TECHNICAL BRIEF

Readiness for PSD2 Requirements with Transmit Security

Improving Compliance and UX with Natively Integrated Identity Services and Extended Passkeys Security

Payment Services Directive 2 (PSD2) — the European regulation for electronic payment services — seeks to make payments more secure, reduce fraud, boost innovation and encourage banking services to adapt to new technologies. The two main areas of impact are customer authentication and third-party access to consumer accounts. The regulation enables better service and enhanced innovation by allowing third-party services to access accounts through an application programming interface (API) if customers give consent.

It also mandates stronger requirements for online transactions using multifactor authentication (MFA) with a high level of assurance for devices used as a possession-based authentication factor — requiring even strong authentication methods like passkeys to be fortified with additional layers of security to meet PSD2 standards.

PSD2 impacts all customers in EU member nations

PSD2 applies directly to consumers in all EU member nations. While the primary focus is on EU banks and payment processors, companies whose headquarters are outside the EU may be subject to PSD2 if they have customers or users within EU jurisdiction. As a result, companies based in the US should expect their European business units to comply with PSD2 mandates. And if a US business receives a good portion of web traffic or customers from the EU or is considering expansion into the EU market, they should also strongly consider PDS2 compliance.

As a leader in identity security, Transmit Security is trusted by Citibank, Metrobank, HSBC and other leading financial enterprises to prevent fraud, improve customer experience and simplify regulatory compliance. This paper explains how Transmit Security enables organizations to comply with PSD2 via multiple MFA methods, including added security layers for passkeys, while providing their customers with smooth, end-to-end identity experiences across channels, devices and applications.

Improving Security and Preventing Fraud with Strong Customer Authentication

PSD2 establishes new digital security requirements known as Strong Customer Authentication (SCA). SCA requires the use of at least two authentication factors for bank operations, including payments and access to accounts online or via apps. It also outlines a stricter definition of what counts as an authentication factor.

The use of multifactor authentication increases the security of online banking and digital payments, as a fraudster would need both authentication factors in order to access a user's account. In addition, one authentication factor must be coupled to a unique, one-time code that allows the user initiating the transaction to verify and approve both the payment amount and payee.

Strong Customer Authentication (SCA)

Strong customer authentication security measures have been defined by the Regulatory Technical Standards (RTS) and, as of December 31, 2020, are directly applicable in the Member States of the EU and all European e-commerce transactions.

SCA must be applied in the following scenarios:

- When a customer — individual or corporate — accesses their payment account online (including an aggregated view of their payment accounts)
- When making an electronic payment
- When carrying out any action through a remote channel that could be vulnerable to payment fraud or other abuses

Readiness for Article 2 - Transaction Monitoring

In addition to strong authentication, PSD2 requires the implementation of transaction monitoring capabilities that can be used to prevent the authentication of payments using compromised devices, credentials and other elements.

Transaction monitoring elements required by Article 2 require:

- lists of compromised or stolen authentication elements
- the amount of each payment transaction
- known fraud scenarios in the provision of payment services
- signs of malware infection in any sessions of the authentication procedure

Low-risk transactions that are exempt from SCA must be safeguarded by even more robust monitoring capabilities that take into account anomalies in payments and risk factors such as the payer's usual spending habits, transaction history and location.

Achieving Article 2 compliance in one solution

Transmit Security's robust transaction monitoring capabilities provide transaction monitoring capabilities for both standard transactions, as specified by Article 2, and additional detection of transaction anomalies to meet the requirements for monitoring low-risk transactions.

The solution provides:

Continuous real-time assessments of account compromise for each user based on behavioral anomalies. A history of authentication events, risk and trust signals for each request and real-time actions taken to prevent fraudulent transactions is centrally stored for each user.

Data on the amount, banks, branches and accounts involved in each transaction is continuously tracked to detect activity from known fraud scenarios, as well as transactions attempted using known fraudulent IPs, devices, addresses and other entities.

Malware detection capabilities based on known signatures and indicators of new malware variants, such as manipulation of OS files, changes to runtime configurations, the illegitimate use of device manipulation and rooting tools, abuse of accessibility services and SMS OTP harvesting.

Readiness for Article 4 - Multifactor Authentication Defined

Under SCA, online and card payments must be confirmed using a combination of two independent authentication factors from the categories “knowledge,” “possession” and “inherence.” The written information on a bank card (card number, expiration date and CVV) is no longer a valid factor for authentication.

Article 4 - PSD2 Regulatory Technical Standards

Article 4.1 states that the authentication shall be based on two or more elements, which are categorized as knowledge, possession and inherence, and shall result in the generation of an authentication code.

