Berlin Group NextGenPSD2 XS2A Framework
Status Update and Future Outlook

THE Berlin GROUP
A EUROPEAN STANDARDS INITIATIVE

Digital Financial Services Forum Bukarest, 04.10.2018

Dr. Ortwin Scheja, SRC Security Research & Consulting GmbH

NextGenPSD2 - Rationale & Benefits

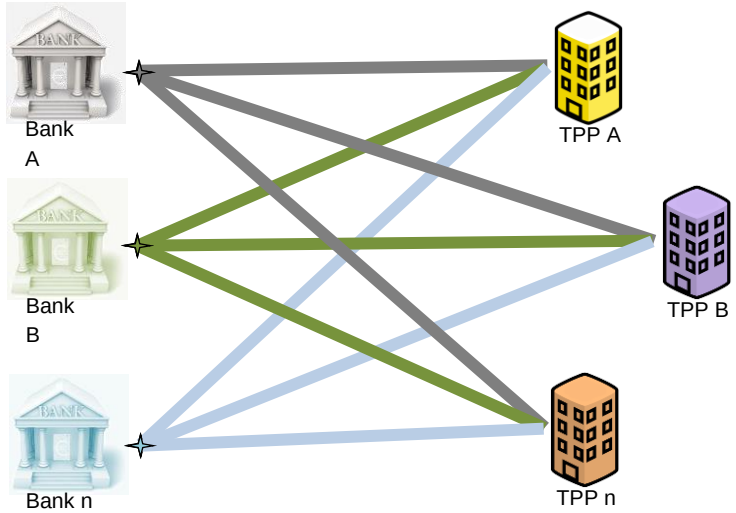
- PSD2 mandates banks (ASPSPs), upon bank customer consent, to provide TPPs access to the following banking services:

1. Confirmation of availability of funds services (PSD2 Art. 65)
2. Payment initiation services (PSD2 Art. 66)
3. Account information services (PSD2 Art. 67)

- PSD2 Art. 98 mandates the European Banking Authority (EBA) to develop Regulatory Technical Standards (RTS), specifying high-level SCA and XS2A requirements (≠ detailed technical standards)
- EBA RTS Art. 30 requires ASPSPs to offer at least one interface (with requirements) for TPPs

NextGenPSD2 - Rationale & Benefits

- When each European bank develops (and tests, and maintains) its own proprietary XS2A communication standard
  - Network complexity
  - High testing efforts and operational risks
  - High documentation efforts
  - Risk increase due to pan-European scale
  - With thousands of banks and TPPs in Europe, it's easy to imagine why development, testing and maintenance of proprietary, bank-specific XS2A interfaces would create a pan-European IT nightmare with high costs for all stakeholders involved



Complexity x 1,000s

NextGenPSD2 - Rationale & Benefits

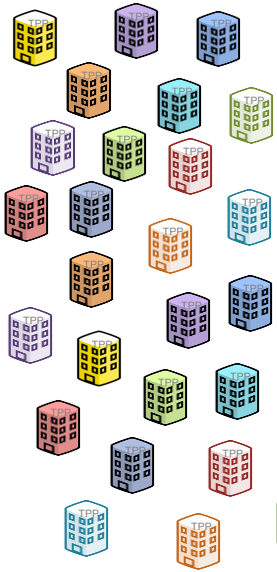
Uniform and interoperable
communications
between banks and TPPs

Banks

THE *Berlin* GROUP
A EUROPEAN STANDARDS INITIATIVE

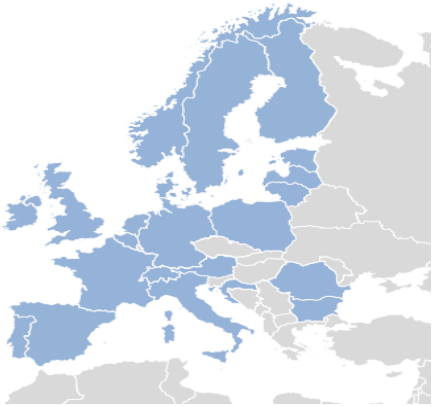
API*

TPPs



*APIs have to comply to the standards and will be provided by API providers, not by the Berlin Group

