Release 3.1.10 Enhancements to Open Banking Standards

Consultation Summary Document

The contents of this document does not constitute legal advice. Participants are responsible for their own compliance with all regulations and laws that apply to them.

Date : 22 02 2022
Version : 0.2
Classification : PUBLIC

Contents

1. Introduction

OBIE is currently consulting on version 3.1.10 of the OBIE Standard. This version includes updates on:

- **90-day changes** – there are several changes to the Customer Experience Guidelines (CEGs) and API Specifications required to support the change from 90-day re-authentication at the ASPSP to reconfirmation of consent at the AISP as outlined in the UK RTS[1].

- **Transaction Risk Indicators** which introduce enhancements to the risk block that will enable improved risk assessment of open banking payments.

- **Terminology** - The adoption of more customer-friendly terminology in illustrative wireframes to reflect the Common Terminology Guide to improve customer awareness and understanding.

- **Errata corrections** - Updates driven by errata identified in 3.1.9.

Proposed changes have been made to the API Specifications, Customer Experience Guidelines, Operational Guidelines and MI Specifications and these are described in the relevant change logs. At the request of the Expert Advisory Group, that has been assisting in development of the proposed changes, we have summarised the key proposed changes in this document providing a supporting rationale for the recommended approach.

We also note a number of key implementation issues confronting the open banking ecosystem, which although have modest implications for the Standards themselves are of significant importance in terms of an orderly transition to the new regulatory framework and as a consequence to end user outcomes. OBIE has set out some recommended approaches to these various implementation challenges for consideration by the industry, recognising that a common approach to many of these issues would deliver considerable benefits to all parties.

OBIE welcomes responses to the consultation from all interested parties. Written consultation responses are due on 4 March 2022. Responses to the consultation questions raised in this document should be sent by e-mail to obiepolicy@openbanking.org.uk. Responses to the specific changes in the Standard should be submitted via the confluence links[2] as previously indicated. Please submit one response document per organisation.

[1] UK RTS, Article 10A & Article 36(6)
[2] https://openbanking.atlassian.net/wiki/spaces/WOR/pages/2319909036/Feedback+-+V3.1.10+Draft1

2. Regulatory Considerations

In November 2021, the FCA published its Policy Statement[3] and updates to the FCA Approach Document V5[4]. This included two key changes to the UK RTS:

(i) Article 10A :This allows an ASPSP not to apply SCA every 90 days when allowing access to the PSU's account via an AISP.
(ii) Article 36 (6): The AISP will need to reconfirm the PSU's consent every 90 days in order to continue access to their account(s).

Practically SCA will be required when access is set up, followed by reconfirmation of consent by the AISP every 90 days, with the following considerations:

- **Nature of Consent:** Must be clear and specific to enable the customer to make an informed decision.
  a. It can be confirmed for single or multiple accounts in one reconfirmation. It is up to the AISP to ensure synchronisation if consent was given at different times (i.e., the 90 days expire at different times).
  b. If consent is delegated, it can be given to the delegate e.g., an accountant provided that it is authorised by the customer and verified by the AISP.

- **Reconfirmation of consent:**
  a. AISPs will be responsible for reconfirming consent and will not have to communicate this with the ASPSP.
  b. Following the initial application of SCA for set up, the ASPSP should only apply SCA for objective and proportionate reasons.
  c. If the PSU does not reconfirm consent, the AISP must no longer access the data until the PSU subsequently reconfirms consent.

- **Other Feedback:**
  a. The data under Article 10A includes standing orders and direct debits

[3] https://www.fca.org.uk/publication/policy/ps21-19.pdf
[4] https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

3. Token Management for new SCA exemption

Historically, ASPSPs have taken a variety of approaches to token management. We believe current implementations support either the use of access tokens only or the use of both access tokens and refresh tokens. The Standards are silent on this issue and currently, either one is permissible.

OBIE cannot introduce any mandatory requirements in this area, however, it has been asked to assess the possible approaches, provide a view on how they fit within the new regulatory requirements and propose a recommended single approach for the industry to voluntarily adopt. In assessing each of the identified options we have considered the following regulatory requirements within the UK RTS (read in line with the FCA Policy Statement and FCA Approach Document):

1. The AISP does not access PSU's account if the PSU has not re-confirmed their consent within the last 90 days.
2. The ASPSP will need to apply SCA if the AISP is accessing account information outside the parameters of Article 10 A from the PSU's account e.g. accessing more than 90 days' worth of transactions.
3. The AISP is not required to inform the ASPSP when PSU has reconfirmed their consent nor may the ASPSP ask for that information from the AISP.

