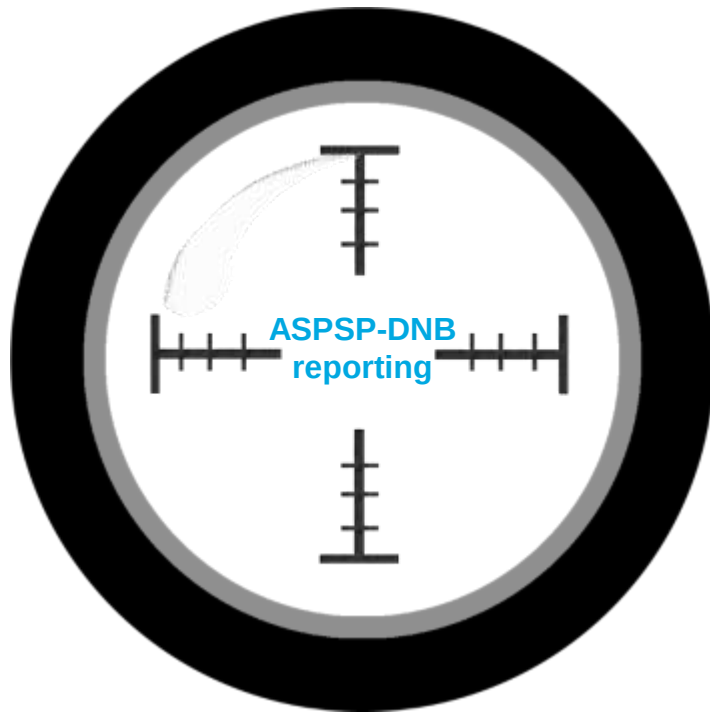


NISP-NL

Plenary work session #1: 'Conformance testing' and 'reporting' workstream

Amsterdam
6 February 2019

Objective of today is to present NISP-NL conformance testing approach and detail standards ASPSP-DNB fallback exemption reporting



- Present NISP-NL conformance testing approach
- Create overview of ASPSP-DNB exemption fallback reporting requirements
- Propose reporting standards (i.e. processes and templates) for ASPSP-DNB fallback exemption reporting
- See BVN website for report-out on this NISP-NL meeting

Today's meeting forms the first in four plenary NISP-NL work sessions that aim ensure smooth and successful exemption process for AS-PSPs



Plenary work session 1:	Plenary work session 2:	Plenary work session 3:	Plenary work session 4:
Date: Wed 6-2-2019 / 14.00-16.30h	Date: Tue 12-2-2019 / 10.00-12.30h	Date: Tue 19-2-2019 / 14.00-16.30h	Date: Tue 26-2-2019 / 10.00-12.30h
Goal: Kick-off detailing ASPSPs-DNB reporting process and templates, discussing scoping of detailing processes and templates and discuss conformance testing	Goal: Kick-off streamlining of testing and wide usage, discuss scoping of information sharing between TPPs and ASPSPs	Goal: Refine and agree on ASPSPs-DNB reporting processes and templates and discuss conformance testing	Goal: Refine information sharing re testing, kick-off identifying/addressing common issues addressed by TPPs
Main participants: ASPSPs & Betaalvereniging, DNB	Main participants: TPPs, ASPSPs & Betaalvereniging, DNB	Main participants: ASPSPs & Betaalvereniging, DNB	Main participants: TPPs, ASPSPs & Betaalvereniging, DNB
Subworkstream: 2a: ASPSP-DNB Reporting, <i>1b: conformance testing</i>	Subworkstream: 2b: Implementation coordination	Subworkstream: 2a: ASPSP-DNB Reporting, <i>1b: conformance testing</i>	Subworkstream: 2b: Implementation coordination

Agenda

- Conformance testing approach NISP-NL
- Break
- Overview exemption fallback reporting requirements
- Exemption fallback reporting timelines
- Proposed reporting standards

- **Conformance testing approach NISP-NL**
- Break
- Overview exemption fallback reporting requirements
- Exemption fallback reporting timelines
- Proposed reporting standards

Recap: Conformance Testing results can support ASPSPs in fallback exemption procedure



Test scenarios
(1, 2, n)

1. Define test input

- ASPSPs use test scenarios that are either proprietary or as presented by market initiatives, such as **NISP Conformance Testing documentation**
- XS2A requirements **form the norm** for conformance testing



AS-PSP
environment

2. Perform conformance test

- ASPSPs internally test **compliance of dedicated interface** by testing conformance of dedicated interface to PSD2 XS2A requirements
- ASPSPs can use **NISP conformance** testing documentation



Reported results
(1, 2, n)

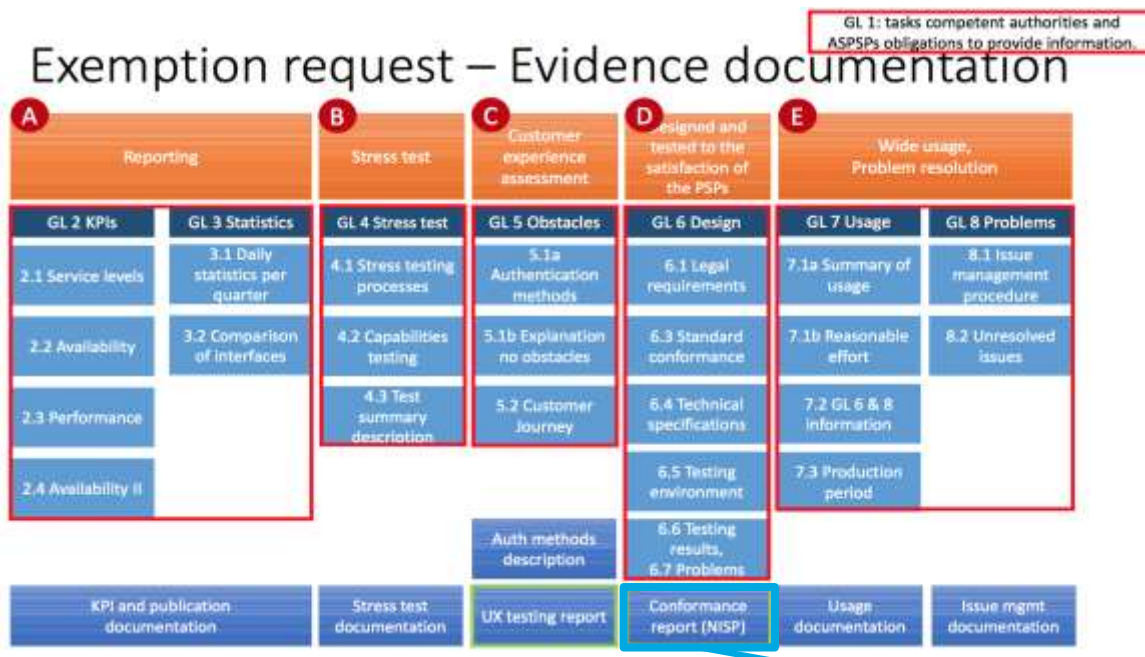
3. Report test output

- ASPSPs add test results to **application** for **exemption** to the **fallback** mechanism to attest compliance of the interface with the respective market initiative standard

Two background reasons that influence the suitability and/or usefulness of the existing **NISP conformance testing documentation**:

1. ASPSPs may **deviate** from the NextGenPSD2 standard in some aspects
2. ASPSPs make use of **in-house proprietary testing scenarios**, allowing them to provide **evidence** in fallback exemption procedure that dedicated interface meets all legal requirements for access and data under PSD2 & RTS