Article 4.2 adds another layer of security to the authentication specification, outlining that authentication code should not be repeatable, guessable or backward traceable.

Achieving Article 4 compliance in one solution

Transmit Security offers native multifactor authentication services outlined by SCA as well as the ability to orchestrate third-party authentication methods.

- **Knowledge:** PIN code and knowledge-based answers
- **Possession:** device ID, OTP and hardware token, across various channels
- **Inherence:** facial recognition and fingerprint scan

Native support for FIDO2 WebAuthn via the Transmit APIs enable true passwordless authentication by leveraging the biometric platform authenticators on users’ personal devices. As a result, two-factor authentication for possession and inherence is achieved.

Transmit Security keeps track of recent authentication events and knows which authenticators should be available to each user at any given time. The platform performs this without the need to hard-code logic into an application.

Transmit Security’s true passwordless authentication service addresses Article 4.2 by using the auth-code flow as a return value and enabling random challenges. The cryptographic challenge response is not vulnerable to brute-force attacks and utilizes secure communication.

Passkeys compliance with PSD2 multifactor authentication

Passkeys extend FIDO authentication to multiple devices by discovering other devices within the same ecosystem and syncing passkeys across those devices. Because they are not device-bound, additional security layers are needed to ensure that the device can be used as a reliable authentication factor since:

- Passkeys do not give users control over device enrollment; instead, they automatically sync to all of a user's devices over the cloud, which may include lost, stolen or shared devices
- Multiple users' passkeys can be accessed on the same device

To ensure passkeys meet the definition of SCA under PSD2, Transmit Security's out-of-the-box support for passkeys includes added security layers that ensure compliance with PSD2's strict guidance on multifactor authentication.

It accomplishes this through:

Securing passkeys enrollment by evaluating trust in users throughout their entire application journey using machine learning with anomaly detection to calculate a risk score and recommendation on whether to Trust, Allow, Deny or Challenge the request, along with a list of the top reasons for the recommendation.

Securing passkeys authentication by building user profiles over time using a novelty detection approach that analyzes users' behavioral, network, location, device and other data so that our services can tell with a high level of assurance whether a request is being made by the account owner.

Mitigating new device login and recovery risks through strong device fingerprinting that determines whether the recovering device was previously registered and user anomaly detection that determines whether the user is logging in from a previously known origin, preventing login from a lost or stolen device.

Mitigating step-up risks throughout the entire user lifecycle through what is commonly known as continuous adaptive risk and trust assessment (CARTA). This ensures that the full context of previous user actions is aggregated and used to re-assess risk during step-up without losing information about user's past behavior, both historically and throughout sessions.

Readiness for Article 5 - Dynamic Linking

To ensure each transaction is authorized by the payer, SCA requires that all remote Internet and mobile payments are safeguarded by a unique, one-time-use authentication code that dynamically links the transaction to a specific amount and payee.

Elements required by Article 5 include:

- The payer must be aware of the payee and transaction amount prior to authentication.
- The authentication code must be specific to the payment amount and the payee agreed to by the payer when initiating the transaction.
- The connection between transaction details and code must be maintained throughout the process.
- Any change to the amount or the payee shall result in the invalidation of the authentication code generated.

Simplified transaction signing

Transmit Security's Authentication Services include multiple out-of-the-box transaction-signing capabilities that address the requirement for a unique authentication code to dynamically link the transaction to a specific amount and a specific payee.

Customers can utilize one-time passwords (OTPs) for transaction signing. In addition to the OTP itself, this easy-to-use method offers two possession factors of device ID and email account.

A stronger method available within Transmit Security's Authentication Services uses our added security layers for passkeys to establish possession and inherence. This method ties the transaction detail to the challenge that is signed by the private key during the FIDO handshake. Upon validation, the transaction details are provided inside the signed ID token. This offers full coverage of dynamic linking requirements via cryptographic signing throughout the transaction flow, and the FIDO Relying Party (RP) can re-verify the details before accepting the token as valid.

Readiness for Articles 7 and 8 - Device Requirements

To qualify for SCA under PSD2, authentication factors must meet certain requirements to prevent their unauthorized use. Articles 7 and 8 establish the conditions that qualify devices to be used as possession-based authentication factors, as well as the requirements for inherence-based authentication factors that are tied to specific devices, such as biometric platform authenticators.

Measures required by Articles 7 and 8 include:

- Mitigating the risk of possession elements being used by unauthorized persons
- Mechanisms that prevent replication of possession elements
- Ensuring a low probability of device use by an unauthorized person
- Steps to mitigate that devices used in authentication are resistant to unauthorized use

Addressing Articles 7 and 8 with Transmit Security

Readiness is achieved through Transmit Security's state-of-the-art device fingerprinting that meets PSD2 standards for preventing unauthorized use with an industry-leading 99.97% accuracy rate. These capabilities are backed by our AI-based Detection and Response Services for risk, trust, fraud, bots and behavior, which learn individual users' behavior to detect anomalies in usage patterns.