The options and conclusions are based on OBIE's understanding of the possible technical frameworks of TPPs and ASPSPs based on EAG discussions for token management. ASPSPs and TPPs are solely responsible for the practical assessment of their technical and security infrastructures to ensure that can support their preferred options within the regulatory timelines.

3.1. Option 1 - Incremental issuance of new tokens (on request) (preferred option)

When the ASPSP has implemented the new SCA exemption (UK RTS, Article 10A) changes,

- The ASPSP **will** issue new token(s) when the AISP calls with an existing valid token however, the ASPSP **may** need the PSU to re-authenticate in order to issue the new token(s)
- The ASPSP **will** need the PSU to re-authenticate if the token is expired.
- Please refer to Re-authentication of the access journey[5] in the CEG.

The validity of the new token would need to be long-lived to enable the AISP to seamlessly access the PSU's account information, provided the PSU continues to reconfirm their consent every 90 days to the AISP as required in UK RTS, Article 36 (6). For example,

- If the ASPSP only issues 'access token' then the validity of the 'access token' needs to be long-lived. The ASPSP **may** need to ask the PSU to re-authenticate to get a new long-lived access token.

5 https://consultation.standards.openbanking.org.uk/customer-experience-guidelines/dashboards/ais-consent-dashboard-revocation-refresh/v3-1-10-draft/

- If the ASPSP issues both 'access token' and 'refresh token' then the validity of the 'refresh token' needs to be long-lived. The ASPSP **may** need to ask the PSU to re-authenticate to get a new long-lived refresh token.

ASPSPs may have different views on how long a long-lived token validity should be. It could be until consent expiry if the consent has an expiry date or an ongoing token where the consent is without an expiry date. In case of ongoing consent the ASPSP may define their own validity period for the token (e.g., 12 months validity) and issue new token(s) provided the PSU is not required to re-authenticate when the token expires.

Advantages	• An AISP can access PSU's account information without disruption provided that the PSU is reconfirming consent every 90 days. • PSU needs to re-authenticate with the ASPSP only in permitted circumstances
Disadvantages	• There may still be a one last time re-authentication required for the ASPSP to share the new token(s) with the AISP.

3.2. Option 2 - Reset all existing tokens (bulk change)

When the ASPSP has implemented the new SCA exemption (UK RTS, Article 10A):

- The ASPSP would modify the existing expiry date of all the access and refresh token(s) that are still valid without the PSU requiring them to be present to re-authenticate. The ASPSP must communicate the change in token(s) expiry date to the AISPs.
- The ASPSP would need the PSU to re-authenticate to issue the new token(s) if the AISP calls with an expired token(s). Please refer to Re-authentication of the access journey[6] in the CEG.

The validity of the new token would need to be long-lived to enable the AISP to seamlessly access the PSU's account information, provided the PSU continues to reconfirm their consent every 90 days to the AISP. For example,

- If the ASPSP only issues 'access token' then the validity of the 'access token' needs to be long-lived,
- If the ASPSP issues both 'access token' and 'refresh token' then the validity of the 'refresh token' needs to be long-lived

ASPSPs may have different views on how long a long-lived token validity should be. It could be until consent expiry if the consent has an expiry date or an ongoing token where the consent is without an expiry date. In case of ongoing consent the ASPSP may define their own validity period for the token (e.g., 12 months validity) and issue new token(s) provided the PSU is not required to re-authenticate when the token expires

6 https://consultation.standards.openbanking.org.uk/customer-experience-guidelines/dashboards/ais-consent-dashboard-revocation-refresh/v3-1-10-draft/

Advantages	• AISP can access the PSU's account information without disruption if the PSU is reconfirming consent every 90 days. • PSU needs to re-authenticate with the ASPSP only in permitted circumstances.
Disadvantages	• Within the current construct of FAPI, it isn't apparent how the bulk change to existing token(s) by an ASPSP could be communicated to an AISP.

