White Paper

The Impact of Payment Services Directive II (PSD2) on Authentication & Security

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

RSA

First Edition June 2016

Published by:
Goode Intelligence

Sponsored by:
RSA

www.goodeintelligence.com
info@goodeintelligence.com

CONTENTS

This white paper from Goode Intelligence (GI) explores the implications of the European Commission's Payment Services Directive II (PSD2) for authentication and security.

WHAT IS PAYMENT SERVICES DIRECTIVE II?

Overview

The European Commission's (EC) Payment Services Directive II (PSD2) replaces the existing PSD, first introduced in 2007, and aims to standardize and modernize how payments work across the European Union (EU).

PSD was developed to create a legally binding single payment services market that EU member states could regulate. PSD2 builds on the first directive and is also a direct reaction to a wave of innovative technology-led payment services. It now means that previously unregulated third party payment service providers (TPPs) can be regulated as they will now fall under PSD2.

PSD2 focuses on consumer protection, developing a framework that "nurtures competition, innovation and security"[1] across the EU.

The main objectives of PSD2 are to:

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

The European Parliament adopted PSD2 in October 2015 and EU member states have two years in which to implement the new procedures. The EC states that there is a different date of application for the new security measures, including *Strong Customer Authentication*

[1] Directive on Payment Services (PSD2), European Commission:
http://ec.europa.eu/finance/payments/framework/index_en.htm

(SCA) and standards for secure communication. This is subject to the adoption of the regulatory technical standards which are being developed by the European Banking Authority (EBA) and adopted by the EC. It is anticipated that the new security measures shall apply 18 months after the adoption of the standards by the EC.

[Breakout Box: EBA Framework for Strong Customer Authentication. The EBA's guidelines were published in December 2014 to provide a "solid legal basis" for the security of internet payments within the EU and PSPs operating in the EU. The EBA security guidelines provide PSPs with a minimum set of guidelines to ensure they have a secure framework to protect internet payments against fraud and pre-empted the security requirements found in PSD2.]

Payment Security and Strong Customer Authentication (SCA)

PSD2 provides rules for payment security and customer authentication, concentrating on protecting consumers when paying on the internet.

For payment security, the directive states that "all payment service providers, including banks, payment institutions or third party providers (TPPs), will need to prove that they have certain security measures in place ensuring safe and secure payments. The payment service provider will have to carry out an assessment of the operational and security risks at stake and the measures taken on a yearly basis."

PSD2 also acknowledges the need for authentication mechanisms to match the context of the payment transaction. Specifically, Article 98.3 specifies exemptions for strong customer authentication in certain scenarios including:

- Low value payments
- Outgoing payments to trusted beneficiaries
- Low-risk transactions based on a transaction risk analysis

What is Strong Customer Authentication (SCA)?

Under PSD2, PSPs will be obliged to apply Strong Customer Authentication (SCA) when a payer initiates an electronic payment transaction. The EC defines SCA as a process that "validates the identity of the user of a payment service or of the payment transaction".

SCA is based on the use of two or more elements:

1. Knowledge – something only the user knows, e.g. a password or a PIN
2. Possession - something only the user possesses, e.g. a card or an authentication code (One-Time-Password or OTP) generating device
3. Inherence – something the user is, e.g. biometric authenticator such as fingerprint, voice or eye-print

PSD2 states that these elements have to be independent of each, meaning that if one element is breached or compromised then this does not compromise the "reliability" of the others. The design of the authentication solution must also protect the confidentiality of the authentication data or identity credentials.

The security requirements for 'remote' transactions, including online payments, are even stricter and are intended to minimise the risks of mistaken or fraudulent transactions. Remote transactions require a dynamic link to the amount of the transaction and the account of the payee.