Participants NextGenPSD2 Taskforce



Updated: 24-09-2018

NextGenPSD2 Status Update - Achievements

- Resolved Challenges
  - Create a workable pan-European Taskforce structure for a new standards theme
  - Work with sometimes fuzzy and overlapping PSD2, (non-final) EBA RTS and GDPR definitions
  - Diversity of banking payment products and infrastructures across Europe
  - Diversity of authentication methods and -infrastructures across Europe
  - Transition from SOAP to REST services and JSON data encoding vs. XML
  - Allow banks to use existing account report formats
  - Incorporate Retail and Corporate Business
  - Complexity of eIDAS certificates in relation to PSD2

- Continuous alignment with
  - other XS2A standardisation initiatives
  - SWIFT, ISO20022, ISO TC68, OpenID, W3C, a.o.
  - ongoing discussions in ERPB, EBA/NCAs, API EG

NextGenPSD2 Status Update - Achievements

- NextGenPSD2 Framework Version 1.2 published July 2018

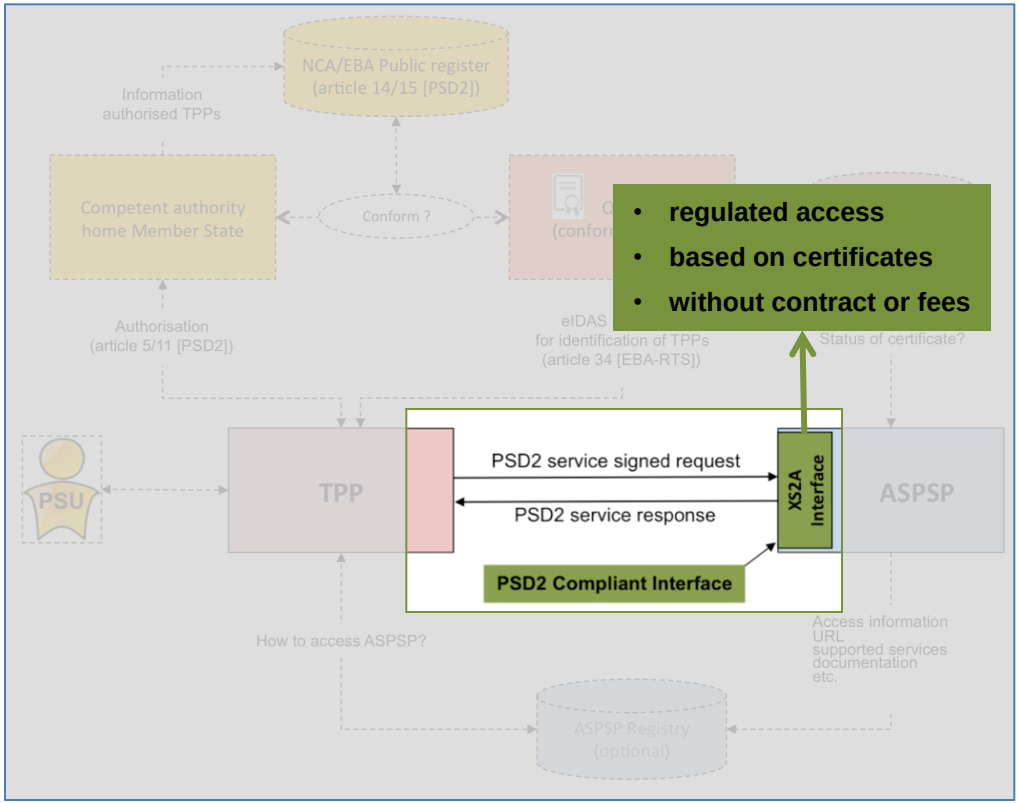
- Publicly available, for free: www.berlin-group.org/psd2-access-to-bank-accounts

NextGenPSD2 Status Update - Achievements

Version 1.0	◆ Influence of the TPP on the choice of the SCA Approach ◆ Support recurring, future dated, multiple and batch payments ◆ Full multicurrency support of accounts for PIS and AIS
Version 1.1	◆ Far-reaching convergence with other API initiatives, ISO/SWIFT adaptions ◆ Small improvements: new functionality, errata
Version 1.2	◆ Introduce “Distributed (Multiple) SCA” approach for corporates ◆ Introduce cancellation ◆ Introduce signing baskets
Version 1.3 to be published	◆ Card account endpoints ◆ Regulatory Impact, clarifications and errata from implementations
Version 2.x as value add services (ideas)	◆ Introduce “Delegated SCA” where TPP performs SCA with liability shift ◆ Push notifications and Push account entries for instant payments ◆ Offer a registration for “confirmation of funds”

