficient funds are available at the time of the request, "false" otherwise.

При интерпретирането на Искането за Потвърждение на средствата за много-валутни сметки се прилагат следните правила:

- Допълнителен номер на карта може да отговаря на под-сметка (валута).
- Ако няма номер на картата, но се съдържа Идентификаторът на Ползвателя - по подразбиране се проверява сметката на клиента.
- Ако няма номер на картата, но се съдържа Идентификатор на Ползвателя, Идентификатора на Сметката и Код на валутата – проверява се наличността на средства в съответната под-сметка.
- Ако се съдържат Номера на картата* и Идентификаторът на потребителската Сметка - проверява се под-сметката, адресирана към картата.
- Ако Номерът на картата* не е регистриран към под-сметка, или Номерът на картата* е регистриран към друга под-сметка, то номерът на картата се игнорира и се проверява наличността по сметката.

*Номер на карта не може да се подава в явен вид. Ако не се ползва маска за това поле, заявката може да бъде отхвърлена.

Example

Request

```
POST https://api.testbank.com/v1/funds-confirmations
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date: Sun, 06 Aug 2017 15:02:37 GMT
{
  "account": {"iban": "DE23100120020123456789"},
  "instructedAmount": {"currency": "EUR", "amount": "123"}
}
```

Response

```
{"fundsAvailable": "true"}
```

11. Структура на основни платежни продукти

Стандартът определя структурите на платежните продукти, които трябва да се поддържат от ДПУОС. Трябва да се обърне внимание на факта че структурите на основните продукти за плащане на европейския пазар са разширени с цел съвместимост към местните специфики.

11.1. Единично плащане

11.1.1. Структура в JSON формат

National standard Single Payments	The following table gives an overview on the Bulgarian National standard generic defined JSON structures of standard payment products for single payments.			
Data Element	Type	sepa-credit-transfers (SCT)	cross-border-transfers (non SEPA)	instant-sepa-credit-transfers (SCT Inst)
endToEndIdentification	Max35Text	optional	optional	optional
debtorAccount (incl. type)	Account Reference	optional	optional	optional
debtorId	Max35Text	optional	n.a.	optional
ultimateDebtor	UltimateDebtor Type	optional	n.a.	optional
instructedAmount (inc. Curr.)	Amount	mandatory	mandatory	mandatory
transactionCurrency *	Currency Code	n.a.	n.a.	n.a.
creditorAccount	Account Reference	mandatory	mandatory	mandatory
creditorAgent	BICFI	optional	optional	optional
creditorAgentName **	Max140Text	n.a.	optional	n.a.
creditorName	Max70Text	mandatory	mandatory	mandatory
creditorId	Max35Text	optional	n.a.	optional
creditorAddress	Address	optional	mandatory	optional
ultimateCreditor	Max70Text	optional	n.a.	optional
purposeCode*	Purpose Code	n.a.	n.a.	n.a.
chargeBearer	Charge Bearer Code	optional	conditional	n.a.
remittanceInformationUnstructured	Max140Text	optional	optional	optional
remittanceInformation UnstructuredArray *	Array of Max140Text	n.a.	n.a.	n.a.
remittanceInformationStructured *	Remittance	n.a.	n.a.	n.a.
requestedExecutionDate *	ISODate	n.a.	n.a.	n.a.
requestedExecutionTime *	ISODateTime	n.a.	n.a.	n.a.
serviceLevel	Service Level Code	optional	optional	n.a.

* Маркираните полета не са приложими за текущата версия на стандарт БИСТРА, но е възможно да се използват в следващи версии

** Атрибутите се подават със стойност само в случаите, когато сметката на получателя не е в IBAN формат и за Банката на получателя не е предоставен SWIFT BIC.

Account Reference

Attribute	Type	Condition	Description
iban	IBAN	Conditional	
bban	BBAN	Conditional	payment accounts without IBAN
pan *	String	n.a.	
maskedPan	String	Conditional	

msisdn	String	Conditional	
currency	Currency Code	optional	

* С цел опростяване на архитектурните решения изисквани от PCI DSS, в тази версия на стандарта, атрибут rap не се използва.

Amount

Attribute	Type	Condition	Description
currency	Currency Code	Mandatory	ISO 4217 code
content	Floating Point Number	Mandatory	The decimal separator is a dot.

Address

Attribute	Type	Condition	Description
street	Max70Text	Optional	
buildingNumber	String	Optional	
city	String	Optional	
postalCode	String	Optional	
country	Country Code	Mandatory	

Remittance

Attribute	Type	Condition	Description
reference	Max35Text	Mandatory	The actual reference
referenceType	Max35Text	Optional	
referenceIssuer	Max35Text	Optional	

Ultimate Debtor Type

Attribute	Type	Condition	Description
Tax Type-Tax Id-Payment Category	Max70Text	conditional	- Tax Type (Tax Type Code) – Mandatory, if position 13 in creditor account is equal to "8". - Tax Id (9, 10 or 13 digits) – Mandatory, if position 13 in creditor account is equal to "8". - Payment Category (6 digit code) – May be used, if positions 13 and 14 in creditor account are equal to "8" and "4".

Codes Table

Code attribute	Type	Description
Service Level Code	String 4 letters	SEPA - Used for SEPA payment URGP – Used for payments through RTGS System SDVA – Used for Cross border CT. Payment must be executed with same day value to the creditor. NEXT - Used for Cross border CT. Payment must be executed with next working day value to the creditor SPOT - Used for Cross border CT. Payment must be executed with spot working day value to the creditor INST – Used for instant payments (SEPA instant payments)

Charge Bearer Code	String 4 letters	DEBT - Borne By Debtor CRED - Borne By Creditor SHAR - Shared In Credit Transfer context SLEV - Used for SEPA payments
Tax Type Code	String 3 letters	EGH / EGN - Personal ID EIK / EIK - Corporate ID LNC / LNC - Foreign Person ID

Examples

1. SEPA credit transfer

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "chargeBearer": "SLEV",
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "DE23100120020123456789"},
  "remittanceInformationUnstructured": "Information for Merchant and payment"
}
```

2. SEPA credit transfer (budget transfer)

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver TD NRA SOFIA",
  "creditorAccount": {"iban": "BG47BNBG96668123456789"},
  "ultimateDebtor": "EGN-9904281234-110000",
  "remittanceInformationUnstructured": "Tax payment ZDDFL info"
}
```

3. SEPA credit transfer (instant transfer)

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "paymentType": {"ServiceLevel": "INST"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "BG96BGBK43210123456789"},
  "remittanceInformationUnstructured": "Information for Merchant and payment"
}
```

4. SEPA credit transfer (with URGP marker for RTGS)

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "serviceLevel": "URGP",
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "BG96BGBK43210123456789"},
  "remittanceInformationUnstructured": "Information for Merchant and payment"
}
```

5. Cross border credit transfer

Request Body with IBAN present on SPOT value date

```
{
```

```

    "instructedAmount": {"currency": "USD", "amount": "123.50"},
    "paymentType": "SPOT",
    "chargeBearer": "SHAR",
    "debtorAccount": {"iban": "BG94BANK12341234567890"},
    "creditorName": "Receiver Merchant123",
    "creditorAccount": {"iban": "TR73TURKBANK000000001234567890"},
    "creditorAddress": {"country": "TR", "city": "Istanbul", "street": "Main Street 25"},
    "remittanceInformationUnstructured": "Information for Merchant and payment"
}

```

Request Body without IBAN and SWIFT BIC for Creditor Agent and NEXT value date

```

{
    "instructedAmount": {"currency": "USD", "amount": "123.50"},
    "paymentType": "NEXT",
    "chargeBearer": "SHAR",
    "debtorAccount": {"iban": "BG94BANK12341234567890"},
    "creditorAccount": {"bban": "0123456789"},
    "creditorAgentName": "BANK Name of the Merchant, Turkey, Istanbul, 21 Central street",
    "creditorName": "Receiver Merchant123",
    "creditorAddress": {"country": "TR", "city": "Istanbul", "street": "Main Street 25"},
    "remittanceInformationUnstructured": "Information for Merchant and payment"
}

```

6. Instant SEPA credit transfer

Request Body

```

{
    "instructedAmount": {"currency": "EUR", "amount": "123.50"},
    "debtorAccount": {"iban": "BG94BANK12341234567890"},
    "creditorName": "Receiver Merchant123",
    "creditorAccount": {"iban": "BG96BGBK43210123456789"},
    "remittanceInformationUnstructured": "Information for Merchant and payment"
}

```

11.1.2. Структура в XML ISO20022 код

Level	Data elements	ISO	Type	Description	BGN Budget Transfer	BGN Credit Transfer	SEPA Credit Transfer	Cross-border CT
1	<GrpHdr>	[1..1]		GroupHeader	M	M	M	M
1.1	<MsgId>	[1..1]	Text	MessageIdentification	M	M	M	M
1.2	<CreDtTm>	[1..1]	DateTime	CreationDateTime	M	M	M	M
1.3	<NbOfTx>	[1..1]	Text	NumberOfTransactions	M	M	M	M
1.4	<CtrlSum>	[0..1]	Quantity	ControlSum	M	M	M	M
1.5	<InitgPty>	[1..1]	±	InitiatingParty	Opt	Opt	Opt	Opt
1.5.1	<Nm>	[0..1]	Text	Name	Opt	Opt	Opt	Opt
1.5.2	<PstlAdr>	[0..1]	±	PostalAddress	Opt	Opt	Opt	Opt
1.5.2.1	<StrtNm>	[0..1]	Text	StreetName	Opt	Opt	Opt	Opt
1.5.2.2	<BldgNb>	[0..1]	Text	BuildingNumber	Opt	Opt	Opt	Opt
1.5.2.3	<PstCd>	[0..1]	Text	PostCode	Opt	Opt	Opt	Opt
1.5.2.4	<TwnNm>	[0..1]	Text	TownName	Opt	Opt	Opt	Opt
1.5.2.5	<Ctry>	[0..1]	CodeSet	Country	Opt	Opt	Opt	Opt
1.5.3	<Id>	[0..1]	±	Identification	Opt	Opt	Opt	Opt
1.5.3.1	<OrgId> <PrvtId>	[1..1]	±	Organisation Identification <OrgId> [1..1] ± Or} Private Identification <PrvtId> [1..1] ±	Opt	Opt	Opt	Opt
2	<PmtInf>	[1..*]		Payment Information	M	M	M	M
2.1	<PmtInfId>	[1..1]	Text	Payment Information Identification	M	M	M	M
2.2	<PmtMtd>	[1..1]	CodeSet	Payment Method	M	M	M	M
2.4	<PmtTpInf>	[0..1]	±	Payment Type Information	M	n.a.	n.a.	n.a.
2.4.1	<CtgyPurp>	[0..1]		CategoryPurpose	M	n.a.	n.a.	n.a.
2.4.1.1	<Cd>	[1..1]	Text	Constant "GOVT"	M	n.a.	n.a.	n.a.
2.4.2	<SvcLvl>	[0..1]	±	Service Level	Opt	Opt	Opt	Opt
2.4.2.1	<Cd>	[1..1]	CodeSet	Code	Opt	Opt	Opt	Opt
2.5	<Dbtr>	[1..1]	±	Debtor	M	M	M	M
2.5.1	<Nm>	[0..1]	Text	Name	M	M	M	M
2.5.2	<PstlAdr>	[0..1]	±	PostalAddress	M	M	M	M
2.5.2.1	<StrtNm>	[0..1]	Text	StreetName	Opt	Opt	Opt	Opt
2.5.2.2	<BldgNb>	[0..1]	Text	BuildingNumber	Opt	Opt	Opt	Opt
2.5.2.3	<PstCd>	[0..1]	Text	PostCode	Opt	Opt	Opt	Opt
2.5.2.4	<TwnNm>	[0..1]	Text	TownName	Opt	Opt	Opt	Opt
2.5.2.5	<Ctry>	[0..1]	CodeSet	Country	M	M	M	M
2.5.3	<Id>	[0..1]	±	Identification	M	M	M	M
2.5.3.1	<OrgId> <PrvtId>	[1..1]	±	Organisation Identification <OrgId> [1..1] ± Or} Private Identification <PrvtId> [1..1] ±	M	M	M	M
2.6	<DbtrAcct>	[1..1]	±	DebtorAccount	M	M	M	M
2.6.1	<Id>	[1..1]	±	Identification	M	M	M	M
2.6.1.1	<IBAN>	[1..1]	IdentifierSet	IBAN	M	M	M	M

