

NISP-NL

Providing a checklist for ASPSP testing facility and summary of NISP TPP Integration Testing documentation
TPP Integration Testing workstream

Amsterdam
28 January 2019

Table of contents

- **Recap**
- Introduction TPP Integration Testing
- Deliverable: TPP Integration Testing checklist
- Deliverable: Summary NISP TPP Integration Testing documentation

Recap: Activities and deliverables have been defined for TPP Integration Testing sub-workstream to ensure successful testing by Dutch ASPSPs

	1a: TESTING – TPP INTEGRATION TESTING	1b: TESTING – CONFORMANCE TESTING	1c: TESTING – GENERAL
GOAL	Provide ASPSPs with checklist for compliant TPP Integration Testing facility	Support ASPSPs to interpret value of NISP Conformance Testing documentation, as input for requesting exemption to fall back obligation	Ensure alignment with relevant stakeholders for overall testing workstream
ACTIVITIES	- Define checklist for TPP Integration Testing: avoid duplication of ASPSPs effort by jointly creating overview of integration testing based on the RTS on SCA, the exemption GL, the EBA Opinion on implementation of RTS on SCA and NISP documentation, and determine what functionality and features are essential to include in testing facility to enable seamless and consistent experience for TPPs Note: ASPSPs cross-check individually current designs/implementation against checklist	- Create insights in and correctly scope NISP Conformance Testing: avoid duplication of ASPSPs effort by jointly interpreting NISP Conformance Testing docs, determining applicability to Dutch context and including insights on NISP Conformance Testing documentation, which enables ASPSPs to better understand and perform Conformance Testing Note: ASPSPs perform conformance test individually	- Inform DNB on NISP documents and to what extent these apply to the Dutch ASPSP context: ensure correct scoping, interpretation and understanding of NISP documents - Provide continuous feedback to NISP regarding TPP Integration and Conformance testing: ensure continuous improvement of NISP deliverables and as a result of that improve quality of Dutch ASPSP's NextGenPSD2 implementation
DELIVERABLES	- Checklist TPP Integration Testing - Summary of NISP TPP Integration Testing recommendations	Insights in value NISP ASPSP Conformance Testing	- NL applicability of NISP deliverables - Alignment DNB and market participants on scope NISP deliverables, including report-out

Recap: Sub-workstream 1a provides checklist for ASPSP testing facility in February and enables individual ASPSPs to improve current testing facility design

