Last modification: 15-05-2017 / 04:35 PM GMT+01:00

cloakware®
for payments & banking

by irdeto

White Paper

CLIENT-SIDE SECURITY IN PSD2 RTS: YOUR GUIDE TO COMPLIANCE

Practical lessons on how to correctly implement PSD2 RTS requirements

INTRODUCTION

As disruption continues to fracture the payments & banking landscape, safeguarding sensitive customer data will require financial services providers to extend cyber security beyond the firewall.

On 23 February 2017, the European Banking Authority (EBA) released the final draft of the Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Common and Secure Communication (CSC) under the revised Payment Services Directive 2 (PSD2)[1]. These RTS are key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union.

This paper examines the recent PSD2 RTS mandate for secure internet client-to-server communications and recommends a path to compliance.

[1] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

TABLE OF CONTENTS

THE INTRODUCTION OF OPEN BANKING

The internet and mobile communications have opened up payments and banking to innovative new business models. As a result, unconventional service providers are diving into the market. In fact, some of the biggest names in social media/ technology (Apple, Google, Facebook) now provide convenient online payment services for consumers.

In spite of this, incumbent financial services providers (banks, etc) have retained control over access to sensitive customer data. But this is about to change.

New regulations, such as PSD2 in Europe, are coming into effect around the globe. These regulations are designed to expand customer data access to what PSD2 calls TPPs (third-party providers). While not as highly regulated as banks, TPPs will be able to provide many bank-like functions to consumers, without incurring fees from issuers.

"These guidelines address a number of security concerns, including open APIs"

The new industry dynamics are forcing incumbent financial services providers to open their customer data stores to TPPs. The most feasible way of doing this is to allow TPPs to integrate their web and mobile applications with the provider's back- end systems via Application Programming Interfaces (APIs). The upside to this is that innovation in the financial industry is likely to get an enormous boost. The downside, however, is that sensitive customer data will move out of the provider's control and be exposed to the internet via third-party applications. This exposure will greatly increase the attack surface for hackers.

To mitigate this imminent threat, the European Banking Authority (EBA) has proposed tough new security guidelines as part of the PSD2 Regulatory Technical Standards (RTS). These guidelines address a number of security concerns, including open APIs and internet client-to-server data communications.

To help understand these new security guidelines, let's take a closer look at why internet client data communications are so vulnerable to attack.

THE VULNERABILITIES OF CLIENT-SIDE API COMMUNICATION

APIs enable the communication of data between software components. This communication may occur only between back-end systems (known as server-to-server communication (S2S)), which sit inside the firewall, or between applications that sit on the client side and the server side (known as client-to-server (C2S) or client-side communication).

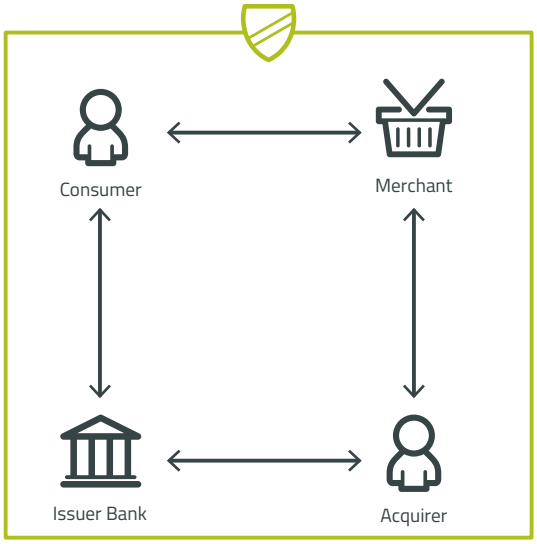

figure 1: The 4-corner model prior to PSD2

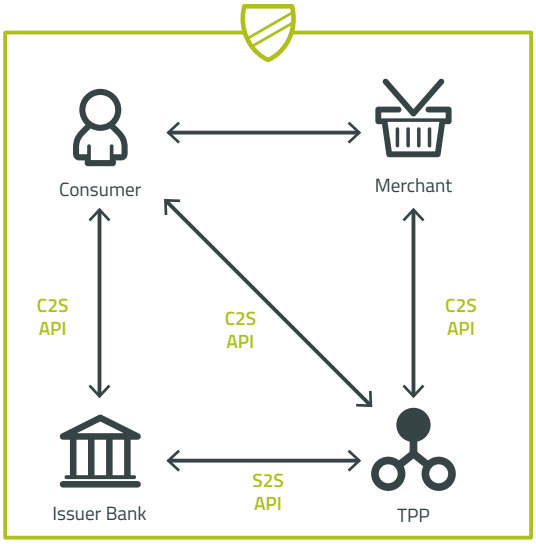

figure 2: The Post-PSD2 landscape

Figure 1 shows the payments & banking landscape before PSD2, known in the industry as the four-corner model. Figure 2 shows the landscape after PSD2, once Third-party Providers (TPPs) entered the arena.

