OneSpan

DATASHEET

PSD2 COMPLIANCE

HIGHLIGHTS

Requirements for PSD2 compliance

- Two-factor authentication
- Transaction Monitoring Mechanisms & Transaction Risk Analysis
- Independence of authentication elements
- Dynamic linking
- Replication protection

PSD2 COMPLIANCE

PSD2 changes online payment and banking landscape

In the short term, PSD2 will bring stronger protection for consumers that become victim of payment fraud, thus increasing the confidence of EU citizens in e-commerce, e-banking and other online activities. PSD2 will also cause a shift in liability for fraudulent payments: today merchants are generally responsible for fraud; under PSD2 financial institutions and other payment service providers will be primarily liable.

In the medium term, PSD2 will stimulate innovation in payment instruments. Newly regulated payment service providers will be able to build novel payment instruments by leveraging their right to access the banking accounts of consumers and businesses. Finally PSD2 will strengthen the security requirements for electronic payments, and require strong, multi-factor authentication.

What are the strong authentication requirements for PSD2 compliance?

One of the key elements of PSD2 consists of the need to perform strong authentication of users of electronic payment services. There are specific criteria that must be fulfilled to achieve compliancy. We can discern five key elements in the PSD2 regulation:

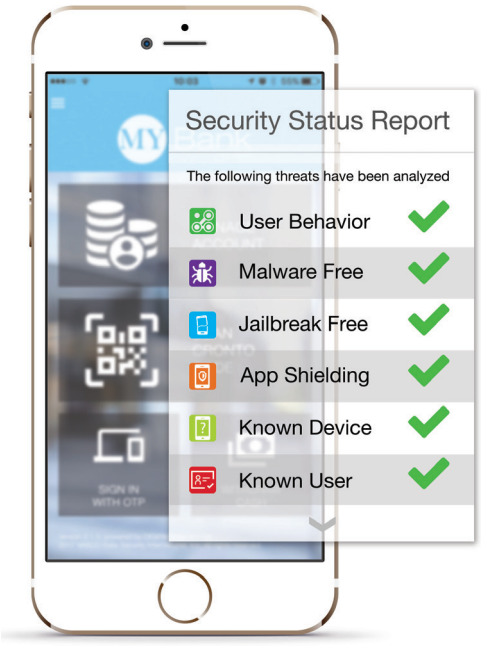
- Two-factor authentication
- Transaction Monitoring Mechanisms & Transaction Risk Analysis
- Independence of authentication elements
- Dynamic linking
- Replication protection

Two-factor authentication

Authentication must be based on a combination of at least 2 elements: a possession element (i.e. something only the user has, such as a token), a knowledge element (i.e. something only the users knows, such as a password) or an inherence element (i.e. such as a fingerprint or face scan). Furthermore, the authentication factors must be independent from each other.

Transaction monitoring mechanisms & transaction risk analysis

PSD2 mandates the usage of transaction monitoring mechanisms to prevent, detect and block fraudulent payments. Transaction risk analysis should be based on elements such as the amount of the payment, known fraud scenarios, signs of malware infection in the payment session etc. The regulation foresees that



low-risk payments can be exempted from strong customer authentication. However, this entails that transaction risk analysis should include additional elements such as payment patterns, location of payer and payee, information about the device used to conduct the payment etc.

Replication protection

PSD2 mandates the use of dedicated mobile app cloning countermeasures in applications. Mobile phones in particular are very vulnerable to cloning if they do not contain countermeasures. These countermeasures can include encrypting data used by the app using a cryptographic key stored inside the device's Secure Element, or using a password or PIN to encrypt the data that is used by the app to generate an OTP (one-time password).

Dynamic Linking

In case of a payment transaction, the authentication code must be dynamically linked to the amount and the payee, meaning that this code will change if either the amount or the payee is changed during the transaction. Additionally, payment information needs to be exchanged via a secure channel, and must be clearly shown to the user.

Independence of authentication elements

If the authentication mechanism relies on a multi-purpose device including mobile phone or tablet, payment service providers must adopt additional security measures to mitigate the risk resulting from the multi-purpose device being compromised. This includes the use of separated secure execution environments as well as measures that ensure the software or device has not been altered. Payment Service Providers must also use security controls to detect, prevent and respond to the alteration of mobile apps and devices. RASP technology for mobile apps provides such security controls. It protects the confidentiality and integrity of mobile apps, can detect whether a device is rooted, whether an app runs inside a debugger or emulator, etc.

OneSpan's solution suite for PSD2 compliance

- OneSpan's Multi-factor Authentication Solution – Enables quick compliance through strong, customizable and easy-to-deploy, authentication options including biometrics with next generation behavioral and contextual authentication options
- OneSpan's Secure Channel Technology – Ensures confidentiality, integrity and authenticity of every payment transaction
- OneSpan's Mobile Security Suite with App Shielding – Mitigates malicious attacks on mobile apps and reduces exposure to related fraud
- OneSpan's Secure Provisioning Tools – Dramatically reduces the risks of unauthorized use on authentication platforms
- OneSpan's Fraud Prevention Solution – Enables compliance with strict regulations, satisfying transaction monitoring and risk analysis requirements through real-time detection and accurate risk scoring

OneSpan

OneSpan enables financial institutions and other organizations to succeed by making bold advances in their digital transformation. We do this by establishing trust in people's identities, the devices they use, and the transactions that shape their lives. We believe that this is the foundation of enhanced business enablement and growth. More than 10,000 customers, including over half of the top 100 global banks, rely on OneSpan solutions to protect their most important relationships and business processes. From digital onboarding to fraud mitigation to workflow management, OneSpan's unified, open platform reduces costs, accelerates customer acquisition, and increases customer satisfaction.

CONTACT US
For more information:
info@OneSpan.com
www.OneSpan.com