3.3. Option 3 – Automatic reissuing of a 90-day token

When the ASPSP has implemented the new SCA exemption (UK RTS, Article 10A):

- The ASPSP would issue a new refresh token with a 90-day validity to an AISP with an existing valid token(s) without requiring the PSU to be present to re-authenticate provided the ASPSP uses the rotation of token technique to reissue a new refresh token.
- The issuance of the refresh token is not dependent on the AISP reconfirming the consent with the PSU (which will be managed separately), and the AISP can request its tokens from the ASPSP independently within the 90-day period.
- The PSU would only need to re-authenticate to issue the new refresh token if the AISP calls with an expired refresh token i.e. outside the 90 day period. Please refer to Re-authentication of the access journey[7] in the CEG.

Advantages	• The AISP can access PSU's account information without disruption provided that the AISP requests a new token within the 90-day period. The AISP would separately manage their consent with the PSU. • PSU needs to re-authenticate with the ASPSP only in permitted circumstances.
Disadvantages	• The AISP will need to ensure that it requests the token within the 90 period, failing which it will need PSU re-authentication for the AISP to obtain new tokens from the ASPSP. This could be perceived as an obstacle. This option works only if the refresh token rotation technique is used to issue a new refresh token without the PSU being present to re-authenticate. • This option does not work for ASPSPs who have only implemented access tokens. • Susceptible to network failures – if the new refresh token is not received due to a network failure, PSU will be forced to re-authenticate. • This option only works if both ASPSP and TPP support refresh token rotation.

7 https://consultation.standards.openbanking.org.uk/customer-experience-guidelines/dashboards/ais-consent-dashboard-revocation-refresh/v3-1-10-draft/

3.4. Conclusions

The following conclusion is based on feedback received during the EAG process between 13 Jan 2022 and 24 Feb 2022. ASPSPs and TPPs will be best placed to determine how to adhere to the obligations of Article 10A based on their own implementations.

Option 2: At present there is no agreed approach to enable bulk exchange of tokens between ASPSPs and AISPs. Without agreed approach(es), this option does not appear to offer a credible approach to meet the obligations of Article 10A.

Option 3: As not all ASPSPs have implemented refresh tokens, this option does not appear to offer a credible approach to meet the obligations of Article 10A

Therefore, Option 1 is the only approach that appears credible for the ecosystem at present.

.

3.5. Consultation Questions

1. Do you agree with our conclusions that Options 2 & 3 are not credible at present?
2. Do you believe that option 1 is the only credible approach?
3. Would there be benefit in having a common approach for the duration of long lived tokens? If so, what approach is recommended?
4. Are there other alternatives that should be considered?

4. Access Dashboards

4.1. Introduction

One of the implications of the FCA Policy changes regarding 90-Day reauthentication is that it creates additional consent management responsibilities for the TPP and removes the requirement of the ASPSP to reauthenticate the PSU every 90 days. The implications of this are that customers are more likely to manage open banking data sharing in the AISP domain. However, access dashboards will remain an important tool to enable customers to control their open banking connections.

A customer's primary interaction will be with the AISP, both to manage the service being offered and the permission to access the data required for that service. Access dashboards provide customers with a second line of control to ensure that customers are always able to manage all their open banking connections. This is analogous to how direct debits are managed today; customers can manage their service and the direct debit used to pay for the service with their service provider, but they are also able to cancel the direct debit directly with their ASPSP.

4.2. Ensuring access dashboards continue to provide customer benefit

Access dashboards provide customers with a number of benefits including:

i. They provide a single place where customers can go to revoke any of the open banking connections to their payment account(s).

ii. They provide a single place where customers can see the open banking connections to their payment account(s).

The EAG highlighted that it might be challenging for ASPSPs to be absolutely sure whether there was an active permission for data sharing as they are not informed as to whether a customer has confirmed their consent to continue with the data sharing service. For a permission to be active there needs to be a live connection and the customer must have provided active consent within the last 90 days.

It was indicated at the EAG that "date last accessed" would provide additional information to PSUs to enable them to determine whether connections were still being used. It was generally felt that provision of this information would be helpful but several ASPSPs indicated that it would require significant effort to build and maintain this information.

It was also highlighted that AISPs are likely to cancel unused connections as they will ask customers to reconfirm or cancel the data sharing permission. Similarly having dormant connections could generate additional operational risk and cost for AISPs. Therefore, we consider that there is a low likelihood of connections being out of date and being represented as active in the access dashboard when consent has not been reconfirmed. ASPSPs may opt to use a different descriptor to show the status of the connections and several members of the EAG thought that "connected" was a more accurate status descriptor than "active". The actual choice of descriptor is up to the ASPSP.

