SOUTH EASTERN EUROPE

PSD2 Regulatory Guidance
What is required and how to address it?

TABLE OF CONTENTS

1 Purpose and conventions

This document provides guidance on PSD2 regulatory requirements.

1.1 Abbreviations

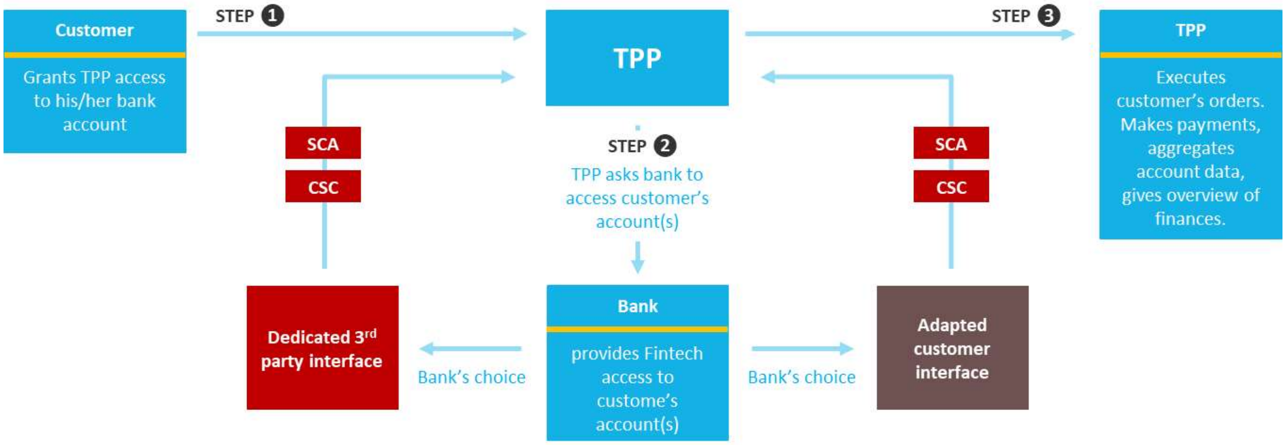
The following abbreviations are used in this document:

Abbreviation	Meaning
PSD2	Payment Services Directive 2
RTS	Regulatory Technical Standard
XS2A	Access to Accounts
SCA	Strong Customer Authentication
TPP	Third Party Provider
PSP	Payment Service Provider
ASPSP	Account Servicing Payment Service Provider
PSU	Payment Service User
TMM	Transaction Monitoring Mechanism
TRA	Transaction Risk Analysis
API	Application Programming Interface
BG	Berlin Group
IAM	Identity and Access Management
UX	User Experience
OAS2	Open API Specification v2
TLS	Transport Layer Security
WYSIWYS	What You See Is What You Sign

2 What is required by PSD2 and how to address it?

PSD2 regulation serves as a catalyst that will open up the field for new players with access to account (XS2A) and increase the level of security at which consumers transact with strong customer authentication (SCA).
XS2A can enable banks to go beyond compliance and incorporate their innovation into the own digital offer and possibly third party products and services to their clients taking advantage from new partnerships with FinTechs.
SCA is expected to increase the trust in digital offers and services, so that many of those who were rather careful and sceptic about digital, will increasingly switch from brick and mortar to digital.
Transaction monitoring mechanisms (TMM) and transaction risk analysis (TRA) are expected to bring down the fraud levels and reduce friction introduced when unnecessary SCA interrupts user experience during transaction.
Reduced friction at increased security level is expected to encourage the digital generation to do what they like best, interact with bank entirely digitally.

What does the PSD2 compliance really mean? The figure below describes the interactions between banks' customer (PSU), third party providers (TPP) and account servicing payment service provider (ASPSP or banks).