Recap: DNB aims to receive as much standardised evidence as possible, also in ASPSP (conformance) testing



Evidence documentation and evaluation

Cluster	Guideline	Evidence documentation	Method of evaluation
A KPI Reporting	GL 2-3	ASPSP provided documents on KPIs, measurement and publication	Evaluated using standing supervisory practice
B Stress test	GL 4	ASPSP provided documents on stress test design and execution	Evaluated using standing supervisory practice
C Obstacles	GL 5	ASPSP provided documents on Authentication methods and Customer Experience (UX)	Evaluated using UX evaluation, UK Customer Experience Guideline
D Design & Test	GL 6	API initiative provided documents on Conformance ASPSP conformance declaration	Evaluated using NISP conformance proof or own assessment when NISP n/a
E Usage	GL 7-8	ASPSP provided documents on wide usage TPP input on (unresolved) issues	Evaluated against Dutch market situation

- DNB advises to use as much standardised evidence as possible, also in providing ASPSP testing results
- Standardisation of testing results is possible either using NISP conformance testing documentation or ASPSP-proprietary testing, but require collaboration between ASPSPs and DNB

Three options for NISP-NL collaboration regarding conformance testing



Test scenarios
(1, 2, n)

Option 1:

Define test input

- ASPSPs and DNB consent on **generic** (and minimum) **testing scenarios** in **proprietary testing** compliance of ASPSP's dedicated interface
- Pre-defined test input can serve as **check on completeness** of test scenarios covered by AS-PSP's proprietary testing scenarios

***Note:** Prerequisite for this option is that minimum testing scenarios are defined



AS-PSP
environment

Option 2:

Perform conformance test by Test-TPP*

- Dutch ASPSPs create **independent 'test-TPP'** under NISP-NL collaboration
- 'Test-TPP' tests **to what extent dedicated interface** meets all **legal requirements**



Reported results
(1, 2, n)

Option 3:

Report test output

- ASPSPs and DNB consent on **reporting standards for testing results** (processes and/or templates) when adding testing results to application for fallback exemption
- Option allows for ASPSPs to execute **proprietary testing scenarios** and for DNB to optimise fallback exemption procedure

ASPSPs and NISP-NL can define generic conformance testing scenarios (1/2)

Option 1 is in scope for
NISP-NL collaboration
based on 6-2-2019
meeting



Test scenarios
(1, 2, n)

Option 1:

Define test input

- ASPSPs and DNB consent on **generic** (and minimum) **testing scenarios** in **proprietary testing** compliance of ASPSP's dedicated interface
- Pre-defined test input can serve as **check on completeness** of test scenarios covered by AS-PSP's proprietary testing scenarios

- ASPSPs need to define **test scenarios that reflect the requirements** of the RTS on SCA
- Existing **NISP conformance test** documentation probably not useable in all details, across the board
- **Standardisation** in **conformance testing** to be found in **generic** and **minimum testing scenarios** in testing the compliance of their dedicated interfaces
- Test scenarios can be **standardised for all ASPSPs** into generic test scenarios, covering the XS2A compliance scope
- Testing scenarios entail at least: CAF, PIS, AIS, SCA **use cases**
- Pre-defined test input can serve as **check on completeness** of test scenarios covered by AS-PSP's proprietary testing scenarios

ASPSPs and NISP-NL can define generic conformance testing scenarios (2/2)

Option 1 is in scope for
NISP-NL collaboration
based on 6-2-2019
meeting



Test scenarios
(1, 2, n)

Option 1:

Define test input

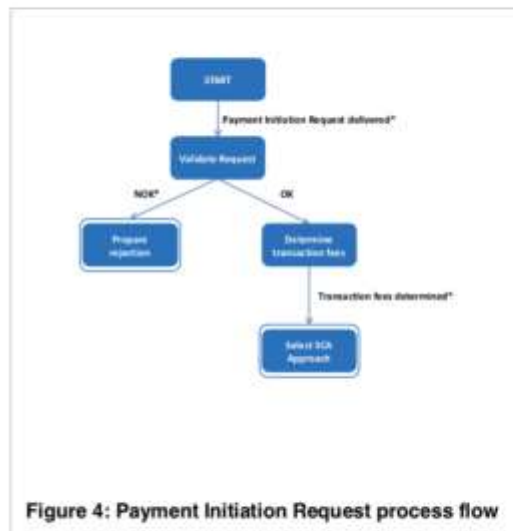
- ASPSPs and DNB consent on **generic** (and minimum) **testing scenarios** in **proprietary testing** compliance of ASPSP's dedicated interface
- Pre-defined test input can serve as **check on completeness** of test scenarios covered by AS-PSP's proprietary testing scenarios

- Testing scenarios will be detailed in **process flows**
- **Process flows** will be provided for PSD2 services (i.e. PIS, AIS, CAF) and commonly used subprocesses (e.g. different SCA methods)
- For each PSD2 service, different **detailed scenarios** are provided in the NISP-NL testing deliverable
- Detailed scenarios are for example the **different payment products** and payment types an AS-PSP offers or the **different AIS consent scopes** TPP or AS-PSP can agree on with the PSU (e.g. Balance or Balance&Transactions for all or dedicated accounts)
- These detailed scenarios depend on an **individual AS-PSP's** dedicated interface design and therefore **differ per AS-PSP**

'Defining generic test input' exemplified: Payment Initiation Request Flow

6.1.1 Payment initiation request

This scenario tests if a payment can be initiated.



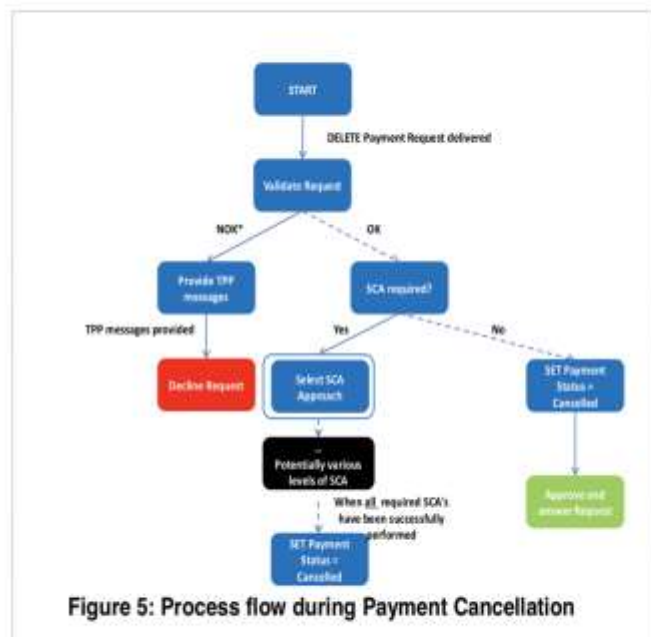
Processing event	Outcome	Description high-level scenario(s)	Description detailed scenario(s)
1 Start	Payment Initiation Request Delivered	Test to be performed for all payment products and payment types AS-PSPs offers to PSU in online interface: Single Payment, Bulk Payment, and Periodic Payment	Payment products are for example Single, Bulk, Periodic, Scheduled payments. Payment types are for example: sepa-credit-transfers, instant-sepa-credit-transfers, target-2-payments, cross-border-credit-transfers, pain.001-sepa-credit-transfers, pain.001-instant-sepa-credit-transfers, pain.001-target-2-
2 Validate request	NOK	The correct response code should be returned per payment request	- 403 (Product invalid): if product not available to PSU - 404 (Product unknown): if product not supported by AS-PSP - 400 (Execution date invalid): if requested execution date not valid for AS-PSP
	OK	Payment should not be rejected if the currency of product is not the same as currency of TPP's account	
3 Prepare Rejection	Rejected	Correct response should be returned in the case of a rejected request	If response code 4xx or 5xx is returned, payment initiation response should be "RJCT"
4 Determine transaction fees	Transaction fees determined	Check if Transaction fee is included in response	Either with "true" or "false", depending on whether the payment destination involves specific transfer cost for PSU
5 Select SCA approach	Continuation of the payment process		

Note: In order to imply as little extra work for ASPSPs as possible, all relevant test scenarios will be described on a generic (and minimum) level, describing CAF, PIS, AIS and SCA flows

‘Defining generic test input’ exemplified: Payment Cancellation Flow

6.1.2 Payment Cancellation

This scenario describes a payment cancellation initiation.



