PSD2, XS2A, CSC, SCA AND OTHER ACRONYMS

Fiorano®
Enabling change at the speed of thought®

Everything you wanted to know about the Second Payment Services Directive but didn't know whom to ask.

Fiorano Software

Business Whitepaper V1.0
October 2018

PSD2 is around the corner. Banks will be forced to share data with competing service providers, and customers will have real choice - for the first time.

PSD2 is designed to force traditional banks to open up systems via. APIs and share data with their competitors.

With regulatory timelines just around the corner, banks are left with very little time to put in place the essential technology required to meet requirements related to publishing ASPSP interfaces and developer sandboxes.

The regulation itself is an interesting acronym, and there being many more associated with it we felt it an appropriate time to publish this ready-reckoner to explain the many terms flying around related to the PSD2, that we are all dealing with on a daily basis.

Though we have tried to make this compilation as comprehensive as possible there's always a chance we may have inadvertently left something out. If you think that is the case or would like to see something added, please do let us know.

Biju Suresh Babu,
ns.biju@fiorano.com, @nsbiju

Index

PSD

The original Payment Services Directive (2007/64/EC) is an EU Directive, administered by the European Commission (Directorate General Internal Market) to regulate payment services and payment service providers throughout the EU and EEA. The original PSD's purpose was to increase pan-European competition and participation in the payments industry also from non-banks, and to provide a level playing field by harmonizing consumer protection, and the rights and obligations for payment providers and users.

PSD2

The Revised Directive on Payment Services (EU)2015/2366, commonly known as PSD2, was adopted by the European Parliament on 08th October 2015 as a step towards a digital single market, to benefit consumers and businesses and help the economy grow. On 13th January 2018, Directive 2007/64/EC was repealed and replaced by (EU)2015/2366. All companies in the EU have till September 2019 to comply with national laws and regulations pertaining to PSD2.

EBA

The European Banking Authority, the independent EU authority working to ensure effective and consistent prudential regulation and supervision across the European banking sector, along with the European Securities and Markets Authorities (ESMA) and the European Occupational Pensions Authority (EIOPA).

EC

European Commission

ERPB

Euro Retail Payments Board – the legal entity under the European Central Bank setup in 2013 to replace the SEPA Council and develop an integrated, innovative and competitive market for retail payments in the EU. It is an ERPB Working Group on PIS which recently highlighted practical gaps in the RTS regarding PSD2 interfaces and other elements.

EU 2018/389

Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regards to regulatory technical standards for strong customer authentication and common and secure open standards of communication

EU 2015/2366

Directive of the European Parliament and of the council on 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) no. 1093/2010, and repealing Directive 2007/64/EC

ASPSP

Account Servicing Payment Service Provider – The legal entity providing and maintaining a payment account for a payer as defined by the PSRs, and in the context of the open banking ecosystem are the entities that publish Read/Write APIs to permit payments initiated by Third Party Account Information or Payment Initiation Service Providers via. API endpoints.

TPP

Third Party Providers – Organisations that use APIs developed to standards to access customers' accounts in order to deliver Account Information or Payment Initiation related Services. TPPs may be either AISPs or PISPs or both. *See AISP and PISP*

AIS

Account Information Services – an online service which provides consolidated information on payment accounts held by a payment service user with Payment Service Providers. In the UK, PSD2 will bring existing payment service providers under the scope of the regulation and also ensure that AISPs (*See AISP*) can receive access to payment accounts, whilst also placing requirements on them to ensure security for users.

AISP

Account Information Service Provider – Organisations registered under a specific country's relevant CA / NCA to provide AIS services, or who have passport-ed into a separate host country CA / NCA to provide AIS services. *See CA / NCA*

PIS

Payment Initiation Services – an online service which accesses a user's payment account to initiate the transfer of funds on their behalf with the users consent and authentication. Payment Initiation Services provide an alternative to paying online using a credit card or debit card. PSD2 will ensure that PISPs receive access to payment accounts, whilst also placing requirements on them to ensure security for users.