Customer
Grants TPP access to his/her bank account
STEP 1
TPP
STEP 3
TPP
Executes customer's orders. Makes payments, aggregates account data, gives overview of finances.
SCA
CSC
STEP 2
TPP asks bank to access customer's account(s)
SCA
CSC
Dedicated 3rd party interface
Bank's choice
Bank
provides Fintech access to custome's account(s)
Bank's choice
Adapted customer interface

3 Providing access to accounts (XS2A) to TPPs

PSD2 requires ASPSPs to provide access to payment accounts to payment service providers (AISP, PISP and PIISP) with explicit consent from payment service users (PSU). Dedicated interface (API) has to meet requirements concerning secure communication.

PSD2 requirements	How to address?
Explicit consent of the PSU Access to payment accounts and initiation of transactions require explicit consent of payment services user. **Requirement sources** ▪ Directive articles 64, 94	**Recommendations** ▪ Use OAuth2 framework to manage consents and allow access to APIs. Use IAM solution that has been tested and certified by OpenID Foundation. ▪ Customize consent management screens to adhere to UK Open Banking Consent Model Guidelines to provide best practice UX for users coming from UX research done in UK. ▪ Use redirection or decoupled consent flows to maintain customers mindshare. **Alternatives** ▪ Consider using explicit API endpoints to manage consents such as those in BG API as alternative to OAuth2 only if you want to avoid IAM solution that handle OAuth2 protocol and you have competence in building custom security UX and protocols.
Access by TPPs Access to following services by TPPs: ▪ confirmation on the availability of funds ▪ payment initiation service ▪ account information service At least one interface is required, either dedicated interface (API) or adapted customer interface (screen scraping). **Requirement sources** ▪ Directive articles 65-67 ▪ RTS articles 30-38	**Recommendations** ▪ Expose a dedicated API for TPP that covers all services. ▪ Follow pan European or locally API specification to achieve interoperability and reduce compliance effort **Alternatives** ▪ Using an adapted UI of online banking as a primary or fall back interface requires moderate investment to ensure that only data consent by customer are available to TPP and more significant investment to make the UI stable over time. ▪ If your local environment adopts specific API consider also exposing pan European BG API compliant endpoints for better interoperability
Documentation Specification of access interface publicly available to TPPs at least 6 months before RTS final date. Revisions documented 3 months before the change. **Requirement sources** ▪ RTS article 30(3-4)	**Recommendations** ▪ Publish API documentation in HTML format ▪ Document concerns common across API endpoints such as authentication and error handling ▪ Document reference descriptions of each endpoint parameters and payloads

	▪ Provide machine readable API descriptions in OAS2 (Swagger) format ▪ Provide documentation of multiple API versions and log of changes ▪ Provide references to implementation guidelines published by standardization efforts such as Berlin Group **Alternatives** ▪ Using an adapted UI of online banking as a primary or fall-back interface requires moderate investment to ensure that only data consent by customer are available to TPP and more significant investment
Testing facility Facility to test connectivity and functionality of TPP applications with ASPSP at least 6 months ahead of RTS final date. Support for TPPs developers must be available. **Requirement sources** ▪ RTS article 30(5)	**Recommendations** ▪ Create an isolated sandbox environment that resembles production with following differences: ▫ Simulated handling of payment transactions ▫ Preloaded set of fake customers, their accounts and transactions ▫ Simulated transaction risk handling ▫ Simulated SCA ▪ Provide Q/A forum for TPP developers to receive support **Alternatives** ▪ Consider having isolated sandbox for each TPP
Certificates Mutual authentication of TPPs and ASPSPs with QSEAL or QWAC eIDAS certificates **Requirement sources** ▪ RTS article 34	**Recommendations** ▪ Ensure that API gateway supports mutual TLS authentication using QSEAL and QWAC certificates that follow ETSI PSD2 profile ▪ Ensure that TPP claims extracted from certificate match those asserted by TPP when session is initiated **Alternatives** ▪ Handling certificates in API integration flows may lead to inconsistent implementation
SLA monitoring Defining, monitoring and publishing SLA KPIs for performance and availability of dedicated interface **Requirement sources** ▪ RTS article 32(1,2,4)	**Recommendations** ▪ Create a central logging facility that collect logs from dedicated interface (API) and customer interfaces (omnichannel) ▪ Subscribe to API monitoring service from providers such as apimetrics.com, runscope.com and newrelic.com ▪ Define synthetic, safe and idempotent API probing requests that correlate to availability and performance of critical use cases ▪ Configure timeout of 30 seconds