Processing event	Outcome	Description high-level scenario(s)	Description detailed scenario(s)
1 Start	Payment Initiation Request delivered	Test to be performed for all payment products and types AS-PSPs offers to PSU in online interface	Payment products are for example Single, Bulk, Periodic, Scheduled payments. Payment types are for example: sepa-credit-transfers, instant-sepa-credit-transfers, target-2-payments, cross-border-credit-transfers, pain.001-sepa-credit-transfers, pain.001-instant-sepa-credit-transfers, pain.001-target-2-payments, pain.001-cross-border-credit-transfers
2 Validate request	NOK	For each payment product and payment type, check if AS-PSP supports only creation and no cancellation, or if cancellation is no longer possible	- 403 (Product_invalid): if product not available to PSU - 400 (resource_blocked): if payment resource has reached status where cancellation is no longer possible
3 SCA required	OK		
	NO	For each payment product and payment type, check if cancellation is immediately executed without need of SCA	
	YES	If SCA is required, check (1) that for each payment product and payment type cancellation is not executed without SCA, and (2) that it is executed if SCA is successfully performed	
4 Set Payment status = cancelled	n.a.	Check if after cancellation payment resource can no longer be addressed for further authorisation	409 (Status_invalid): for any call corresponding to authorisation

Note: In order to imply as little extra work for ASPSPs as possible, all relevant test scenarios will be described on a generic (and minimum) level, describing CAF, PIS, AIS and SCA flows

Testing of the test scenarios can be done by NISP-NL-created 'Test-TPP', which verifies if dedicated interface functions as desired for Dutch ASPSPs

Option 2 is out of scope for NISP-NL collaboration based on 6-2-2019 meeting



AS-PSP
environment

Option 2:

*Perform conformance test by Test-TPP**

- Dutch ASPSPs create **independent 'test-TPP'** under NISP-NL collaboration
- 'Test-TPP' tests **to what extent dedicated interface** meets all **legal requirements**

- Conformance Testing assesses whether dedicated interface adheres to **requirements** set out in **PSD2 XS2A**
- Dutch ASPSPs may create an **independent 'test-TPP'** under NISP-NL collaboration, that tests to what extent dedicated interface meets all legal requirements

Delivering test results in a standardised manner when requesting exemption fallback smoothens processing of the fallback request

Option 3 is in scope for
NISP-NL collaboration
based on 6-2-2019
meeting



Reported results
(1, 2, n)

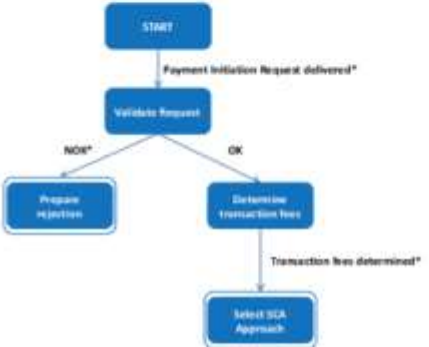
Option 3:

Report test output

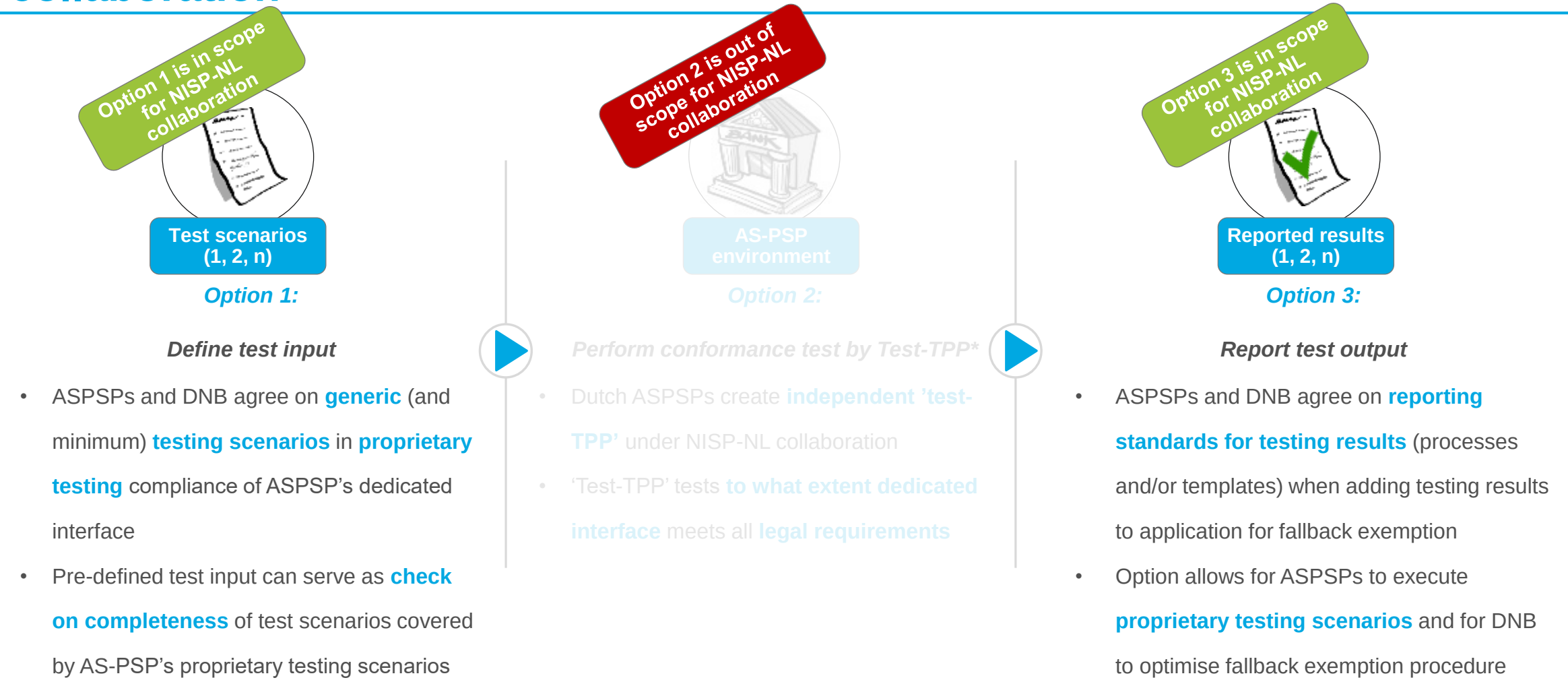
- ASPSPs and DNB consent on **reporting standards for testing results** (processes and/or templates) when adding testing results to application for fallback exemption
- Option allows for ASPSPs to execute **proprietary testing scenarios** and for DNB to optimise fallback exemption procedure