PISP

Payment Initiation Service Provider - Organisations registered under a specific country's relevant CA / NCA to provide PIS services, or who have passport-ed into a separate host country CA / NCA to provide PIS services.

PSR

The Payment System Regulator – the economic regulator for the £81 trillion payment systems industry in the UK. Together with the UK's FCA, the PSR monitors and enforces the EU's PSD2 in the UK. The term PSR/PSRs is also used to broadly refer to the regulations such as the Payment Services Regulations 2017 (PSRs 2017)

CBPII

Card Based Payment Instrument Issuer - for PSD2, CBPIIs sit along-side AISPs and PISPs as Payment Services Providers. CBPIIs can request confirmation from an ASPSP on whether a customer has funds available in his or her account to complete a transaction at a given point of time, and ASPSPs must provide a yes or no answer. Banks / ASPSPs need to ensure their systems and processes are in place to respond to requests from CBPIIs within a very short timescale, even for accounts in respect of which the ASPSP itself may not be offering cards.

PSU

Payment Services User – the end customer or user (a person) in a PSD2 transaction, who makes use of an Account Information (AIS) or Payment Initiation (PIS) service as a payee, payer or both, by providing TPPs access to his/her bank account.

CA / NCA

Competent Authority / National Competent Authority for consumer protection – the national authority competent for the protection of consumer rights when dealing with credit or financial institutions in each EU Member State. As a trusted source, NCAs also may publish an NCA Public Register as a standard and secure service for validation of TPP's regulatory access levels by ASPSPs. The CA for the United Kingdom is the FCA. A list of CAs' web-sites, categorised by country, is provided here.

MSCA

Member State Competent Authority – the PSD2 Regulator in each member state, responsible for approving / rejecting TPP applications, issuing Authorisation numbers and adding authorised TPPs to the countries Home Public Register.

URN / GURN

Unique Reference Number / Global Unique Reference Number – a unique code combining Country + NCA code + an entities registration number to uniquely identify a payment institution within a public registry. The unique authorisation number may contain a PSD header to differentiate PSD identifiers, and could take the format of:

PSD-<Country_Code>-<HomeNCA>-<Entities_number_in_the_registry>

eIDAS

The electronic Identification Authentication & Trust Services Regulation - an EU regulation that sets out rules for electronic identification and trust services. It refers to a range of services that help verify the identity of individuals and businesses online or the authenticity of electronic documents. In the PSD2 context, banks and TPPs will use Qualified Certificates for websites and Qualified Certificates for Electronic Seals, which will be issued by QTSPs based on the ETSI TS 119 495 standard published in May 2018. Qualified certificates will include unique numbers such as URN/GURN to identify payment institutions as well as an entities NCA. Along with APIs and SCA, eIDAS is technically required to be part of the access mechanisms ASPSPs need to implement and make available to TPPs, in time for the September 2019 timeline. All TSPs are bound by Article 13 of the eIDAS to provide clear limitations for which their trust services may be used, and to assume a liability for any damage caused intentionally or negligently, or a failure to comply with the eIDAS.

ETSI

An independent recognised European standards body and not-for-profit organization, dealing with telecommunications, broadcasting and other electronic networks and services. In Europe, the ETSI supports European regulations and legislation through the creation of harmonised European Standards. Along with other European Standards Organisations (ESOs) CEN and CENELEC, the ETSI is the only other ESO whose standards are recognised as European Standards.

ETSI TS 119495

ETSI TS 119 495 v1.1.2(2018-07) Electronic Signatures and Infrastructures Technical Specifications; Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements specifies profiles of qualified certificates for electronic seals and website authentication to be used by payment service providers under the PSD2 for providing evidence with legal assumptions of authenticity (including identification and authentication of the source) and integrity of a transaction.