2.7	++<DbtrAgt>	[1..1]	±	DebtorAgent	M	M	M	M
2.7.1	+++<FinInstnId>	[1..1]	±	Financial Institution Identification	M	M	M	M
2.7.1.1	++++<BICFI>	[0..1]	IdentifierSet	BICFI	M	M	M	M
2.7.1.2	++++<Nm>	[0..1]	Text	Name	M	M	M	M
2.7.1.3	++++<PstlAdr>	[0..1]	±	PostalAddress	Opt	Opt	Opt	Opt
2.7.1.3.1	++++<StrtNm>	[0..1]	Text	StreetName	Opt	Opt	Opt	Opt
2.7.1.3.2	++++<BldgNb>	[0..1]	Text	BuildingNumber	Opt	Opt	Opt	Opt
2.7.1.3.3	++++<PstCd>	[0..1]	Text	PostCode	Opt	Opt	Opt	Opt
2.7.1.3.4	++++<TwnNm>	[0..1]	Text	TownName	Opt	Opt	Opt	Opt
2.7.1.3.5	++++<Ctry>	[0..1]	CodeSet	Country	BG	BG	BG	BG
2.8	++<CdtTrfTxInf>	[1..*]		Credit Transfer Transaction Information	M	M	M	M
2.8.1	+++<PmtId>	[1..1]		PaymentIdentification	M	M	M	M
2.8.1.1	++++<InstrId>	[0..1]	Text	InstructionIdentification	Opt	Opt	Opt	Opt
2.8.1.2	++++<EndToEndId>	[0..1]	Text	EndToEndIdentification	Opt	Opt	Opt	Opt
2.8.2	+++<Amt>	[1..1]	Text	Amount	M	M	M	M
2.8.2.1	++++<InstdAmt Ccy="AAA">	[1..1]	Amount	InstructedAmount	"BGN"	"BGN"	"EUR"	M
2.8.3	+++<ChrgBr>	[0..1]	CodeSet	ChargeBearer DEBT BorneByDebtor CRED BorneByCreditor SHAR Shared In a Credit Transfer context SLEV - in case of SEPA pmnt	Opt	Opt	Opt	M
2.8.4	+++<CdtrAgt>	[1..1]	±	CreditorAgent	M	M	M	M
2.8.4.1	++++<FinInstnId>	[1..1]	±	Financial Institution Identification	M	M	M	M
2.8.4.1.1	++++<BICFI>	[0..1]	IdentifierSet	BICFI	M	M	M	Opt
2.8.4.1.2	++++<Nm>	[0..1]	Text	Name	M	M	M	M
2.8.4.1.3	++++<PstlAdr>	[0..1]	±	PostalAddress	Opt	Opt	Opt	Opt
2.8.4.1.3.1	++++<StrtNm>	[0..1]	Text	StreetName	Opt	Opt	Opt	Opt
2.8.4.1.3.2	++++<BldgNb>	[0..1]	Text	BuildingNumber	Opt	Opt	Opt	Opt
2.8.4.1.3.3	++++<PstCd>	[0..1]	Text	PostCode	Opt	Opt	Opt	Opt
2.8.4.1.3.4	++++<TwnNm>	[0..1]	Text	TownName	Opt	Opt	Opt	Opt
2.8.4.1.3.5	++++<Ctry>	[0..1]	CodeSet	Country	M	M	M	M
2.8.5	+++<Cdtr>	[0..1]	±	Creditor	M	M	M	M
2.8.5.1	++++<Nm>	[0..1]	Text	Name	M	M	M	M
2.8.5.2	++++<PstlAdr>	[0..1]	±	PostalAddress	M	M	M	Opt
2.8.5.2.1	++++<StrtNm>	[0..1]	Text	StreetName	Opt	Opt	Opt	Opt
2.8.5.2.2	++++<BldgNb>	[0..1]	Text	BuildingNumber	Opt	Opt	Opt	Opt
2.8.5.2.3	++++<PstCd>	[0..1]	Text	PostCode	Opt	Opt	Opt	Opt
2.8.5.2.4	++++<TwnNm>	[0..1]	Text	TownName	Opt	Opt	Opt	Opt
2.8.5.2.5	++++<Ctry>	[0..1]	CodeSet	Country	Opt	Opt	Opt	Opt
2.8.6	+++<CdtrAcct>	[0..1]	±	CreditorAccount	M	M	M	M
2.8.6.1	++++<Id>	[1..1]	±	Identification	M	M	M	Opt
2.8.6.1.1	++++<IBAN>	[1..1]	IdentifierSet	IBAN	M	M	M	Opt
2.8.6.1.2	++++<Othr>	[1..1]		Other	n.a.	n.a.	n.a.	Opt
2.8.6.1.2.1	++++<Id>	[1..1]	Text	Identification	n.a.	n.a.	n.a.	Opt

2.8.8	+++<Tax>	[0..1]		Tax	Opt	n.a.	n.a.	n.a.
2.8.8.1	++++<Dbtr>	[0..1]		Debtor	Opt	n.a.	n.a.	n.a.
2.8.8.1.1	++++<TaxId>	[0..1]	Text	TaxIdentification	Cond	n.a.	n.a.	n.a.
2.8.8.1.2	++++<TaxTp>	[0..1]	Text	TaxType EGN / EIK / PNF	Cond	n.a.	n.a.	n.a.
2.8.8.1.3	++++<Authstn>	[0..1]		Authorisation	Opt	n.a.	n.a.	n.a.
2.8.8.1.3.1	++++<Nm>	[0..1]	Text	Name	Opt	n.a.	n.a.	n.a.
2.8.8.2	+++<Rcrd>	[0..*]		Record	Opt	n.a.	n.a.	n.a.
2.8.8.2.1	++++<Ctgy>	[0..1]	CodeSet	Payment Category	Opt	n.a.	n.a.	n.a.
2.8.9	+++<RmtInf>	[0..1]		Remittance Information	M	M	M	M
2.8.9.1	++++<Ustrd>	[0..*]	Text	Unstructured	M	M	M	M

11.2. Периодично плащане / Плащане с бъдещ вальор

Периодично плащане - Request Body

ДПУОС трябва да посочи в своята спецификация дали приема този вид плащания. Структурата на тези плащания може да включва всеки tag на основното плащане (раздел 11.1.1.) като в допълнение се използват маркерите описани в раздел 5.3.4.

Плащане с бъдещ вальор - Request Body

ДПУОС трябва да посочи дали приема този вид плащания. Структурата на тези плащания може да включва всеки tag на основното плащане (раздел 11.1.1.) като в допълнение се използва специфичния атрибут "requestExecutionDate" като незадължително поле (optional) вместо (n.a).

11.3. Масово плащане

Тази спецификация предлага функция за масово / групово плащане в JSON кодиране като незадължителна крайна точка. Форматът на масовото плащане представлява масив от единични плащания, предшестван от единна платежна информация, приложима към всяко отделно плащане в масива.

Data element	Type	Condition	Description
batchBookingPreferred	String	Optional	If this element equals true, the PSU prefers only one booking entry. If this element equals false, the PSU prefers individual booking of all contained individual transactions. The ASPSP will follow this preference according to contracts agreed on with the PSU.
debtorAccount (incl. type)	Account Reference	Mandatory	
paymentInformationId	Max35Text	n.a.	Unique identification as assigned by the sending party to unambiguously identify this bulk payment. This attribute may be used by ASPSPs or communities as an optional field. Remark for Future: This attribute might be made mandatory in the next version of the specification.
requestedExecutionDate	ISODate	Optional	If contained, the payments contained in this bulk will be executed at the addressed date. This field may not be used together with the field requestedExecutionTime.

Data element	Type	Condition	Description
requestedExecutionTime	ISODateTime	Optional	If contained, the payments contained in this bulk will be executed at the addressed Date/Time. This field may not be used together with the field requestedExecutionDate.
payments	Bulk Entry	Mandatory	The Bulk Entry Type is a type which follows the JSON formats for the supported products for single payments, see Section 11.1, excluding the data elements • debtorAccount, • requestedExecutionDate, • requestedExecutionTime. These three data elements may not be contained in any bulk entry.

Example

```
{
  "batchBookingPreferred": true,
  "debtorAccount": {"iban": "DE40100100103307118608"},
  "requestedExecutionDate": "2018-08-01",
  "payments":
    [{JSON based payment initiation 1}, {JSON based payment initiation 2}]
}
```

12. Подпис (Signatures)

При случаите в които ДПУОС изисква от ДПУ да се представи с цифров подпис (по дефинициите на [\[signHTTP\]](#)) в блока HTTP-Requests, подписът трябва да покрива изброените по-надолу изисквания съгласно или в допълнение на секция 4 [\[signHTTP\]](#)

12.1. Задължителна заглавка "Digest"

Когато ДПУ се представи с цифров подпис, задължително трябва да включи и Digest заглавка по дефиницията на [\[RFC3230\]](#). Тя трябва да съдържа шифриран (Hash) низ, изчислен от тялото на съобщението. Ако съобщението не съдържа тяло (body), Digest заглавката трябва да съдържа хеша (hash) на празното съобщение. Алгоритмите, които могат да бъдат използвани за изчисляване на Digest в контекста на тази спецификация, са SHA-256 и SHA-512, както е дефинирано в [\[RFC5843\]](#).