	▪ If possible use one solution to monitor performance and availability of both API and customer UI ▪ Inform TPPs of unavailability using the technical contact point they provided during registration ▪ Report problems to authorities **Alternatives** ▪ You can create a simple SLA monitoring service and host it on the public cloud. Make sure you build compliant alerting after unplanned unavailability is detected
Traceability of interactions Ensuring that interactions with PSU and TPPs are traceable. **Requirement sources** ▪ RTS article 29	**Recommendations** ▪ Create a central logging facility that collect logs from both dedicated interface (API) and customer interfaces (omnichannel) ▪ Use structured instead of formatted text logging ▪ Emit log entries in asynchronous manner to avoid blocking the request call chain ▪ Ensure that log entry timestamps are chronological by syncing servers to reference time source **Alternatives** ▪ Using an adapted UI of online banking as a primary or fall-back interface requires moderate investment to ensure that only data consent by customer are available to TPP and more significant investment

4 Implementing strong customer authentication (SCA)

Strong customer authentication requires use of multiple independent authentication elements based on knowledge, possession and inherence to protect sensitive transactions.

PSD2 requirements	How to address?
Authentication code Authentication using two or more elements including knowledge, inherence and possession results in generation of authentication code. **Requirement sources** ▪ RTS article 4	**Recommendations** ▪ Use authentication solution that supports multiple elements (knowledge, possession, inherence) ▪ Ensure that authentication solution can generate authentication code used for PSU account access, payment transaction initiation and any sensitive action which may imply risk of fraud or other abuse ▪ Ensure that solution works with both multipurpose devices such as mobile phones and special purpose devices such as different hardware tokens and fobs to ensure independence from HW vendors ▪ Use OATH compliant solution to ensure portability and interoperability ▪ Ensure authentication code confidentiality and integrity is protected in communication **Alternatives** ▪ Consider using FIDO compliant authentication solution that uses asymmetric cryptography and variety of authenticators
Blocking access Consecutive failed attempts to authenticate should result in temporary or permanent block. **Requirement sources** ▪ RTS article 4	**Recommendations** ▪ Ensure that solution configuration allows PSU access to be blocked temporarily after a set number of consecutive failed attempts to authenticate during a day and permanently after additional attempts ▪ Ensure that PSU is alerted of temporary block before it becomes permanent **Alternatives** ▪ Differentiate the length of block duration and number of attempts based on risks involved (compromised credentials, signs of malware infection, unusual location, unknown device and known fraud scenarios)
Dynamic linking Generated authentication code must be specific to transaction content such as amount and payee	**Recommendations** ▪ Ensure that authentication solution can generate authentication code specific to transaction content such as amount and payee