OB / OBUK

Open Banking is a term used to refer to a secure way to give service providers access to an individual's financial information. Open Bankingin the UK is designed to bring more competition and innovation to financial services. While the initial scope for Open Banking was mandatory for the CMA9, the OBIE emerged from this to then set the standard for PSD2 in the UK.

OBIE

The Open Banking Implementation Entity – the company set up by the CMA in 2016 to deliver Open Banking in the UK. The OBIEs trading name is Open Banking Limited and its role is to: (a) Design the specifications for the APIs that banks and building societies (in the UK) use to securely provide Open Banking and PSD2; (b) Support regulated TPPs, Banks and ASPSPs to use the Open Banking standards; (c) Create security and messaging standards; (d) Produce guidelines for participants in the Open Banking ecosystem; (e) Set out the processes for managing disputes and complaints; and crucially (f) Manage the Open Banking Directory which allows regulated participants to enrol in Open Banking.

CMA

Competition & Markets Authority (UK), a London headquartered, independent non-ministerial department that works to promote competition for the benefit of consumers both within and outside the UK.

CMA 9

The nine largest banks and building societies in Great Britain and Northern Ireland, based on the volume of personal and business current accounts. The CMA 9 setup and funded the OBIE based on an order by the CMA in 2016.

API

Application Programming Interface – A set of software functions and procedures that allow the creation of applications which access the features or data of an operating system, application, or other service. From a PSD2 standpoint, while the RTS does not explicitly specify the use of APIs for banks to promote and control data sharing, in reality APIs are the only long term and sustainable method to deliver XS2A elegantly.

XS2A

Access2Account – the technical acronym for access to customers payment accounts by third party providers (via. APIs). Under the XS2A, banks must (through an API format) provide a service exposing customer account information and payment initiation to any third party registered under a Competent Authority and with the consent of the PSU.

SCA

Strong Customer Authentication – the principle of ensuring customer protection in PSD2 transactions by applying an increased level of security in electronic payments. SCA is to be applied under certain conditions as defined in the PSD2 RTS: (a) When a customer (individual or corporate) accesses their payment account online (including just an aggregated view); (b) When making an electronic payment and (c) When carrying out any action through a remote channel which may imply a risk of payment fraud or other abuses. In practice, SCA will be applied using mechanisms to check a customer's identity using at least any two of: (i) Knowledge (ii) Possession and (iii) Inherence. The specification requires a unique authentication code to be used which dynamically links the transaction to a specific amount and a specific payee. The RTS also lists a number of possible exemptions to SCA to try and keep electronic payments as convenient and seamless as possible.

JWT

JSON Web Token - an open standard that defines a compact and self contained way for securely transmitting data between entities as a JSON object. Information contained within a signed JWT can be trusted as they are digitally signed using a secret key pair. TPPs who want to onboard with an ASPSP must generate a TPP registration request JWT which contains the SSA and other claims. In the UK the JWT is issued and signed by the Open Banking Directory.

SSA

Software Statement Assertion - A JSON Web Token (JWT) containing client metadata about an instance of TPP client software. ASPSPs must not accept client registration requests that do not contain a valid SSA. ASPSPs are required to provide: (i) a service that can validate and process a request JWT and the SSA JWT it receives from TPPs, supporting both the PS256 and ES 256 all types; (ii) a service to create and return client credentials based on the security characteristics obtained from metadata; (iii) Storing the Software Statement ID from the SSA against the client and validating the TPP, App and SSID.org_jwks_endpoint; (iv) a discovery specification endpoint that confirms with the OIDC discovery specification advertising supported mechanisms and algorithms available to TPPs

CSR

Certificate Signing Request - Once a Software Statement has been created a CSR is required in order for ASPSPs and TPPs to sign requests and create digital certificates to encrypt messages over the public network.