12.2. Изисквания в заглавка "Signature"

Както е дефинирано в Секция 4, заглавка "Signature / Подпис" трябва да присъства задължително. Структурата на заглавката на "Подпис" е дефинирана в [\[signHTTP\]](#), секция 4.1.2.2, а в следващата таблица са изброени изискванията към заглавката "Signature" от [\[signHTTP\]](#) и допълнителните изисквания, специфични за PSD2-интерфейса.

Elements of the "Signature" Header				
Element	Type	Condition	Requirement Error! Reference source not found.	Additional Requirement
keyId	String	Mandatory	The keyId field is a string that the server can use to look up the component they need to validate the signature.	Serial Number of the TPP's certificate included in the "TPP-Signature-Certificate" header of this request. It shall be formatted as follows: keyId="SN=XXX,CA=YYYYYYYYYYYYYYYY" where "XXX" is the serial number of the certificate in hexadecimal coding given in the TPP-Signature-Certificate-Header and "YYYYYYYYYYYYYYYY" is the full Distinguished Name of the Certification Authority having produced this certificate.

Elements of the "Signature" Header				
Element	Type	Condition	Requirement Error! Reference source not found.	Additional Requirement
Algorithm	String	Mandatory (Optional in [signHTTP])	The "Algorithm" parameter is used to specify the digital signature algorithm to use when generating the signature. Valid values for this parameter can be found in the Signature Algorithms registry located at http://www.iana.org/assignments/signature-algorithms and MUST NOT be marked "deprecated". It is preferred that the algorithm used by an implementation be derived from the key metadata identified by the 'keyId' rather than from this field. [...]The 'algorithm' parameter [...] will most likely be deprecated in the future.	Mandatory The algorithm must identify the same algorithm for the signature as described for the TPP's public key (Subject Public Key Info) in the certificate (Element "TPP-Signature-Certificate") of this Request. It must identify SHA-256 or SHA-512 as Hash algorithm.
Headers	String	Mandatory (Optional in [signHTTP])	The "Headers" parameter is used to specify the list of HTTP headers included when generating the signature for the message. If specified, it should be a lowercased, quoted list of HTTP header fields, separated by a single space character. If not specified, implementations MUST operate as if the field were specified with a single value, the `Date` header, in the list of HTTP headers. Note that the list order is important, and MUST be specified in the order the HTTP header field-value pairs are concatenated together during signing.	Mandatory. Must include • "digest", • "x-request-id", Must conditionally include • "psu-id", if and only if "PSU-ID" is included as a header of the HTTP-Request. • "psu-corporate-id", if and only if "PSU-Corporate-ID" is included as a header of the HTTP-Request. • "tpp-redirect-uri", if and only if "TPP-Redirect-URI" is included as a header of the HTTP-Request. No other entries may be included. Remark: It is intended to introduce a new http header in a coming version. This new header shall indicate the creation date of a request on the side of the TPP. This new header shall also to be included in this "Headers" element.

Elements of the "Signature" Header				
Element	Type	Condition	Requirement Error! Reference source not found.	Additional Requirement
Signature	String	Mandatory	The "signature" parameter is a base 64 encoded digital signature, as described in RFC 4648 [RFC4648] , Section 4. The client uses the `algorithm` and `headers` signature parameters to form a canonicalised `signing string`. This `signing string` is then signed with the key associated with `keyId` and the algorithm corresponding to `algorithm`. The `signature` parameter is then set to the base 64 encoding of the signature.	[No additional Requirements]

Example

Когато ДПУ изпраща заявка без подпис (пр.1 в раздел 5.3.1), тя изглежда така:

Request

```
POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Encoding: gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-ID: PSU-1234
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
TPP-Redirect-URI:
    https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&code_Cchallenge_Mmethod="S256"
Date: Sun, 06 Aug 2017 15:02:37 GMT
```

Request Body

```
{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "paymentType": {"ServiceLevel": "URGP"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "BG96BGBK43210123456789"},
  "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

Тялото на съобщението за инициране на плащане може да се изчисли по метод Base64 в символен низ:

```
ew0KImluc3RydWN0ZWRBbW91bnQiOiB7ImN1cnJlbnN5IjogIkJHTiIsICJjb250ZW50IjogIjEyMy41MCMJ9LA0KI
mRlYnRvckFjY291bnQiOiB7ImliYW4iOiAiQkc5NEJBTKsxMjM0MTIzNDU2Nzg5MCMJ9LA0KInBheW11bnRUeXB1Ij
p7IlN1cnZpY2VMZXZlbCIgOiAiVGVHUCJ9LA0KImNyZWVpdG9yTmFtZSI6ICJSZW50IjogIjEyMy41MCMJ9LA0KI
sDQoiY3JlZGl0b3JBY2NvdW50IjogeyJpYmFuIjogIkJHOTZCR0JLNDMyMTAxMjM0NTY3ODkifSwNCiJyZW1pdHRh
bmN1SW5mb3JtYXRpb25VbnN0cnVjdHVyZWQiOiAiUmVmIE51bWJlciBNZXJjaGFudCINCn0=
```

Example

Когато ДПУ изпраща същата заявка с подпис rsa-sha256

Тялото на съобщението за инициране на плащане трябва да бъде преизчислено по алгоритъм SHA-256 в криптиран символен низ (hash):

```
6dea20996b11661f0d41e6fb4c97f7118fdb91b91e7e2697449629ae9f21fe36
```

и след това той да бъде преизчислен по метод Base64 като символен низ за Digest:

NmRlYTIwOTk2YjExNjYxZjBkNDFlNmZiNGM5N2Y3MTE4ZmRiOTFiOTFlN2UyNjk3NDQ5NjI5YWU5ZjIxZmUzNg==

Тогава заявката за инициране на плащане ще има следния вид:

Request

```
POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Encoding: gzip
Content-Type: application/json
X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address: 192.168.8.78
PSU-ID: PSU-1234
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
TPP-Redirect-URI:
    https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&code_Cchallenge_Mmethod="S256"
Date: Sun, 06 Aug 2017 15:02:37 GMT
Digest: SHA-256=
    NmRlYTIwOTk2YjExNjYxZjBkNDFlNmZiNGM5N2Y3MTE4ZmRiOTFiOTFlN2UyNjk3NDQ5NjI5YWU5ZjIxZmUzNg==
Signature:
    keyId="SN=9FA1,CA=CN=D-TRUST%20CA%202-1%202015,O=D-Trust%20GmbH,C=DE",
    algorithm="rsa-sha256",
    headers="Digest X-Request-ID PSU-ID TPP-Redirect-URI Date",
    signature="Base64 (RSA-SHA256 (
        ODA5OTZkNWJmZTU3NDJjMDhlZDk2YTY5MmJlY2NjMGI5NDZkNGM4NjI2MWZkMTBkNTE3ZTc5N2IyOGExN2QzZQ==) )"
TPP-Signature-Certificate: TPP's_eIDAS_Certificate

{
  "instructedAmount": {"currency": "EUR", "amount": "123.50"},
  "debtorAccount": {"iban": "BG94BANK12341234567890"},
  "paymentType": {"ServiceLevel": "URGP"},
  "creditorName": "Receiver Merchant123",
  "creditorAccount": {"iban": "BG96BGBK43210123456789"},
  "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

- Криптирания текст (hash) се преизчислява по метод Base64 в символен низ за Digest:

NmRlYTIwOTk2YjExNjYxZjBkNDFlNmZiNGM5N2Y3MTE4ZmRiOTFiOTFlN2UyNjk3NDQ5NjI5YWU5ZjIxZmUzNg==

- Необходимите параметри за образуване на подпис са следните:

```
Digest: SHA-256
X-Request-ID:
PSU-ID:
TPP-Redirect-URI:
Date: Sun, 06 Aug 2017 15:02:37 GMT
```

- Стойностите на параметрите съответно са:

```
NmRlYTIwOTk2YjExNjYxZjBkNDFlNmZiNGM5N2Y3MTE4ZmRiOTFiOTFlN2UyNjk3NDQ5NjI5YWU5ZjIxZmUzNg==
99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-1234
https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&code_Cchallenge_Mmethod="S256"
Sun, 28 Jan 2018 16:45:37 GMT
```

- За низът от стойности на параметри се изчислява hash по метода SHA-256:

80996d5bfe5742c08ed96a692beccc0b946d4c86261fd10d517e797b28a07d3e

- Стойността на кодирувания (hash) символния низ в SHA-256 отново се преобразува в код Base64:

ODA5OTZkNWJmZTU3NDJjMDhlZDk2YTY5MmJlY2NjMGI5NDZkNGM4NjI2MWZkMTBkNTE3ZTc5N2IyOGExN2QzZQ==

13. Изисквания при използване на OAuth2 метод на ЗУИ

Requirements on the OAuth2 Protocol

Използването на API за OAuth2 протокол е дефинирано в [\[RFC 6749\]](#). Този протокол може да се използва по избор. В този раздел са определени допълнителни изисквания за протокола.

Изискванията за обмен на данни между ДПУ и OAuth Server на ДПУОС са идентични с изискванията за обмен на данни между ДПУ и интерфейса Достъп до сметка (Раздел 3).

Отговорът от тип "code", както и разрешаващите типове "авторизационен код / authorization_code" и "актуализация на токън / refresh_token" се препоръчват от тази спецификация.

От ДПУОС се изисква да предоставя на ДПУ конфигурационни данни, съответстващи на спецификацията "OAuth 2.0 Authorization Server Metadata".