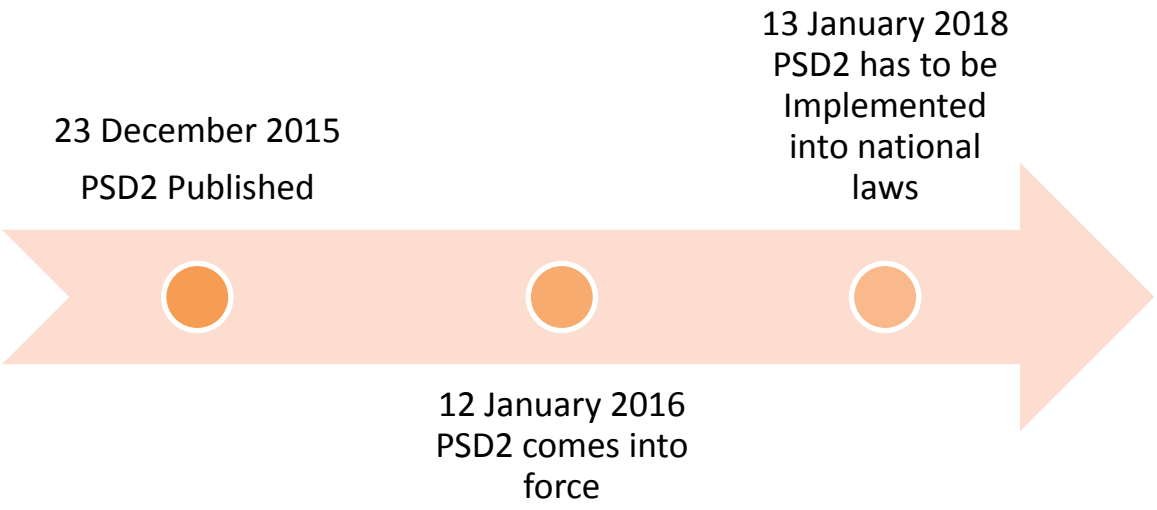
Who is affected

PSD2 applies to all payment service providers (PSPs), including banks, payment institutions or third party providers (TPPs) and relates to all electronic means of payment.

There are exemptions to this rule and the EBA will define what these exemptions are. The EC provides an example of low value payments at the point of sale (POS) to facilitate the use of mobile and contactless payments.

Timelines for Compliance

The new rules will apply in all EU Member States two years after the publication of the directive, which was 23 December 2015. It came into force on 12 January 2016 and Member States will have until 13 January 2018 to implement it into national laws. In the two years from its publications, the PSD rules will be in force.

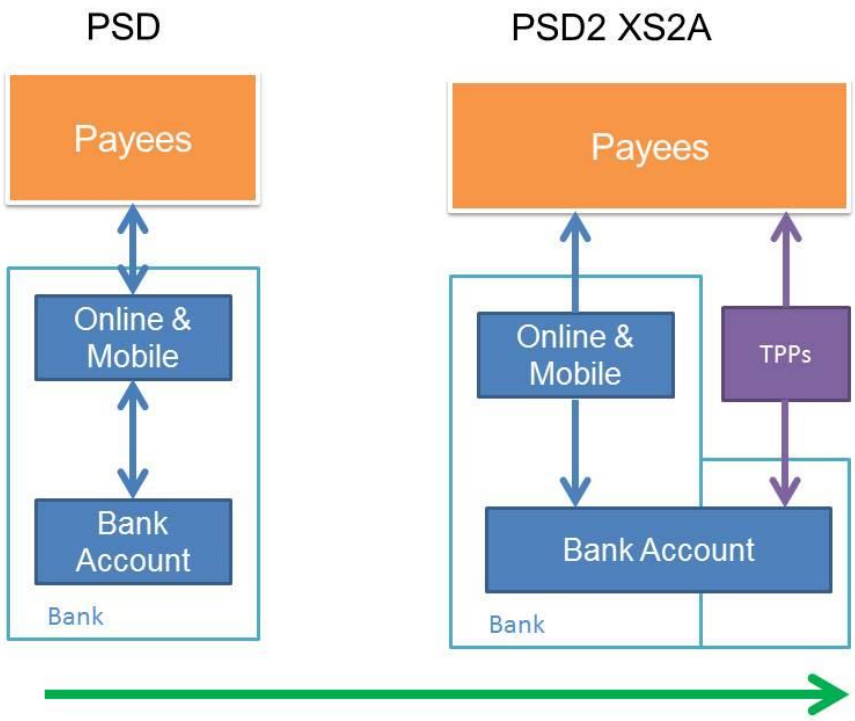


The impact of PSD2 XS2A on Convenient Authentication

The inclusion of TPPs is important to authentication and security, in particular in its ability for customer's to differentiate between services. PSD2 aims to open up the European payments market to new entrants and to also allow third parties 'access to account' via APIs. This is called PSD2 XS2A.

Figure 1 details the changes that PSD2 XS2A will introduce by allowing TPPs access to payment account details within a bank's payment infrastructure via APIs.

Figure 1: The impact of PSD2 XS2A



The APIs would allow customers to perform payment functions from a variety of applications including social media and messaging platforms. This raises questions on how security, including SCA, is managed. Exactly how security and authentication is managed in terms of allowing TPPs to access bank accounts, defined as Account Information Service Providers (AS PSP) in PSD2, has still to be clarified by the EBA. What it does do is make the authentication process incredibly important from a usability perspective. This is because consumers will have more choice when performing payment functions and the decision to use one app over another could well be made on how convenient the authentication mechanism is.

MEETING THE NEEDS OF PSD2 WITH RSA ADAPTIVE AUTHENTICATION

PSD2 requires payments services providers to implement strong customer authentication (SCA) when accessing payment accounts online, initiating electronic payments and through remote channels that have a risk of payment fraud.

SCA is based on the use of the use of two or more elements that include *Knowledge*, *Possession* and *Inherence* and the authentication mechanism must work in a range of payment channels that include web and mobile.

Figure 2: Payment Workflow with Adaptive Authentication

Source: RSA

Additionally, transaction details, e.g. payee and transaction amount information, need to be presented to the customer as part of the strong authentication mechanism. This has to be achieved in a manner that supports the "development of user-friendly, accessible and innovative means of payment".