Requirement sources ▪ RTS article 5	▪ Besides payment initiation, protect other sensitive actions such as granting of consent for account access and whitelisting of beneficiary with authentication code ▪ Ensure that device used for authentication supports WYSIWYS (what you see is what you sign) display of transaction content to be confirmed ▪ Offer authentication methods that offer lowest friction (mobile phone, no manual entry) for end users such as push message authentication and QR code authentication **Alternatives** ▪ Use of special purpose hardware tokens that support transaction signing provides increased resilience to tampering but increases friction for users and cost of licensing, distribution and maintenance for PSP
Preventing replication Use of elements categorizes as possession requires measures designed to prevent replication of the elements. **Requirement sources** ▪ RTS article 8	**Recommendations** ▪ Use soft token solution that prevents cloning of possession-based credentials
Independence of the elements Breach of one knowledge, possession or inherence element used in authentication shall not compromise reliability of the other elements. Using multi-purpose devices requires separated secure execution environment and mechanism to detect and prevent alteration. **Requirement sources** ▪ RTS article 9	**Recommendations** ▪ Use runtime application self-protection RASP for mobile applications to mitigate the risks of malicious alterations such as malware infections, rooting and jailbreaking ▪ Ensure that solution for mobile tokens prevents cloning of possession-based credentials **Alternatives** ▪ Use of special purpose hardware tokens that support transaction signing provides increased resilience to tampering but increases friction for users and cost of licensing, distribution and maintenance for PSP
Confidentiality and integrity of personalized security credentials Confidentiality and integrity of personalized security credentials is assured in all phases of authentication: ▪ Masked when displayed ▪ Not stored in plaintext ▪ Secret material protected from disclosure	**Recommendations** ▪ Use authentication solution that ensures confidentiality and integrity of personalized security credentials throughout their full lifecycle. ▪ Use solution that removes friction from delivery and renewal process such as standalone soft token mobile application or soft token embedded in PSP application

■ Created in secure environment ■ PSU associated with credentials, authentication devices and software in secure environment controlled by PSP or remotely using SCA ■ Delivered in secure manner to legitimate user ▫ verified authenticity of software used ▫ with features delivered over separate channels ▫ with activation before usage takin place in secure environment ■ Renewed or re-activated according to creation, association and delivery procedures ■ Destroyed, deactivated and revoked in secure manner with appropriate records **Requirement sources** RTS articles 22-27	■ For remote delivery and activation consider using solution that supports DSKPP protocol ■ Ensure that solution for mobile tokens prevents cloning of personalized security credentials by third parties or payment service user **Alternatives** ■ Use of special purpose hardware tokens that support transaction signing provides increased resilience to tampering but increases friction for users and cost of licensing, distribution and maintenance for PSP

5 Handing exemptions from SCA to reduce friction

In order to allow user friendly and accessible means of payment while ensuring security of payment transactions PSD2 is allowing SCA exemptions based on lower risk involved in specific payment service.

PSD2 requirements	How to address?
Payment account information Repeated access to balance and 90 days transaction history within 90 days since application of SCA **Requirement sources** ▪ RTS article 10	**Recommendations** ▪ Use solution with SCA exemption rule capabilities integrated within API execution flow ▪ Ensure that solution can track SCA application across all online access interfaces – dedicated API and customer facing UI ▪ Ensure SCA is still applied when ▫ user accesses payment information for the first time ▫ user creates or amends a list of trusted beneficiaries ▫ user creates series of recurring transactions with same amount and same payee **Alternatives** ▪ Risk based authentication capability in some authentication solutions can be extended to cover some of SCA exemption rules but this extensibility is usually limited to simple rules
Contactless payments at point of sale Contactless electronic payments below 50 EUR, with no more than 5 payments up to cumulative amount of 150 EUR since last application of SCA. **Requirement sources** ▪ RTS article 11	
Unattended terminals for transport fares and parking fees Payment from unattended terminals for transport fares or parking fees. **Requirement sources** ▪ RTS article 12	
Trusted beneficiaries Payment to a payee who is on the list of trusted beneficiaries maintained by payer. **Requirement sources** ▪ RTS article 13	
Recurring transactions Repeated payment within a series of recurring payments of same amount and to the same payee. **Requirement sources** ▪ RTS article 14	
Transfer between own accounts Credit transfers between accounts held by the same natural or legal person. **Requirement sources** ▪ RTS article 15	
Low-value transactions Remote electronic payments below 30 EUR, with no more than 5 payments up to	

cumulative amount of 100 EUR since last application of SCA. **Requirement sources** ▪ RTS article 16	
Secure corporate payments Payments initiated by legal persons over dedicated secure protocols and processes available only to user who are not consumers. **Requirement sources** ▪ RTS article 17	
Transaction risk analysis Transaction posing low risk when fraud rate for that type of transaction is equivalent or below to reference fraud rate, amount of transaction does not exceed exemption threshold value, and none of the enumerated fraud indicators are present **Requirement sources** ▪ RTS article 18	**Recommendations** ▪ Use transaction monitoring mechanisms such as fraud detection engine to assess level of transaction risk **Alternatives** ▪ Use of special purpose hardware tokens that support transaction signing provides increased resilience to tampering but increases friction for users and cost of licensing, distribution and maintenance for PSP

6 Monitoring transactions for risk and fraud

In order to apply the SCA procedure and exemptions PSD2 requires PSPs to use transaction monitoring mechanisms to detect unauthorized or fraudulent transactions.