13.1. Заявка за авторизация (Authorization Request)

В "Заявка за авторизация" на ДПУ към авторизационния сървър на ДПУОС са дефинирани следните параметри:

Query Parameters

Attribute	Condition	Description
response_type	Mandatory	"code" is recommended as response type.
client_id	Mandatory	organizationIdentifier as provided in the eIDAS certificate. The organizationIdentifier attribute shall contain information using the following structure in the presented order: - "PSD" as 3-character legal person identity type reference; - 2 character ISO 3166 country code representing the NCA country; - hyphen-minus "-" and - 2-8 character NCA identifier (A-Z uppercase only, no separator) - hyphen-minus "-" and - PSP identifier (authorization number as specified by NCA).
scope	Mandatory	PIS: The scope is the reference to the payment resource in the form "PIS:<paymentId>". AIS: The scope is the reference to the consent resource for account access in the form "AIS:<consentId>" PIIS: The scope is the reference to the consent resource for granting consent to confirmation of funds in the form "PIIS:<consentId>". Note: The resource ids chosen by the ASPSP need to be unique to avoid resource conflicts during the SCA process.
state	Mandatory	A dynamical value set by the TPP and used to prevent XSRF attacks.
redirect_uri	Mandatory	The URI of the TPP where the OAuth2 server is redirecting the PSU after the authentication.
code_challenge	Mandatory	PKCE challenge according to cryptographic RFC 7636 (https://tools.ietf.org/html/rfc7636) used to prevent code injection attacks.
code_challenge_method	Optional	Code verifier transformation method, is "S256" or "plain". "S256" is recommended by this specification.

Example

```
GET /authorise?response_type=code&client_id="PSDES-BDE-3DFD21" &
scope=ais%3A1234-werti9-983+offline_access&
state= S8NJ7uqk5fY4EjNvP_G_FtyJu6pUsvH9jsYni9dMAJw&
redirect_uri=https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb&
code_challenge_method="S256"
code_challenge=5c305578f8f19b2dcdb6c3c955c0aa709782590b4642eb890b97e43917cd0f36 HTTP/1.1
Host: api.testbank.com
```

13.2. Отговор за авторизация (Authorization Response) се състои от следните данни

HTTP Response Code 302

Query Parameters

Attribute	Condition	Description
Location:	Mandatory	redirect URI of the TPP
code	Mandatory	Authorization code
state	Mandatory	Same value as for the request.

Example

```
HTTP/1.1 302 Found
Location: https://client.example.com/cb
?code=Sp1xl0BeZQQYbYS6WxSbIA
&state=S8NJ7uqk5fY4EjNvP_G_FtyJu6pUsvH9jsYni9dMAJw
```

13.3. Заявка за токън (Token Request)

ДПУ изпраща заявка с POST до крайната точка "токън", за да размени кода за авторизация, предоставен в отговор на авторизацията за достъп с токън или за обновяване на токън. Използват се следните параметри:

Request Parameters

Attribute	Condition	Description
grant_type	Mandatory	"authorisation_code" is recommended as response type.
client_id	Mandatory	cp. Definition in Section Error! Reference source not found.
code	Mandatory	Authorisation code from the authorisation response
redirect_uri	Mandatory	the exact uri of the TPP where the OAuth2 server redirected the user agent to for this particular transaction
code_verifier	Mandatory	PKCE verifier according to cryptographic RFC 7636 (https://tools.ietf.org/html/rfc7636) used to prevent code injection attacks.

Example

```
POST /token HTTP/1.1
Host: https://api.testbank.com
Content-Type: application/x-www-form-urlencoded
client_id="PSDES-BDE-3DFD21"
&grant_type=authorisationCode
&code=Sp1xl0BeZQQYbYS6WxSbIA
&redirect_uri= https%3A%2F%2Fclient%2Eexample%2Ecom%2Fcb
&code_verifier=7814hj4hj4ai87qghjz9hahdeu9qu771367647864676787878
```

ДПУ се удостоверява по време на тази заявка, като използва "OAuth 2.0 Mutual TLS Client Authentication and Certificate Bound Access Tokens" заедно със сертификата му по eIDAS.

13.4. Отговор от токън (Token response)

ДПУОС използва в отговора си следните параметри

Response Parameters

Attribute	Condition	Description
access_token	Mandatory	Access Token bound to the scope as requested in the authorisation request and confirmed by the PSU.
token_type	Mandatory	Set to "Bearer"
expires_in	Optional	The lifetime of the access token in seconds
refresh_token	Optional	Refresh Token, which can be utilised to obtain a fresh access tokens in case the previous access token expired or was revoked. Especially useful in the context of AIS.
scope	Mandatory	the scope of the access token

Example

```

HTTP/1.1 200 OK
Content-Type: application/json
Cache-Control: no-store
Pragma: no-cache
{
  "access_token": "SlAV32hkKG",
  "token_type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "tGzv3JokF0XG5Qx2TlKWIA"
  "scope": "exampleScope"
}

```

13.5. Обновяване на тип разрешение с токън (Refresh Token Grant Type)

ДПУОС може да издаде нов тип разрешение с токън по свое усмотрение, напр. ако ДПУ използва стандартната стойност на обхвата "offline_access" или ако индикатора за повторение "recurringIndicator" е настроен на "true".

13.6. Заявки API (API request)

При използване на подход на ЗУИ OAuth, последващите заявки за приложния програмен интерфейс (API) се разрешават чрез съответния OAuth Access Token. Достъпът с токън се изпраща до приложния програмен интерфейс (API), като се използва заглавката "Authorization" и "BEARER", както е дефинирано в [RFC 6750](#).

Следва пример за заявка за API

```

GET /v1/payments/sepa-credit-transfers/1234-wertiq-983/status HTTP/1.1
Host: https://api.testbank.com
Authorization: Bearer SlAV32hkKG

```

14. Типове данни и конструкции (Complex Data Types and Code Lists)

В следващите таблици се съдържат дефиниции на конструирани типове данни използвани в секциите на параметрите в този документ

14.1. PSU Data

Attribute	Type	Condition	Description
password	String	Conditional	Contains a password in plaintext.
encrypted Password	String	Conditional	Is used when a password is encrypted on application level.
additional Password	String	Conditional	Contains an additional password in plaintext
additional Encrypted Password	String	Conditional	Is provided when the additional password is used and is encrypted on application level.

14.2. TPP Message Information

Attribute	Type	Condition	Description
category	String	Mandatory	Only "ERROR" or "WARNING" permitted
code	Message Code	Mandatory	
path	String	Conditional	
text	Max500Text	Optional	Additional explaining text.

14.3. Amount

Attribute	Type	Condition	Description
currency	Currency Code	Mandatory	ISO 4217 Alpha 3 currency code
amount	String	Mandatory	The amount given with fractional digits, where fractions must be compliant to the currency definition. Up to 14 significant figures. Negative amounts are signed by minus. The decimal separator is a dot. Example: Valid representations for EUR with up to two decimals are: • 1056 • 5768.2 • -1.50 • 5877.78

14.4. Address

Attribute	Type	Condition	Description
streetName	Max70text	Optional	

buildingNumber	String	Optional	
townName	String	Optional	
postalcode	String	Optional	
country	Country code	Mandatory	

14.5. Remittance

Attribute	Type	Condition	Description
reference	Max35text	Mandatory	The actual reference.
referenceType	Max35text	Optional	
referenceIssuer	Max35text	Optional	

14.6. Links

Attribute	Type	Condition	Description
scaRedirect	href Type	Optional	A link to an ASPSP site where SCA is performed within the Redirect SCA approach.
scaOAuth	href Type	Optional	The link refers to a JSON document specifying the OAuth details of the ASPSP's authorisation server. JSON document follows the definition given in https://tools.ietf.org/html/draft-ietf-oauth-discovery .
confirmation	href Type	Optional	"confirmation": Might be added by the ASPSP if either the "scaRedirect" or "scaOAuth" hyperlink is returned in the same response message. This hyperlink defines the URL to the resource which needs to be updated with - a confirmation code as retrieved after the plain redirect authentication process with the ASPSP authentication server or - an access token as retrieved by submitting an authorization code after the integrated OAuth based

Attribute	Type	Condition	Description
			authentication process with the ASPSP authentication server.
startAuthorisation	href Type	Optional	A link to an endpoint, where the authorisation of a transaction or the authorisation of a transaction cancellation shall be started. No specific data is needed for this process start.
startAuthorisationWith PsuIdentification	href Type	Optional	The link to an endpoint where the authorisation of a transaction or of a transaction cancellation shall be started, where PSU identification shall be uploaded with the corresponding call.
updatePsuIdentification	href Type	Optional	The link to the payment initiation or account information resource, which needs to be updated by the PSU identification if not delivered yet.
startAuthorisationWith ProprietaryData	href Type	Optional	A link to the endpoint, where the authorisation of a transaction or of a transaction cancellation shall be started, and where proprietary data needs to be updated with this call. The TPP can find the scope of missing proprietary data in the ASPSP documentation. The usage of this hyperlink is not further specified in the specification but is used analogously to e.g. the startAuthorisation withPsuIdentification hyperlink.
updateProprietaryData	href Type	Optional	The link to the payment initiation or account information resource, which needs to be updated by the proprietary data.
startAuthorisationWith PsuAuthentication	href Type	Optional	The link to an endpoint where the authorisation of a transaction or of a transaction cancellation shall be started,

Attribute	Type	Condition	Description
			where PSU authentication data shall be uploaded with the corresponding call.
updatePsuAuthentication	href Type	Optional	The link to the payment initiation or account information resource, which needs to be updated by a PSU password and eventually the PSU identification if not delivered yet.
updateAdditionalPsuAuthentication	href Type	Optional	The link to the payment initiation or account information resource, which needs to be updated by an additional PSU password.
startAuthorisationWithEncrypted TransactionAuthorisation	href Type	Optional	The link to an endpoint where the authorisation of a transaction or of a transaction cancellation shall be started, where encrypted PSU authentication data shall be uploaded with the corresponding call.
updateEncryptedPsuAuthentication	href Type	Optional	The link to the payment initiation or account information resource, which needs to be updated by an encrypted PSU password and eventually the PSU identification if not delivered yet.
updateAdditionalEncryptedPsuAuthentication	href Type	Optional	The link to the payment initiation or account information resource, which needs to be updated by an additional encrypted PSU password.
startAuthorisationWithAuthenticationMethodSelection	href Type	Optional	This is a link to an endpoint where the authorisation of a transaction or of a transaction cancellation shall be started, where the selected SCA method shall be uploaded with the corresponding call.
selectAuthenticationMethod	href Type	Optional	This is a link to a resource, where the TPP can select the applicable second factor

Attribute	Type	Condition	Description
			authentication methods for the PSU, if there were several available authentication methods.
startAuthorisationWithAuthenticationMethodSelection	href Type	Optional	This is a link to an endpoint where the authorisation of a transaction or of a transaction cancellation shall be started, where the selected SCA method shall be uploaded with the corresponding call."
startAuthorisationWithTransactionAuthorisation	href Type	Optional	A link to an endpoint, where an authorization of a transaction or a cancellation can be started, and where the response data for the challenge is uploaded in the same call for the transaction authorization or transaction cancellation at the same time in the Embedded SCA Approach.
authoriseTransaction	href Type	Optional	The link to the payment initiation or consent resource, where the "Transaction Authorisation"Request" is sent to. This is the link to the resource which will authorise the payment or the consent by checking the SCA authentication data within the Embedded SCA approach.
self	href Type	Optional	The link to the payment initiation resource created by the request itself. This link can be used later to retrieve the transaction status of the payment initiation.
status	href Type	Optional	Status of the resource.
scaStatus	href Type	Optional	A link to retrieve the status of the authorisation or cancellation-authorisation sub-resource.
account	href Type	Optional	A link to the resource providing the details of one account

Attribute	Type	Condition	Description
balances	href Type	Optional	A link to the resource providing the balance of a dedicated account.
transactions	href Type	Optional	A link to the resource providing the transaction history of a dedicated account.
cardAccount	href Type	Optional	A link to the resource providing the details of one card account.
cardTransactions	href Type	Optional	A link to the resource providing the transaction history of a dedicated card account.
transactionDetails	href Type	Optional	A link to the resource providing details of a dedicated transaction.
first	href Type	Optional	Navigation link for paginated account reports.
next	href Type	Optional	Navigation link for paginated account reports.
previous	href Type	Optional	Navigation link for paginated account reports.
last	href Type	Optional	Navigation link for paginated account reports.
download	href Type	Optional	Download link for huge AIS data packages.
cardAccount	href Type	Optional	A link to the resource providing the details of one card account."
cardTransactions	href Type	Optional	A link to the resource providing the transaction history of a dedicated card account.