- ASPSPs should deliver **results of conformance testing** as **input** for their exemption request
- DNB has indicated using as much **standardised proof** as possible is **advised**
- **NISP-NL collaboration** may agree on **standards** in **reporting** on testing results
- Standardising reporting implies **little extra work** for ASPSPs, as ASPSPs can perform proprietary testing and are **only** asked to **report on the results** of their **testing** in a **standardised way**

'Standardising reporting output' exemplified: Payment Initiation Request Flow

6.1.1 Payment initiation request					
This scenario tests if a payment can be initiated.					
	Processing event	Outcome	Description high-level scenario(s)	payment type to be tested per payment product	Test result OK / NOK / n/a
 Figure 4: Payment Initiation Request process flow	1 Start	Payment Initiation Request Delivered	Test to be performed for all payment products and payment types ASPSPs offers to PSU in online interface. ayment products are for example Single, Bulk, Periodic, Scheduled payments. Payment types are for example: sepa-credit-transfers, instant-sepa-credit-transfers, target-2-payments, cross-border-credit-transfers, pain.001-sepa-credit-transfers, pain.001-instant-sepa-credit-transfers, pain.001-target-2-payments, pain.001-cross-border-credit-transfers	payment type to be tested to be inserted by AS-PSP payment type to be tested to be inserted by AS-PSP payment type to be tested to be inserted by AS-PSP payment type to be tested to be inserted by AS-PSP payment type to be tested to be inserted by AS-PSP payment type to be tested to be inserted by AS-PSP payment type to be tested to be inserted by AS-PSP	
	2 Validate request	NOK	The correct response code should be returned per payment request Error codes should be returned for 'Product Invalid', 'Product Unknown' and 'Execution date invalid'		
		OK	Payment should not be rejected if the currency of product is not the same as currency of TPP's account Correct response should be returned in the case of a rejected request. If response code 4xx or 5xx is returned, payment initiation response should be 'RJCT'		
	3 Prepare Rejection	Rejected			
	4 Determine transaction fees	Transaction fees determined	Check if Transaction fee is included in response, either with "true" or "false" depending on whether the payment destination involves specific transfer cost for PSU		
	5 Select SCA approach	Continuation of the payment process	See SCA scenarios		

Decision as result from the 6-2-2019 workshop: Option 1 and 3 of conformance testing will be pursued in NISP-NL collaboration



***Note:** Prerequisite for this option is that minimum testing scenarios are defined

Agenda

- Adjusted conformance testing approach NISP-NL
- **Break**
- Overview exemption fallback reporting requirements
- Exemption fallback reporting timelines
- Proposed reporting standards

Agenda

- Adjusted conformance testing approach NISP-NL
- Break
- **Overview exemption fallback reporting requirements**
- Exemption fallback reporting timelines
- Proposed reporting standards

Recap: Reporting workstream aims to define templates and processes for ASPSP-DNB fallback reporting

	2a: EVIDENCE GATHERING – ASPSP-DNB REPORTING	2b: EVIDENCE GATHERING – IMPLEMENTATION COORDINATION
GOAL	Define templates and processes for ASPSP reporting obligations* towards DNB	Ensure national coordination on implementation by ASPSPs
ACTIVITIES	• <i>Align on processes and define templates for ASPSP – DNB reporting:</i> agree on e.g. point of contact, timelines, touchpoints, response lead-times, hand-in deadlines, and develop common view on e.g. type of information, breadth/ depth of information, document format/structure • <i>Refine evidence gathering templates and processes based on continuous (mutual) feedback:</i> periodically review current templates and processes in order to optimise both	• <i>Streamline ‘testing’ and ‘wide usage’ period:</i> engage in discussion on what ASPSPs will offer under PSD2 XS2A and how TPPs expect to test ASPSP’s interface. ASPSPs will offer information for TPPs on individual implementation timelines, to enable TPPs to optimally prepare for and utilise testing period, with wide coverage of ASPSPs dedicated interfaces • <i>TPP testing:</i> actual testing of ASPSPs dedicated interfaces by TPPs • <i>Identify commonalities in issues encountered by TPPs:</i> jointly identify and – where possible – address issues impacting both TPPs and ASPSPs, that TPPs report as a result of testing or production use of ASPSP’s dedicated interfaces
DELIVERABLES	1. Common processes ASPSP-DNB reporting 2. Common templates ASPSP-DNB reporting	3. Overview of TPP and ASPSP testing needs 4. Test coordination of dedicated interfaces among Dutch ASPSPs by TPPs

*Note: reporting pertains to all ASPSP reporting obligations following from the fallback exemption guidelines

When requesting an exemption, ASPSPs have to provide evidence along seven topics

GL 1 Exemption for contingency mechanism						
GL 2 KPIs	GL 3 Statistics	GL 4 Stress test	GL 5 Obstacles	GL 6 Design	GL 7 Usage	GL 8 Problems
Service levels	Daily statistics per quarter	Stress testing processes	Authentication methods	Legal requirements	Summary of usage	Issue management procedure
Availability	Comparison of interfaces	Capabilities testing	Explanation no obstacles	Standard conformance	Reasonable effort	Unresolved issues
Performance		Test summary description	Customer journey	Technical specifications	GL 6 & 8 information	
				Testing environment	Production	
				Testing results, problems		
GL 9 Consultation of the EBA / host NCAs						

Overview reporting requirements Guideline 2: KPIs

GL #	Theme	GL text
2.1	KPIs	The ASPSP should define key performance indicators (KPIs) and service level targets, including for problem resolution, out of hours support, monitoring, contingency plans and maintenance for its dedicated interface, that are at least as stringent as those for the interface(s) made available to its own payment service users (PSUs) for directly accessing their payment accounts online
2.2		The ASPSP should define at a minimum, the following KPIs of the availability of the dedicated interface:
2.2a		The uptime per day of all interfaces
2.2b		The downtime per day of all interfaces
2.3		In addition to the KPIs on availability in Guideline 2.2, the ASPSP should define, at a minimum, the following KPIs for the performance of the dedicated interface:
2.3.a		The daily average time (in milliseconds) taken, per request, for the ASPSP to provide the payment initiation service provider (PISP) with all the information requested in accordance with Article 66(4)(b) of PSD2 and Article 36(1)(b) of the RTS
2.3.b		The daily average time (in milliseconds) taken, per request, for the ASPSP to provide the account information service provider (AISP) with all the information requested in accordance with Article 36(1)(a) of the RTS
2.3.c		The daily average time (in milliseconds) taken, per request, for the ASPSP to provide the card-based payment instrument issuer (CBPII) or the PISP with a 'yes/no' confirmation in accordance with Article 65(3) of PSD2 and Article 36(1)(c) of the RTS
2.3.d		The daily error response rate – calculated as the number of error messages concerning errors attributable to the ASPSP sent by the ASPSP to the PISPs, AISPs and CBPIIs in accordance with Article 36(2) of the RTS per day, divided by the number of requests received by the ASPSP from AISPs, PISPs and CBPIIs in the same day
2.4		For the purpose of calculating the availability indicators set out in Guideline 2.2 for the dedicated interface, the ASPSP should do the following:
2.4.a		Calculate the percentage uptime as 100% minus the percentage downtime
2.4.b		Calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight
2.4.c		Count the interface as 'down' when five consecutive requests for access to information for the provision of payment initiation services, account information services or confirmation of availability of funds are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple PISPs, AISPs or CBPIIs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided

Overview reporting requirements Guideline 3: Publication of statistics and Guideline 4: Stress testing

GL #	Theme	GL text
3.1	Publication of statistics	For the purpose of Article 32(4) of the RTS, the ASPSP should provide its competent authority with a plan for publication of daily statistics on a quarterly basis on the availability and performance of the dedicated interface as set out in Guidelines 2.2 and 2.3, and of each of the interfaces made available to its own PSUs for directly accessing their payment accounts online, together with information on where these statistics will be published and the date of first publication
3.2		The publication referred to in Guideline 3.1 above should enable PISPs, AISPs, CBPIIs and PSUs to compare the availability and performance of the dedicated interface with the availability and performance of each of the interfaces made available by the ASPSP to its PSUs for directly accessing their payment accounts online on a daily basis

GL #	Theme	GL text
4.1	Stress testing	For the purpose of the stress tests referred to in Article 32(2) of the RTS, the ASPSP should have in place processes to establish and assess how the dedicated interface performs when subjected to an extremely high number of requests from PISPs, AISPs and CBPIIs, in terms of the impact that such stresses have on the availability and performance of the dedicated interface and the defined service level targets
4.2		The ASPSP should undertake adequate stress testing of the dedicated interface including but not limited to:
4.2.a		The capability to support access by multiple PISPs, AISPs and CBPIIs
4.2.b		The capability to deal with an extremely high number of requests from PISPs, AISPs and CBPIIs, in a short period of time without failing
4.2.c		The use of an extremely high number of concurrent sessions open at the same time for payment initiation, account information and confirmation on the availability of funds requests
4.2.d		Requests for large volumes of data
4.3		The ASPSP should provide the competent authority with a summary of the results of the stress tests, including the assumptions used as a basis for stress testing each of the elements in letters (a) to (d) of Guideline 4.2 above and how any issues identified have been addressed

Overview reporting requirements Guideline 5: Obstacles

GL #	Theme	GL text
5.1	Obstacles	The ASPSP should provide the competent authority with:
5.1.a		A summary of the method(s) of carrying out the authentication procedure(s) of the PSUs that are supported by the dedicated interface, i.e. redirection, decoupled, embedded or a combination thereof
5.1.b		An explanation of the reasons why the method(s) of carrying out the authentication procedure(s) referred to in paragraph (a) is/are not an obstacle, as referred to in Article 32(3) of the RTS, and how such method(s) allow(s) PISPs and AISPs to rely on all the authentication procedures provided by the ASPSP to its PSUs, together with evidence that the dedicated interface does not give rise to unnecessary delay or friction in the experience available to the PSUs when accessing their account via a PISP, AISP or CBPII or to any other attributes, including unnecessary or superfluous steps or the use of unclear or discouraging language, that would directly or indirectly dissuade the PSUs from using the services of PISPs, AISPs and CBPIIs
5.2		As part of the explanation referred to in letter (b) of Guideline 5.1, the ASPSP should provide the competent authority with a confirmation that:
5.2.a		The dedicated interface does not prevent PISPs and AISPs from relying upon the authentication procedure(s) provided by the ASPSP to its PSUs
5.2.b		No additional authorisations or registrations are required from PISPs, AISPs or CBPIIs, other than those imposed in Articles 11, 14 and 15 of PSD2
5.2.c		There are no additional checks by the ASPSP on the consent, as referred to in Article 32(3) of the RTS, given by the PSU to the PISP or the AISP to access the information on the payment account(s) held with the ASPSP or to initiate payments
5.2.d		No checks on the consent given by the PSU to the CBPII in accordance with letter (a) of Article 65(2) of PSD2 are performed

Overview reporting requirements Guideline 6: Design and testing to the satisfaction of TPPs (1/2)

GL #	Theme	GL text
6.1	Design and testing to the satisfaction of TPPs	For the purpose of evidencing compliance with the requirement in letter (b) of Article 33(6) of the RTS regarding the design of the dedicated interface, the ASPSP should provide the competent authority with:
6.1.a		Evidence that the dedicated interface meets the legal requirements for access and data in PSD2 and the RTS, including:
6.1.a.i		- A description of the functional and technical specifications that the ASPSP has implemented
6.1.a.ii		- A summary of how the implementation of these specifications fulfils the requirements in PSD2 and the RTS
6.1.b		Information on whether, and if so how, the ASPSP has engaged with PISPs, AISPs and CBPIIs
6.2		For the purpose of these Guidelines, a 'market initiative' means a group of stakeholders that have developed functional and technical specifications for dedicated interfaces and, in doing so, have obtained input from PISPs, AISPs and CBPIIs
6.3		Where the ASPSP is implementing a standard developed by a market initiative:
6.3.a		The information referred to in point (i) of letter (a) of Guideline 6.1 may consist of information regarding which market initiative standard the ASPSP is implementing, whether or not it has deviated in any specific aspect from such standard, and if so, how it has deviated and how it meets the requirements in PSD2 and the RTS
6.3.b		The information referred to in point (ii) of letter (a) of Guideline 6.1 may include, where available, the results of the conformance testing developed by the market initiative, attesting compliance of the interface with the respective market initiative standard
6.4		For the purpose of the requirement in letter (b) of Article 33(6) of the RTS regarding the testing of the dedicated interface, the ASPSP should make the technical specifications of the dedicated interface available to authorised PISPs, AISPs and CBPIIs or payment service providers that have applied to their competent authorities for the relevant authorisation in accordance with Article 30(3) of the RTS including, at a minimum, publishing a summary of the specification of the dedicated interface on its website in accordance with the third sub-paragraph of Article 30(3) of the RTS

Overview reporting requirements Guideline 6: Design and testing to the satisfaction of TPPs (2/2)

GL #	Theme	GL text
6.5	Design and testing to the satisfaction of TPPs	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:
6.5.a		• A stable and secure connection
6.5.b		• The ability of ASPSPs and authorised PISPs, AISP and CBPIIs to exchange the relevant certificates in accordance with Article 34 of the RTS
6.5.c		• The ability to send and receive error messages in accordance with Article 36(2) of the RTS
6.5.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
6.5.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
6.5.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
6.5.g		• The ability of PISPs and AISP to rely on all the authentication procedures provided by the ASPSP to its PSUs
6.6		The ASPSP should provide the competent authority with a summary of the results of the testing referred to in Article 30(5) of the RTS for each of the elements to be tested in accordance with letters (a) to (g) of paragraph 6.5 above, including the number of PISPs, AISP and CBPIIs that have used the testing facility, the feedback received by the ASPSP from these PISPs, AISP and CBPIIs, the issues identified and a description of how these issues have been addressed
6.7		For the purpose of assessing whether the ASPSP meets the requirements in letter (b) of Article 33(6) of the RTS, the competent authority may also take into account any problems reported to it by PISPs, AISP and CBPIIs in relation to Guideline 6.5 above

Overview reporting requirements Guideline 7: Wide usage of the interface and Guideline 8: Resolution of problems