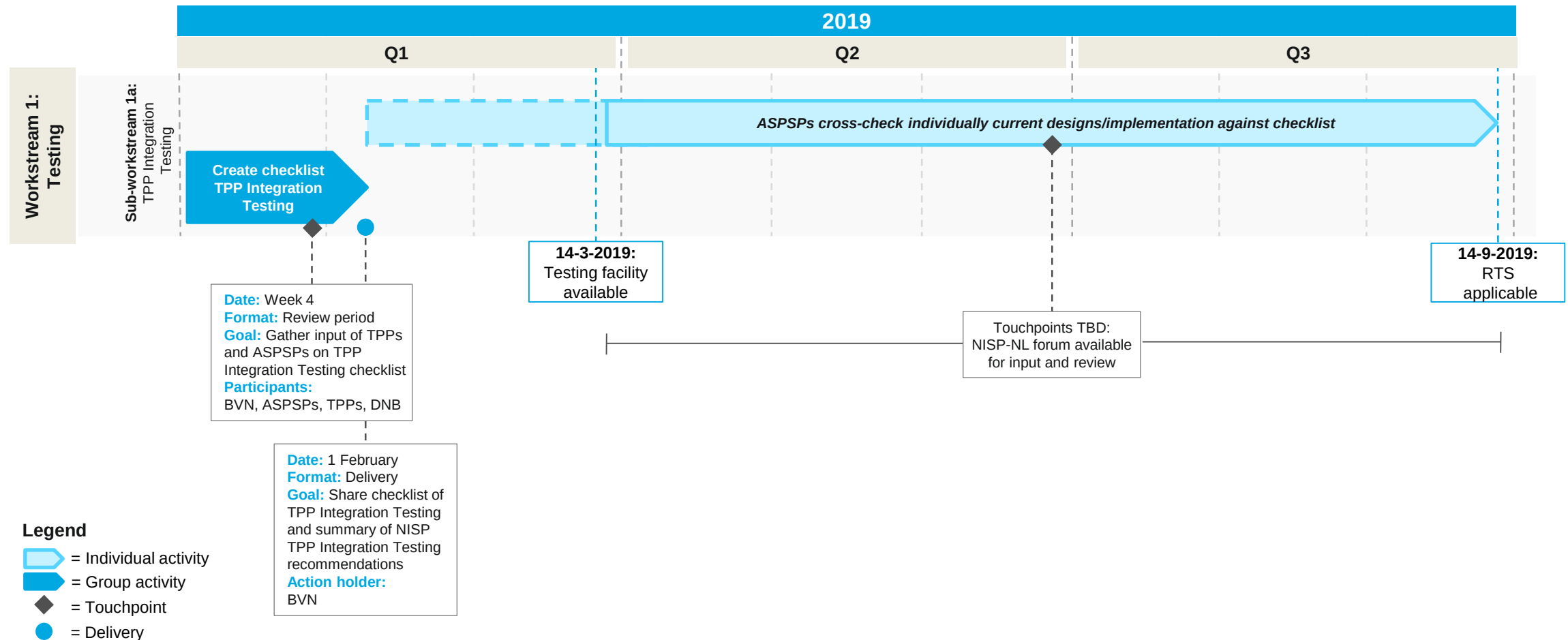
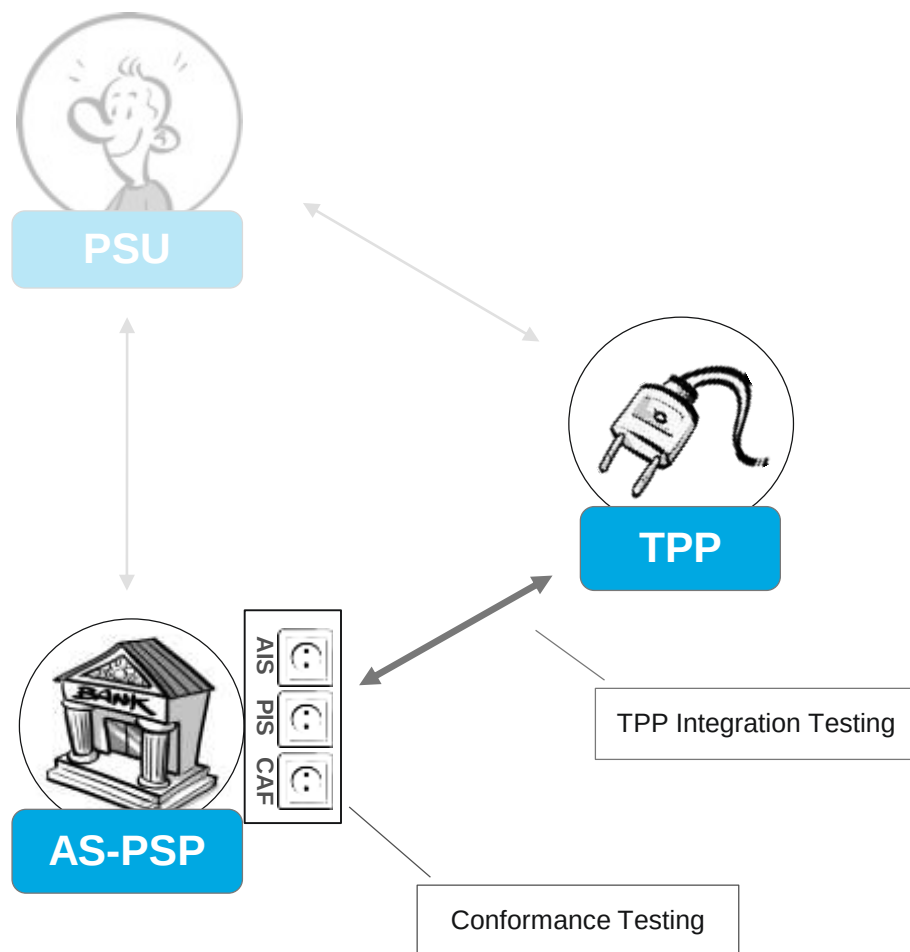