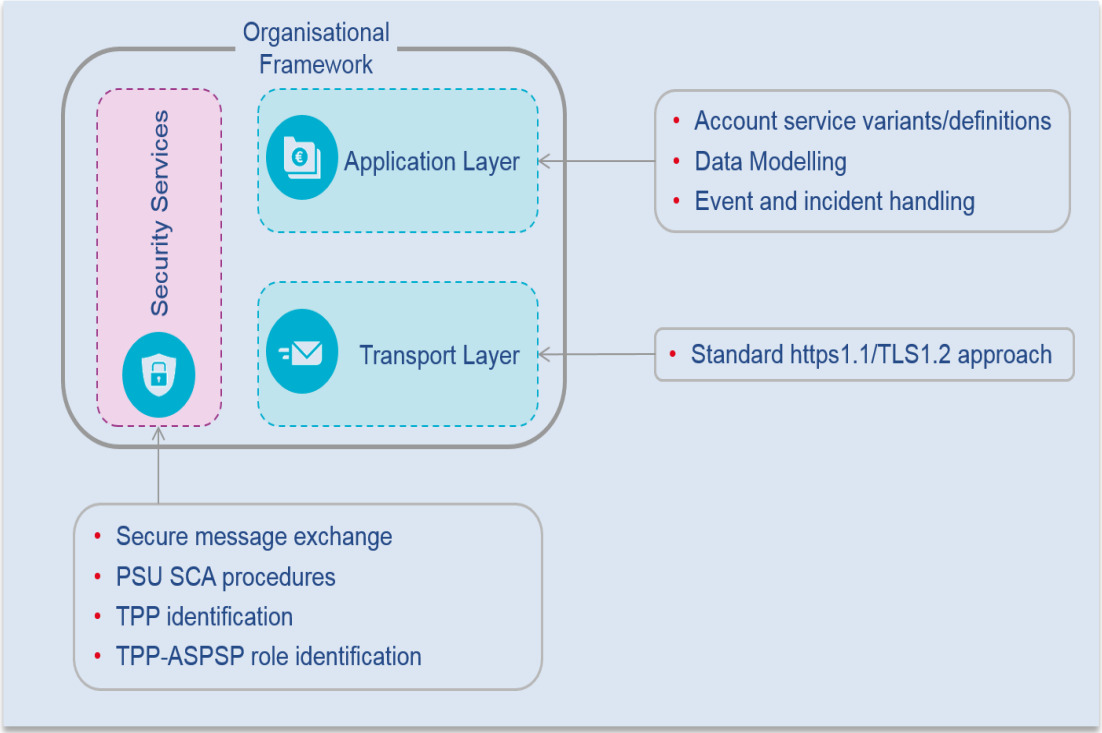
NextGenPSD2 - Key Characteristics

- Scope of work



NextGenPSD2 - Key Characteristics

- NextGenPSD2 Interface Design
  - 3 levels of communication are standardised



NextGenPSD2 - Key Characteristics

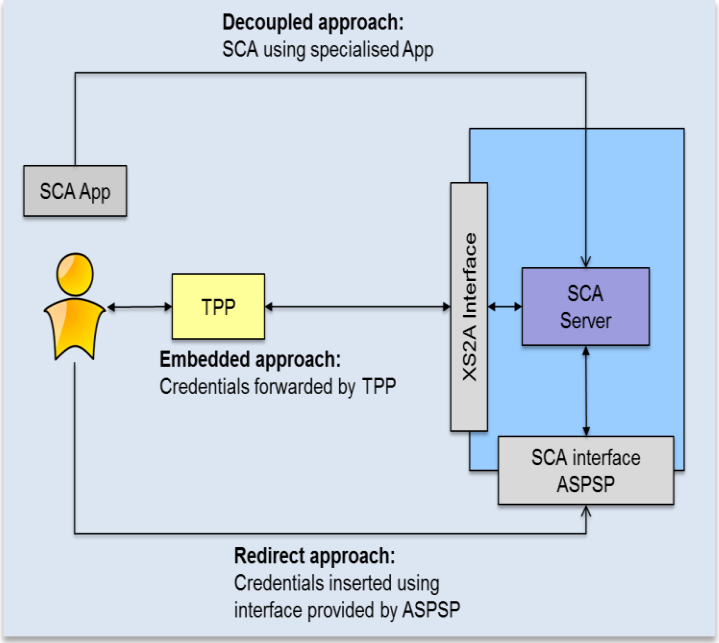
- NextGenPSD2 Interface Design
  - Currently defined transactions for core PSD2 services