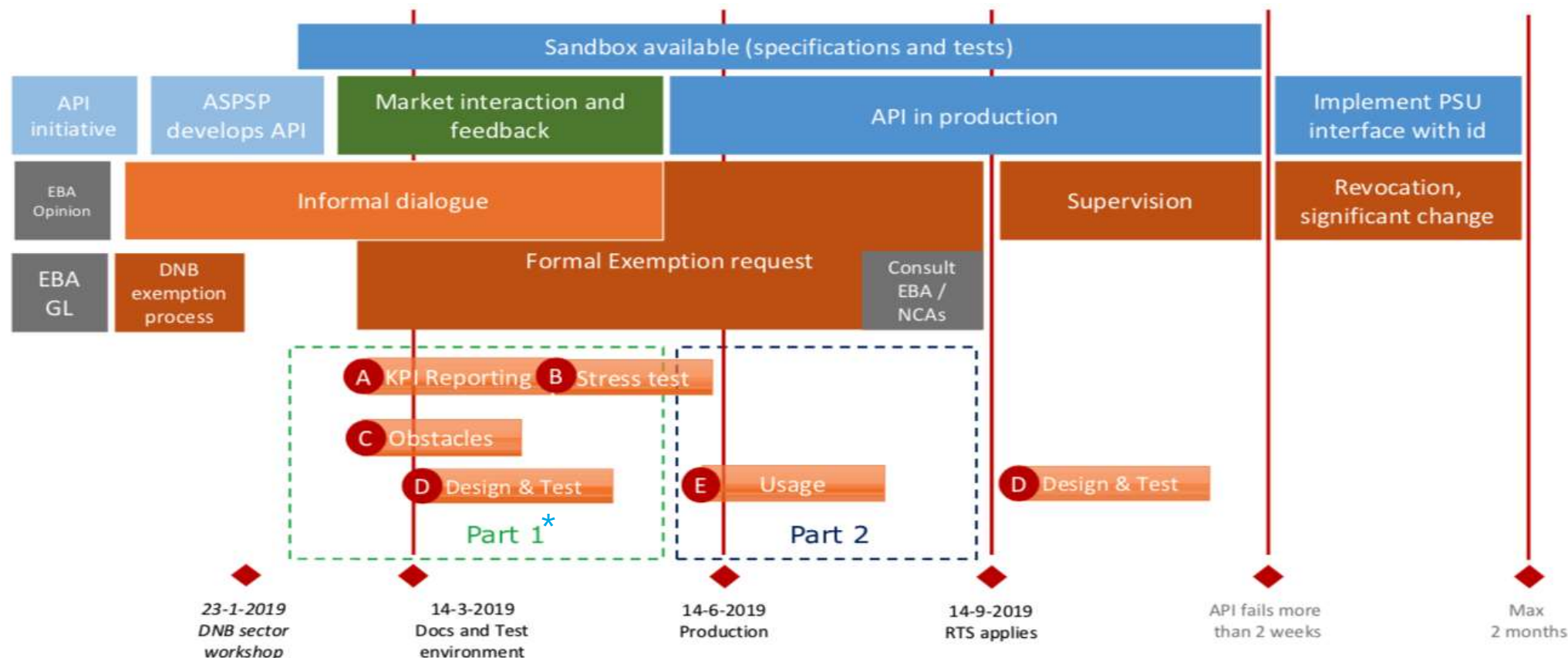
GL #	Theme	GL text
7.1	Wide usage of the interface	For the purposes of evidencing compliance with the requirement in letter (c) of Article 33(6) of the RTS, the ASPSP should provide the competent authority with:
7.1.a		A description of the usage of the dedicated interface for the period referred to in letter (c) of Article 33(6), including but not limited to:
7.1.a.i		- The number of PISPs, AISPs and CBPIIs that have used the interface to provide services to customers
7.1.a.ii		- The number of requests sent by those PISPs, AISPs and CBPIIs to the ASPSP via the dedicated interface that have been replied to by the ASPSP
7.1.b		Evidence that the ASPSP has made all reasonable efforts to ensure wide usage of the dedicated interface, including by communicating its availability via appropriate channels, including, where relevant, the website of the ASPSP, social media, industry trade bodies, conferences and direct engagement with known market actors
7.2		In addition to the evidence referred to in Guideline 7.1, the competent authority should take into account the information received in the context of Guidelines 6 and 8 when assessing whether or not the ASPSP meets the requirement in Article 33(6)(c) of the RTS
7.3		The 3-month period referred to in letter (c) of Article 33(6) of the RTS may run concurrently with the testing referred to in Article 30(5) of the RTS

GL #	Theme	GL text
8.1	Resolution of problems	For the purpose of Article 32(1) and letter (d) of Article 33(6) of the RTS, the ASPSP should provide the competent authority with:
8.1.a		Information on the systems or procedures in place for tracking, resolving and closing problems, particularly those reported by PISPs, AISPs and CBPIIs
8.1.b		An explanation of the problems, particularly those reported by PISPs, AISPs and CBPIIs, that have not been resolved in accordance with the service level targets set out in Guideline 2.1

Agenda

- Conformance testing approach NISP-NL
- Break
- Overview exemption fallback reporting requirements
- **Exemption fallback reporting timelines**
- Proposed reporting standards

Subset of Guidelines reports to be handed in as 'Part 1' of fallback exemption process on 14-3-2019



*** for some reporting items the required data cannot be made available on 14-3-2019;
for these items, the (internal) process of obtaining the data needs to be detailed on 'part-1' deadline**

Prioritisation in standardisation-work is made due to exemption process timelines

GL 1 Exemption for contingency mechanism						
GL 2 KPIs	GL 3 Statistics	GL 4 Stress test	GL 5 Obstacles	GL 6 Design	GL 7 Usage	GL 8 Problems
Service levels	Daily statistics per quarter*	Stress testing processes	Authentication methods	Legal requirements	Summary of usage	Issue management procedure
Availability*	Comparison of interfaces	Capabilities testing*	Explanation no obstacles	Standard conformance*	Reasonable effort	Unresolved issues
Performance*		Test summary description*	Customer journey	Technical specifications	GL 6 & 8 information	
				Testing environment	Production	
				Testing results, problems		
GL 9 Consultation of the EBA / host NCAs						

*** for some reporting items the required data cannot be made available on 14-3-2019;
for these items, the (internal) process of obtaining the data needs to be detailed on 'part-1' deadline**

Agenda

- Conformance testing approach NISP-NL
- Break
- Overview exemption fallback reporting requirements
- Exemption fallback reporting timelines
- **Proposed reporting standards**

Three main categories of reporting standardisation are distinguished for 'Part 1' delivery

Category	Guideline
Operational	2.1, 2.2, 2.3a-d, 2.4a-c, 3.1, 3.2
Testing	4.1, 4.2, 4.3, 6.3b, 6.5
Qualitative compliance evidence	5.1a-b, 5.2a-d, 6.1a-b, 6.2, 6.3.a, 6.4

NOTE:

Reporting workstream focuses on standardising AS-PSP reporting output, and does not include discussions on how to obtain the data internally per AS-PSP

- Standardisation in '**Operational**' category focuses on providing concrete templates for AS-PSPs to fill in
- '**Testing**' category includes stress testing, conformance testing and testing facility
- Given the nature of '**Qualitative compliance evidence**' category, standardisation focuses on providing generic guidance to AS-PSPs rather than concrete templates to fill in

NISP-NL will deliver standardised output in excel for operational aspects of fallback exemption