The OBIE Standard supports the provision of when data was last shared but does not mandate the provision of this information. OBIE believes that access dashboards provide benefits to customers by enabling them to see and control their open banking connections.

Informing customers of when data was last shared would increase the utility of the dashboards but we do not consider that we have sufficient basis to recommend that this should be a mandatory requirement on the CMA9 under the CMA Order (Roadmap Item A2(b)(iii) Consent and Access Dashboards) at this time.

4.3. Consultation Questions

5. Do you agree that absence of the time and date of when data was last shared does not fundamentally undermine the intended purpose of access dashboards?

6. Would it be useful to develop guidance for TPPs to facilitate a common industry approach to the timely cancelation of unused connections?

7. Is “Connected” a better descriptor to show the status of the connections than “Active”? Are there alternative descriptors which would be better for end users?

5. Transaction Risk Indicators

5.1. Introduction

OBIE Standards include data elements specifically designed for risk scoring purposes. Specific agreed fields are included in the Risk section of the payload (OBRisk1). The Risk section is sent by the initiating party (the PISP) to the ASPSP.

The key findings of our previous evaluation were that enhancing the range, availability and reliability of transaction risk indicators (TRIs) within the OBIE Standards would be of benefit in identifying and preventing fraud.

The objective of these enhancements is to provide improved payload information from the PISP that enables the ASPSP to better understand the underlying nature of the transaction and improved their risk-scoring ability. This should improve detection of fraudulent transactions and reduce the number of false positives, thereby improving customer outcomes.

Subsequent evaluation, which included extensive consultation with ecosystem participants, concluded that it would be beneficial to:

i. revise and expand the available “Payment Context Codes”;

ii. include a number of additional TRIs relating to “Payment Characteristics” and the nature of the destination account;

iii. utilise new “Recommended UK Purpose Code in ISO 20022 Payment Messaging List” developed by the Bank of England & Pay.UK in preference to Merchant Category Codes.

5.2. Proposed changes

The proposed fields in OBRISK1 for Version 3.1.10 are shown in entirety in the tables below with proposed definitions and rationale for their inclusion. (Amendments shown in red).

Table 1 – Proposed revised list of Payment Context Codes

Payload Field	Payment Context Code
Rationale for inclusion	The conclusion of our TRI Evaluation was that APP fraud risk varies depending on the PIS business model. We recommended that it would be useful and appropriate to expand the current Payment Context Code to include more categories which provide the ASPSP with more granular information as to the nature of the PISP operating model.
Possible Values	**Definition**
Bill Payment	Providing means for a PSU to initiate a payment to from a bill received from a consumer or business.
Invoice[8] Payment	Providing means for a PSU to initiate an invoice received from a consumer or business.
PISP Payee	The PISP has an underlying contract with the merchant for the provision of open banking payment acceptance services. This PISP is the payee (with the appropriate licence to hold funds), so that they hold funds they receive from PSUs and pay sums to merchants when required.
Ecommerce Merchant Initiated Payment	The PISP has an underlying contract with the merchant for the provision of open banking payment acceptance services. The open banking payment option is an available option on the merchant's customer facing website. The transaction is a payment to the merchant for specified goods and services comprised in the transaction.
Face To Face Point of Sale	In person payments from a consumer to a business.
Transfer to Self	Conforms to the agreed "Sweeping definition" (when agreed).
Transfer to Third Party	Transfer of funds held by a company or individual that falls outside the "Sweeping definition."

[8] An invoice has a different legal status from a bill, follows a specific invoice template contains required information that provides a business with a record of what products and services have been sold and supports internal accounting and VAT procedures. It is a legal document that requests payment from a client for services or products that have been rendered and can be legally enforced to collect outstanding payments. Invoices must contain specific information. . It must be handled in the appropriate way. For example, once an invoice has been finalised, it should not be deleted, but rather cancelled with a credit note.

