KuppingerCole Report

WHITEPAPER

by John Tolbert | January 2019

ForgeRock Identity Platform capabilities for Authentication under PSD2

The Revised Payment Service Directive (PSD2) will drive many changes in technical infrastructure at financial institutions across Europe. Banks and other financial service providers must quickly prepare for PSD2. ForgeRock Identity Platform provides strong customer authentication capabilities that can help businesses meet the technical challenges posed by PSD2.

by **John Tolbert**
jt@kuppingercole.com
January 2019

Commissioned by ForgeRock

Table of Contents

Related KuppingerCole Research Documents

Leadership Compass: Access Management and Federation - 71102

1 Executive Summary

In the European Union, the Revised Payment Services Directive (PSD2) will radically alter the financial services landscape. It has already begun to create a more competitive environment, with new business entities arising to offer additional financial services, such as acquiring account information and presenting it to consumers, and initiating payments directly from accounts at traditional financial institutions to merchants and other electronic service providers.

From a technical perspective, PSD2 necessitates improvements in two major functional areas:

- Strong Customer Authentication (SCA), transactional risk analysis, and malware mitigation in transaction processing
- Opening new financial service APIs, and properly securing them

Concerning SCA, in most cases, authorization and access control are predicated upon authentication, i.e. determining if the subject is who/what it purports to be. Regulations often stipulate the level of authentication assurance that is necessary for certain types of actions to be performed on systems and data. PSD2, at a high level, requires "strong authentication". The directive relies upon the standard definition, which requires two of these three factors: something you know, something you have, and something you are.

The problems with username/password authentication are well-known. Both usernames and passwords are easily and often forgotten. Password resets are expensive, in terms of both help desk costs and lost productivity. Passwords are easily guessed by hackers. Password databases can be broken via brute force attacks. There is no such thing as a strong password. Telling users to choose complex passwords and use different passwords for every site is futile. Most cyber-attacks and data breaches that have made the news in recent years have involved the perpetrator(s) gaining access to systems and data by compromising usernames and passwords.

Higher assurance authentication is fundamental to reducing risk of fraud and data loss. Stronger authentication techniques also enable greater compliance with regulations such as PSD2, as we will see below.

Fortunately, better alternatives to passwords exist. Many enterprises have deployed SmartCards, USB tokens, or other types of strong authentication tokens for the highest levels of assurance. Biometric solutions, using something about oneself as an authenticator, such as fingerprints or iris scans, are gaining traction due to their popularity among users. Out-of-band and step-up authentication and authorization options via mobile devices are becoming more common and accepted by users.

PSD2 will spur the adoption of these new authenticators in the quest to achieve SCA. Authenticators with a higher degree of usability, such as mobile push and mobile biometrics apps, are likely to be preferred and become dominant. Authenticator form factors such as Smart Cards and USB tokens will probably not be deployed by banks or FinTechs due to the fact they are less user friendly.

With regards to APIs, please see KuppingerCole's **Leadership Brief**.

PSD2 will radically change the financial sector in the EU

This paper will dive deeper into the technical requirements that banks and financial service providers face in preparing for EU PSD2 with regards to strong customer authentication. We will also discuss the ramifications for banks and other financial services organizations. Lastly, we will consider how ForgeRock Identity Platform can help banks and TPPs prepare for PSD2.

2 Highlights

- EU PSD2 took effect in January 2018. The Regulatory Technical Specifications (RTS) govern the implementation of Strong Customer Authentication (SCA) and Secure Communications; the deadline for testing components is March 14, 2019, and the deadline for implementation is September 14, 2019.
- PSD2 introduces the concept of Third-Party Providers (TPPs), which include Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs). AISP and PISP functions have historically been performed by banks; competition in the financial sector will emerge from non-traditional, non-banking types of businesses.
- Trust frameworks must be defined at the national and international levels and be put in place between banks and TPPs.
- Banks must prepare for PSD2 by creating APIs for AISPs and PISPs to use
- Both banks and TPPs must
  - Strongly authenticate customers
  - Conduct transactional risk analysis to mitigate the need for SCA for every transaction
  - Detect and prevent the influence of malware in all transactions
- All banks should begin a PSD2 readiness assessment as soon as possible
  - Document architectural deficiencies
  - Incorporate PSD2 risks in enterprise risk management model
  - Budget for, procure, and implement infrastructure and services needed for PSD2 compliance as soon as possible

3 PSD2: The background and Regulatory Technical Specifications

PSD2 will revolutionize payments and financial services across the EU. PSD2 aims to foster competition in the financial sector, increase transactional security, and improve customer experiences.