CN

Subject Common Name - the Software Statement ID (SSID) for the software statement that the certificate has been created for

ECDSA

Elliptical Curve Digital Signing Algorithm - A request object signing algorithm supported by Open Banking

MATLS

Mutual Authentication TLS - the mechanism used to protect the Open Banking directory Rest APIs and bank end points. Third parties must use the transport certificate issued to them by the OB Directory in order to exchange an authorization code for an access token. The ASPSP will ensure that the TLS certificate being used matches that of the OAuth client.

OIDC

Open ID Connect - built on top of the OAuth 2.0 protocol and often used for federated authentication, in the context of PSD2 and Open Banking OIDC provides identity tokens. Anyone entering the Open Banking UK ecosystem must be OIDC enabled.

chipTAN

Related to SCA, refers to transaction authentication codes received on a chip-enabled security device separate to the PSUs mobile device.

smsTAN

Also related to SCA and sometimes referred to as SMS OTP (One Time Password), refers to transaction authentication codes received via. The SMS channel on the PSUs mobile device.

ETV

Exempted Threshold Value, related to SCA, refers to a specific amount electronic transactions should not exceed to qualify as being low-risk and hence exempt from SCA.

TRA

Transaction Risk Analysis - method for analysing risk levels associated in associated PSD2 transactions. The ETV is linked to corresponding fraud rate categories under PSD2 specific TRA.

CSC

Common and Secure Communication - specifications for safeguarding the confidentiality and integrity of data to ensure the security of communication sessions between ASPSPs, AISPs, PISPs and CBPIIs. The RTS for SCA and CSC comes under Article 98 of the PSD2

CRL

Certificate Revocation Lists – One of two commonly accepted mechanisms to check the validity of Trust certificates such as eIDAS, the other being the Online Certificate Status Protocol to check the validity of a certificate in real time. While OCSP is considered the most accurate approach, real-world latency and network load considerations often result in CRLs being chosen, which essentially is a list of revoked certificates.

ISO 20022

The ISO standard for APIs in financial services developed by the International Organisation for Standardisation (ISO) as an established way to develop message standards within the financial services industry. ISO 20022 is a single, common language for all financial communications supporting interoperability between all parties. When APIs are implemented in a cross industry setting, between many institutions with differing data sets, ISO 20022 can add value by providing common business data semantics in a standardised and uniform structure.

JSON

The de-facto data exchange standard in most mobile applications, JSON is intrinsically linked with APIs and is commonly used along with ISO20022 elements. As an example, Open Banking UK uses both JSON and ISO 20022.

OLO

One Leg Out transactions – Under PSD2, OLO transactions are those where either the payer / recipient service provider is based outside the EU. OLO transactions were largely out of scope in the original PSD, as were transactions in non-EU currencies. PSD2 brings all OLO transactions within scope so long as any one of the service providers is located in the EU, in respect to the parts of the transaction carried out in the EU and in all currencies.

STET

STET S.A – headquartered in France, is a European leader in payments processing (SIPS) and is owned by 6 major banks – BNP Paribas, BPCE, Crédit Agricole, Banque Fédérative du Crédit Mutuel, La Banque Postale and Société Générale. STET is an active contributor to European discussions and efforts to provide the market with harmonised payment solutions and, from a PSD2 standpoint, is one of the competing standards or guidelines vying for dominance against the Berlin Group and Open Banking UK. It is however interesting to note that STET is one of the key participants of the Berlin Group.

ZBP

The Polish Bank Association initiative for PSD2, spearheaded by the Polish Banking Federation.

SBA

The Slovak Banking Associations standardisation initiative for PSD2.

Berlin Group

A pan-European payments interoperability harmonisation in initiative and technical standardisation body, with the primary objective of defining open and common scheme- and processor-independent standards in the inter-banking domain. The Berlin Group currently has participation from 25 major players in the payments industry from 10 different Euro-zone countries and from the UK, Sweden, Denmark, Norway, Iceland, Turkey, Bulgaria, Hungary, Serbia and Switzerland, together representing more than 25 billion card-originated transactions annually within the Single Euro Payments Area (SEPA). For PSD2, the Berlin Group has worked on a detailed 'Access to Account Framework' with data model at conceptual, logical and physical data levels, and associated messaging based on the EBA RTS.