Table 2. Proposed Additional Risk Indicators to be included in the Risk Block

Payload field	Rationale for inclusion	
Contract Present Indicator	If the PISP has a contractual relationship with the merchant, it must have undertaken some form of validation of the recipient account and/or due diligence on the merchant. Transactional fraud risk is significantly reduced after these checks	
Beneficiary Payment Details Pre-Populated Indicator	Malicious Redirection APP fraud relies on victims being persuaded to make payments to an account that the payer believes belongs to a legitimate payee, where they are deceived into inputting the sort code and account number of an account controlled by a fraudster. By removing the need for PSUs to input payment details this risk is eradicated.	
Integrated Check-out & Pay Indicator	There are differential risks between integrated check-out and other means of bill presentation to customers (e.g., sending a payment link via SMS or email). Indication that open banking payments is integrated into the checkout facility will assist ASPSPs in risk scoring.	
Payee Account Name	ASPSPs use Confirmation of Payee (CoP) to reduce misdirection fraud. It was though that provision of this information may facilitate risk scoring by the ASPSP and act as a substitute for the need for a CoP check. Only provided if the PISP has a contract with the Payee.	
Beneficiary Account Type	This has been identified as a key risk indicator in the UK Finance Proof of Concept project and so should be included when known by the PISP to assist risk scoring by the ASPSP.	
Payload field	**Description**	**Possible Values**
Contract Present Indicator	Indicates PISP has a contract with the payee and has undertaken some form of validation / due diligence on the payee	True False
Beneficiary Payment Details Pre-Populated Indicator	Indicates that the PISP, rather than the PSU has generated the following fields and they are immutable and have not been changed by the PSU in the transactional journey: a) Payee Account Name; and b) Payee Account Identification details (sort code & account number or full IBAN); and	True False
Integrated Check-out & Pay Indicator	Indicated that the creation of the open banking payment instruction is integrated into the checkout facility. The open banking payment option is an available option on the merchant's customer facing website. There is an integrated check-out and pay facility between merchant and PISP.	True False
Payee Account Name	The account name is the name or names of the account owner(s) represented at an account level. Only provided is the PISP has a contract with the payee	Name of the account
Beneficiary Account Type	Indicates the nature of the destination account, if known by the PISP	Personal Business

Table 3. Existing Risk Indicators being retained in the Risk Block

Payload field	Rationale and Description	Possible Values
Merchant Customer Identification	The unique customer identifier of the PSU by the merchant Existing component having this ID, which reflects the customer's account with the merchants would be useful in the event of fraud and indicate if the customer's account had been taken over or if a new fraudulent account had been set up and allows ASPSP to build trust in a given account ID.	Max70Text
Delivery Address	Information that locates and identifies a specific address to which good have been shipped. Existing component - the ASPSP has the relevant data to compare the delivery address to the PSU address	as defined by postal services or in free format text.

Table 4. Merchant Category Codes and Payment Context Codes

It was proposed to replace Merchant Category Code with Payment Purpose Code. At the request of the EAG and to ensure backward compatibility it is proposed to maintain both fields for a a period, but the ambition remains to fully migrate from merchant category code to Payment Purpose Code.

Payload field	Rationale and Description	Possible Values
Merchant Category Code	Existing component- feedback received that MCC should be retained in addition to PPC until a later date.	Category code, related to the type of services or goods the merchant provides for the transaction that conforms to ISO 18245.
Payment Purpose Code	Category code, related to the type of services or goods that corresponds to the underlying purpose of the payment. This will facilitate the risk scoring of different transactions.	Conforms to Recommended UK Purpose Code in ISO 20022 Payment Messaging List.

5.3. Consultation Questions

8. Does the inclusion of "**Payee Account Name"** add value given that **"Creditor Name"** is an existing component of the payment payload?
9. If so, should the "**Payee Account Name"** match the account name in AIS or be consistent with what would be returned in a CoP check?
10. Does "Integrated check-out and pay facility between merchant and PISP" need more definition?
11. Should "Invoice & bill payments" be separate or combined?
12. Are all of the key PISP models covered in the proposed "Payment Context Codes "categories?
13. Should "Merchant Category Codes" be retained in addition to "Payment Purpose Codes" until a future date?
14. In relation to "Beneficiary Account Type" – are there other possible account types that would be accessible by PISPs?
15. Is there a need for a "Definition Document" to sit alongside the Standard?

6. Considerations

6.1. Assumptions

The options in section 3 are presented for consideration, however, there could be other mechanisms that the ASPSPs may find appropriate to issue new token(s) without disruption to the AISP services.

6.2. Dependencies

ASPSPs must publish details (on the transparency calendar and their development portals) explaining which approach they have implemented for the issuance of new tokens and when they will be ready with the new SCA exemption change.

OBIE to enhance the transparency calendar to enable the ASPSPs to capture the necessary information.

6.3. Constraint

ASPSP implementations of access & refresh tokens are based on the FAPI specification and NOT the Open Banking Standard. Therefore, OBIE is not able to define a common approach for token management, as it does not have visibility of each ASPSP implementation and the custodianship of the FAPI specification resides with the Open ID Foundation.

