THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

How to use this document:

1. Please fill in your professional details in the section below
2. For each line in the comments sheet, please assign a sequence comment N° (in ascending order)
3. For each line in the comments sheet, please assign a comment ID:
   - T = Technical comment (correction or clarification of a concrete technical requirement defined by the specification standards, not altering or expanding any functional features). Please provide an exact reference of the comment to the location in the applicable document.
   - E = Editorial comment (correction or clarification of a topic description without implying any technical changes. Only the descriptive part of the specification might be affected). Please provide an exact reference of the comment to the location in the applicable document.
   - G = General comment (any other type of comment, which may also include altered or expanded functionality for which a justification must be provided)

Fields of the form which are marked grey must not be completed by the contributor.
Please send your completed comments sheet exclusively by email to: consultation@berlin-group.org until Friday 17 November 2017 (COB).

Date:	31-10-17
Name of contributor:	Michael Adams
Email of contributor:	Michael_adams@quali-sign.com
Telephone of contributor:	+44 7808 203856
Title/Position:	Founder
Organisation:	Quali-Sign Ltd
Type of Organisation (FinTech/ASPSP/both):	FinTech – Mobile app developer
Address:	Woodview, Hough Lane, Alderley Edge, Cheshire, SK9 7JE
Country:	United Kingdom
Your reference:	

To ensure open and transparent consultation, the Berlin Group may wish to publish the received market feedback on the Berlin Group public website, only mentioning the organisation name and their submitted comments.

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

Document:

01. NextGenPSD2 Access to Account Interoperability Framework - General Introduction Paper V099_20171002.pdf

Comment (N° / ID)	Comment/question (when applicable with justification/rationale or reference section/page n°)	Suggested Resolution (alternative)	Agreed Resolution (Workgroup)
	No comments		

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

Document:

02. NextGenPSD2 Access to Account Interoperability Framework - Operational Rules V099_20171002.pdf

Comment (N° / ID)	Comment/question (when applicable with justification/rationale or reference section/page n°)	Suggested Resolution (alternative)	Agreed Resolution (Workgroup)
1 / G	Page 7. - Section 3.3.1 (Bullet 1). With reference to “Please note: An ASPSP may of course also support other [PSD2]-compliant interfaces.”, it is our assumption that any functionality deemed out of scope on day 1, will need to be implemented by ASPSPs via an additional API e.g. Corporate Banking / Bulk payments / Multiple user authorisation.	ASPSPs must meet the entirety of the required XS2A API scope within the RTS timescales. In order to do so, out of scope functionality already available via existing APIs, such as EBICS, must be considered.	
2 / G	Page 10 - Section 4.1 “For the current version of the XS2A interface the initiation of the following payment transactions is not supported by the core services but may be supported by extended services” The reference to ‘extended services’ is unclear. For example the current design for ‘Embedded’ SCA capture only supports single payments. If it is implied that bulk payments (for example) could be supported via extended services, an alternative SCA capture procedure will be required.	See suggested resolution for 1 / G which could be applied to Bulk Payments, Scheduled Payments, Recurring Payments and Debit Payments.	
3 / G	Page 17 – Section 5.1.2 “For the exchange of the messages the protocol http (https) is used” Whilst this approach offers encryption of data during transmission between the servers of the TPP and ASPSP, this is only at the transport level and is not end-to-end. This is introducing unnecessary risk and is less secure than the ASPSP’s direct channel. Under GDPR Article 33, data deemed to present a specific risk will require an impact assessment. Data that presents a specific risk includes any data that can predict a person’s 'economic situation, location, health, personal preferences, reliability or behaviour'. It is clear that payment and account activity data will be deemed to present a specific risk.	We believe that all payload data (payment and account activity) must be encrypted end-to-end.	