Table of contents

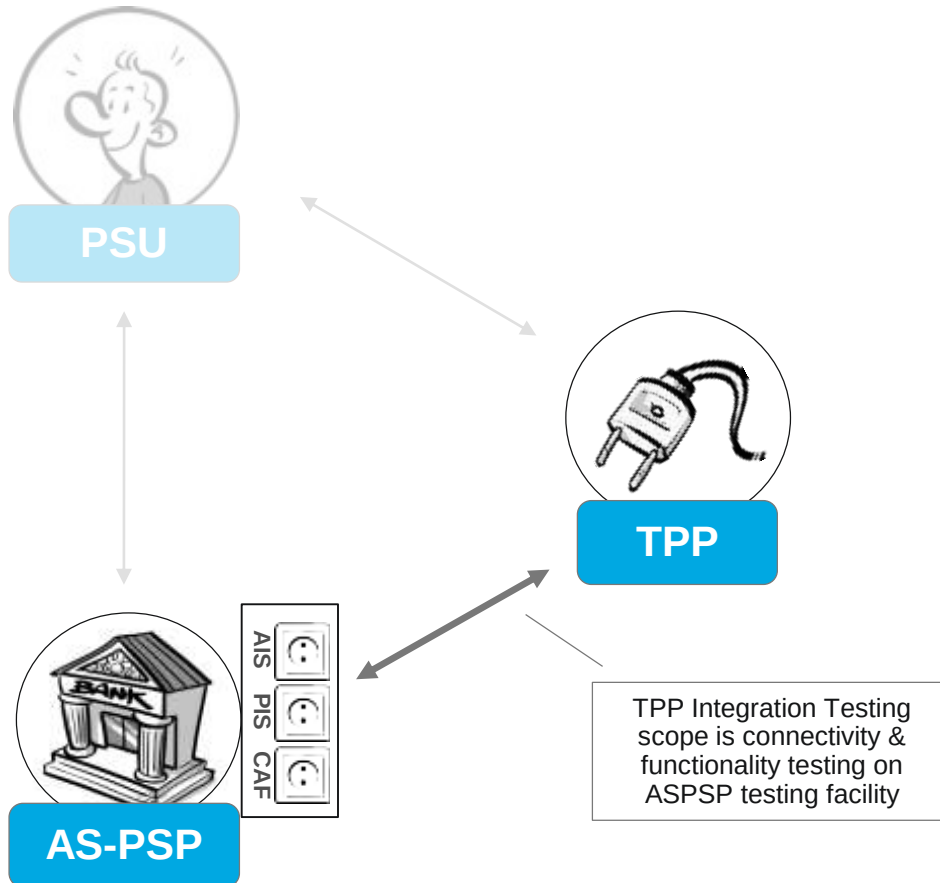
- Recap
- **Introduction TPP Integration Testing**
- Deliverable: TPP Integration Testing checklist
- Deliverable: Summary NISP TPP Integration Testing documentation

ASPSPs *must* offer testing facility for TPP Integration Testing and *can* perform Conformance Testing internally



- RTS on SCA stipulate several requirements on testing of PSD2 XS2A implementations of ASPSPs
- In NISP-NL collaboration, two types of testing are distinguished:
 1. **Conformance Testing** is an optional action when applying for a fallback exemption and pertains to an individual ASPSP testing to what extent its dedicated interface is PSD2 XS2A compliant (possibly using a conformance testing tool issued by a market initiative such as NISP)
 2. **TPP Integration Testing** pertains to an ASPSP offering a testing facility to enable TPPs to test the connectivity and functionality of the dedicated interface

The 2 deliverables ‘Checklist of TPP Integration Testing’ and ‘summary of NISP documentation’ pertain to scope of ASPSP testing facility



