PSD2 RFP Template

Contents

Vendor Response	Description
OOTB	Capability is supported Out of the Box with configuration
Custom	Capability requires customization service
3PT	Capability is available with 3rd party components

API Gateway

Req#	Requirement	Vendor Response	Comments
GW-1	Does the product offer API gateway capability?		
GW-2	Does the product support OpenAPI Specification (fka. Swagger) to define API endpoints? Describe what OAS version are supported.		
GW-3	Does the product offer facility to manage API consumption with rate limits (messages/time interval) and quotas (raw # of requests permitted)? Describe how the product facilitates API consumption management.		
GW-4	Does the product offer possibility to restrict visibility and access to APIs to certain developers?		
GW-5	Does the product offer configurable policy to manage access control to APIs to customers and TPP applications?		
GW-6	Does the product facilitate rapid prototyping of mock APIs? Describe how the product facilitates mocks.		
GW-7	Does the product support publishing of backend SOAP, XML and messaging style services as APIs? Describe how the product support publishing of non-REST services as APIs.		
GW-8	Does the product support API mashups where multiple calls to backend systems using different protocols are needed in order to expose single API endpoint? Describe how the product facilitates API mashups.		
GW-9	Does the product offer graphical payload mapping and construction of call flows to backend systems?		
GW-10	Does the product offer preconfigured flows for Berlin Group NextGenPSD2 Framework to simplify integration with backend systems?		
GW-11	Does the platform support extensions using common languages like Java, C# or JavaScript?		
GW-12	Does the product support compression of traffic?		
GW-13	Does the proxy support HTTP & HTTPS?		

GW-14	Does the proxy provide support for CORS?		
GW-15	Does the proxy support caching? Describe what caching policies can be applied on endpoint and API level.		
GW-16	Does the product support API revisions, versioning and lifecycle governance? Describe how API lifecycle is supported.		
GW-17	Does the product support API protection with OAuth2 protocol?		
GW-18	Does the product support mutual TLS authentication?		
GW-19	Does the product support mutual TLS authentication using QWAC certificates that conform to ETSI TS 119 495? Describe how the product handles PSD2 specific data from certificates.		
GW-20	Does the product support HTTP message signing and validation using QSEAL certificates that conform to ETSI TS 119 495? Describe how the product handles PSD2 specific data from certificates and what specifications it follows for HTTP signing.		
GW-21	Does the product support Berlin Group NextGenPSD2 XS2A Framework requirements for OAuth2 protocol? Describe how the product supports the requirements such as the Mutual TLS Client Authentication and Certificate Bound Access Tokens.		
GW-22	Does the product offer capabilities to expose Berlin Group NextGenPSD2 XS2A framework compliant endpoints? Describe how the product facilitates BG specific handling of headers, hypermedia links, error codes.		
GW-23	Does the product offer compliance test suite for Berlin Group NextGenPSD2 XS2A framework?		
GW-24	Does the product offer compliance test suite for [country] interoperability profile for Berlin Group NextGenPSD2 XS2A framework?		
GW-25	Does the product offer security measures to protect against OWASP TOP 10 threats? Describe the measures.		
GW-26	Does the product offer the capability to check TPP status against the public registry such as PRETA?		

	Describe how the registry can be configured information is handled		
GW-27	Does the product offer the capability to cache TPP registry records?		
GW-28	Does the product support the use of cloud based eIDAS certificates for transaction authorization?		
GW-29	Does the product offer logging facility that captures timestamps?		
GW-30	Does the product offer structured logging?		
GW-31	Does the product offer support to trace the execution different components and processes that participate in API request processing?		
GW-32	Does the product log TPP and customer usage data (chargeable activity records) that can be used as an input for billing process?		
GW-33	Does the product offer TPP and customer usage data (chargeable activity records) via an API to allow an easy integration with existing systems?		
GW-34	Does the product provide the ability to perform synthetic transaction testing from different global locations?		
GW-35	Does the product provide reports and dashboards to monitor TPP activity and API usage? Describe reports / dashboards available with the product.		