QWAC

Qualified Website Authentication Certificates – provide a method to authenticate 'Internet Entity Identity' and encrypt communications in order to provide confidentiality. QWACs are used with specific protocols at the Transport layer and are not designed to be used at the Application layer.

QSEALC

Qualified Electronic Seal Certificates – used at the Application layer, with messages being passed between communicating parties to prove origin, authenticity and integrity that the data comes from the party that it is meant to. From an SCA/CSC standpoint, QSEALCs can be used to establish the PSD2 'Financial Identity' as opposed to the internet identity in the QWAC.

TSP / QTSP

Trust Service Providers (TSPs) are commercial organisations or government entities that provide digital services which enable the issuance and proving mechanisms to secure information from official sources and protect it against tampering in transit, allowing Trust. A Qualified status (hence QTSP) is awarded to TSPs who undergo national accreditation under eIDAS through a written Conformity Assessment. The Qualified status is intended to provide the European Market with a reliable standard that ensures a basic level of confidence when choosing a Trust service supplier, it also guarantees a level of interoperability across the European Trust infrastructure. QTSPs are regulated by each EU Member State under an appointed Member State Supervisory Body (MSSB).

All TSPs are bound by Article 13 of the eIDAS to provide clear limitations for which their trust services may be used, and to assume a liability for any damage caused intentionally or negligently, or a failure to comply with the eIDAS.

Passport / Passporting

To both enhance cooperation between competent authorities (CAs) and ensure a consistent and efficient notification process for payment institutions intending to exercise the right of establishment and the freedom to provide services on a cross-border basis across the EU, the EBAs RTS on the framework for cooperation and exchange of information between CAs for passport notifications under the PSD2 outlines the format and notification templates to be used between Competent Authorities when a payment institution in one Member State applies to provide services in another Member State via. A 'Passport' application that may be either a Branch Passport application, a Services Passport application or an Agent Passport application.

RTS

Regulatory Technical Standards – published by the European Banking Authority (EBA) specify various technical requirements (e.g. SCA, CSC, Passporting) that PSD2 players must meet to provide services in a format that is accepted, taking into account the various objectives of the PSD2, including enhanced security, promoting competition, ensuring technology and business-model neutrality, contributing to the integration of payments in the EU. RTS's are technology and business-model neutral.

FCA

The Financial Conduct Authority, the NCA in the UK responsible for enforcing PSD2.

CVM

Customer Verification Method – used for verifying customers (e.g. using signatures) during card payment transactions.

NFC

Near Field Technology – one of the underlying technologies used in mobile devices where payment transactions from PSUs may be initiated. NFC allows devices to talk to each other and is often used in contactless payments.

