PSD2 Strong Customer Authentication

A guide to PSD2 compliance using Symantec Validation and ID Protection

WHITE PAPER

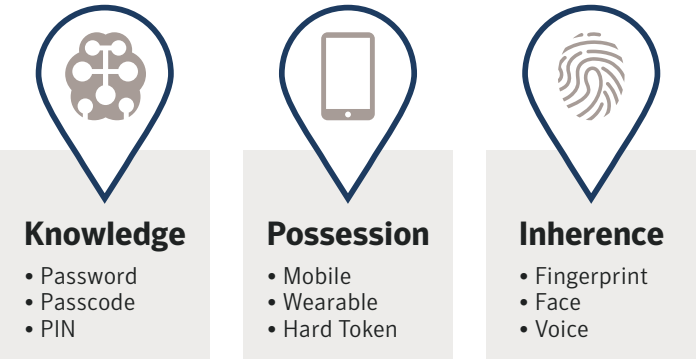
Symantec

PSD2 At a Glance

The revised Payment Services Directive (PSD2) creates a single, integrated European Union (EU) market for payment services by standardizing regulations for financial institutions and payment service providers. PSD2 promotes transparency and fair competition, and removes barriers to creating new payment services.

What's changing?

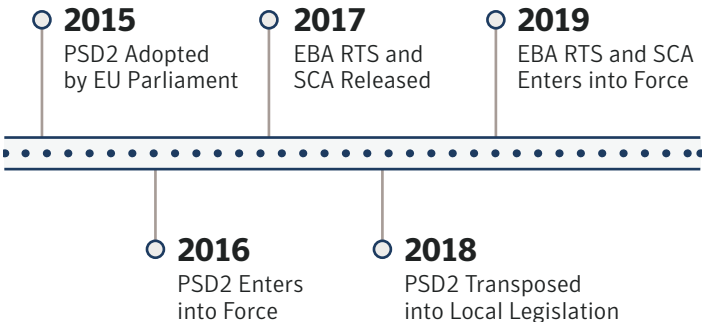
A key PSD2 change is the introduction of Strong Customer Authentication (SCA), designed to improve security and reduce the risk of payments fraud. Drafted by the European Banking Authority (EBA), the SCA Regulatory Technical Standards (RTS) include multifactor authentication (MFA). Specifically, the MFA standard requires that payment service providers verify at least two of the following three identity characteristics: Knowledge, Possession, Inherence. See examples below.



MFA is required whenever customers access their online payment accounts, initiates an online payment transaction, or carries out an action through a remote channel that presents a risk of payment fraud.

Are you ready?

PSD2 directly impacts EU enterprises, and indirectly impacts other regions. Enterprises around the world often adopt foreign compliance requirements; for example, many US companies now align their policies with the EU's General Data Protection Regulation requirements. What steps are you taking to prepare for SCA?



Symantec Validation & ID Protection

Symantec Validation and ID Protection is a cloud-based, multifactor authentication platform powered by the Symantec Global Intelligence Network (the world's largest civilian cyber threat intelligence database). It identifies cyber threats (such as malware), enabling you to make intelligent, risk-based decisions, and ensures your enterprise is in compliance with PSD2 Strong Customer Authentication. You get the utmost in security; your customers get the utmost in convenience.

Meeting SCA Requirements

SCA requirements are quite extensive. There are multiple chapters, each with multiple articles, each with multiple requirements. Here we simply illustrate how Validation and ID Protection aligns nearly completely with SCA article requirements.

Article	Chapter 1, 2, 3, & 4 Requirements	Relevance
1	Subject matter	N/A
2	General authentication requirements	✔
3	Review of security measures	N/A
4	Authentication code	✔
5	Dynamic linking	✔
6	Requirements for the elements categorised as knowledge	N/A
7	Requirements for the elements categorised as possession	✔
8	Requirements of devices and software linked to the elements categorised as inherence	✔
9	Independence of the elements	✔
19	General requirements	✔
20	Creation and transmission of credentials	✔
21	Association with the payment service user	✔
22	Delivery of credentials, authentication devices and software	✔
23	Renewal of personalized security credentials	✔
24	Destruction, deactivation and revocation	✔

Let's delve a bit further into several key SCA articles.

Article 2: **General Authentication Requirements**

Article 5: **Dynamic Linking**

Article 7: **Possession**

Article 8: **Inherence**

Article 9: **Independence of Elements**

Article 24: **Destruction, Deactivation, and Revocation**

Article 2 General Authentication Requirements

Requirement

Payment service providers must ensure that transaction monitoring mechanisms consider risk factors such as compromised credentials, fraud scenarios, signs of malware infection, and more.

Validation and ID Protection

Symantec's Global Intelligence Network provides cyber threat intelligence, including device health (such as malware infection) and configuration (such as jailbroken/rooted), critical for risk-based decision making.

Article 5 Dynamic Linking

Requirement

Payment transaction and payee information must be visible to the payer. During the transaction, the authentication code must be unique to the payment transaction and correspond to the agreed amount when accepted by the payment service provider.

Validation and ID Protection

Authentication codes are unique to the transaction and push notifications are customizable to display payee, transaction amount, and more. Checks the authentication code against the original transaction data to ensure it has not been altered in transit.

Article 7 Possession

Requirement

Payment service providers must mitigate the risk that unauthorized users access SCA elements categorized as Possession; providers must also take steps to prevent the replication of such Possession elements.

Validation and ID Protection

Protects private key material in the authenticator with multiple layers that prevent exporting and replicating the authenticator to another device.

Article 8 Inherence

Requirement

At a minimum, access devices and software must mitigate the risk that unauthorized users are authenticated as payers or able to uncover and misuse Inherence elements.

Validation and ID Protection

Authenticators use the biometric features built into existing mobile platforms to ensure that Inherence elements are provided by proven, secure, and reliable technology.

Article 9 Independence of Elements

Requirement

Elements must be independent to prevent the breach of one element from compromising the reliability of other elements.

Validation and ID Protection

Requires all elements are validated independently for the authentication or transaction to succeed.

Article 24 Destruction, Deactivation, and Revocation

Requirement

Payment service providers must ensure personalized security credentials can be securely destroyed, deactivated, or revoked.

Validation and ID Protection

The payment service provider is able to disable and remove authenticators. Future authentications using such authenticators will fail.

Take the Next Step

With Symantec Validation and ID Protection, you needn't stress about meeting PSD2 requirements for Strong Customer Authentication. Partner with Symantec. We're a global security leader with the expertise, resources, and commitment to protect your enterprise and your customers.

To learn more, visit the **Symantec VIP page**.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com, subscribe to our blogs, or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

20B272470_WP_PSD2_EN