API Developer Portal

Req#	Requirement	Vendor Response	Comments
DP-1	Does the product offer portal for developers?		
DP-2	Can the customer customize, skin, and modify the portal without vendor involvement? Describe to what extent portal can be changed without vendor involvement.		
DP-3	Does the product offer developer onboarding? Describe how the product facilitates onboarding.		
DP-4	Does the product offer possibility to customize the portal and onboarding forms? Describe to what extent poral can be customized.		
DP-5	Does the system support multiple entities with different branding? Describe how much is shared or can be unique to different brands.		
DP-6	Does the product support OpenAPI Specification (fka. Swagger) to generate documentation? Describe what OAS version are supported.		
DP-7	Does the product provide interactive documentation to allow API consumers to easily try out published APIs before coding?		
DP-8	Does the product offer documentation content for Berlin Group NextGenPSD2 Framework?		
DP-9	Dows the product support markdown format for authoring developer guide articles?		
DP-10	Does the product offer Q/A facility for developer support?		
DP-11	Does the product support alerting TPPs on downtime incidents and other important notices?		
DP-12	Does the product offer dashboard with API status and SLA metrics?		
DP-13	Does the product offer download of machine readable API descriptions in OAS (fka. Swagger) format? Describe what versions of OAS are supported		
DP-14	Does the product support localization of portal and documentation content? Describe what languages are available.		

API Sandbox

Req#	Requirement	Vendor Response	Comments
SB-1	Does the product offer sandbox for developers?		
SB-2	Does the product offer isolation of multiple developers in sandbox environment? Describe process and setup to sustain multiple TPPs trying to work in parallel.		
SB-3	Does the product offer capabilities to simulate Berlin Group NextGenPSD2 XS2A framework compliant endpoints? Describe how the product simulates BG specific handling of headers, hypermedia links, error codes, SCA methods and flows.		
SB-4	Does the product offer capability to simulate different types of payment accounts accessible online (current, giro, saving, card etc)?		
SB-5	Does the product offer capability to simulate transaction history with at least one transaction for each available type (credit transfer, direct debit, standing order, cancelled transaction, fees transaction etc)?		
SB-6	Does the product offer capability to simulate multicurrency accounts?		
SB-7	Does the product offer capability to simulate accounts with overdraft limits where available balance is different from book balance?		
SB-8	Does the product offer simulation of payment processing?		
SB-9	Does the product offer capability to generate test data needed for sandbox?		
SB-10	Does the product offer capability to issue test certificates for TPP authentication and message signing that conform to ETSI TS 119 495?		
SB-11	Does the product offer capability to issue test personalized SCA credentials linked to test users?		
SB-12	Does the product offer the capability to simulate SCA exemptions?		
SB-13	Does the product offer capability to test every possible error code that may be encountered in live environment?		

	Describe how the product facilitates testing of situations such as account locked, duplicate payment instruction, rejected as high risk.		
SB-14	Does the product offer compliance test suite for Berlin Group NextGenPSD2 XS2A framework?		
SB-15	Does the product offer the possibility to test multiple versions of APIs with same instance of sandbox? Describe how the product can be used to test released version in conjunction with next version of API.		

Identity and Access

Req#	Requirement	Vendor Response	Comments
IAM-1	Does the product offer identity and access management facilities?		
IAM-2	Does the product offer functionality of OAuth2 authorization server? Describe what grants are supported by the product.		
IAM-3	Does the product support Berlin Group NextGenPSD2 XS2A Framework requirements for OAuth2 protocol? Describe how the product supports the requirements such as the Mutual TLS Client Authentication and Certificate Bound Access Tokens.		
IAM-4	Does the product offer functionality of OpenID Connect authorization server? Describe what optional parts of the specification such as Discovery, Dynamic registration, Session Management, Front and Back channel log-out are supported.		
IAM-5	Does the product offer management of password-based credentials for customers?		
IAM-6	Does the product offer use of personalized security credentials (tokens, certificates) for authentication to user accounts?		
IAM-7	Describe the process used by a client to give access to a TPP. Provide sequence diagrams or other diagrammatic material explaining the steps performed by the client.		
IAM-8	Does the product offer customer-facing UI for capturing consent?		
IAM-9	Does the product offer customer-facing UI dashboard to list consents previously authorized and revoke specific consent?		
IAM-10	Does the product offer customer-facing UI to view log of TPP access events?		
IAM-11	Does the consent UI adapt to different device form factors (screen sizes)?		
IAM-12	Does the consent UI follow Open Banking Consent Model Guidelines for UI?		
IAM-13	Does the product support SSO with online banking applications to allow consent UI to be included in online banking applications?		
IAM-14	Does the product support redirect-based consent confirmation SCA flow?		
IAM-15	Does the product support OAuth2 based consent confirmation SCA flow?		