Directive 2015/2366/EU[1], more commonly known as PSD2, has been in work for a number of years. It amends and succeeds **Directive 2007/64/EC**[2]**,** the original PSD. During the transition to PSD2, PSD remains in effect. It is important to note that EU Directives are legislative directions that EU member states must enact, whereas EU Regulations are binding legislative acts across all member states. Directives establish a minimum set of legal requirements that must be incorporated into national laws. As PSD2 comes into force by adoption of EU member states' legislative bodies, small variations may arise, but the basic tenets and Regulatory Technical Specifications (RTS) should be adhered to across all states.

3.1 Background and goals of PSD2

The original PSD helped establish the Single Euro Payments Area (SEPA), facilitated cross-border payments, cut fees and increased choices for consumers, strengthened the rights of consumers, and decreased transaction settlement times. In 2013, the European Commission began a review process of PSD in light of new technical and business developments, such as the rise of new financial technology service businesses, as well as new security technologies.

PSD2 will build on the success of the original PSD and introduce new requirements. The main goals of PSD2 are:

- Contribute to a more integrated and efficient European payments market
- Improve the level playing field for payment service providers (including new players)
- Make payments safer and more secure
- Protect consumers
- Encourage lower prices for payments[3]

PSD2 defines the new business entities Payment Initiation Service Providers (PISP), which will have the ability to start payment processes directly between consumers and merchants; and Account Information Service Providers (AISP) that will have the ability to aggregate account information about consumers and businesses. These business functions have typically been performed by banks or related banking services. Competition in the financial sector within these newly defined roles will emerge from non-traditional, non-banking types of businesses.

As an EU directive rather than a regulation, PSD2 must be instantiated into national laws of EU member states. Therefore, certification of permitted TPPs and enforcement will occur primarily at the national

[1] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366
[2] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007L0064
[3] http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en

level. Operational certification, trust frameworks, enforcement, and penalties levied for non-compliance are likely to vary between jurisdictions.

3.2 Strong Customer Authentication

Clients of financial services must use strong authentication methods to access financial resources. As written, PSD2 defines strong authentication in the traditional way: something you have, something you know, and something you are. Thus, SCA means using a two or multi-factor authentication (MFA) event from the very start. SmartCards, USB tokens, and software tokens have been used for strong authentication in enterprise contexts, but will not be deployed by banks and TPP nor would they be accepted by consumers.

Rather, we expect that banks and TPPs will expand the use of mobile apps, especially biometrics on smartphones. Smartphones are nearly ubiquitous across the EU and have a number of features that facilitate their use as an authentication platform, including the fact that they are usually associated with an individual across many locations, have fast CPUs capable of processing cryptographic functions, and contain components for secure processing, i.e. Secure Elements and Trusted Execution Environment for Android, and Secure Enclave for iOS.

PSD2 RTS provides a few exceptions to SCA: transactions under €30; remote, unattended payment kiosks, such as parking meters or transport stations; and in cases where "transactional risk analysis" has been performed sufficiently.

3.3 Market changes and risks

Banks will still hold money and make loans, but new companies are emerging that will also provide services to handle account aggregation and payment management. While banks will still have to retain significant capital reserves, the TPPs do not. PISPs must have €50,000 on hand plus a variable amount of indemnity insurance[4] This significantly lowers the barrier for new businesses to enter the financial services market, thereby increasing competition, while simultaneously increasing costs and risks for banks to operate. Banks will need to modernize their IT infrastructure and to look to new business models to maintain and grow revenue.

New FinTech companies have formed and will continue to startup to meet these new opportunities. Even established businesses will become AISPs and PISPs. Banks and payment clearing houses may face competition from brick-and-mortar retailers, e-commerce vendors, telecommunications providers, mobile network operators, online gaming sites, and social media sites.

Designed for consumers, PSD2 increases competition in the financial market

The directive, when implemented, will allow consumers more freedom to choose how to handle their financial business.