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

Document:

02. NextGenPSD2 Access to Account Interoperability Framework - Operational Rules V099_20171002.pdf

Comment (N° / ID)	Comment/question (when applicable with justification/rationale or reference section/page n°)	Suggested Resolution (alternative)	Agreed Resolution (Workgroup)
4 / G	Page 21 – Section 5.3. Please consider the use case whereby a TPP issues a mobile app to their customers which communicates directly with the ASPSP rather than via a TPP server. The RTS does not explicitly rule out this approach, however it does mandate that TPP identifies itself via an eIDAS Web Site or Company Seal certificate. This is impractical for a mobile device which communicates directly with the ASPSP.	The use of Terminal Certificates could provide a solution. The TPP app would provision a Terminal Certificate (signed by their eIDAS Company Seal credentials) to the user device. The TPP would continue to register their eIDAS Company Seal certificate with the directory service, however this certificate would be equivalent to a Document Verifier certificate. The ASPSP could therefore identify the TPP from the certificate chain of the Terminal Certificate. The issued Terminal Certificate could be used for identification at both transport and application layers. This approach would fully meet the RTS requirement to identify a TPP and would also support the use of TPP issued mobile apps.	
5 / G	Page 24 – Section 5.5.1 “Depending on the device used, the PSU may also be redirected to a special authentication app of the ASPSP” How does the ASPSP and TPP locally (i.e. on the device) identify themselves as the owners of their respective apps? It is clear from the RTS that this must be performed via the use of an eIDAS Qualified Web Site or Company Seal certificate. It is not viable to deploy these certificates to a mobile device.	See resolution for 4 / G	
6 / G	Page 25 – Section 5.5.2 “ASPSP decides about SCA yes/no and method/approach to be used”. The decision to apply ‘Decoupled’ SCA is best left in the hands of the PSU.	The PSU should be able to specify once only to their TPP, their SCA preference. If the ASPSP chooses not to support ‘Decoupled’ SCA, it should reject the payment initiation request.	

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

Document:

02. NextGenPSD2 Access to Account Interoperability Framework - Operational Rules V099_20171002.pdf

Comment (N° / ID)	Comment/question (when applicable with justification/rationale or reference section/page n°)	Suggested Resolution (alternative)	Agreed Resolution (Workgroup)
7 / G	Page 26 – Section 5.5.3 "In particular the TPP has to provide a means of displaying the challenge data to the PSU since the PSU needs this data to calculate the OTP." The design for Embedded SCA has been tailored to accommodate the use of EMV smartcards together with a handheld TAN reader. It is our understanding that SCA is achieved in this situation using a symmetric key unique to the card and a copy of which is held at the ASPSP. Banks currently advise their customers that "We will never ask you to use your card reader over the phone." Inserting the TPP between the PSU / TAN reader and the ASPSP introduces the opportunity for a 'man in the middle' attack. This is generally recognised as not an acceptable solution.	The use of EMV smartcards with a symmetric key + TAN reader should only be used in the 'Redirect' SCA procedure. For 'Embedded' SCA, alternative technologies must be considered, for example digital signatures and X.509 certificates. The PSU's SCA credentials can still be stored on a smartcard which supports asymmetric cryptographic functions.	
8 / G	Page 26 – Section 5.5.3 Figure 13 The current design for Embedded SCA involves an unnecessarily large number of interactions between the PSU, TPP and ASPSP. This degrades the PSU experience and is impractical in the case of the 'point of sale' scenario (e.g. purchase of petrol at a petrol station).	The procedure should be designed to minimise the number of interactions required.	
9 / G	Page 26 – Section 5.5.3 The eIDAS regulation provides legal certainty over the strength of an electronic signature. Operating outside of this legal framework leaves the ASPSP's at risk of retaining liability in the event of fraud, even if SCA has been captured. This standard offers no support for eIDAS Qualified Electronic Signatures.	The standard should at least allow for the capture of eIDAS compliant 'Advanced Electronic Signatures'. If the ASPSP issues the PSU with a bank card that has been certified as an 'Qualified Signature Capture Device' with a 'Qualified Certificate' issued by a 'Qualified Trust Services Provider', the signature will then be recognised as a 'Qualified Electronic Signature' and be legally binding.	

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

Document:

02. NextGenPSD2 Access to Account Interoperability Framework - Operational Rules V099_20171002.pdf

Comment (N° / ID)	Comment/question (when applicable with justification/rationale or reference section/page n°)	Suggested Resolution (alternative)	Agreed Resolution (Workgroup)

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

6-weeks market consultation
NextGenPSD2 Access to Account Interoperability Framework

COMMENTS SHEET V1.00

Distribution: Publicly available

Document:

03. NextGenPSD2 Access to Account Interoperability Framework – Implementation Guidelines V099_20171002

Comment (N° / ID)	Comment/question (when applicable with justification/rationale or reference section/page n°)	Suggested Resolution (alternative)	Agreed Resolution (Workgroup)
	No comments.		