Guideline	Reporting metric	Dedicated interface	Current PSU interface 1	Current PSU interface 2	Current PSU interface n	Remarks
2.1	Problem resolution towards TPPs	Provide SLA regarding problem resolution towards TPP	Provide SLA regarding problem resolution towards TPP for the PSU interface	Provide SLA regarding problem resolution towards TPP for the PSU interface	Provide SLA regarding problem resolution towards TPP for the PSU interface	Ensure comparability of PSU interface and dedicated interface SLAs in terms of information provided
	Problem resolution towards PSU	Provide SLA regarding problem resolution towards PSU	Provide SLA regarding problem resolution towards PSU for the PSU interface	Provide SLA regarding problem resolution towards PSU for the PSU interface	Provide SLA regarding problem resolution towards PSU for the PSU interface	Ensure comparability of PSU interface and dedicated interface SLAs in terms of information provided
	out of hours support	Provide SLA regarding out of hours support for the dedicated interface	Provide SLA regarding out of hours support for the PSU interface	Provide SLA regarding out of hours support for the PSU interface	Provide SLA regarding out of hours support for the PSU interface	Ensure comparability of PSU interface and dedicated interface SLAs in terms of information provided
	monitoring	Provide SLA regarding monitoring of the dedicated interface	Provide SLA regarding monitoring of the PSU interface	Provide SLA regarding monitoring of the PSU interface	Provide SLA regarding monitoring of the PSU interface	Ensure comparability of PSU interface and dedicated interface SLAs in terms of information provided
	contingency plan	Provide SLA regarding contingency plans for the dedicated interface	Provide SLA regarding contingency plans for the PSU interface	Provide SLA regarding contingency plans for the PSU interface	Provide SLA regarding contingency plans for the PSU interface	Ensure comparability of PSU interface and dedicated interface SLAs in terms of information provided
	maintenance	Provide SLA regarding maintenance of the dedicated interface	Provide SLA regarding maintenance of the PSU interface	Provide SLA regarding maintenance of the PSU interface	Provide SLA regarding maintenance of the PSU interface	Ensure comparability of PSU interface and dedicated interface SLAs in terms of information provided
Guideline	Reporting metric	Dedicated interface	Current PSU interface 1	Current PSU interface 2	Current PSU interface n	Remarks
2.2	Uptime per day	calculate the percentage uptime as 100% minus the percentage downtime	calculate the percentage uptime as 100% minus the percentage downtime	calculate the percentage uptime as 100% minus the percentage downtime	calculate the percentage uptime as 100% minus the percentage downtime	Ensure comparability of PSU interface and dedicated interface KPIs in terms of information provided
	downtime per day	- Calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight - count the interface as 'down' when five consecutive requests for access to information for the provision of FIS, AIS or CAF are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple TPPs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided	- Calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight - count the interface as 'down' when five consecutive requests for access to information for the provision of FIS, AIS or CAF are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple TPPs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided	- Calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight - count the interface as 'down' when five consecutive requests for access to information for the provision of FIS, AIS or CAF are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple TPPs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided	- Calculate the percentage downtime using the total number of seconds the dedicated interface was down in a 24-hour period, starting and ending at midnight - count the interface as 'down' when five consecutive requests for access to information for the provision of FIS, AIS or CAF are not replied to within a total timeframe of 30 seconds, irrespective of whether these requests originate from one or multiple TPPs. In such a case, the ASPSP should calculate downtime from the moment it has received the first request in the series of five consecutive requests that were not replied to within 30 seconds, provided that there is no successful request in between those five requests to which a reply has been provided	Ensure comparability of PSU interface and dedicated interface KPIs in terms of information provided

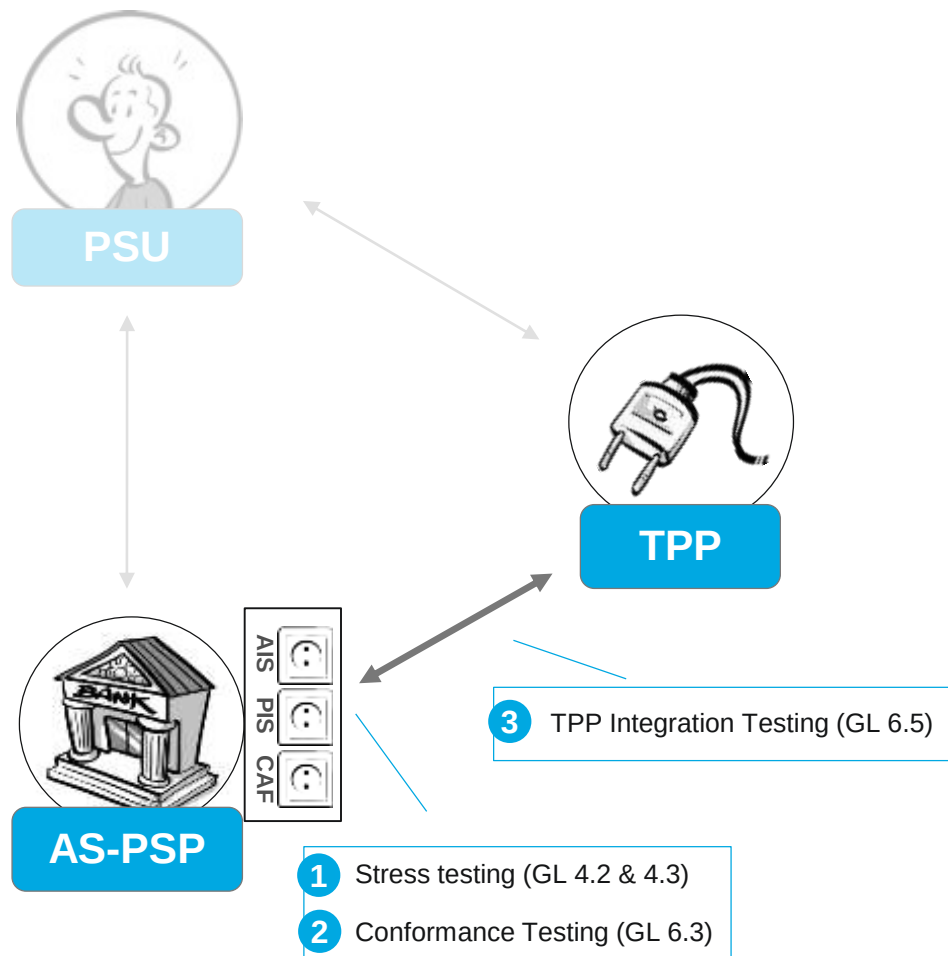
Screenshot from excel supporting reporting on GL 2