- In order to enable TPPs to test the dedicated interface, **ASPSPs** must offer a **testing facility**, that caters for **functionality** and **connectivity testing**
- **Scope of TPP Integration Testing sub-workstream** pertains to legal requirements regarding the offering of a testing facility
- **Scope of NISP's TPP Integration Testing documentation** is broader, since it provides recommendations for ASPSPs to offer a PSD2/RTS ready testing facility that suits TPPs' needs
- For the **NISP-NL collaboration** TPP Integration Testing sub-workstream, the **compliance** of the **design** of the **dedicated interface**, and the different test scenarios that follow from that design are **out of scope**

- **NISP-NL collaboration for TPP Integration Testing sub-workstream has 2 deliverables:**
 1. **TPP Integration Testing checklist** that elaborates on legal requirements to which ASPSP must adhere in providing testing facility
 2. **Summary of NISP TPP Integration Testing documentation**, detailing NISP's testing facility recommendations banks can adhere to

Table of contents

- Recap
- Introduction TPP Integration Testing
- **Deliverable: TPP Integration Testing checklist**
- Deliverable: Summary NISP TPP Integration Testing documentation

NISP-NL TPP Integration Checklist uses all relevant legal sources to derive ASPSP compliance requirements



PSD2



RTS on SCA and CSC



GL exemption
Contingency
Mechanism



EBA opinion
implementation RTS on
SCA and CSC

RTS on SCA and GL on fallback exemption determine majority of TPP Integration Testing requirements

Source	Article
RTS 30(4)	Account servicing payment service providers shall ensure that, except for emergency situations, any change to the technical specification of their interface is made available to authorised payment initiation service providers, account information service providers and payment service providers issuing card-based payment instruments, or payment service providers that have applied to their competent authorities for the relevant authorisation, in advance as soon as possible and not less than 3 months before the change is implemented.
RTS 30(5)	Account servicing payment service providers shall make available a testing facility, including support, for connection and functional testing to enable authorised payment initiation service providers, payment service providers issuing card-based payment instruments and account information service providers, or payment service providers that have applied for the relevant authorisation, to test their software and applications used for offering a payment service to users. This testing facility should be made available no later than six months before the application date referred to in Article 38(2) or before the target date for the market launch of the access interface when the launch takes place after the date referred to in Article 38(2). However, no sensitive information shall be shared through the testing facility.
RTS 32(1)	Subject to compliance with Article 30 and 31, account servicing payment service providers that have put in place a dedicated interface shall ensure that the dedicated interface offers at all times the same level of availability and performance, including support, as the interfaces made available to the payment service user for directly accessing its payment account online.
RTS 34(1)	For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation.
GL 6.5	The testing facility should allow ASPSPs, authorised PISPs, AISP and CBPIIs or payment service providers that have applied to their competent authorities for the relevant authorization to test the dedicated interface in a secure, dedicated testing environment with non-real PSU data, for the following: a. A stable and secure connection; b. The ability of ASPSPs and authorised PISPs, AISP and CBPIIs to exchange the relevant certificates in accordance with Article 34 of the RTS; c. The ability to send and receive error messages in accordance with Article 36(2) of the RTS; d. The ability of PISPs to send, and of ASPSPs to receive, payment initiation orders and the ability of ASPSPs to provide the information requested in accordance with letter (b) of Article 66(4) of PSD2 and letter (b) of Article 36(1) of the RTS; e. The ability of AISP to send, and of ASPSPs to receive, requests for access to payment account data, and the ability of ASPSPs to provide the information requested in accordance with letter (a) of Article 36(1) of the RTS; f. The ability of CBPIIs and PISPs to send, and of ASPSPs to receive, requests from CBPIIs and PISPs and the ability of the ASPSP to send a 'yes/no' confirmation to CBPIIs and PISPs in accordance with letter (c) of Article 36(1) of the RTS; g. The ability of PISPs and AISP to rely on all the authentication procedures provided by the ASPSP to its PSUs.