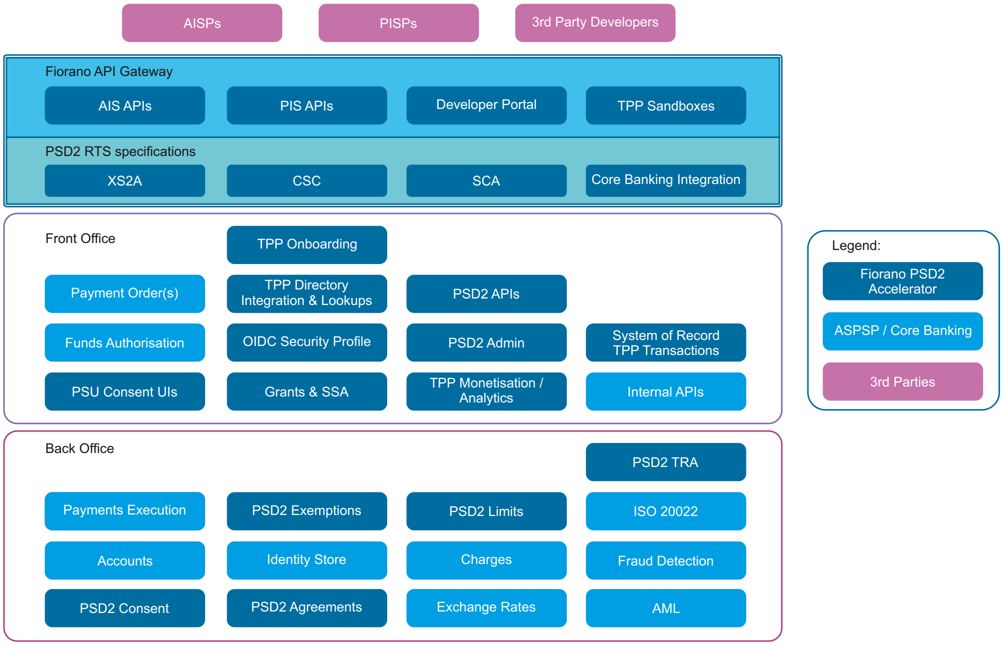
Fiorano & PSD2

Overwhelmed by all the jargons and acronyms?

At Fiorano, our experts keep themselves abreast of the changes and developments in various regulatory standards and guidelines to be able to act as advisers to Banks, TPPs and other financial organisations that need to comply with them.

Additionally, the Fiorano PSD2 Accelerator is built to technology specifications mandated by the RTS and offers end-to-end functionality for PSD2 XS2A, SCA and CSC to help you stay compliant without having to understand every little detail.

Fiorano PSD2 Accelerator for ASPSPs:



If you would like to see a demo of the PSD2 Accelerator or schedule a consultation session with our solution experts to understand the steps you need to take to comply with PSD2 before the deadline approaches, reach out to us at **psd2compliance@fiorano.com.**

References:

- www.fca.gov.uk
- eba.europa.eu / ec.europa.eu
- www.psr.org.uk
- www.preta.eu / www.openbankingeurope.eu
- www.ico.org.uk
- www.etsi.org & ETSI TS 119 495 technical specification v1.1.2(2018-07)
- www.openbanking.org.uk
- www.gov.uk/government/organisations/competition-and-markets-authority
- www.stet.eu/en/psd2
- www.zbp.pl
- www.berlin-group.org
- www.iso20022.org
- tools.ietf.org/html/rfc7519
- openbanking.atlassian.net
- www.forgerock.com/industries/financial-services/open-banking/UK-Spec
- www.europeanpaymentscouncil.eu
- www.cliffordchance.com

Fiorano PSD2 Accelerator

Built on Fiorano's class leading enterprise MQ, Middleware and API Management technology, the Fiorano PSD2 Accelerator brings together all the technology components Banks require to deliver ASPSP Interfaces including XS2A, SCA and CSC, in a clean, simple to implement software bundle that can be deployed on premises or in the cloud.

www.fiorano.com/psd2

Fiorano®
Enabling change at the speed of thought®

About Fiorano

Established in Silicon Valley in 1995, Fiorano is a global leader in high-performance enterprise middleware, API Management and peer-to-peer distributed computing systems.

With decades of experience working with organisations in the Financial Services, Defence, Public and Healthcare sectors all over the world, Fiorano technology has been put to the test and proven time-and-time again with leading organisations including ABN AMRO, Boeing, British Telecom, Capgemini, McKesson, NASA, POSCO Steel, Qwest Communications, Rabobank, Schlumberger, Lockheed Martin, the United States Coast Guard, the NHS, Vodafone and others who have all deployed Fiorano to drive innovation through open, standards-based microservices, typically built in just days.

www.fiorano.com