14.7. href Type

Attribute	Type	Condition	Description
href	String	Mandatory	

14.8. Authentication Object

Attribute	Type	Condition	Description
authenticationType	Authentication Type	Mandatory	Type of the authentication method.
authenticationVersion	String	Conditional	Depending on the "authenticationType". This version can be used by differentiating authentication tools used within performing OTP generation in the same authentication type. This version can be referred to in the ASPSP's documentation.

Attribute	Type	Condition	Description
authenticationMethodId	Max35Text	Mandatory	An identification provided by the ASPSP for the later identification of the authentication method selection.
name	String	Mandatory	This is the name of the authentication method defined by the PSU in the Online Banking frontend of the ASPSP. Alternatively this could be a description provided by the ASPSP like "SMS OTP on phone +49160 xxxxx 28". This name shall be used by the TPP when presenting a list of authentication methods to the PSU, if available.
explanation	String	Optional	detailed information about the SCA method for the PSU

14.9. Authentication Type

Name	Description
SMS_OTP	An SCA method, where an OTP linked to the transaction to be authorized is sent to the PSU through a SMS channel.
CHIP_OTP	An SCA method, where an OTP is generated by a chip card, e.g. an TOP derived from an EMV cryptogram. To contact the card, the PSU normally needs a (handheld) device. With this device, the PSU either reads the challenging data through a visual interface like flickering or the PSU types in the challenge through the device key pad. The device then derives an OTP from the challenge data and displays the OTP to the PSU.
PHOTO_OTP	An SCA method, where the challenge is a QR code or similar encoded visual data which can be read in by a consumer device or specific mobile app. The device resp. the specific app then derives an OTP from the visual challenge data and displays the OTP to the PSU.
PUSH_OTP	An OTP is pushed to a dedicated authentication APP and displayed to the PSU.
SMTP_OTP	An OTP is sent via email to the PSU.

14.10. Challenge

Attribute	Type	Condition	Description
image	String	Optional	PNG data (max. 512 kilobyte) to be displayed to the PSU, Base64 encoding, cp. [RFC 4648]. This attribute is used only, when PHOTO_OTP or CHIP_OTP is the selected SCA method.
data	Array of Strings	Optional	A collection of challenge data
imageLink	String	Optional	A link where the ASPSP will provides the challenge image for the TPP.
otpMaxLength	Integer	Optional	The maximal length for the OTP to be typed in by the PSU.
otpFormat	String	Optional	The format type of the OTP to be typed in. The admitted values are "characters" or "integer".
additional Information	String	Optional	Additional explanation for the PSU to explain e.g. fallback mechanism for the chosen SCA method. The TPP is obliged to show this to the PSU.

14.11. Message Code

The permitted message error codes and related http response codes are listed below.

14.11.1. Service unspecific HTTP Error Codes

Message Code	HTTP Response Code	Description
CERTIFICATE_INVALID	401	The contents of the signature/corporate seal certificate are not matching PSD2 general PSD2 or attribute requirements.
ROLE_INVALID	401	The TPP does not have the correct PSD2 role to access this service.
CERTIFICATE_EXPIRED	401	Signature/corporate seal certificate is expired.
CERTIFICATE_BLOCKED	401	Signature/corporate seal certificate has been blocked by the ASPSP.
CERTIFICATE_REVOKED	401	Signature/corporate seal certificate has been revoked by QSTP.
CERTIFICATE_MISSING	401	Signature/corporate seal certificate was not available in the request but is mandated for the corresponding.
SIGNATURE_INVALID	401	Application layer eIDAS Signature for TPP authentication is not correct.
SIGNATURE_MISSING	401	Application layer eIDAS Signature for TPP authentication is mandated by the ASPSP but is missing.
FORMAT_ERROR	400	Format of certain request fields are not matching the XS2A requirements. An explicit path to the corresponding field might be added in the return message. This applies to headers and body entries. It also applies in cases where these entries are referring to erroneous or not existing data instances, e.g. a malformed IBAN.
PARAMETER_NOT_CONSISTENT	400	Parameters submitted by TPP are not consistent. This applies only for query parameters."
PARAMETER_NOT_SUPPORTED	400	The parameter is not supported by the API provider. This code should only be used for parameters that are described as "optional if supported by API provider."
PSU_CREDENTIALS_INVALID	401	The PSU-ID cannot be matched by the addressed ASPSP or is blocked, or a password resp. OTP was not correct. Additional information might be added.
SERVICE_INVALID	400 (if payload) 405 (if HTTP method)	The addressed service is not valid for the addressed resources or the submitted data.
SERVICE_BLOCKED	403	This service is not reachable for the addressed PSU due to a channel independent blocking by the ASPSP. Additional information might be given by the ASPSP.
CORPORATE_ID_INVALID	401	The PSU-Corporate-ID cannot be matched by the addressed ASPSP.
CONSENT_UNKNOWN	403 (if path) 400 (if header)	The Consent-ID cannot be matched by the ASPSP relative to the TPP.
CONSENT_INVALID	401	The consent was created by this TPP but is not valid for the addressed service/resource.
CONSENT_EXPIRED	401	The consent was created by this TPP but has expired and needs to be renewed.

Message Code	HTTP Response Code	Description
TOKEN_UNKNOWN	401	The OAuth2 token cannot be matched by the ASPSP relative to the TPP.
TOKEN_INVALID	401	The OAuth2 token is associated to the TPP but is not valid for the addressed service/resource.
TOKEN_EXPIRED	401	The OAuth2 token is associated to the TPP but has expired and needs to be renewed.
RESOURCE_UNKNOWN	404 (if account-id in path) 403 (if other resource in path) 400 (if payload)	The addressed resource is unknown relative to the TPP. An example for a payload reference is creating a signing basket with an unknown resource identification.
RESOURCE_EXPIRED	403 (if path) 400 (if payload)	The addressed resource is associated with the TPP but has expired, not addressable anymore.
RESOURCE_BLOCKED	400	The addressed resource is not addressable by this request, since it is blocked e.g. by a grouping in a signing basket.
TIMESTAMP_INVALID	400	Timestamp not in accepted time period.
PERIOD_INVALID	400	Requested time period out of bound.
SCA_METHOD_UNKNOWN	400	Addressed SCA method in the Authentication Method Select Request is unknown or cannot be matched by the ASPSP with the PSU.
SCA_INVALID	400	Method Application on authorisation resource (e.g. Confirmation Request) blocked since SCA status of the resource equals "failed".
STATUS_INVALID	409	The addressed resource does not allow additional authorisation.

14.11.2. PIS specific error codes

Message Code	HTTP Response Code	Description
PRODUCT_INVALID	403	The addressed payment product is not available for the PSU .
PRODUCT_UNKNOWN	404	The addressed payment product is not supported by the ASPSP.
PAYMENT_FAILED	400	The payment initiation POST request failed during the initial process. Additional information may be provided by the ASPSP.
REQUIRED_KID_MISSING	401	The payment initiation has failed due to a missing KID. This is a specific message code for the Norwegian market, where ASPSP can require the payer to transmit the KID.
EXECUTION_DATE_INVALID	400	The requested execution date is not a valid execution date for the ASPSP.
CANCELLATION_INVALID	405	The addressed payment is not cancellable e.g. due to cut off time passed or legal constraints.

Message Code	HTTP Response Code	Description
EXECUTION_DATE_INVALID	400	The requested execution date is not a valid execution date for the ASPSP.
CANCELLATION_INVALID	405	The addressed payment is not cancellable e.g. due to cut off time passed or legal constraints.
BENEFICIARY_WHITELISTING_REQUIRED	201	Only used in responses to a Payment Initiation Request (see Section 5.3). Indicates that in order to execute the payment, the PSU needs to explicitly add the beneficiary to a credit transfer whitelist via a banking channel.
FUNDS_NOT_AVAILABLE	202	Only used in responses to a Get Transaction Status Request (see Section 5.4) or a Get Payment Request (see Section 5.4) in case of "transactionStatus"= "RJCT". Indicates that the reason for rejecting the payment is that the required funds have been found to be not available for the specific (e.g due to missing funds or due to configured limits) during processing after the initial acceptance of the payment initiation.
CONTENT_INVALID	200	Only used in responses to a Get Transaction Status Request (see Section 5.4) or a Get Payment Request (see Section 5.4) in case of "transactionStatus"= "RJCT". Indicates that the reason for rejecting the payment is that the content of the payment initiation has been found invalid during processing after the initial acceptance of the payment initiation.

14.11.3. AIS specific error codes

Message Code	HTTP Response Code	Description
CONSENT_INVALID	401	The consent definition is not complete or invalid. In case of being not complete, the bank is not supporting a completion of the consent towards the PSU. Additional information will be provided.
SESSIONS_NOT_SUPPORTED	400	The combined service flag may not be used with this ASPSP.
ACCESS_EXCEEDED	429	The access on the account has been exceeding the consented multiplicity without PSU involvement per day.
REQUESTED_FORMATS_INVALID	406	The requested formats in the Accept header entry are not matching the formats offered by the ASPSP.

14.11.4. PIIS specific error codes

Message code	HTTP Response Code	Description
CARD_INVALID	400	Addressed card number is unknown to the ASPSP or not associated to the PSU.
NO_PIIS_ACTIVATION	400	The PSU has not activated the addressed account for the usage of the PIIS associated with the TPP.