IAM-16	Does the product support the use of cloud based eIDAS certificates for customer authentication?		
IAM-17	Does the product offer single-sign on capability for online banking applications?		
IAM-18	Does the product offer anonymization, export and deletion of personal data in accordance with GDPR?		
IAM-19	Does the product offer possibility for admins to block / unblock TPP access?		

Strong Customer Authentication

Req#	Requirement	Vendor Response	Comments
SCA-1	Does the product offer strong customer authentication capabilities?		
SCA-2	Does the product support a mixture of soft and hard tokens? Describe vendors supported for 3rd party tokens.		
SCA-3	Does the product support SCA authentication methods that combine at least two elements of knowledge, possession and inherence? Describe what SCA authentication methods are supported.		
SCA-4	Does the product support SCA transaction authorization methods that combine at least two elements of knowledge, possession and inherence? Describe what SCA transaction authorization methods are supported.		
SCA-5	Does the product protect the confidentiality and integrity of authentication codes? Describe how authentication codes are protected.		
SCA-6	Does the product support dynamic linking of authentication code to transaction content such as payee and amount? Describe how different transaction authorization methods support dynamic linking.		
SCA-7	Does the product support What You See Is What You Sign principle for authorization of sensitive transactions? Describe what details can end user see for payment consent and account access consent.		
SCA-8	Does the product support customization and theming of payment and consent authorization screens? Describe to what extent can bank influence the presentation of consent details.		
SCA-9	Does the product support blocking access with temporary and permanent lockout? Describe the lockout process and how can bank parametrize the number of attempts and lockout duration to reflect it's policy.		
SCA-10	Does the product support alert the user when lockout happens?		

	Describe how the product can alert the user.		
SCA-11	Does the product support setting lockout duration and number of attempts based on risk?		
SCA-12	Does the product support prevention of credential replication (cloning) for possession-based credentials such as soft tokens? Describe how the product prevents cloning.		
SCA-13	Does the product offer capability to apply SCA exemptions? Describe which exemptions are supported.		
SCA-14	Does the product offer capabilities to mitigate the risk of malicious alterations?		
SCA-15	Does the product provide separate execution environment on multipurpose devices such as mobile phones?		
SCA-16	Does the product ensure confidentiality and integrity of personalized security credentials (PSC) by masking credentials when displayed and avoiding credential persistence as plaintext?		
SCA-17	Does the product ensure confidentiality and integrity of PSC by ensuring secure environment for creation, renewal, association and deactivation?		
SCA-18	Does the product ensuring delivery of PSC in secure manner with verified authenticity of applications and with activation of elements delivered over separate channels?		
SCA-19	Does the product offer white label branding of soft tokens? Describe to what extent application UI can be changed.		
SCA-20	Does the product offer SDK for soft token capability to be embedded in bank's existing mobile app? Describe what mobile app platforms are compatible with the SDK.		
SCA-21	Does the product support device identification and device binding for soft tokens?		
SCA-22	Does the product offer protection of personalized security credentials on mobile devices with secure enclave?		
SCA-23	Does the product offer protection of personalized security credentials on mobile devices with TEE?		

SCA-24	Does the product offer protection from key logging attacks on mobile devices?		
SCA-25	Does the product offer protection from overlay attacks on mobile devices?		
SCA-26	Does the product offer protection from repackaging and injection attacks on mobile devices?		
SCA-27	Does the product offer hook and debugging prevention?		
SCA-28	Does the product offer jailbreak and root detection?		
SCA-29	Does the product offer capability to collect device risk indicators for mobile devices and report to fraud monitoring?		
SCA-30	Does the product support push notification authentication across various mobile platforms?		
SCA-31	Does the product support QR code authentication across various mobile platforms?		
SCA-32	Does the product conform to OATH standard TOTP, HOTP and OCRA specifications?		
SCA-33	Does the product support DSKPP protocol for soft token provisioning?		