Use Case	Service	
Initiation of a single payment	PIS	
Initiation of a future dated single payment	PIS	optional
Initiation of a bulk payment	PIS	optional
Initiation of a recurring payment	PIS	optional
Cancellation of Payments	PIS	
Grouping transactions to signing baskets	PIS/AIS	optional
Establish account information consent	AIS	
Get list of reachable accounts	AIS	optional
Get account details of the list of accessible accounts	AIS	
Get balances for a given account	AIS	
Get transaction information for a given account	AIS	
Get a confirmation on the availability of funds	PIIS	

  - Optional support of sessions (set of consecutively executed transactions), subject to appropriate PSU consent
  - Value add services (non-core PSD2) follow later

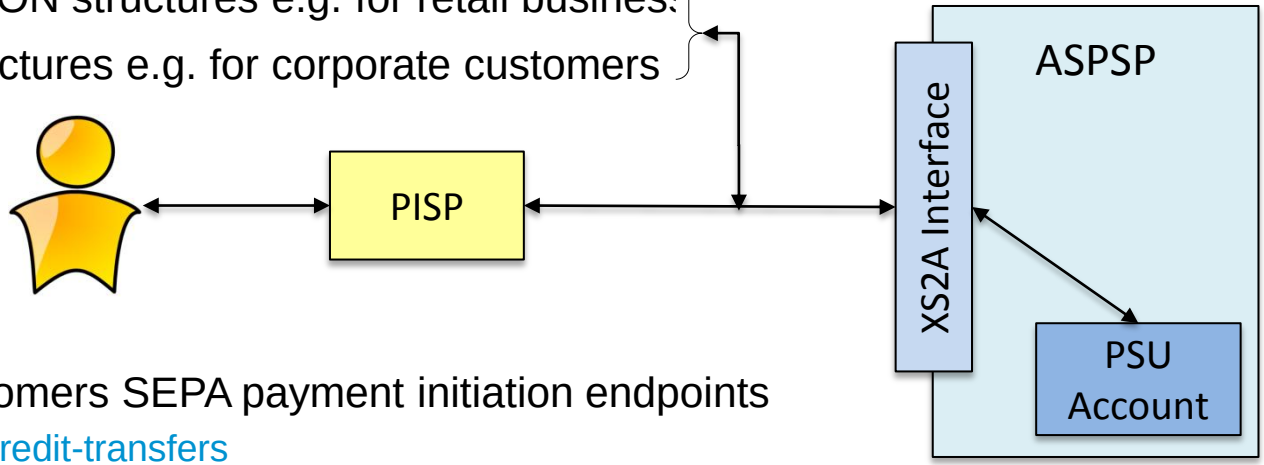
NextGenPSD2 - Key Characteristics

- NextGenPSD2 Strong Customer Authentication
  - Strong Customer Authentication (SCA) for PIS and AIS is a PSD2 and EBA RTS requirement
  - Different SCA architectures supported - TPP can indicate redirect preference



NextGenPSD2 - Key Characteristics

- Simple payment JSON structures e.g. for retail business
- Full SEPA XML structures e.g. for corporate customers



- Typical private customers SEPA payment initiation endpoints
  - /payments/sepa-credit-transfers
  - /payments/instant-sepa-credit-transfers
  - /payments/target-2-payments
  - /payments/crossborder-credit-transfers
- Typical corporate XML endpoint e.g.
  - /payments/pain.001-sepa-credit-transfers