14.11.5. Signing Basket Specific Error Codes

Message code	HTTP Response Code	Description
REFERENCE_MIX_INVALID	400	The used combination of referenced objects is not supported in the ASPSPs signing basket function.
REFERENCE_STATUS_INVALID	409	At least one of the references is already fully authorised.

14.12. Error Information

Attribute	Type	Condition	Description
title	Max70Text	Optional	Short human readable description of error type. Could be in local language. To be provided by ASPSPs.
detail	Max500Text	Optional	Detailed human readable text specific to this instance of the error. XPath might be used to point to the issue generating the error in addition. Remark for Future: In future, a dedicated field might be introduced for the XPath.
code	Message Code	Mandatory	Message code to explain the nature of the underlying error.

14.13. Transaction status

Identification – Payment Transaction Status Code			
	Code	Name	Definition
1	ACCP	Accepted Customer Profile	Preceding check of technical validation was successful. Customer profile check was also successful.
2	ACSC	Accepted Settlement Completed	Settlement on the debtor's account has been completed. Usage : this can be used by the first agent to report to the debtor that the transaction has been completed. Warning: this status is provided for transaction status reasons, not for financial information. It can only be used after bilateral agreement
3	ACSP	Accepted Settlement In Process	All preceding checks such as technical validation and customer profile were successful and therefore the payment initiation has been accepted for execution.
4	ACTC	Accepted Technical Validation	Authentication and syntactical and semantical validation are successful
5	ACWC	Accepted With Change	Instruction is accepted but a change will be made, such as date or remittance not sent.

6	ACWP	Accepted Without Posting	Payment instruction included in the credit transfer is accepted without being posted to the creditor customer's account.
7	RCVD	Received	Payment initiation has been received by the receiving agent.
8	PDNG	Pending	Payment initiation or individual transaction included in the payment initiation is pending. Further checks and status update will be performed.
8	PART	Partial acceptance	A number of transactions have been accepted, whereas another number of transactions have not yet achieved 'accepted' status. Remark: This code may be used only in case of bulk payments. It is only used in a situation where all mandated authorizations have been applied, but some payments have been rejected."
9	RJCT	Rejected	Payment initiation or individual transaction included in the payment initiation has been rejected.
10	CANC	Cancelled	Payment initiation has been cancelled before execution Remark: Change Request to ISO20022 is still needed.

14.14. Consent Status

Code	Description
received	The consent data have been received and are technically correct. The data is not authorised yet.
rejected	The consent data have been rejected e.g. since no successful authorisation has taken place.
partiallyAuthorised	The consent is due to a multi-level authorisation, some but not all mandated authorisations have been performed yet.
valid	The consent is accepted and valid for GET account data calls and others as specified in the consent object.
revokedByPsu	The consent has been revoked by the PSU towards the ASPSP.
expired	The consent expired.
terminatedByTpp	The corresponding TPP has terminated the consent by applying the DELETE method to the consent resource.

ДПУОС може да добави допълнителни кодове. Тези кодове след това се съдържат в документацията на ДПУОС за интерфейса XS2A.

14.15. SCA Status

Attribute	Description
received	An authorisation or cancellation-authorisation resource has been created successfully.
psuIdentified	The PSU related to the authorisation or cancellation-authorisation resource has been identified.
psuAuthenticated	The PSU related to the authorisation or cancellation-authorisation resource has been identified and authenticated e.g. by a password or by an access token.
scaMethodSelected	The PSU/TPP has selected the related SCA routine. If the SCA method is chosen implicitly since only one SCA method is available, then this is the first status to be reported instead of "received".
started	The addressed SCA routine has been started.
unconfirmed	SCA is technically successfully finalised by the PSU, but the authorisation resource needs a confirmation command by the TPP yet.
finalised	The SCA routine has been finalised successfully
failed	The SCA routine failed
exempted	SCA was exempted for the related transaction, the related authorisation is successful.

14.16. Account Access

Attribute	Type	Condition	Description
accounts	Array of Account Reference	Optional	Is asking for detailed account information. If the array is empty, the TPP is asking for an accessible account list. This may be restricted in a PSU/ASPSP authorization dialogue.
balances	Array of Account Reference	Optional	Is asking for balances of the addressed accounts. If the array is empty, the TPP is asking for the balances of all accessible account lists. This may be restricted in a PSU/ASPSP authorization dialogue
transactions	Array of Account Reference	Optional	Is asking for transactions of the addressed accounts. If the array is empty, the TPP is asking for the transactions of all accessible account lists. This may be restricted in a PSU/ASPSP authorization dialogue
additional Information	Additional Information Access	Optional if supported by API provider	Is asking for additional information as added within this structured object. The usage of this data element requires at least one of the entries "accounts", "transactions" or "balances" also to be contained in the object. If detailed accounts are referenced, it is required in addition that any account addressed within the additionalInformation attribute is also addressed by at least one of the attributes "accounts", "transactions" or "balances".
availableAccounts	String	Optional if supported by API provider	Only the value "allAccounts" is admitted.
availableAccounts WithBalance	String	Optional if supported by API provider	Only the value "allAccounts" is admitted.
allPsd2	String	Optional if supported by API provider	Only the value "allAccounts" is admitted.

14.17. Additional Information Access

Attribute	Type	Condition	Description
ownerName	Array of Account Reference	Optional	Is asking for account owner name of the accounts referenced within. If the array is empty in the request, the TPP is asking for the account owner name of all accessible accounts. This may be restricted in a PSU/ASPSP authorization dialogue. If the array is empty, also the arrays for accounts, balances or transactions shall be empty, if used. The ASPSP will indicate in the consent resource after a successful authorisation, whether the ownerName consent can be accepted by providing the accounts on which the ownerName will be delivered. This array can be empty.

14.18. Account Reference

This type is containing any account identification which can be used on payload-level to address specific accounts. The ASPSP will document which account reference type it will support. Exactly one of the attributes defined as "conditional" shall be used.

Remark: The currency of the account is needed, where the currency is an account characteristic identifying certain sub-accounts under one external identifier like an IBAN. These sub-accounts are separated accounts from a legal point of view and have separated balances, transactions etc.

Attribute	Type	Condition	Description
iban	IBAN	Conditional	
bban	BBAN	Conditional	This data elements is used for payment accounts which have no IBAN.
pan	String	Conditional	Primary Account Number (PAN) of a card, can be tokenised by the ASPSP due to PCI DSS requirements.
maskedPan	String	Conditional	Primary Account Number (PAN) of a card in a masked form.
msisdn	String	Conditional	An alias to access a payment account via a registered mobile phone number.
currency	Currency Code	Optional	ISO 4217 Alpha 3 currency code

14.19. Account Details

Remark: The ASPSP shall give at least one of the account reference identifiers listed as optional below.

Attribute	Type	Condition	Description
resourceId	Max35Text	Conditional	This is the data element to be used in the path when retrieving data from a dedicated account, cp. Section 6.5.3 or Section 6.5.4 below. This shall be filled, if addressable resource are created by the ASPSP on the /accounts.
iban	IBAN	Optional	This data element can be used in the body of the Consent Request Message for retrieving account access consent from this payment account, cp. Section 6.3.1.1.
bban	BBAN	Optional	This data element can be used in the body of the Consent Request Message for retrieving account access consent from this account, cp. Section 6.3.1.1. This data elements is used for payment accounts which have no IBAN.
msisdn	Max35Text	Optional	An alias to access a payment account via a registered mobile phone number. This alias might be needed e.g. in the payment initiation service, cp. Section 5.3.1. The support of this alias must be explicitly documented by the ASPSP for the corresponding API Calls.
currency	Currency Code	Mandatory	Account currency
ownerName	Max140Text	Optional	Name of the legal account owner. If there is more than one owner, then e.g. two names might be noted here. For a corporate account, the corporate name is used for this attribute. Even if supported by the ASPSP, the provision of this field might depend on the fact whether an explicit consent to

Attribute	Type	Condition	Description
			this specific additional account information has been given by the PSU.
name	Max70Text	Optional	Name of the account given by the bank or the PSU in Online-Banking
displayName	Max70Text	Optional	Name of the account as defined by the PSU within online channels.
product	Max35Text	Optional	Product Name of the Bank for this account, proprietary definition
cashAccountType	Cash Account Type	Optional	ExternalCashAccountType1Code from ISO 20022
status	String	Optional	Account status. The value is one of the following: • "enabled": account is available • "deleted": account is terminated • "blocked": account is blocked e.g. for legal reasons If this field is not used, than the account is available in the sense of this specification.
bic	BICFI	Optional	The BIC associated to the account.
linkedAccounts	Max70 Text	Optional	This data attribute is a field, where an ASPSP can name a cash account associated to pending card transactions.
usage	Max4Text	Optional	Specifies the usage of the account - PRIV: private personal account - ORGA: professional account
details	Max500 Text	Optional	Specifications that might be provided by the ASPSP - characteristics of the account - characteristics of the relevant card
balances	Array of Balances	Conditional	
_links	Links	Optional	Links to the account, which can be directly used for retrieving account information from this dedicated account. Links to "balances" and/or "transactions" These links are only supported, when the corresponding consent has been already granted.

14.20. Card Account Details

Attribute	Type	Condition	Description
resourceId	Max35Text	Conditional	This is the data element to be used in the path when retrieving data from a dedicated account, cp. Section 6.7.2, cp. Section 6.7.3 or Section 6.7.4 below. This shall be filled, if addressable resource are created by the ASPSP on the /card-accounts endpoint.
maskedPan	Max35Text	Optional	Primary Account Number (PAN) of a card in masked form. This data element can be used in the body of the Consent

Attribute	Type	Condition	Description
			Request Message for retrieving account access consent from this card, cp. Section 6.3.1.1.
currency	Currency Code	Mandatory	Account currency
ownerName	Max140Text	Optional	Name of the legal account owner. If there is more than one owner, then e.g. two names might be noted here. For a corporate account, the corporate name is used for this attribute. Even if supported by the ASPSP, the provision of this field might depend on the fact whether an explicit consent to this specific additional account information has been given by the PSU.
name	Max70Text	Optional	Name of the account given by the bank or the PSU in Online-Banking
displayName	Max70Text	Optional	Name of the account as defined by the PSU within online channels.
product	Max35Text	Optional	Product Name of the Bank for this account, proprietary definition
debitAccounting	Boolean	Optional	If true, the amounts of debits on the reports are quoted positive with the related consequence for balances. If false, the amount of debits on the reports are quoted negative.
status	String	Optional	Account status. The value is one of the following: "enabled": account is available "deleted": account is terminated "blocked": account is blocked e.g. for legal reasons If this field is not used, than the account is available in the sense of this specification.
usage	Max500Text	Optional	Specifies the usage of the account - PRIV: private personal account - ORGA: professional account
details	Max500Text	Optional	Specifications that might be provided by the ASPSP - characteristics of the account - characteristics of the relevant card
creditLimit	Amount	Optional	Defines the credit limit of the PSU for all cards related to this card account in total.
balances	Array of Balances	Conditional	The specific card account balances associated to this card accounts.
_links	Links	Optional	Links to the cardAccount, which can be directly used for retrieving account information from this dedicated account. Links to "balances" and/or "cardTransactions" These links are only supported, when the corresponding consent has been already granted.