[4] https://www.eba.europa.eu/documents/10180/1901998/Final+Guidelines+on+PII+under+PSD2+%28EBA-GL-2017-08%29.pdf/6411f24d-e430-4e05-ab03-1393a3f865cb

4 Technical capabilities for PSD2 RTS architecture

Complying with PSD2's regulatory technical specifications almost certainly means building new capabilities, functions, and features. Correspondingly, banks and TPPs should begin designing their PSD2 solution architecture.

Banks have the most work to do to prepare for PSD2. They must provide the ability to strongly authenticate customers, employ user behavioral analysis for "continuous authentication", stand up and secure APIs for TPPs, and put Consumer Identity and Access Management (CIAM) solutions in place. TPPs also need to ready their infrastructure, but which capabilities they need to deploy depends on the role(s) they will play.

4.1 SCA and Transaction Risk Analysis

Many CIAM and IAM solutions on the market today support the concept of SCA. Companies that have to comply with PSD2's SCA provisions must decide whether their current IAM solutions:

- Support the types of strong authenticators customers want to use
- Perform transactional risk analysis
- Allow definition of and evaluation of risk-based policies for transactional authorization

Neither passwords nor Knowledge-Based Authentication (KBA) alone constitute SCA. Banks and other financial institutions are already offering mobile apps. The mobile channel will become even more widely used as an authentication mechanism.

PSD2 states that banks and/or TPPs can obviate the need to elicit an SCA event for every transaction if transactional risk analysis is performed instead. Risk adaptive authentication is a technical solution that collects user and device data over time and uses pattern-matching techniques to discern consistencies and inconsistencies in current user requests compared to historical data. These factors are then examined at runtime in accordance with policies pre-determined by administrators. If the risk level in a particular transaction is found to be greater than allowed by policy, the adaptive authentication solution can require additional actions, such as collecting more information, or triggering "step-up" authentication. Alternatively, if the transaction risk cannot be mitigated by additional actions, the transaction itself can be denied.

Risk factors that can typically be evaluated include:

- Geo-location
- Geo-velocity
- IP address
- Time of day/week
- Device ID/ fingerprint
- Device health assessment
- Known compromised IP/network check

- User attributes
- User history
- User on new device check
- Jailbroken mobile device check
- Known compromised credential check
- Fraud indicator check
- Transaction type
- Transaction amount

Banks and TPPs need the ability to define granular policies that allow administrators to set thresholds for the risk factors listed above.

4.2 CIAM

In order to offer SCA, a proper Identity and Access Management (IAM) solution is needed. Traditional IAM systems are designed to provision, authenticate, authorize, and store information about employee users. They are generally deployed in an inward-facing way to serve a single enterprise. Enterprises often have LDAP directories and/or Microsoft Active Directory (AD) that contain user information. Other options include using Identity-as-a-Service (IDaaS) providers. Traditional IAM scales in well-defined environments of up to hundreds of thousands of users.

Consumer IAM systems are designed to provision, authenticate, authorize, collect and store information about consumers from across many domains. Unlike regular IAM systems though, information about these consumers may arrive from many unauthoritative sources. CIAM systems generally feature password-based authentication, but also support social logins and mobile authentication methods. In PSD2 use cases, information collected about Payment Service Users (PSUs) can be used for many different purposes, such as authorization for transactions, or to comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) initiatives. Moreover, CIAM systems must be able to manage millions of identities, and process potentially billions of logins and transactions per day.

Banks and other financial institutions have both employee and customer facing IAM solutions in place today. Some use the same systems for both environments, while others use these dedicated CIAM systems. Both these new PISPs and AISPs as well as traditional banks and financial service enterprises will increasingly utilize CIAM technologies for AML and KYC.

CIAM will be a key ingredient for retaining and gaining financial customers in the post-PSD2 world

With a potential for increased competition in the financial services market, CIAM, employed for the purposes of increasing brand loyalty among and marketing additional financial services to consumers, will likely become an important differentiator and competitive advantage for those businesses which implement CIAM.