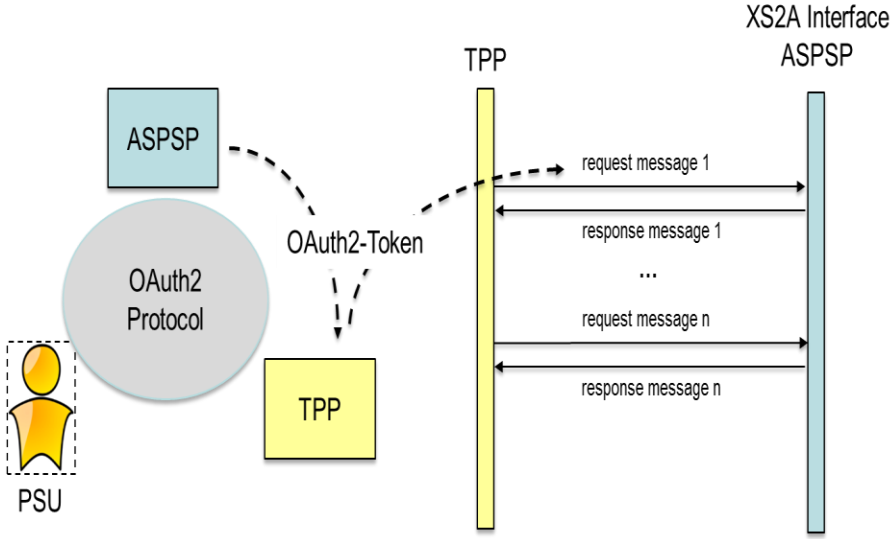
Supported payment endpoints are published by ASPSP. Can differ for retail and corporates.

NextGenPSD2 - Key Characteristics

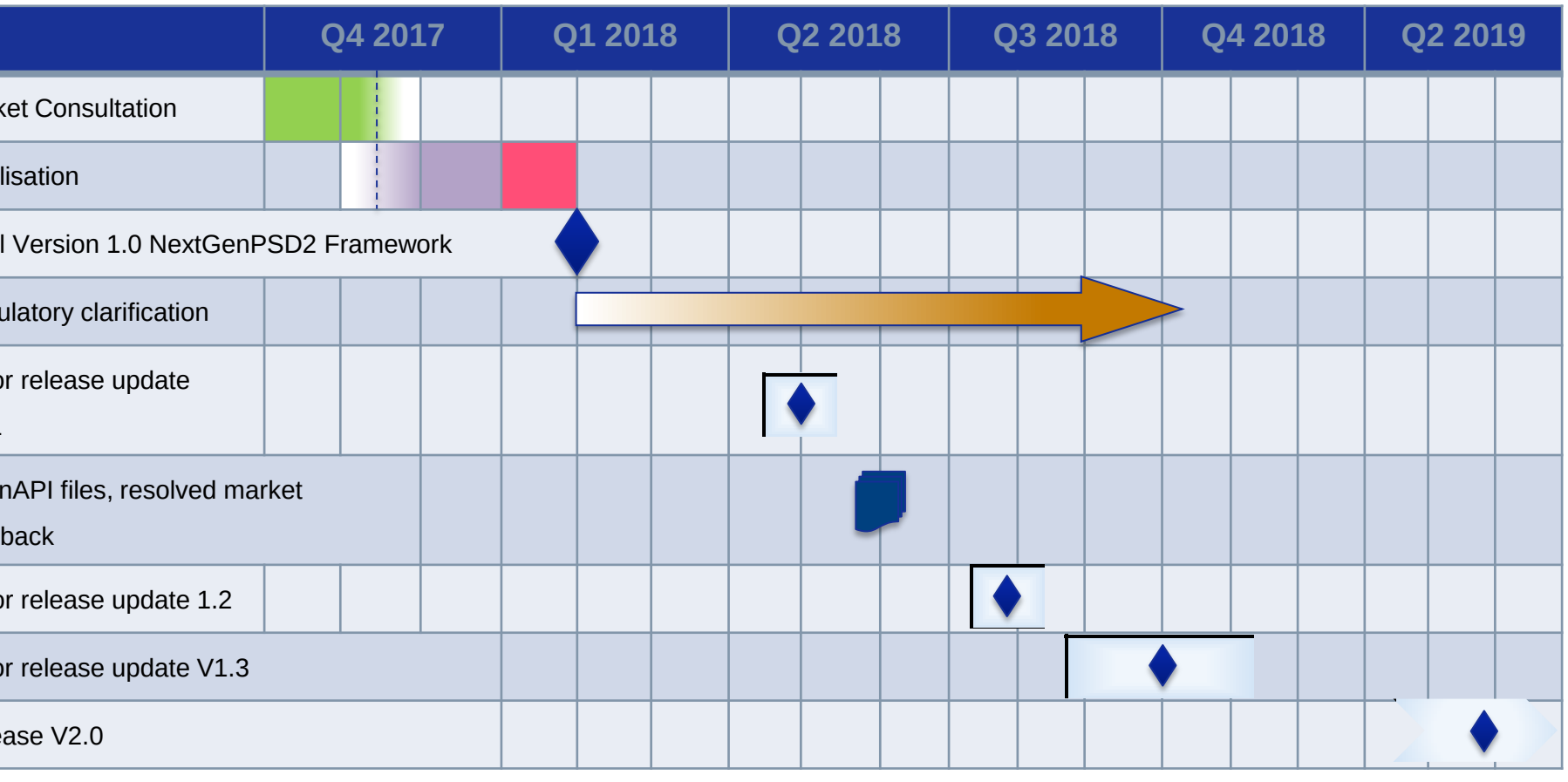
- NextGenPSD2 PSU Consent Management
  - Each NextGenPSD2 transaction is subject to PSU consent
  - PSU consent is a 2-step process in PIS or AIS
    1. Consent to initiate a payment or access data (from PSU to TPP, obeying EBA RTS Art. 32.3)
    2. Consent to execute a payment or share data with the TPP (consent authorisation, from PSU to ASPSP, obeying e.g. PSD2 Art. 64 and EBA RTS Art. 10)
  - PSU authorises consent towards ASPSP
    1. By executing SCA as part of a payment transaction
    2. By executing SCA as part of the establishing of the consent via the dedicated consent API (a token will be provided to the TPP and can be used in AIS when the PSU is not involved)
  - NextGenPSD2 Consent API separates consent handling from account access
  - NextGenPSD2 Consent API facilitates easy revocation of consent