14.21. Balance Type

Следните видове салда изключват кредитните лимити, освен ако елементът creditLimitIncluded присъства и е равен на true в съответния балансов елемент.

Пояснение: Това определение следва логиката на ISO20022 за определяне на видове баланс.

Type	Description
closingBooked	Balance of the account at the end of the pre-agreed account reporting period. It is the sum of the opening booked balance at the beginning of the period and all entries booked to the account during the pre-agreed account reporting period. For card-accounts, this is composed of invoiced, but not yet paid entries
expected	Balance composed of booked entries and pending items known at the time of calculation, which projects the end of day balance if everything is booked on the account and no other entry is posted. For card accounts, this is composed of - invoiced, but not yet paid entries, - not yet invoiced but already booked entries and - pending items (not yet booked)
openingBooked	Book balance of the account at the beginning of the account reporting period. It always equals the closing book balance from the previous report.
interimAvailable	Available balance calculated in the course of the account 'servicer's business day, at the time specified, and subject to further changes during the business day. The interim balance is calculated on the basis of booked credit and debit items during the calculation time/period specified. For card-accounts, this is composed of - invoiced, but not yet paid entries, - not yet invoiced but already booked entries
interimBooked	Balance calculated in the course of the account servicer's business day, at the time specified, and subject to further changes during the business day. The interim balance is calculated on the basis of booked credit and debit items during the calculation time/period specified.
forwardAvailable	Forward available balance of money that is at the disposal of the account owner on the date specified.
nonInvoiced	Only for card accounts, to be defined yet.

14.22. Balance

Attribute	Type	Condition	Description
balanceAmount	Amount	Mandatory	
balanceType	Balance Type	Mandatory	
creditLimitIncluded	Boolean	Optional	A flag indicating if the credit limit of the corresponding account is included in the calculation of the balance, where applicable.
lastChangeDateTime	ISODateTime	Optional	This data element might be used to indicate e.g. with the expected or booked balance that no action is known on the account, which is not yet booked.
referenceDate	ISODate	Optional	indicates the date of the balance
lastCommitted Transaction	Max35Text	Optional	entryReference of the last committed transaction to support the TPP in identifying whether all PSU transactions are already known.

14.23. Account Report

Attribute	Type	Condition	Description
booked	Array of transactions	Conditional	Shall be contained if bookingStatus parameter is set to "booked" or "both".
pending	Array of transactions	Optional	Not contained if the bookingStatus parameter is set to "booked" or "information".
information	Array of transactions	Optional	Only contained if the bookingStatus is set to "information" or "all" and if supported by ASPSP.
_links	Links	mandatory	The following links might be used within this context: • account (mandatory) • first (optional) • next (optional) • previous (optional) • last (optional)

14.24. Transactions

Attribute	Type	Condition	Description
transactionId	String	Mandatory	Can be used as access-ID in the API, where more details on a transaction is offered. If this data attribute is provided this shows that the AIS can get access on more details about this transaction using the GET Transaction Details Request as defined in
entryReference	Max35Text	Optional	Is the identification of the transaction as used e.g. for reference for delta function on application level. The same identification as for example used within camt.05x messages.
batchIndicator	Boolean	Optional	If this indicator equals true, then the related entry is a batch entry.
batchNumberOf Transactions	Integer	Conditional	Shall be used if and only if the batchIndicator is contained and equals true.
endToEndId	Max35Text	Optional	Unique end to end identity.
mandateId	Max35Text	Optional	Identification of Mandates, e.g. a SEPA Mandate ID
checkId	Max35Text	Optional	Identification of a Cheque
creditorId	Max35Text	Optional	Identification of Creditors, e.g. a SEPA Creditor ID
bookingDate	ISODate	Optional	The Date when an entry is posted to an account on the ASPSPs books.
valueDate	ISODate	Optional	Date and time at which assets become available to the account owner in case of a credit entry, or cease to be available to the account owner in case of a debit entry. Usage: If entry status is pending and value date is present, then the value date refers to an expected/requested value date.
transactionAmount	Amount	Mandatory	The amount of the transaction as billed to the account.

Attribute	Type	Condition	Description
currencyExchange	Array of Report Exchange Rate	Optional	
creditorName	Max70Text	Optional	Name of the creditor if a "Debited" transaction
creditor Account	Account Reference	Conditional	
creditorAgent	BICFI	Optional	
ultimate Creditor	Max70Text	Optional	
debtorName	Max70Text	Optional	Name of the debtor if a "Credited" transaction
debtorAccount	Account Reference	Conditional	
debtorAgent	BICFI	Optional	
ultimateDebtor	Max70Text	Optional	
remittance Information Unstructured	Max140Text	Optional	
remittanceInformationUnstructuredArray	Array of Max140Text	Optional	Remark for Future: In version 2.0 these two unstructured remittance fields might be merged.
remittance Information Structured	Max140Text	Optional	Reference as contained in the structured remittance reference structure (without the surrounding XML structure).
remittanceInformationStructuredArray	Array of Remittance	Optional	NOTE: More details about the Remittance Data Type will be published in an Errata in due course. For usage of the fields e.g. for domestic elements, Berlin Group should be contacted. This would enable to publish usage of structured remittance information in the domestic payment documentation, cp. [XS2A-DP].
entryDetails	Array of Entry Details	Optional	Might be used by the ASPSP to transport details about transactions within a batch.
additional Information	Max500Text	Optional	Might be used by the ASPSP to transport additional transaction related information to the PSU.
additionalInformationStructured	Structured Additional Information	Conditional	Is used if and only if the bookingStatus entry equals "information". Every active standing order related to the dedicated payment account result into one entry.
purposeCode	Purpose Code	Optional	
bankTransactionCode	Bank Transaction Code	Optional	Bank transaction code as used by the ASPSP and using the sub elements of this structured code defined by ISO20022 For standing order reports the following codes are applicable:

Attribute	Type	Condition	Description
			"PMNT-ICDT-STDO" for credit transfers, "PMNT-IRCT-STDO" for instant credit transfers "PMNT-ICDT-XBST" for cross-border credit transfers "PMNT-IRCT-XBST" for cross-border real time credit transfers and "PMNT-MCOP-OTHR" for specific standing orders which have a dynamical amount to move left funds e.g. on month end to a saving account
proprietaryBank TransactionCode	Max35Text	Optional	proprietary bank transaction code as used within a community or within an ASPSP e.g. for MT94x based transaction reports
balanceAfterTransaction	Balance	Optional	This is the balance after this transaction. Recommended balance type is interimBooked.
_links	Links	Optional	The following links could be used here: transactionDetails for retrieving details of a transaction.

14.25. Entry Details

Attribute	Type	Condition	Description
endToEndId	Max35Text	Optional	Unique end to end identity.
mandateId	Max35Text	Optional	Identification of Mandates, e.g. a SEPA Mandate ID
checkId	Max35Text	Optional	Identification of a Cheque
creditorId	Max35Text	Optional	Identification of Creditors, e.g. a SEPA Creditor ID
transactionAmount	Amount	Mandatory	The amount of the transaction as billed to the account.
currencyExchange	Array of Report Exchange Rate	Optional	
creditorName	Max70Text	Optional	Name of the creditor if a "Debited" transaction
creditor Account	Account Reference	Conditional	
creditorAgent	BICFI	Optional	
ultimate Creditor	Max70Text	Optional	
debtorName	Max70Text	Optional	Name of the debtor if a "Credited" transaction
debtorAccount	Account Reference	Conditional	
debtorAgent	BICFI	Optional	
ultimateDebtor	Max70Text	Optional	
remittance Information Unstructured	Max140Text	Optional	
remittance Information Unstructured Array	Array of Max140Text	Optional	Remark for Future: In version 2.0 these two unstructured remittance fields might be merged.

Attribute	Type	Condition	Description
remittance Information Structured	Max140Text	Optional	Reference as contained in the structured remittance reference structure (without the surrounding XML structure). Remark For Future: This field will be re-typed in a future version of the interface to the structured data type Remittance or might be omitted. For migration reasons, this is not supported in version 1.3.x.
remittance Information Structured Array	Array of Remittance	Optional	NOTE: More details about the Remittance Data Type will be published in an Errata in due course. For usage of the fields e.g. for domestic elements, Berlin Group should be contacted. This would enable to publish usage of structured remittance information in the domestic payment documentation, cp. [XS2A-DP].
purposeCode	Purpose Code	Optional	

14.26. Structured Additional Information Data Type

Attribute	Type	Condition	Description
standingOrderDetails	Standing Order Details	Mandatory	Details of underlying standing orders.