5 What you need from IAM systems for PSD2

In chapter 4 we see that, at a high level, banks and financial institutions need CIAM solutions with risk adaptive authentication mechanisms to achieve PSD2 compliance. Most CIAM solutions today possess a common set of features including account management, user dashboards, basic authentication options, user history retention, and the ability to white-label their registration and login pages for seamless branding. The most capable CIAM solutions offer these features plus risk adaptive authentication options, integration and processing of multiple forms of fraud and threat intelligence, fine-grained consent management for GDPR compliance, and identity and marketing analytics. At KuppingerCole, we believe that there are certain functionalities offered by CIAM solution providers that banks and other financial service providers should begin to deploy in anticipation of PSD2.

Core CIAM functions for PSD2:

- **Secure user account management**: including MFA and Privileged Account Management (PAM) requirements for CIAM system administration, auditing, and integration with SIEMs and threat intelligence services.
- **Consent management**: GDPR mandates that in order to use and store data about users, users must give clear, unambiguous, and explicit consent for each purpose. CIAM solutions provide facilities for collecting, storing, and allowing users to review and edit consents.
- **KYC and AML:** some CIAM solutions are positioned to serve the financial sector, and as such, they are designed to collect and analyze KYC and AML data on users for compliance with these types of regulations in various geographies.
- **MFA:** multi-factor authentication options will enable banks and FinTechs to meet and exceed PSD2 SCA requirements. Mobile apps and push notifications are preferred. Biometric-based mobile authenticators can assist with SCA and can provide a better user experience, but deployers may encounter operational issues. Token-less authenticators are more popular with financial consumers and are generally lower cost in the long term.
- **Risk analytics:** the purpose of risk analytics in financial use cases is to reduce fraud. Thus, of the risk factors listed above, the following are the most important to include in authentication policies for PSD2: transaction types and amounts, geo-velocity, IP ranges known to be sources of fraud (ranges change very frequently), device fingerprints, and user history. A runtime examination of the union of device history and user transaction history can show whether a current transaction request is likely to be valid. Administrators need to be able to write policies to programmatically test for questions such as “does the transaction request fit within historical patterns for this user?”, “is this a normal location from which this user would initiate a transaction?”, or “has impossible travel occurred between requests?”.

6 ForgeRock Identity Platform as a foundation for PSD2 compliant architectures

ForgeRock Identity Platform can provide CIAM, SCA, and risk-adaptive multi-factor authentication functionality that directly address the technical requirements of PSD2.

ForgeRock is a leading, venture-backed IAM vendor, headquartered in the US but with many offices around the world. ForgeRock supports most of the latest identity management and federation standards. In fact, ForgeRock is a significant contributor to several international standards organizations, such as Open ID Foundation, Open Identity Exchange, OASIS, etc. ForgeRock was selected by the UK Open Banking Implementation Entity (OBIE) to provide a Reference Bank Application to be used by leading banks and third-parties to build their own applications in accordance with Open Banking standards. In doing so, ForgeRock has helped fine-tune the UK Open Banking standards and security conformance test suite.
ForgeRock Identity Platform is a developer and administrator friendly product. The Common Services module provides a single format UI for administrators to control all functions of the ForgeRock Identity Platform. For consumer IAM applications, administrators can enable self-service registration, social logins, OIDC and OAuth2 SSO support. Customer administrators can create authentication policies and choose from a wide variety of MFA options for their consumers. Developers can extend the core functionality of ForgeRock Identity Platform through its RESTful APIs and script with Groovy or JavaScript.

ForgeRock solutions are designed for on-premises deployment or deployment within IaaS providers. ForgeRock Identity Platform runs on RHEL/Centos, SuSE, Ubuntu, Solaris x64 and Sparc, and Window Servers. It can run in Apache Tomcat, JBoss Application Server, JBoss Enterprise Application Platform, IBM WebSphere, Oracle WebLogic Server, and WildFly AS. It can read and store user information in ForgeRock Directory Services, IBM Tivoli, Microsoft Active Directory, Oracle Unified Directory, or Oracle Directory Server Enterprise Edition.

The following sections will describe how ForgeRock components address the major technical requirements of PSD2: Strong Customer Authentication and Transactional Risk Analysis in the context of Consumer Identity and Access Management solutions.