RSA Adaptive Authentication is a risk-based authentication and fraud detection platform that provides advanced protection across both Web and mobile users. The Adaptive Authentication Mobile Module leverages RSA's proven Risk Engine which includes a mobile-optimized risk model that analyzes a variety of risk indicators, including mobile device identifiers, location and behavioral profiles, to identify fraudulent or suspicious activity.

Adaptive Authentication can be used to secure multiple types of payment including web and mobile (browsers, WAP browsers and mobile apps). The Adaptive Authentication Mobile SDK also supports biometrics for step-up authentication including fingerprint and EyeVerify's Eyeprint ID.

These features enable RSA Adaptive Authentication to support the requirements of PSD2, including strong customer authentication, payment transaction signing and intelligent security applied to post-authentication activities.

RSA Adaptive Authentication allows organizations to match the authentication experience to the context of the payment transaction. All transactions are monitored by measuring over 100 risk indicators and assigned a unique risk score. For payments that are considered to be low-risk, strong authentication is completely invisible to the end user, supporting the need for an optimized user experience. Conversely, high-risk payments would be matched against the appropriate authentication mechanism, depending on what an organization chooses. RSA Adaptive Authentication supports numerous means of step-up authentication for both Web and mobile transactions including out-of-band SMS and biometrics via fingerprint and eyeprint.

RSA Adaptive Authentication works in conjunction with other products and services including RSA Web Threat Detection to enhance fraud identification and investigation across a number of financial attacks including fraudulent payments, account takeover, password guessing, and advanced malware. Tight integration with other security tools such as Web Threat Detection enable organizations to meet the tougher security demands of PSD2 allowing them to strengthen security in an integrated joined-up approach

OTHER SECURITY IMPLICATIONS FROM PSD2

It is not only strong customer authentication mechanisms that are a part of PSD2, the directive has a number of other obligations that impact how an organization designs and deploys security solutions.

The EBA will play an ever-more important role in defining security protocols, technical standards and policies going forward. This could include establishing a security certification programme managed by the EBA.

Non-authentication security proposals include:

- The establishment of formal internal security frameworks to assess and report on operational matters including security issues
- Security Incident reporting to both regulators and customers
- Mandatory security assessment reporting to regulators on security measures and their effectiveness

The need for integrated security solutions for PSD2 compliance

The directive requires that security should be integrated and not deployed in isolation to ensure that payment services are “safe and secure”. RSA’s integrated security solutions enable organizations to meet the security requirements of PSD2, including authentication, authorization and other security aspects of the directive. This enables organizations involved in the payment industry to deploy integrated security solutions that protect both the payee and payment services infrastructure. The ability to protect major components of the PSD2 payment ecosystem in a connected way ensures that organizations fully meet the requirements of the PSD2 allowing them to significantly reduce their threat exposure.

The ability to blend external threat intelligence, risk-based authentication, behavioral analytics, and eCommerce fraud detection with both payment transaction monitoring and transaction signing allows payment service providers to concentrate on the business of providing innovative and convenient payment solutions.

SUMMARY

This white paper explored the implications of the European Commission’s Payment Services Directive II (PSD2) for authentication and security.

PSD2 focuses on consumer protection, developing a framework that “nurtures competition, innovation and security” across the EU. The directive creates a legally binding requirement for organizations operating in the EU payments industry to deploy Strong Customer Authentication (SCA). SCA is based on the use of two or more elements:

1. Knowledge – something only the user knows, e.g. a password or a PIN
2. Possession - something only the user possesses, e.g. a card or an authentication code (One-Time-Password or OTP) generating device
3. Inherence – something the user is, e.g. biometric authenticator such as fingerprint, eyeprint or voice recognition

PSD2 also fosters payment innovation and opens up the payment infrastructure to third party providers (TTPs) through ‘access to account’ (XS2A) APIs. Authentication mechanisms that are convenient and work across all payment channels will differentiate these TTPs in what will be a very competitive environment.

RSA Adaptive Authentication is a risk-based authentication and fraud detection platform that provides advanced protection across both Web and mobile users meeting the needs of PSD2 SCA and also ensuring that the business can develop user-friendly, accessible and innovative means of payment.

The directive additionally aims to strengthen security across the entire payment ecosystem and recommends an integrated approach in managing security for the full payment lifecycle from pre-authentication, authentication, transaction initiation and post authentication functions.

RSA's integrated security capabilities allow organizations to blend external threat intelligence, risk based authentication, behavioral analytics, and eCommerce fraud detection with payment transaction monitoring to ensure they comply with all of the security requirements of PSD2.

ABOUT RSA

RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA's award-winning products, organizations effectively detect, investigate, and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud, and cybercrime. For more information, go to www.rsa.com.

ABOUT GOODE INTELLIGENCE

Since being founded by Alan Goode in 2007, Goode Intelligence has built up a strong reputation for providing quality research and consultancy services in mobile security, identity and biometrics.

For more information on this or any other research please visit www.goodeintelligence.com.