Based on the existing six-month implementation window, our expectation is that the CMA9 will deploy their changes to production systems by September 2022. This may result, unless the regulator allows AISPs to delay their implementations, in a period of flux, as AISPs must be ready by end of June. The implication of this would mean that a PSU would continue to reconfirm consent at the AISP and reauthentication at the ASPSP every 90 days potentially from 26 March 2022 (noting that AISPs have until the 26 July 2022 to implement) until the 26 September 2022.

7. Requirements for the Standard

These are stated as requirements of the OBIE solution.

Requirements marked as 'M'(Must) are in the scope of the OBIE solution. All other requirements are listed for future consideration.

All requirements below are 'optional' for implementation by ASPSPs and/or TPPs. For the CMA9 ASPSPs, these requirements are 'conditional' for implementation, as they will for in scope CMA Order (e.g., PCA and BCA) accounts and 'optional' for other accounts. These terms are defined in the document "Categorisation of requirements for standards and implementation".

ID	Description	MoSCoW	ASPSP implementation	Traceability
New SCA exemption				
1	The OBIE's Solution(s) **must** provide guidance to AISPs on how to reconfirm consent with the PSU every 90 days.	M	N/A	CEG >> AIS Consent Dashboard – Revocation, Reconfirm,Re-auth >> **Reconfirm consent at the AISP** CEG >> PSU Notifications >> Figure 4: Example notification to start a reconfirmation of consent journey
2	The OBIE's Solution(s) **must** enable the AISP to redirect the PSU to their ASPSP to re-authenticate when re-authentication is required by the ASPSP.	M	Conditional	CEG >> AIS Consent Dashboard – Revocation, Reconfirm,Re-auth >> **Re-authentication of access**
3	The OBIE's Solution(s) **must** provide guidance to the ASPSPs to ensure that ASPSPs request the PSUs to re-authenticate only in permitted circumstances* i.e.,	M	Conditional	CEG >> AIS Consent Dashboard – Revocation, Reconfirm,Re-auth

	when it has proportional and objective reasons for doing so. *Note: Fraud or unauthorised access or revoked access accidentally at the ASPSP or request more data than permitted under Art 10a e.g., 100days of data and not every 90 days.			
4	The OBIE's Solution(s) **<u>must</u>** provide guidance to the AISPs to ensure that the AISP does not change the data clusters, or any information associated with the original consent while seeking reconfirmation of consent.	M	N/A	CEG >> AIS Consent Dashboard – Revocation, Reconfirm,Re-auth >> **Reconfirm consent at the AISP**
5	The OBIE's Solution(s) **<u>must</u>** provide guidance to ensure that none of the underlined information like the data clusters or any information associated with the original consent are changed when the PSU is re-authenticating at the ASPSP.	M	Conditional	CEG >> AIS Consent Dashboard – Revocation, Reconfirm,Re-auth >> **Re-authentication of access**
6	The OBIE's Solution(s) **<u>must</u>** provide guidance to the AISPs that they need to get explicit reconfirmation of consent from the PSU every 90 days to continue to access the PSU's account at the ASPSP.	M	N/A	Section - Token Management for new SCA exemption
7	The OBIE's Solution(s) **<u>must</u>** provide guidance to the AISPs that they do not need to inform the ASPSP when reconfirmation of consent is completed by the PSU.	M	N/A	Section - Token Management for new SCA exemption

8	The OBIE's Solution(s) **must** provide guidance to the AISPs that they must not access the PSU's account details until the PSU has reconfirmed consent.	M	N/A	Section - Token Management for new SCA exemption
9	The OBIE's Solution(s) **must** provide guidance that if technically required, ASPSPs may ask the PSU to re-authenticate when they are ready with the new SCA exemption changes in order to issue new long-lived token(s) to the AISP.	M	Conditional	Section - Token Management for new SCA exemption
10	The OBIE's Solution(s) must provide guidance to ensure that the PSU must not be required to re-authenticate every 90 days for the ASPSPs to issue a new token to the AISP.	M	Conditional	Section - Token Management for new SCA exemption
11	The OBIE's Solution(s) **must** enable the ASPSPs to provide details on transparency calendar that include - a) When they will be ready with the new SCA Article 10A changes? b) What approach to issue new token(s) is adopted?	M	Conditional	Section - Dependencies
Access dashboards				
12	The OBIE's Solution(s) **must** provide guidance to ensure ASPSPs show the PSU when the AISP has last accessed the account information on the access dashboard.	M	Optional	CEG >> AIS Access Dashboard & Revocation >> Figure 1: ASPSP Access Dashboard for AIS - zero-clicks from home page (desktop)
13	The OBIE's Solution(s) **must** provide guidance to ensure ASPSPs show the PSU the status of the	M	Conditional	CEG >> AIS Access Dashboard & Revocation >> Figure 1: ASPSP