Fraud Monitoring

Req#	Requirement	Vendor Response	Comments
FM-1	Does the product offer fraud monitoring capabilities?		
FM-2	Does the product offer real-time assessment of authentication risk?		
FM-3	Does the product offer real-time assessment of payment fraud risk?		
FM-4	Does the product take into consideration list of compromised authentication elements as a risk factor?		
FM-5	Does the product take into consideration amount of each transaction as a risk factor?		
FM-6	Does the product take into consideration known fraud scenarios in provision of payment services? Describe the list of well-known fraud scenarios that is preconfigured with.		
FM-7	Does the product offer capability to monitor signs of malware infection in any session of authentication procedure?		
FM-8	Does the product take into consideration use and abnormal use of device or software as a risk factor? Describe which indicators of normal and abnormal use are monitored.		
FM-9	Does the product monitor abnormal spending or behavioral pattern of payer?		
FM-10	Does the product monitor unusual information about payer's device/software access?		
FM-11	Does the product consider abnormal location of the payer as a risk factor?		
FM-12	Does the product consider high-risk location of the payee as a risk factor?		
FM-13	Does the product monitor previous spending patterns of the customer?		
FM-14	Does the product monitor payment transaction history of each PSP's customer?		
FM-15	Does the product take into consideration location of the payer and of the payee at the time of payment transaction as a risk factor?		

FM-16	Does the product offer identification of abnormal payment patterns of customer in relation to transaction history?		
FM-17	Does the product offer capability to monitor payment transactions across all online access interfaces such as APIs, PoS, and online banking?		
FM-18	Does the product offer low latency real-time assessment of authentication and payment fraud risk? Describe what is the expected response time in milliseconds and how the system ensures low latency under load?		
FM-19	Does the product offer regulatory fraud reporting according to EBA guidelines on fraud reporting under PSD2? Describe which reports are provided.		
FM-20	Does the product offer workflow support to follow up disputed transactions?		

Integration

Req#	Requirement	Vendor Response	Comments
INT-1	Does the solution offer predefined and documented interfaces for integration?		
INT-2	Do the solution expose interfaces to facilitate single sign-on with online-banking application?		
INT-3	Does the solution expose interface for near to real time ingestion of events to fraud monitoring engine?		
INT-4	Does the solution expose batch-based interface for loading of customer, agreement and transaction data to fraud monitoring engine?		
INT-5	Does the solution expose interface for online banking applications to initiate SCA for authentication and transaction confirmation?		
INT-6	Does the solution offer integration connectors to backend systems for account access and payment initiation?		
INT-7	Does the solution expose integration interface for real-time assessment of authentication risk?		
INT-8	Does the solution expose integration interface for real-time assessment of payment risk?		

Architecture

Req#	Requirement	Vendor Response	Comments
ARC-1	Describe the components of your solution architecture.		
ARC-2	Does your solution support public cloud, private cloud and hybrid deployments?		
ARC-3	Does your solution support container-based deployment?		
ARC-4	Does the solution support scalable environment? Describe what is needed to provision additional capacity per API or per tenant?		
ARC-5	Does the solution architecture support multi-tenancy for both public cloud and private cloud deployments?		
ARC-6	Does the solution support zero downtime patching and updates?		
ARC-7	Does the solution support multi-data center deployment for business continuity?		
ARC-8	Does the solution provide options for customization and extension without vendor involvement? Describe types of changes which are only possible with the involvement of the vendor as opposed to the bank being able to do the changes themselves.		
ARC-9	Does the solution keep tamper resistant audit of all activities performed?		

Vendor Qualification

Please provide the following information regarding you company

- Company ownership and status;
- Up to date company financial reports;
- Business relationship with [bank];
- Quality management certificates held by your company and your solution / platform;
- Which are the key similar projects that you have carried out? State the similarities of scope which these projects entailed;
- List the references for similar solutions that you have implemented to this date;
- Local representation of company in [country].

Vendor Experience

Please provide the following information regarding your company experience and expertise

- Experience with provision of support for offered solutions;
- Technical skills and knowledge:
    - API design and implementation,
    - API lifecycle management,
    - OAuth 2.0 planning and implementation,
    - Banking and financial APIs
    - 2nd factory authentication
- PSD2 consulting expertise:
    - Interpreting PSD2 requirements to minimize risk of non-compliance
    - Open banking strategy formulation
    - Business models for PSD2
    - Payment fraud scenarios and models