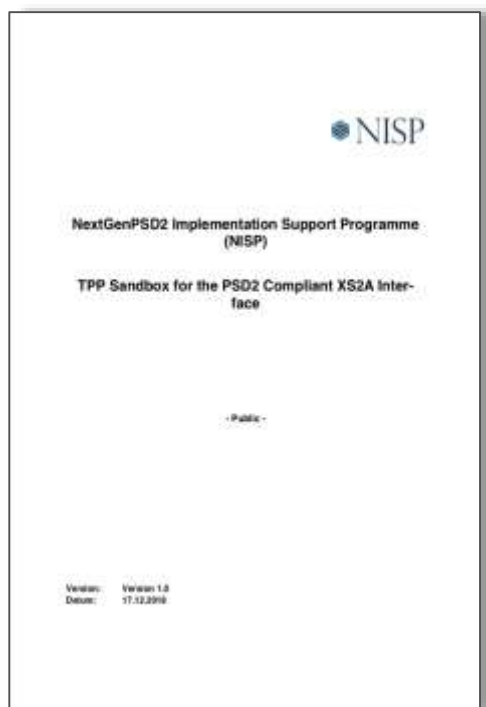
ASPSP testing facility checklist contains 14 requirements

#	Requirement	Legal ground
1	ASPSPs shall address changes to the technical specifications of their interface are made available to authorised PSPs in advance as soon as possible and not less than 3 months before the change is implemented	RTS 30(4)
2	ASPSPs shall make available a testing facility for connection and functional testing to enable TPPs to test their software and applications used for offering a payment service to users	RTS 30(5)
3	ASPSPs shall make available the testing facility no later than six months before the application date of the RTS (i.e. 14-9-2019), or before the target date for the market launch of the access interface when the launch takes place after 14-9-2019	RTS 30(5)
4	ASPSPs shall not share sensitive information, such as as personal data, including personalised security credentials which can be used to carry out fraud, through the testing facility	RTS 30(5)
5	ASPSPs shall provide support to TPPs on their testing facility. ASPSPs are free to decide on the format of support they offer to TPPs	RTS 30(5)
6	ASPSPs and TPPs shall use eIDAS certificates for the purpose of identification when using the testing facility	RTS 34(1)
7	In order for ASPSPs to be able to identify and more easily resolve issues per TPP (role), an optional registration process can be set up	GL 6.6
8	The testing facility should allow TPPs to test for a stable and secure connection	GL 6.5(a)
9	The testing facility should allow TPPs to test for the ability of ASPSPs and authorised PISPs, AISP and CBPIs to exchange the relevant certificates in accordance with Article 34 of the RTS	GL 6.5(b)
10	The testing facility should allow TPPs to test for the ability to send and receive error messages in the case of an unexpected event or error occurring during the process of identification, authentication or the exchange of data elements	GL 6.5(c)
11	The testing facility should allow PISPs to initiate a payment and to receive the same information as available to the PSU when making a payment online	GL 6.5(d)
12	The testing facility should allow AISPs to request for access to and receive payment account data	GL 6.5(e)
13	The testing facility should allow CBPIs and PISPs to request and receive a 'yes/no' confirmation	GL 6.5(f)
14	The testing facility should provide TPPs with the ability to rely on all authentication procedures provided by the ASPSP to its PSUs	GL 6.5(g)

Table of contents

- Recap
- Introduction TPP Integration Testing
- Deliverable: TPP Integration Testing checklist
- **Deliverable: Summary NISP TPP Integration Testing documentation**

NISP-NL deliverable forms summary of NISP TPP Integration Testing documentation



NISP TPP Integration
Testing documentation

- **NISP documentation** aims to **bundle legal requirements** for TPP Integration Testing and aims to **provide common testing framework** between ASPSPs and TPPs
- **Value** of NISP TPP Integration Testing documentation lies in the **recommendations** it describes, providing levers for ASPSPs to offer a testing facility that suits TPPs' needs
- **NISP-NL** collaboration aims to offer a **summary of NISP TPP Integration Testing documentation**, enabling ASPSPs to offer a testing facility that suits TPPs' needs

Summary of NISP TPP Integration Testing documentation, containing recommendations for ASPSP testing facility (1/4)