	consent (Active or connected when the consent is still in authorised state and consent expiry date has not elapsed) on the access dashboard.			Access Dashboard for AIS - zero-clicks from home page (desktop)
Transaction Risk Indicator (TRI)				
14	The OBIE Solution(s) **must** enable PISPs pre-populating in the payment initiation process payload risk scoring fields related to the transaction characteristics: • Payee Account Name and Payee Account Identification Details, that will be immutable and unaltered. • Yes/No field to establish contractual relationship with payee. • Yes/No field to establish integrated check-out and pay facility between merchant and PISP.	M	Optional	Refer to API Specs - https://github.com/OpenBankingUK/read-write-api-docs-pub/commit/b23597e2c7f64ce132bb2a5e49eb965e88df441a https://github.com/OpenBankingUK/read-write-api-docs-pub/commit/a767d307cb49d00087875ae61fc73a6741aa89d6
15	The OB Solution(s) **must** enable the PISP implementing additional **Payment Context Codes** associated with each payment as part of payment consent request to the ASPSP. PCCs will be extended with following fields: • E-commerce Merchant initiated payment; • E-commerce PISP Payee; • Point of Sale; • Funds Transfer • Invoice payment apart from bill payment	M	Optional	

16	The OBIE Solution(s) **<u>must</u>** enable the PISP to provide the payment purpose codes. It will replace Merchant Category Codes. Payment Purpose Codes will be associated with each payment as part of payment consent request to the ASPSP.	M	Optional	
17	The OBIE Solution(s) **<u>must</u>** enable the PISP to provide a new risk- scoring **Beneficiary Account Type** field with each payment as part of payment consent request to the ASPSP.	M	Optional	

8. Terminology

Some of the illustrative wireframes have been updated with more customer-friendly terminology to reflect the Common Terminology Guide to improve customer awareness and understanding.

These changes can be found here.

- Customer Experience Guidelines[9] and Change Log[10]

9. Errata corrections

There were a number of updates to the standard driven by errata identified in 3.1.9.

More details can be found in the known issues log[11].

[9] https://consultation.standards.openbanking.org.uk/customer-experience-guidelines/introduction/section-a/v3-1-10-draft/
[10] https://consultation.standards.openbanking.org.uk/customer-experience-guidelines/change-log/v3-1-10-draft/
[11] https://openbanking.atlassian.net/wiki/spaces/DZ/pages/47546479/Known+Specification+Issues

10. Consultation Questions

Implementation of 90 day changes

1. Do you agree with our conclusions that Options 2 & 3 are not credible at present?
2. Do you believe that option 1 is the only credible approach?
3. Would there be benefit in having a common approach for the duration of long lived tokens? If so what approach is recommended?
4. Are there other alternatives that should be considered?

Dashboards

5. Do you agree that absence of the time and date of when data was last shared does not fundamentally undermine the intended purpose of access dashboards?
6. Would it be useful to develop guidance for TPPs to facilitate a common industry approach to the timely cancelation of unused connections?
7. Is “Connected” a better descriptor to show the status of the connections than “Active”? Are there alternative descriptors which would be better for end users?

Transaction Risk Indicators

8. Does the inclusion of “**Payee Account Name”** add value given that **“Creditor Name”** is an existing component of the payment payload?
9. If so, should the “**Payee Account Name”** match the account name in AIS or be consistent with what would be returned in a CoP check?
10. Does “Integrated check-out and pay facility between merchant and PISP” need more definition?
11. Should “Invoice & bill payments” be separate or combined?
12. Are all of the key PISP models covered in the proposed “Payment Context Codes “categories?
13. Should “Merchant Category Codes” be retained in addition to “Payment Purpose Codes” until a future date?
14. In relation to “Beneficiary Account Type” – are there other possible account types that would be accessible by PISPs?
15. Is there a need for a “Definition Document” to sit alongside the Standard?