PSD2 allows TPPs to access account information from Account Servicing Payment Service Providers (ASPSPs) on behalf of consumers. In the pre-PSD2 era, ASPSPs were known as Issuer Banks. As you can see in figure 2, API communication between TPPs and ASPSPs goes via a server-to-server connection, typically using what's called 2-way TLS security. However, the other API communication flows are client-to-server, passing data via the client between the TPP or the ASPSP.

Data that passes through a client, to an open API is extremely vulnerable to attack as there is no way to control the client device (mobile or browser). Moreover, unlike server-to-server communication, client-side communication comprises diverse elements (multiple types of browsers, devices, and WiFi

connections, etc.) that can be breached. It is simply too easy for a hacker to use the internet to exploit vulnerabilities in a web or mobile application's JavaScript and take control of the data.

As a result, every time you log-on to your mobile banking application, and with each action you take in the application (e.g. requesting your account balance), and with each payment you initiate (either online or in the app), you are opening yourself up to cyber attack. In this type of attack, known as MitM (man-in-the-middle), a hacker secretly positions himself in the middle of a client-to-server API connection. From there, the hacker can steal data or gain access to the bank's back end systems, inject malware, steal money, or commit all sorts of nefarious acts.

"I've never even heard of MitM, what can I do to prevent it?"

To prevent these types of attacks, the EBA has mandated that TPPs (of all types) and ASPSPs have advanced security technologies in place to protect their client-to-server communications from interception by hackers.

At this point you may be thinking: "I've never even heard of MitM, what can I do to prevent it?"

Currently, the vast majority of your security team's time and resources are spent on perimeter security, protecting everything that runs inside the firewall. To mitigate the threat of MitM, you must implement solutions that will protect the applications and APIs that run outside the firewall.

Fortunately, the EBA understands that MitM is a potentially enormous threat not only to consumers, but to your business and to the market in general. They also know that existing security solutions and standards are not enough to prevent MitM. Consequently, they have put forth a set of tough new security requirements in the PSD2 RTS.

A CLOSER LOOK AT PSD2 MANDATES

One of the purposes of PSD2 is to set forth requirements for "common and secure open standards of communication (CSC) between account servicing payment service providers (ASPSPs), payment initiation service providers (PISPs), account information service providers (AISPs), payers, payees and other payment service providers (PSPs)."

In other words, all internet-based communication between consumers and all types of TPPs (generically called PSPs in PSD2), must be governed by common standards that ensure the security of those communications. In support of this mandate, the PSD2 RTS outlines specific security requirements for every aspect of online consumer/provider communications.

Below is verbiage from the relevant PSD2 RTS articles, along with a description of what they mean in plain language and what PSPs must do to comply with them. Please note that the term payment service providers – as used by EBA – refers to all payment institutions in the ecosystem including TPPs.

Article 4.3c

3. *Payment service providers shall ensure that the authentication by means of generating an authentication code includes each of the following measures:*

    c) *the communication sessions are protected against the capture of authentication data transmitted during the authentication and against manipulation by unauthorised parties in accordance with the requirements in Chapter 5.*

Article 5.2

2. *…payment service providers shall adopt security measures which ensure the confidentiality, authenticity and integrity of each of the following:*

    a) *the amount of the transaction and the payee through all phases of authentication.*
    b) *the information displayed to the payer through all phases of authentication including generation, transmission and use of the authentication code.*

These articles call for the protection of user authentication and transaction-related data that is passed from the client to the provider's server during a transaction. Protection must be from capture and manipulation by a third party (MitM).

Articles 9.2 and 9.3

2. *Where any of the elements of strong customer authentication or the authentication code is used through a multi-purpose device including mobile phones and tablets,payment service providers shall adopt security measures to mitigate the risk resulting from the multi-purpose device being compromised.*

3. *For the purposes of paragraph 2, the mitigating measures shall include each of the following:*

    a) *the use of separated secure execution environments through the software installed inside the multi-purpose device;*
    b) *mechanisms to ensure that the software or device has not been altered by the payer or by a third party or mechanisms to mitigate the consequences of such alteration where this has taken place.*

These articles require that each device and software application involved in a "communication session" has a separate and secure "execution environment" to protect against software or device tampering by a third party during the communication session. But if "alteration" does occur, the security in place must be able to minimize damage.

Articles 16, 17, 18

With PSD2, the EBA hopes to not only ensure compliance, but to reward PSPs for decreasing fraud risk. Articles 16, 17 and 18 describe the conditions under which a PSP can exempt themselves from having to use strong customer authentication for transactions under €500.

From Article 16

1. *Subject to compliance with the requirements laid down in Article 2 and to paragraph 2 of this Article, payment service providers are exempted from the application of strong customer authentication, where the payer initiates a remote electronic payment transaction, identified by the payment service provider as posing a low level of risk according to the transaction monitoring mechanisms referred to in Article 2(1).*

Strong customer authentication requires TPPs to request that users authenticate themselves separately with their bank before initiating a transaction. This adds a level of complexity that will make using a PSPs services less than seamless for consumers.