Device fingerprinting further strengthens passkeys compliance with PSD2, as the device identifier achieved by fingerprinting is enabled out-of-the-box and can be used to determine if a device was previously registered and whether the user has previously logged in from the same origin. This mitigates the risk of login from a lost or stolen device and prevents unauthorized users from leveraging lost or stolen devices already enrolled in passkeys to register a fraudulent device on the user's account.

With advanced capabilities that maintain persistent, unique fingerprints that leverage multiple identifiers to dynamically adapt to changes in browsers and devices, Detection and Response ensures that trusted devices meet PSD2 guidelines for a low probability of unauthorized use and are resistant to device spoofing that could replicate end user devices.

In addition, anomaly detection within individual user journeys, network and IP reputation, behavioral biometrics and more provides protection against unauthorized usage in the event that trusted devices are jailbroken, rooted or stolen.

Readiness for Article 9 - Independence of Elements

Article 9 refers to independence of elements and outlines the need to use an isolated environment to process cryptographic signatures for transaction approval. The use of separated secure execution environments is achieved on modern devices via process separation, which isolates the device's operating system from its browser and mobile apps.

Measures required by Article 9 include:

- The use of separated secure execution environments through the software installed inside the multipurpose device
- Mechanisms to ensure that the software or device has not been altered by the payer or by a third party
- Mechanisms to mitigate the consequences of any alterations that have taken place

Addressing Article 9 with Transmit Security

Readiness is achieved by using the FIDO PKI-based challenge response. Unlike traditional password-based authentication, which stores user credentials and shared secrets on the server side, Transmit Security stores each user's authentication keys, PINs and biometrics on their device.

Secrets are never stored in a centralized server, but rather distributed across the end user's devices. This ensures the protection of users' private keys and payment tokens used to approve transactions on mobile and web applications, as well as adherence to the requirements outlined by the RTS.

The use of a trusted execution environment combined with biometric authentication adds further protection against malware attacks, including on jailbroken or rooted mobile devices.

Easily Handle Exemptions to SCA

The RTS defines a few exemptions to SCA:

- For remote payments (online and mobile) of low value (up to €30), except when a cumulative value of €100 is reached, or when 5 payments of up to €30 have been made.
- For contactless card payments up to €50, except when a cumulative value of €150 is reached, or when 5 contactless payments of up to €50 have been made.
- At unattended payment terminals for transport fares and parking fees.
- For online transactions (credit transfer or card-based) made towards a trusted beneficiary (i.e. already identified by the payer).
- For corporate payments, if dedicated payment processes and protocols are used (and if the national competent authority is satisfied with their level of security).
- When the online payment account is consulted, SCA is needed only the first time and every 90 days.
- When the fraud rates observed by the payment service provider are lower than the preset reference fraud rates (as described in an Annex to the RTS).

Powerful risk intelligence and decisioning

SCA exemptions can be easily implemented using Transmit Security's Detection and Response and Orchestration Services.

Detection and Response Services enable easy definition of different profilers to automatically identify the scenarios described in the RTS. For example:

- Calculations of cumulative transaction values across channels and over time
- Profiles of beneficiaries and identification of trusted beneficiariess
- Time passed since the last SCA

Orchestration Services let businesses build customer journeys that incorporate rules and output from profilers into authentication and authorization. For example:

- If the payment value is equal or bigger than €30, then enforce SCA
- If the cumulative value of €100 is reached, then enforce SCA
- If 5 payments of up to €30 have been made, then enforce SCA

In the above example, profilers are marked in blue and actions are marked in red.
Black indicates orchestration logic.

Preparing for PSD3

In order to keep up with a significant increase in the digital payments market and the rapid progression in the digitalization of payments through mobile banking apps and other means, the European Commission has published a set of proposed revisions to PSD2 that are planned to take effect in 2026.

Measures required by PSD3 include:

- The ability to validate the name and IBAN of the payee and report any mismatches to the payer during instant credit transfers.
- Any fraud-related information shared by PSPs to have a clear legal basis for disclosure.
- SCA methods that can be adapted to the needs of all users, rather than dependent upon a specific device or technology.
- Refund rights for victims of APP (authorized push payment) fraud and damages related to mismatches in the payee's name and IBAN.

