PSD2

Testing Considerations

July 2019

Overview

PSD2 is an EU directive which requires all payment account providers across the EU to provide regulated Payment Service Providers (PSPs) access to transaction data from customer accounts, subject to their explicit consent. One way of making this access possible could be through the Competition and Markets Authority's Open Banking remedy, which follows from the 2016 market investigation into competition in the UK's retail banking sector.

Key PSD2 Objectives

- Promote Innovation
- Reduce cost of payment services
- Improve consumer protection
- More secure Payments

Who is impacted?

- Banks, building societies and credit unions
- E-money and Non-bank issuers
- Money remitters
- Merchant acquirers
- Account information services (AIS) providers
- Payment initiation services (PIS) providers
- Firms issuing gift cards or travel cards
- Mobile and fixed line network operators
- Payment Systems Regulated Businesses

Potential operational changes

PIS, AIS and confirmation of availability of funds for CBPII

- An open application programming interface (API) allowing account-information service providers (AISPs) and payment-initiation service providers (PISPs) access to customer account and transaction information.
- Provide confirmation on the availability of funds for the execution of CBPII (Card Based Payment Instrument Issuer) transactions.
- Use of security credentials, sensitive payment data and security considerations in line with Regulatory Technical Standards (RTS).

Reporting & Notifications

- Regular/periodic reporting to FCA (e.g. Fraud/complaints reports).
- Event driven notifications to FCA (e.g. AIS/PIS denial, major operation/ security incidents).

Strong Customer Authentication

- Applying two-factor authentication to all electronic payments.
- Implementing SCA exemptions (e.g. whitelisting).
- Implementing fraud solutions to mitigate the risk of fraud attack from third-party access to customer account data.

Complaint Handling

- Changes to complaints recording and reporting (retention for 3 years).
- Applying complaint handling time limits in line with the regulatory requirements.

Testing Considerations

Potential Operational Changes	Testing considerations
PIS, AIS and confirmation of availability of funds Non-Functional Test Environment Security Conformance Testing with TPPs Mobile devices Test data API validations	– A robust test approach to validate conformance of security, digital performance, and operational OBIE requirements – An appropriate Test Environment Strategy to enable end to end tests with TPP's using 'Production like' environments – Physical mobile devices to validate web to mobile / mobile to web / mobile to mobile redirection – Data mapping to ensure correct data is exposed for target OB fields – Adequate test coverage of different payment types across retail and business customers – Functional tests to validate for Consent, AIS, PIS, confirmation of funds, access dashboards APIs – End to end customer journeys tests which align with the Open Banking (OB) customer experience guidelines
Reporting and Notifications Regulatory Reporting	– Comprehensive tests of MI and reporting solution to generate periodic reports for FCA (including PSD transaction information, fraud / operational & risk assessment, complaints, etc) – Comprehensive tests of event driven notifications to FCA (AIS / PIS denial, major operation / security incidents, etc)
SCA Fraud solutions SCA exemptions Two-factor authentication	**Develop tests to validate:** – Electronic payments initiated by the payer are covered under the SCA solution (unless called out under SCA exemptions) and the customer experience is consistent across all journeys and channels – Dynamic linking to electronic remote payment transactions – Fraud rules implemented consistently across channels
Complaint Handling Regulatory requirements for complaint handling	**Develop tests to validate:** – Changes to complaints recording and reporting (retention for 3 years) – Complaint handling time limits are in line with the regulatory requirements

Challenges for Testing

Challenges	The KPMG Way
Business Requirements  Lack of understanding of the PSD2 regulation may lead to poor implementation which does not conform to the PSD2 requirement	– Conduct static reviews of the business requirements by payment and PSD2 SMEs.
Coexistence of tests (e.g. UAT/NFT) in Test Environments  Mixture of test types and technology delivery plans cause heavy reliance on a strong test environment strategy. Constrained timelines may result in functional and non functional tests to co-exist causing disruptions	– Define 'fit for purpose' test environments strategy detailing how each environment will be used to support system, integration and different aspects of non-functional testing. – Develop a test environment plan to ensure dedicated test windows are scheduled reducing impact on test phases.
Tests with TPPs (Third Party providers)  Evidence of testing with the Third Party providers is mandatory to prove the ability to service external requests, but may be a challenge due to its complexity	– Manage Integration testing with TPP systems detailing clear plan for interaction and tests to be conducted for integration and E2E test scenarios.
Inputs to Exemption application  A lack of knowledge of the exemption process and supporting evidence required may result in invalid exemption applications	– Conduct detailed SME reviews of the exemption requirements to ensure there is clarity on how the evidence from various test phase are to be presented to support the exemption process.
Test Data  If test data cannot be sourced from production, data synthesis may be required to build the right data set to allow successful test scenarios	– Support in defining data dictionaries to illustrate what data is being used to execute a scenario and more specifically what data will be transferred to TPP's through the API's. – Create dummy data (synthesised) or extract and obfuscate Production data.
Coexistence with other legislations: FSMA, GDPR, SEPA, CPR, etc  With numerous regulations existing around Payments such as FSMA, GDPR, SEPA, CPR, etc. a siloed PSD2 implementation strategy may impact the overarching regulatory compliance for the financial institution	– Develop PSD2 quality assurance plan to demonstrate how the project will adhere to any other specific regulatory requirements i.e. GDPR for personal data.

KPMG's unique mix of testing specialists, industry SMEs and our 'Accelerated Testing' framework can reduce the cost of change by up to 25%. **For information on how KPMG can help with your PSD2 implementation, please get in touch.**

kpmg.com/uk

CREATE. | CRT114240B | July 2019.

Daryl Elfield
Testing Partner
T: +44 (0) 20 7311 6330
E: daryl.elfield@kpmg.co.uk

John Hallsworth
Open Banking Lead Partner
T: +44 (0) 20 7896 4840
E: john.hallsworth@kpmg.co.uk