NISP Chptr	Topic	Summarised NISP recommendation
2	Definition of the TPP sandbox	Each TPP is testing against each test environment (also called 'testing facility') of the ASPSPs. The test facility can: • be used as portal which will offer the registration process for the TPP, implemented by each ASPSP independently • offer a selection of banks, in the case of multiple member banks • forward the TPP incoming messages to the APIs of the selected ASPSP or member bank behind
3.1	Assumptions for certificate handling	• Permitted trust centers (QTSPs) will deliver certificates for production and testing, and the delivery of these TLS and electronic seal certificates is following the [eIDAS] requirements and is only dependent on the registry entry of the corresponding national competent authority • For testing, ASPSPs can also choose to distribute their own test certificates (see 3.3)
3.2	Service level of the sandbox	• The testing facility should be available 24/7 for online testing and ASPSPs should inform TPPs about planned downtimes of the testing facility • TPPs should receive first level support for the sandbox, e.g. by the means of an e-mail address for questions • The APIs of the ASPSP in operational use are improved and enhanced permanently and the testing environment has to be adapted accordingly. In the case of two supported versions of an endpoint, these endpoints will be addressable in the same sandbox and the test endpoints will be taken out of the sandbox as soon as the corresponding version in production has been deactivated • It is advised that the TPPs should re-test new versions of the API
3.3	Optional registration process	• ASPSPs may offer a (non-mandatory) registration process for a TPP, enabling ASPSPs to provide tailored support to TPPs and to report on a per TPP role level on testing coverage in the 6 month testing period starting 14-3-2019 • Registration process can entail: - ASPSPs can ask only for the delivery of documentation, including at least the e-mail address of the TPP and its functional role: PIS only, AIS only, PIIS, or combinations of these roles or property of the TPP - Registration can be implicit by using client test certificates for access to interface documentation - The delivery of a proprietary corresponding test certificate for communication might be performed to the TPP if relevant and supported by the ASPSP. This test certificate could be used for early testing, where no official registration of the TPP has happened yet or eIDAS test certificates are not available yet - The scope of the testing can be identified by e.g. offered coding/endpoints and services or offered list of recommended integration test scenarios - Test identifications will be offered by the ASPSP to trigger different behaviour of the interface - The available test accounts for the PSU in question are listed, though the accounts are stateless
3.4	Basic requirements for syntax and semantic checks	The ASPSP test facility shall perform several check functions in order to ensure connection and functional testing, such as: check of the transport level, enforce the correct session layer and TLS flow, security, application layer, check of the available service requests per role, check of the plausibility of data, check of the process flow, and daily deletion of resources created by TPPs

Note: Recommendations made by NISP aim to facilitate ASPSPs in offering testing facility that suits TPPs' needs. Recommendations are therefore not mandatory

Summary of NISP TPP Integration Testing documentation, containing recommendations for ASPSP testing facility (2/4)

NISP Chptr	Topic	Summarised NISP recommendation
3.5	Stress testing	Stress testing is excluded from the integration test environment, as it pertains to internal ASPSP testing
3.6	Stateless mockups of accounts	- The accounts given in the testing environment are stateless, the reset routines of the sandbox (e.g. in a morning daily run) should add transactions, or reset the transactions dates of the entries taking the new date in account, to be able to offer pending and booked transactions - There should be different PSU-IDs, Consent-IDs or Account Identifications to trigger the different reactions of the testing facility
3.7	Stateless mockups of credential checks	- Static passwords or OTPs for PSU authentication have to be static and equal for all PSU-IDs, e.g. 1234 - Accounts cannot be blocked due to too many retries of wrong passwords
3.8	Basic requirements for the SCA processes	SCA methods are mocked for the integration tests, as it is not the focus of TPP Integration Testing, and are described below: - SCA Redirect approach: should be done to a webpage where the authentication result is displayed, the TPP can retrieve the corresponding transaction status from the corresponding payment resource afterwards - SCA OAuth: the OAuth protocol is fully supported in test - SCA Decoupled approach: no authentication app is used as the SCA processing is anyhow out of band. The result of the decoupled method depends only on the usage of the PSU-ID or PSU account identification - SCA Embedded approach: a challenge for the SCA processing, e.g. a flickering code, is generated by the ASPSP test system. This code does not need to correspond to the transaction data, but is syntactically correct
3.9	General test requirements	The test environment offers: - Obvious and unambiguous error codes in responses - Additional information per deviation (e.g. location of syntax or format error) - Harmonised error information (e.g. Type of error: syntax, format or content error, location of the error: XML or JSON path information, additional text about the error if available or an internal reference) - Optionally test reports for TPP under the following ASPSP's requirements (e.g. signed logfile or pass/fail test report)
3.10	Additional test requirements	The test environment may offer in addition: - Signed test reports used as proof of test (Test operation per TPP can be logged and the log-file can be signed as proof for the successful test cycle) - List of TPPs that tested on the sandbox - List of TPPs that run successfully through all documented test scenarios - Analytics of the performed test