Quarter	Dedicated interface			Current PSU interface 1		Current PSU interface 2		Current PSU interface n		Remarks
Reporting metric	Uptime	Downtime	Error response rate	Uptime	Downtime	Uptime	Downtime	Uptime	Downtime	
Answer	Percentage uptime for specified date	Percentage downtime for specified date	Daily error response rate for specified date	Percentage uptime for specified date	Percentage downtime for specified date	Percentage uptime for specified date	Percentage downtime for specified date	Percentage uptime for specified date	Percentage downtime for specified date	
Reporting metric	Daily average time per request - FIS product 1	Daily average time per request - AIS	Daily average time per request - CAF	Daily average time per request - FIS product 1	Daily average time per request - AIS	Daily average time per request - FIS product 1	Daily average time per request - AIS	Daily average time per request - FIS product 1	Daily average time per request - AIS	
Answer	Daily average time in milliseconds taken per request for FIS product 1	Daily average time in milliseconds taken per request for AIS	Daily average time in milliseconds taken per request for CAF	Daily average time in milliseconds taken per request for FIS product 1	Daily average time in milliseconds taken per request for AIS	Daily average time in milliseconds taken per request for FIS product 1	Daily average time in milliseconds taken per request for AIS	Daily average time in milliseconds taken per request for FIS product 1	Daily average time in milliseconds taken per request for AIS	Statistics to be presented are daily statistics
Reporting metric	Daily average time per request - FIS product 2	Daily average time per request - FIS product n		Daily average time per request - FIS product 2	Daily average time per request - FIS product n	Daily average time per request - FIS product 2	Daily average time per request - FIS product n	Daily average time per request - FIS product 2	Daily average time per request - FIS product n	
Answer	Daily average time in milliseconds taken per request for FIS product 2	Daily average time in milliseconds taken per request for FIS product n		Daily average time in milliseconds taken per request for FIS product 2	Daily average time in milliseconds taken per request for FIS product n	Daily average time in milliseconds taken per request for FIS product 2	Daily average time in milliseconds taken per request for FIS product n	Daily average time in milliseconds taken per request for FIS product 2	Daily average time in milliseconds taken per request for FIS product n	

Screenshot from excel supporting reporting on GL 3

- Standardised output allows for **comparison of interfaces** since reporting occurs on statistics of both dedicated interface and current PSU interfaces
- Standard allows for reporting on statistics mentioned in GL 2.1, 2.2, 2.3, 2.4 and 3.2
- Template will be sent out for **review** on 7-2-2019
- It has been discussed with the group that NISP-NL-wide collaboration is not included for GL 3.1 (i.e. 'provide plan of publication of daily statistics on quarterly basis, including information on location of statistics and date of first publication')

Main question in standardisation of testing currently pertains to standardisation of stress testing



- 1 Stress testing (GL 4.2, 4.3):
 - **Question**
 - To what extent are standing supervisory practices regarding stress testing re-usable?
- 2 Conformance testing (GL 6.3.b):
 - Pre-defined conformance testing scenarios allow for check on **completeness by AS-PSPs** and **standardisation in reporting** (as discussed in first section of today's workshop)
- 3 TPP Integration Testing (GL 6.5):
 - Out of scope for this workstream
 - See '**TPP Integration Testing Checklist**' document as presented on BVN website for requirements regarding AS-PSP testing facility

Question: to what extent do you see standardisation in reporting regarding ‘Qualitative compliance evidence’? (1/2)

GL #	GL text
5.1	The ASPSP should provide the competent authority with:
5.1.a	• A summary of the method(s) of carrying out the authentication procedure(s) of the PSUs that are supported by the dedicated interface, i.e. redirection, decoupled, embedded or a combination thereof
5.1.b	• An explanation of the reasons why the method(s) of carrying out the authentication procedure(s) referred to in paragraph (a) is/are not an obstacle, as referred to in Article 32(3) of the RTS, and how such method(s) allow(s) PISPs and AISP to rely on all the authentication procedures provided by the ASPSP to its PSUs, together with evidence that the dedicated interface does not give rise to unnecessary delay or friction in the experience available to the PSUs when accessing their account via a PISP, AISP or CBPII or to any other attributes, including unnecessary or superfluous steps or the use of unclear or discouraging language, that would directly or indirectly dissuade the PSUs from using the services of PISPs, AISPs and CBPIIs
5.2	As part of the explanation referred to in letter (b) of Guideline 5.1, the ASPSP should provide the competent authority with a confirmation that:
5.2.a	• The dedicated interface does not prevent PISPs and AISPs from relying upon the authentication procedure(s) provided by the ASPSP to its PSUs
5.2.b	• No additional authorisations or registrations are required from PISPs, AISPs or CBPIIs, other than those imposed in Articles 11, 14 and 15 of PSD2
5.2.c	• There are no additional checks by the ASPSP on the consent, as referred to in Article 32(3) of the RTS, given by the PSU to the PISP or the AISP to access the information on the payment account(s) held with the ASPSP or to initiate payments
5.2.d	• No checks on the consent given by the PSU to the CBPII in accordance with letter (a) of Article 65(2) of PSD2 are performed

Question: to what extent do you see standardisation in reporting regarding ‘Qualitative compliance evidence’? (2/2)

GL #	GL text
6.1	For the purpose of evidencing compliance with the requirement in letter (b) of Article 33(6) of the RTS regarding the design of the dedicated interface, the ASPSP should provide the competent authority with:
6.1.a	• Evidence that the dedicated interface meets the legal requirements for access and data in PSD2 and the RTS, including:
6.1.a.i	• A description of the functional and technical specifications that the ASPSP has implemented
6.1.a.ii	• A summary of how the implementation of these specifications fulfils the requirements in PSD2 and the RTS
6.1.b	• Information on whether, and if so how, the ASPSP has engaged with PISPs, AISPs and CBPIIs
6.2	For the purpose of these Guidelines, a ‘market initiative’ means a group of stakeholders that have developed functional and technical specifications for dedicated interfaces and, in doing so, have obtained input from PISPs, AISPs and CBPIIs
6.3	Where the ASPSP is implementing a standard developed by a market initiative:
6.3.a	• The information referred to in point (i) of letter (a) of Guideline 6.1 may consist of information regarding which market initiative standard the ASPSP is implementing, whether or not it has deviated in any specific aspect from such standard, and if so, how it has deviated and how it meets the requirements in PSD2 and the RTS
6.4	For the purpose of the requirement in letter (b) of Article 33(6) of the RTS regarding the testing of the dedicated interface, the ASPSP should make the technical specifications of the dedicated interface available to authorised PISPs, AISPs and CBPIIs or payment service providers that have applied to their competent authorities for the relevant authorisation in accordance with Article 30(3) of the RTS including, at a minimum, publishing a summary of the specification of the dedicated interface on its website in accordance with the third sub-paragraph of Article 30(3) of the RTS

Questions?



Next steps NISP-NL collaboration

Plenary work session 1:

Date: Wed 6-2-2019 / 14.00-16.30h

Goal: Kick-off detailing ASPSPs-DNB reporting process and templates, discussing scoping of detailing processes and templates and discuss conformance testing

Main participants: ASPSPs & Betaalvereniging, DNB

Subworkstream: 2a: ASPSP-DNB Reporting, *1b: conformance testing*

Plenary work session 2:

Date: Tue 12-2-2019 / 10.00-12.30h

Goal: Kick-off streamlining of testing and wide usage, discuss scoping of information sharing between TPPs and ASPSPs

Main participants: TPPs, ASPSPs & Betaalvereniging, DNB

Subworkstream: 2b: Implementation coordination

Plenary work session 3:

Date: Tue 19-2-2019 / 14.00-16.30h

Goal: Refine and agree on ASPSPs-DNB reporting processes and templates and discuss conformance testing

Main participants: ASPSPs & Betaalvereniging, DNB

Subworkstream: 2a: ASPSP-DNB Reporting, *1b: conformance testing*

Plenary work session 4:

Date: Tue 26-2-2019 / 10.00-12.30h

Goal: Refine information sharing re testing, kick-off identifying/addressing common issues addressed by TPPs

Main participants: TPPs, ASPSPs & Betaalvereniging, DNB

Subworkstream: 2b: Implementation coordination

NISP-NL

Amsterdam
6 February 2019