14.27. Standing Order Details Data Type

Attribute	Type	Condition	Description
startDate	ISODate	Mandatory	The first applicable day of execution starting from this date the first payment was/will be executed.
endDate	ISODate	Optional	The last applicable day of execution If not given, it is an infinite standing order.
executionRule	String	Optional	"following" or "preceding" supported as values. This data attribute defines the behavior when a transaction date resulting from a standing order falls on a weekend or bank holiday. The payment is then executed either the "preceding" or "following" working day.
withinAMonthFlag	Boolean	Optional	This element is only used in case of frequency equals "Monthly". If this element equals false it has no effect. If this element equals true, then the execution rule is overruled if the day of execution would fall into a different month using the execution rule. Example: executionRule equals "preceding", dayOfExecution equals "02" and the second of a month is a Sunday. In this case, the transaction date would be on the last day of the month before. This would be overruled if withinAMonthFlag equals true and the payment is processed on Monday the third of the Month. Remark: This attribute is rarely supported in the market.
frequency	Frequency Code	Mandatory	The frequency of the recurring payment resulting from this standing order.
monthsOfExecution	Array of Max2Text	Conditional	The format is following the regular expression \d{1,2}. The array is restricted to 11 entries. The values contained in the

Attribute	Type	Condition	Description
			array entries shall all be different and the maximum value of one entry is 12. This attribute is contained if and only if the frequency equals "MonthlyVariable". Example: An execution on January, April and October each year is addressed by ["1". "4", "10"].
multiplier	Numerical	Optional	This is multiplying the given frequency resulting the exact frequency, e.g. Frequency=Weekly and multiplier=3 means every 3 weeks. Remark: This attribute is rarely supported in the market.
dayOfExecution	Max2Text	Optional	"31" is ultimo. The format is following the regular expression \d{1,2}. Example: The first day is addressed by "1". The date is referring to the time zone of the ASPSP.
limitAmount	Amount	Conditional	limitAmount Amount limit for fund skimming, e.g. skim all funds above this limit to savings account, i.e. typically a specific periodic payments with fixed remaining amount rather than fixed transaction amount. Amount may be zero as well as below zero, i.e. negative. Constraints: transactionAmount needs to be zero and bankTransactionCode needs to specify PMNT-MCOP-OTHR for fund skimming

14.28. Card Account Report

Attribute	Type	Condition	Description
booked	Array of Card transactions	Conditional	Shall be contained if bookingStatus parameter is set to "booked" or "both".
pending	Array of Card transactions	Optional	Not contained if the bookingStatus parameter is set to "booked".
_links	Links	Mandatory	The following links might be used within this context: • cardAccount (mandatory when providing transaction reports on card reconciliation accounts under /card-accounts) • card (mandatory when providing transaction reports on single card entry level under /cards)first (optional) • next (optional) • previous (optional) • last (optional)

14.29. Card Transactions

Attribute	Type	Condition	Description
cardTransactionId	Max35Text	Optional	Unique end to end identity.
terminalId	Max35Text	Optional	Identification of the Terminal, where the card has been used.
transactionDate	ISODate	Optional	date of the actual card transaction
acceptorTransactionDateTime	ISODateTime	Optional	Timestamp of the actual card transaction within the acceptance system
bookingDate	ISODate	Optional	booking date of the related booking on the card account

Attribute	Type	Condition	Description
transactionAmount	Amount	Mandatory	The amount of the transaction as billed to the card account.
currencyExchange	Array of Report Exchange Rate	Optional	For card accounts, only one exchange rate is used.
originalAmount	Amount	Optional	Original amount of the transaction at the Point of Interaction in original currency
markupFeePercentage	String	Optional	e.g. "0.3" for 0,3%.
markupFee	Amount	Optional	Any fee related to the transaction in billing currency.
cardAcceptorId	Max35Text	Optional	Identification of the Card Acceptor (e.g. merchant) as given in the related card transaction.
cardAcceptorAddress	Address	Optional	Address of the Card Acceptor as given in the related card transaction.
cardAcceptorPhone	Phone Number	Optional	Merchant phone number
merchantCategoryCode	Merchant Category Code	Optional	Merchant Category Code of the Card Acceptor as given in the related card transaction.
maskedPAN	Max35Text	Optional	The masked PAN of the card used in the transaction.
transactionDetails	Max140Text	Optional	Additional details given for the related card transactions.
invoiced	Boolean	Optional	Flag indicating whether the underlying card transaction is already invoiced.
proprietaryBankTransactionCode	Max35Text	Optional	proprietary bank transaction code as used within a community or within an ASPSP e.g. for MT94x based transaction reports

14.30. Report Exchange Rate

Attribute	Type	Condition	Description
sourceCurrency	Currency Code	Mandatory	Currency from which an amount is to be converted in a currency conversion.
exchangeRate	String	Mandatory	Factor used to convert an amount from one currency into another. This reflects the price at which one currency was bought with another currency.
unitCurrency	Currency Code	Mandatory	Currency in which the rate of exchange is expressed in a currency exchange. In the example 1EUR = xxxCUR, the unit currency is EUR.
targetCurrency	Currency Code	Mandatory	Currency into which an amount is to be converted in a currency conversion.
quotationDate	ISODate	Mandatory	Date at which an exchange rate is quoted.
contractIdentification	String	Optional	Unique identification to unambiguously identify the foreign exchange contract.

14.31. Payment Exchange Rate

Attribute	Type	Condition	Description
unitCurrency	Currency Code	Optional	Currency in which the rate of exchange is expressed in a currency exchange. In the example 1EUR = xxxCUR, the unit currency is EUR.
exchangeRate	String	Optional	Factor used to convert an amount from one currency into another. This reflects the price at which one currency was bought with another currency.
contractIdentification	String	Optional	Unique identification to unambiguously identify the foreign exchange contract.
rateType	String	Optional	Specifies the type used to complete the currency exchange. Only SPOT, SALE and AGRD is allowed.

14.32. Geo Location

Format using [\[RFC 2426\]](#), i.e. "GEO:"<latitude>;< longitude >.

14.33. Frequency Code

The following codes from the EventFrequency7Code of ISO20022 are supported:

- Daily,
- Weekly,
- EveryTwoWeeks,
- Monthly,
- EveryTwoMonths,
- Quarterly,
- SemiAnnual,
- Annual,
- MonthlyVariable

RFU: It needs to be checked for a later version of these Implementation Guidelines whether these codes should be in lowerCamelCase.

14.34. Charge Bearer

Type	Description
DEBT	All transaction charges are to be borne by the debtor.
CRED	All transaction charges are to be borne by the creditor.
SHAR	In a credit transfer context, means that transaction charges on the sender side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor. In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor, transaction charges on the receiver side are to be borne by the debtor.
SLEV	Charges are to be applied following the rules agreed in the service level and/or scheme.

14.35. Other ISO-related basic Types

The following codes and definitions are used from ISO20022

- **Purpose Code:** ExternalPurpose1Code
- **Cash Account Type:** ExternalCashAccountType1Code

- **Bank Transaction Code:** ExternalBankTransactionDomain1Code
- **BICFI:** BICFIIdentifier
- **IBAN:** IBAN2007Identifier - Pattern: [A-Z]{2}[0-9]{2}[A-Z0-9]{1-30}
- **BBAN:** BBANIdentifier
- **Phone Number:** PhoneNumber
- **Merchant Category Code:** Category code conform to ISO 18245
- **Service Level Code:** ExternalServiceLevel1Code

The following code is a concatenated code from ISO20022

- **BankTransactionCode:** This code type is concatenating the three ISO20022 Codes Domain Code, Family Code and SubFamily Code by hyphens, resulting in "DomainCode"- "FamilyCode"- "SubFamilyCode".

Example: PMNT-RCDT-ESCT defining a transaction assigned to the PayMeNT Domain (PMNT), belonging to the family of ReceivedCreditTransfer (RCDT) that facilitated the EuropeanSEPACreditTransfer (ESCT)

For all codes used in JSON structures, not the abbreviation defined for XML encoding, but the name of the code is used as value. The following Codes are used from other ISO standards:

- **Currency Code:** Codes following ISO 4217 Alpha 3
- **Country Code:** Two characters as defined by ISO 3166

Further basic ISO data types:

- **ISODatetime:** A particular point in the progression of time defined by a mandatory date and a mandatory time component, expressed in either UTC time format (YYYY-MM-DDThh:mm:ss.sssZ), local time with UTC offset format (YYYY-MM-DDThh:mm:ss.sss+/-hh:mm), or local time format (YYYY-MMDDThh:mm:ss.sss). These representations are defined in "XML Schema Part 2: Datatypes Second Edition - W3C Recommendation 28 October 2004" which is aligned with ISO 8601.
- **ISODate:** A particular point in the progression of time in a calendar year expressed in the YYYY-MM-DD format.

15. Препратки (References)

- [XS2A-OR] NextGenPSD2 XS2A Framework, Operational Rules, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.3, published 21 December 2018
- [XS2A-IG] NextGenPSD2 XS2A Framework, Implementation Guidelines, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.3, published November 2018
- [XS2A-DP] NextGenPSD2 XS2A Framework, Domestic Payment Definitions, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, current version
- [XS2A-COFC] NextGenPSD2 XS2A Framework, Extended Services, Confirmation of Funds Consent Service, Version 2.0, 01 March 2019
- [XS2A-RSNS] NextGenPSD2 XS2A Framework, Extended Services, Resource Status Notification Service, Version 1.0, 01 March 2019
- [XS2A-SecB] NextGenPSD2 XS2A Framework, Security Bulletin, Version 1.0, 06 November 2019
- [EBA-OP2] Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC, EBA/OP/2020/10, published 4 June 2020
- [EBA-RTS] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive 2015/2366 of the European Parliament and of the Council with regard to Regulatory Technical Standards for Strong Customer Authentication and Common and Secure Open Standards of Communication, C(2017) 7782 final, published 13 March 2018
- [eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 23 July 2014, published 28 August 2014
- [ETSI PSD2] ETSI TS 119 495 V1.1.2; Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366
- [PSD2] Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, published 25 November 2016
- [HAL] Kelley, M., "HAL - Hypertext Application Language", 2013-09-18, http://stateless.co/hal_specification.html
- [FAPI-CBPIA] OpenID Foundation, Financial-grade API (FAPI) Working Group, Cross-Browser Payment Initiation Attack, https://bitbucket.org/openid/fapi/src/master/TR-Cross_browser_payment_initiation_attack.md, 3.01.2019
- [signHTTP] Signing HTTP messages, Network Working Group, Internet Draft, <https://datatracker.ietf.org/doc/draft-cavage-http-signatures/>
- [HAL] Kelley, M., "HAL - Hypertext Application Language", 2013-09-18, http://stateless.co/hal_specification.html

- [OA-SecTop] OAuth 2.0 Security Best Current Practice draft-ietf-oauth-security-topics-13, Lodderstedt et al., 8 July 2019, <https://tools.ietf.org/html/draft-ietf-oauth-security-topics-13>
- [[RFC2426](#)] Dawson, F. and T. Howes, T., "vCard MIME Directory Profile", September 1998, <https://tools.ietf.org/html/rfc2426>
- [[RFC3230](#)] Mogul, J. and A. Van Hoff, "Instance Digests in HTTP", RFC 3230, DOI 10.17487/RFC3230, January 2002, <https://www.rfc-editor.org/info/rfc3230>
- [[RFC4648](#)] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", October 2006, <https://tools.ietf.org/html/rfc4648>
- [[RFC5843](#)] Bryan, A, "Additional Hash Algorithms for HTTP Instance Digests", RFC 5843, DOI 10.17487/RFC5843, April 2010, <https://www.rfc-editor.org/info/rfc5843>
- [[RFC6749](#)] Hardt, D., "The OAuth 2.0 Authorization Framework", October 2012, <https://tools.ietf.org/html/rfc6749>
- [[RFC7807](#)] M. Nottingham, Akamai, E. Wilde, „Problem Details for HTTP APIs“, March 2016, <https://tools.ietf.org/html/rfc7807>