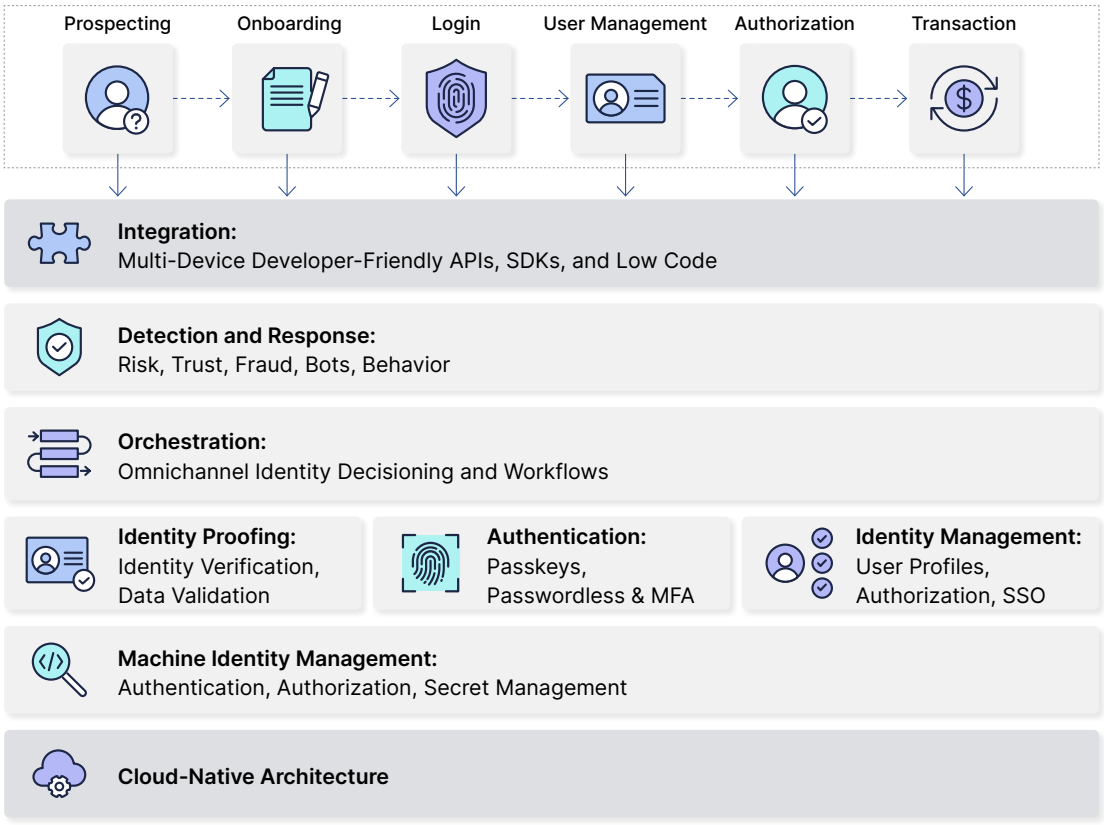
PSD3 readiness with Transmit Security

Transmit Security helps businesses prepare their customer identity security measures for PSD3 by providing:

- Simplified integration with validation software such as IBAN Checker and journey-time orchestration to facilitate real-time name/IBAN checks.
- End-to-end case management capabilities with centralized visibility into the risky behavior taken by each customer at each stage of the user journey, streamlining investigation and reporting of fraud cases. This facilitates the ability to quickly establish and document a legal basis for disclosing fraud-related information for individual cases and quickly assess refund requests for victims.
- APP fraud detection capabilities that leverage both behavioral analysis and increased interaction with the customer via generative AI to detect spoofing attacks and block them in real time — reducing the need to issue refunds in the face of these hard-to-detect attacks.

Holistic Identity Management and Security Controls

The Transmit Security Platform simplifies, accelerates and reduces the cost of customer identity security projects with natively integrated, modular services to fortify security and optimize CX.



Strengthening PSD2 compliance with added passkeys security

By extending FIDO credentials across multiple devices, passkeys weakens their compliance with PSD2 requirements — causing some businesses to opt for MFA methods that use a weaker authentication paradigm.

With Transmit Security's added passkeys security, including multi-method fraud detection and best-in-class device fingerprinting, businesses can reap the security and user experience benefits of passkeys while ensuring compliance with PSD2 and the best possible protection against unauthorized device usage.

Identity Orchestration simplifies PSD2 compliance

Identity Orchestration lets you offload identity logic from your application and create graphically designed workflows for authentication, identity proofing and fraud detection. With it, you can determine which signals to use, how to correlate them, which actions to take and how to seamlessly address regulatory requirements, then instantly deploy journeys without writing code.

Trusted by the most demanding global businesses, Transmit Security orchestrates hundreds of millions of customer interactions every day.