OAuth2 protocol and XS2A interface can be combined if requested by an ASPSP

- OAuth2 protocol can be used to generate and verify access rights of a TPP to resources owned by the PSU
- Integrated as SCA or
- Used as pre-step
  - Result of the OAuth2 protocol can be reused in the execution of transactions at the XS2A interface



NextGenPSD2 - Future Outlook



NextGenPSD2 - Future Outlook

- Major Release V1.2 needed for EBA Opinion Paper input (Cancellation) and Multilevel SCA for Coporates
  - Release 1.2 had a big impact on basic API architecture, to separate authorisation routines
- Minor Release V 1.3 in October 2018
  - Will absorb further regulatory clarification to EBA RTS interpretation
  - Will absorb all errata documents
  - Will integrate additional functionality for card accounts
  - Will integrate a formal and transparent change management process
  - Will be the basis for implementations
- Release V 2.0 in 2019
  - Further technical evolution of the standard
  - Work on IANA-registered content types vs. payment products
  - Will integrate additional functionality
  - Will integrate the first set of extended services, separated form the PSD2 core specification

NextGenPSD2 - Future Outlook

- Since publication of V1.1 increased focus on Implementation Support
  - Contribute to a good quality, change management and evolution of the standards
  - Provide guidance on implementation and interoperability issues
  - Offer support with e.g. compliance best practices guidelines where needed
- Special focus on a Testing Framework
  - EBA RTS Art. 30.5: “ASPSPs shall make available a testing facility, including support, for connection and functional testing ….”
  - Harmonised interoperability standards provide a basis for a common Testing Framework with harmonised testing requirements, common test policy, testcase catalogue and common testtool requirements
  - A common Testing Framework takes care of implementation variants by banks and processors, simplifies interoperability testing and renders cost and maintenance efficiencies
  - A common Testing Framework is also on the wishlist of EBA and EC
- Organise broader market interests
  - NextGenPSD2 Advisory Board with a balanced multi-stakeholder representation from market demand- and supply-side being explored

04 October 2018

NextGenPSD2 Implementation Support Programme
Major Deliverables

Digital Financial Services Forum Bukarest, 04.10.2018

Dr. Ortwin Scheja, SRC

NISP

More information: info@nisp.online / www.nisp.online

NISP Scope & Objectives

NISP (NextGenPSD2 Implementation Support Programme) aims to

- Achieve fallback exemption for NextGenPSD2 implementers, ultimately until September 2019 (the envisaged programme end date)
- Create stable and sustainable implementations
- Create cost synergies in implementation and testing
- Reduce and solve interoperability issues and developer questions
- Coordinate NISP participants for testing