6.1 ForgeRock Intelligent Authentication for SCA and transactional risk analysis

ForgeRock Access Management, as a component of the ForgeRock Identity Platform, performs the authentication and authorization functions. It supports many standard federation protocols, such as FIDO, SAML, XACML, OAuth2 and OpenID Connect; therefore, it can interoperate with and achieve SSO between different domains which may use different vendor products.

It also offers many authentication mechanisms, including:

Device Fingerprinting	MSISDN (mobile phone number – SIM card mapping)
Email/SMS OTP	OATH
FIDO 2.0	Open ID, Open ID Connect
LDAP	Social Login via Facebook, Google, LinkedIn, etc.
Mobile biometrics - iOS and Samsung native apps	Username/Password, HTTP Basic authentication
Mobile Connect	X.509 Certificate
Mobile "swipe" apps	Yubikeys

Third-party authenticators, specifically including other types of biometric authenticators, can be integrated as well. Though not certified yet, ForgeRock supports FIDO 2.0 WebAuthn and CTAP, which allows the use of popular and innovative authentication mechanisms such as Google Titan, Yubico Yubikeys, Microsoft Windows Hello, and Apple TouchID.

Authenticators can be chained together via customizable policies. The latest version features an intuitive, flow-chart-based policy authoring tool called Intelligent Authentication. Authentication Trees allow customer administrators to easily create policies in the GUI that meet the levels of assurance needed for sophisticated use cases. The details of designing complex, risk-adaptive authentication and authorization rules are abstracted by the interface.

Advanced risk engines capable of processing real-time fraud and threat intelligence will be essential for reducing risk under PSD2

ForgeRock Access Management provides adaptive risk capabilities that are needed for transactional risk analysis under PSD2. The risk engine evaluates factors such as account idle time, device fingerprints, geo-location, time of day, time zone, and user and device history. The risk engine can then require step-up authentication, if the request context fails to meet the conditions set in policies. These data sources could include other risk engines, geo-location trackers, trusted device databases (e.g., IMEI device theft tracking for mobile devices), as well as simple transaction engines. For example, ForgeRock Access Management can be configured to query and process input from Equifax, Experian, FireEye Threat Analytics Platform, Guardian Analytics, LexisNexis, and others.

6.2 ForgeRock IDM for CIAM

ForgeRock's Identity Management module provides a rich set of features for CIAM. Users can self-register and manage their accounts, including consent, via the user dashboard. Registration can be expedited by using social network credentials. If provisioning from existing systems, LDAP and SCIM are supported. ForgeRock has several advanced directory synchronization options, including on-demand and scheduled syncs, rollback, reconciliation, change detection and propagation, and LiveSync.

ForgeRock's Identity Platform has built in functionality regarding the identity of things. For PSD2 use cases, their focus on mobile and the ability to strongly associate users to devices such as mobile phones forms a good basis for a second factor in strong customer authentication.

7 Recommendations

PSD2 is fast approaching, and the RTS will require major technology insertions for many banks and TPPs. IAM/CIAM infrastructure may need to be upgraded, authentication services must be expanded to provide strong authenticators, and APIs be exposed and secured.

KuppingerCole recommends beginning your PSD2 journey with a readiness assessment. If your organization is in the financial sector in the EU, now is the time to understand and prepare for meeting the technical requirements for doing business after PSD2.

PSD2 will be a major step forward in payment security and processing. The early work accomplished by the UK in their Open Banking initiative is setting the stage for not only PSD2, but also other payment modernization and financial transformation activities worldwide. For example, Australia is moving toward an API-based payment service model. Other industries, such as telecommunications and insurance, are investigating the possibility of utilizing secured APIs for transactions.

7.1 Recommendations for conducting a PSD2 Readiness Assessment

- Inventory existing IAM and risk management infrastructure: Can it offer strong customer authentication? Does it have sufficiently advanced risk analysis and adaptive authentication functions? Can the risk management solution handle the increased complexity and volume of traffic that will arrive with PSD2? Document functional and architectural gaps.
- Engage neutral, third-party expertise to perform the readiness assessment if your staff lacks the time or experience to effectively evaluate your environment against PSD2 RTS, or for an objective view.

7.2 Recommendations for meeting PSD2's SCA Requirements

- Utilize risk adaptive authentication for transactions that fall under the purview of SCA. Use ongoing transactional risk analysis to reduce the need for customers to re-authenticate.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstrasse 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com