Note: Recommendations made by NISP aim to facilitate ASPSPs in offering testing facility that suits TPPs' needs. Recommendations are therefore not mandatory

Summary of NISP TPP Integration Testing documentation, containing recommendations for ASPSP testing facility (3/4)

NISP Chptr	Topic	Summarised NISP recommendation
4.1	Test coverage	The TPP is recommended to test all services and payment products regarding positive and negative test cases
4.2	Generic tests applicable for all services	• Test certification and roles: when being addressed by the TPP for the different services of the API, the sandbox will check: the correct TLS processing of the TPP, the usage of a permitted eIDAS certificate by the TPP and the correct role when addressing the Payment Initiation, Account Information or Confirmation of Funds Services • Generation and authorisation of resources: to fully reflect the production site behaviour, resources will be generated dynamically in the sandbox and will reflect all status changes of the production system • Existence of endpoints: the sandbox will be in access methods to endpoints the exact reflection of the production API system
4.3	PSU profiles	The sandbox will support different PSU profiles for the production system to recognise PSUs which are e.g. allowed/supported to perform a certain action
4.4	Mocked credentials	This concept supports static credentials for credential checks: • e.g. 'correctPassword' is a tag for a password that is correct for all PSU-IDs • e.g. 'correctOTP' for an OTP that is correct for all SCAs to be performed in an embedded SCA Approach
4.5	Payment initiation	Example tags are given explaining the configuration entry, including their HTTP code and message code
4.6	Cancellation of payment initiations	For testing the cancellation of Payment Initiations, no configuration is needed, since the behaviour on products is a copy of the production system, but note that the cancellation should not be tested too late after the initiation, since the payment resource might be deleted by e.g. daily end of business resetting of the test environment
4.7	Establishing consents	Consents are generated and authorised as resources, in analogy to payment initiation, which is why a series of tags are presented. While the consent generation will be offered by all sandbox implementations, the usage of the consents for follow-up processes differ as they can be: • Mocked consents: the generated <i>consentIds</i> cannot be used afterwards for access to the test accounts • Dynamic consents: the consents are generated and authorised as resources as well

Note: Recommendations made by NISP aim to facilitate ASPSPs in offering testing facility that suits TPPs' needs. Recommendations are therefore not mandatory

Summary of NISP TPP Integration Testing documentation, containing recommendations for ASPSP testing facility (4/4)

NISP Chptr	Topic	Summarised NISP recommendation
4.8	Revocation of consents	With the revocation of consents there will be no configuration, as it is just a copy from production behaviour. The cancellation of mocked up consents will be actively blocked by the sandbox
4.9	Account access	• The ASPSP should offer account_1 to <i>account_m</i> as IBANs or BBANs with different transaction history and balances • ASPSP should have a daily resetting routing, e.g. in the morning, so that the transaction reports always contain pending transactions and booking dates are synchronised • The ASPSPs can implement the account access integration tests differently, either with static predefined consents or with the consents dynamically generated, which is described per section of account access with mocked up consents and account access with generated consents
4.10	Confirmation of funds	A series of tags is suggested for the confirmation of funds

Note: Recommendations made by NISP aim to facilitate ASPSPs in offering testing facility that suits TPPs' needs. Recommendations are therefore not mandatory

NISP-NL

Providing a checklist for ASPSP testing facility

TPP Integration Testing workstream

Amsterdam
28 January 2019