NISP

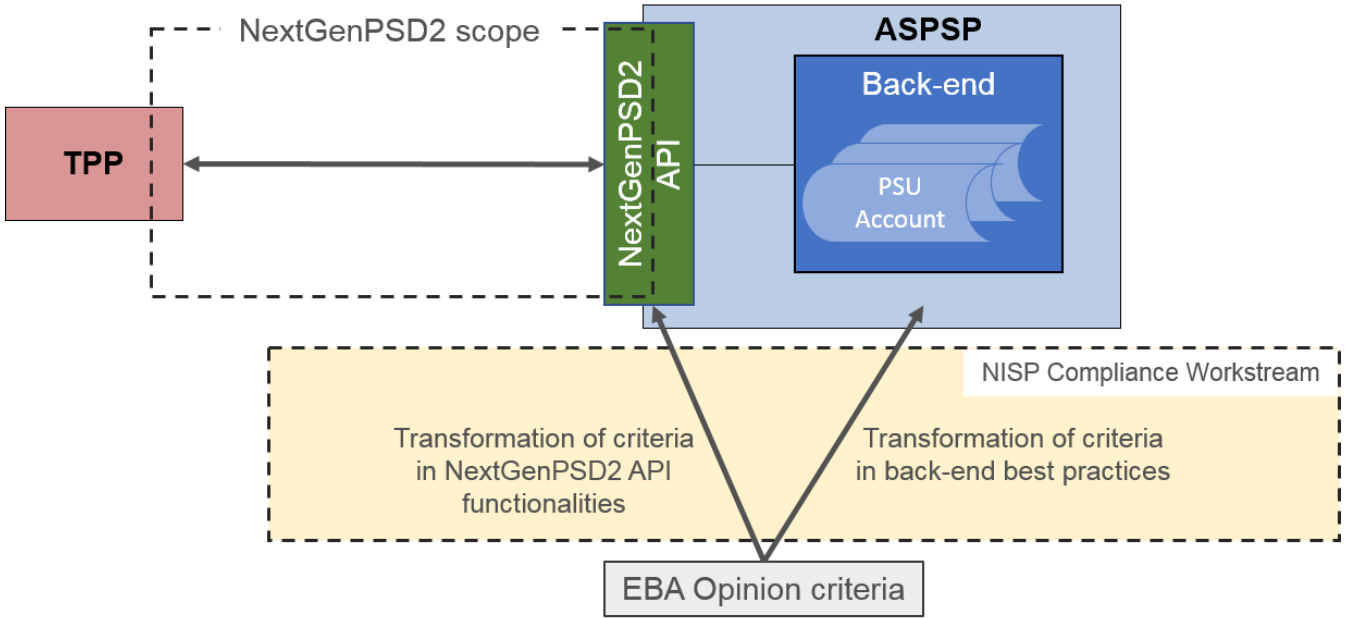
PROGRAM MANAGEMENT

A joint NextGenPSD2 implementation cooperation between banks, banking associations, payment associations, payment schemes and interbank processors in SEPA

NISP Compliance Workstream

NISP Perspective

- Fallback exemption criteria can be fulfilled by APIs only in conjunction with an appropriate ASPSP back-end implementation
- The NISP Compliance Specification is mapping the EBA Opinion criteria to the NextGenPSD2 API definitions and best practices for back-end implementations
- NISP Compliance Specification (functional requirements) is planned to be agreed with the addressed NCAs
- Aim is to identify at an early stage any potential issues in not achieving fallback exemption for NextGenPSD2 API implementations



NISP ASPSP Test Workstream

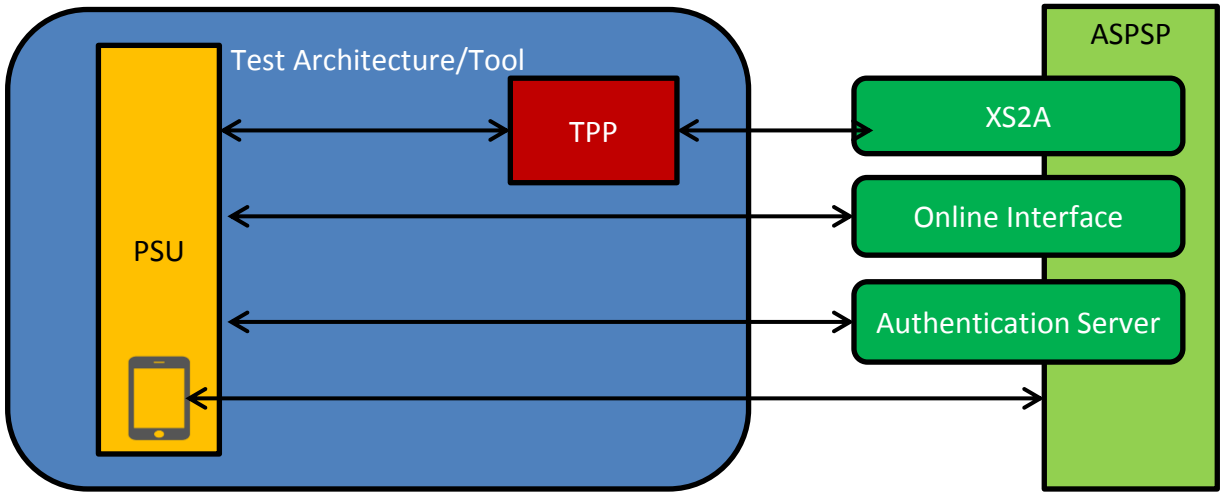
NISP Perspective: Common Testing Framework