PSD2 requirements	How to address?
Minimum risk-based factors to consider Transaction monitoring mechanisms shall consider following risk-based factors at minimum: ▪ list of compromised authentication elements, ▪ amount of each transaction, ▪ known fraud scenarios, ▪ signs of malware infection in authentication procedure, ▪ use and abnormal use of device or software. **Requirement sources** ▪ RTS article 2(2)	**Recommendations** ▪ Use transaction monitoring solution (fraud solution) that takes into account minimum risk factors ▪ Ensure that solution monitors transactions across all online access interfaces – dedicated API, card based and customer facing UI ▪ Ensure that TMM solution receives feed of events from API gateway and SCA solution on failed and successful authentications ▪ Ensure acceptable performance of real-time risk analysis with event based integration that enables TMM to update risk profiles in near real time **Alternatives** ▪ Development or acquisition of purpose-built transaction monitoring solution separate from wholistic fraud monitoring solution can be justified in situations where central fraud solution does not have required capabilities and its extension is not feasible
Fraud indicators not present in transaction posing low risk Transaction posing low does not have ▪ abnormal spending or behavioural pattern of payer, ▪ unusual information about payer's device/software access, ▪ signs of malware infection in any session of authentication procedure, ▪ known fraud scenario in provision of payment services ▪ abnormal location of the payer ▪ high risk location of the payee **Requirement sources** ▪ RTS article 18(2c)	**Recommendations** ▪ Use transaction monitoring mechanism (fraud detection engine) that takes into account specified fraud indicators ▪ Ensure that TMM solution receives feed of events from API gateway or authentication solution on failed and successful authentications, RASP solution on signs of malware infection **Alternatives** ▪ Use of special purpose hardware tokens that support transaction signing provides increased resilience to tampering but increases friction for users and cost of licensing, distribution and maintenance for PSP
Minimum risk-based factors to for TRA exemption For transactions intended for exemption from SCA, TMM shall consider following	**Recommendations** ▪ Use transaction monitoring solution (fraud solution) that takes into account minimum risk factors

risk-based factors at minimum and combine assessment into a risk score: ▪ previous spending patterns of PSU, ▪ payment transaction history of each PSP's PSUs ▪ location of the payer and of the payee at the time of payment transaction, ▪ identification of abnormal payment patterns of PSU in relation transaction history. **Requirement sources** RTS article 18(3)	▪ Ensure that solution monitors transactions across all online access interfaces – dedicated API, card based and customer facing UI ▪ Ensure that TMM solution receives feed of events from API gateway and SCA solution on failed and successful authentications ▪ Ensure acceptable performance of real-time risk analysis with event based integration that enables TMM to update risk profiles in near real time **Alternatives** ▪ Development or acquisition of purpose-built transaction monitoring solution separate from wholistic fraud monitoring solution can be justified in situations where central fraud solution does not have required capabilities and its extension is not feasible
Monitoring At least on quarterly basis PSP shall record and monitor unauthorised transactions, use of SCA and specific exemptions **Requirement sources** ▪ RTS article 21	**Recommendations** ▪ Use transaction monitoring (fraud monitoring) solution that can track total value, average value and number of unauthorised & fraudulent transactions and those that were authorized with SCA and exempted for specific reason **Alternatives** ▪ Separate solution for SCA reporting can be used to monitor these specific aspects but this would require integration with TMM to extract data on fraudulent transactions