Per Articles 16, 17 and 18, PSPs can receive the strong authentication exemption if they are able to do the following:

1. *Achieve fraud rates that are under the reference fraud rates, which is much more difficult to do for card-based transactions than for "credit transfers"*
2. *Perform real-time risk assessment on individual transactions based on:*

    a) *Customer behavior patterns*
    b) *Device/browser abnormalities*
    c) *The presence of malware*
    d) *The presence of known fraud scenarios*
    e) *Location abnormalities/risks*

3. *Ensure fraud rates are externally audited and documented*
4. *Make fraud rates available to regulators*

From a security standpoint, achieving the exemption will require:

- A real-time anti-fraud system (batch or near real-time solutions won't comply)
- Browser/device state detection
- Malware detection/prevention
- Guaranteed secure client-to-server communications

Full compliance will require PSPs to implement the following three things:

- a security solution designed to specifically protect web/mobile apps and their APIs,
- a browser/device state detection solution,
- a proper fraud auditing process. This may involve engaging with a firm that specializes in auditing financial services processes.

Article 19

1. *Payment service providers shall ensure the confidentiality and integrity of the personalised security credentials of the payment service user, including authentication codes, during all phases of authentication including display, transmission and storage.*

2. *For the purpose of paragraph 1, payment service providers shall ensure that each of the following requirements is met:*

   a) *personalised security credentials are masked when displayed and not readable in their full extent when input by the payment service user during the authentication;*
   b) *personalised security credentials in data format, as well as cryptographic materials related to the encryption of the personalised security credentials are not stored in Plaintext;*
   c) *secret cryptographic material is protected from unauthorised disclosure.*

Article 19 calls for the protection of all user security credentials as they travel from the client interface over the network through to the provider's server and into storage. It also addresses how this must be done, basically, using strong encryption that can withstand the hostilities of the internet.

Article 22

1. *Payment service providers shall ensure that the delivery of personalised security credentials, authentication devices and software to the payment service user is carried out in a secure manner designed to address the risks related to their unauthorised use due to their loss, theft or copying.*

2. *For the purpose of paragraph 1, payment service providers shall at least apply each of the following measures:*

   a) *effective and secure delivery mechanisms ensuring that the personalised security credentials, authentication devices and software are delivered to the legitimate payment service user associated with the credentials, the authentication devices and the software provided by the payment service provider;*
   b) *mechanisms that allow the payment service provider to verify the authenticity of the authentication software delivered to the payment services user via the internet;*

Article 22 mandates that not only user credentials, but the software/devices used to authenticate the user are securely delivered to the legitimate user via the internet and that the authenticity of the authentication software be guaranteed by the provider. In this case, anti-manipulation and anti-interception of data that is transferred via the internet must be guaranteed.

Article 25.2

2. *Payment service providers shall ensure that the risks against misdirection of communication to unauthorised parties in mobile applications and other payment services users' interfaces offering electronic payment services are effectively mitigated.*

This is a direct call for all electronic payment services delivered via the web and mobile apps to be protected against "misdirection to unauthorized parties," which is another way of saying MitM.

SATISFYING THE EBA / PROTECTING YOUR ASSETS

With its PSD2 security mandates, the EBA is addressing the potentially massive threat of client-to-server data interception, theft and manipulation caused by MitM attacks. They are also tacitly acknowledging that current internet communication protocols, which are based on HTTPS and SSL/TLS, are not enough.

To comply with the EBA's tough new standards, you need to adopt an "outside the firewall" mindset and approach to security. The best way to protect client-to-server communications against MitM is to harden the applications and APIs that run outside your firewall. This requires an encryption standard that is designed to protect JavaScript and data from tampering and interception even as they are exposed to internet traffic.

Irdeto's award-winning[1] Cloakware for API Protection and Secure Apps are the only solutions on the market that guarantee compliance with PSD2's secure client-to-server communication mandate on both web and mobile, for any type of PSP service.

Combining industry-leading whitebox cryptography with other advanced security techniques, Irdeto provides a turnkey solution that prevents MitM attacks on web and mobile applications by hardening the JavaScript and APIs that run outside your firewall.

Irdeto creates a trusted block of code that is hardened and integrated into the application or browser. This protects JavaScript, APIs and data against:

- modification (tampering)
- manipulation (reverse engineering)
- theft (data siphoning at rest)
- man-in-the-middle attacks

Irdeto's industry-leading security solutions are a key element of a PSD2-compliant environment that will enable PSPs to exempt themselves from the strong customer authentication requirement. Exemption will allow PSPs to provide consumers with the convenience of "one-click" payments. This is an important differentiator for your brand in a market that is increasingly saturated with new and innovative financial services.

[1]Irdeto's Cloakware for API Protection and Secure Apps solutions were awarded the Florin Awards for Best Omni-Channel Payment Security solution in the market during the 2017 European Payment Summit in The Hague.