- Deliverable is a test concept and detailed test case catalogue for internal ASPSP tests
- Reduces actual testing investments for ASPSPs by sharing resources for test definitions
- Aims to support and ease the efforts of the NCAs in evaluating the API implementations on time by proving a.o. Compliance Specification requirements in ASPSP implementations
- Takes care of the different variants and options in implementation
- Guarantees interoperability and simplifies interoperability testing
- Renders maintenance efficiencies

NISP ASPSP Test Workstream

Test Concept
explaining implementer options, abstract test model and test requirements

Test Specification
Excel Sheets with test case definition and automatism of identifying applicable test cases



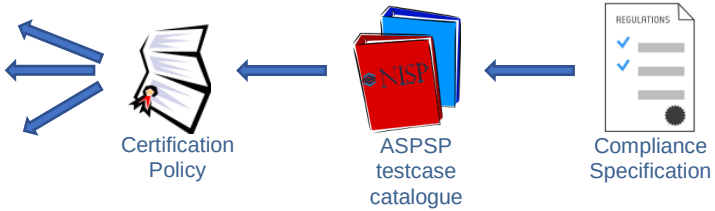
NISP Certification Policy Workstream

NISP Perspective

- ASPSPs intend to support NCAs with technical evaluation of NextGenPSD2 APIs implementations
- A self attestation by ASPSPs or other certification procedures will enable NCAs to assess potential TPP complaints
- The certification policy needs to identify the crucial test cases from the ASPSP test case catalogue
- To enable this, a mapping from the NISP compliance specification to relevant entries of the test case catalogue will be needed
- A close cooperation with NCAs might be needed to identify potential compliancy issues at an early stage

NISP Certific. Pol. Workstream

Define Certification Policy
Test case selection process
Self attestation
Response process to potential TPP complaints to NCAs



NISP Test Coordination Workstream

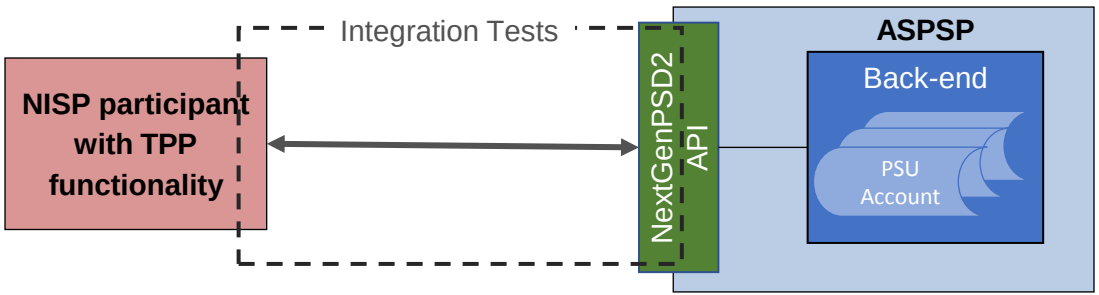
NISP Perspective

- Another important measure to guarantee interoperability is early integration testing
- It is planned to organise early integration tests between NISP participants to guarantee interoperable solutions
- The NISP project plans to coordinate these integration tests and track interoperability issues with NISP participants

NISP Test Coord. Workstream

Coordinate Tests
Conference calls / project server support

Track interoperability issues



More information

THE *Berlin* GROUP

A EUROPEAN STANDARDS INITIATIVE

info@berlin-group.org / www.berlin-group.org/psd2-access-to-bank-accounts