Revised Payment Services Directive (PSD2)

What it is, what it means, and how you can use it to your advantage

ENTRUST

SECURING A WORLD IN MOTION

Table of Contents

ABSTRACT

Make PSD2 work for you

Payment Services Directive 2 (PSD2), the European Commission (EC) and the European Banking Authority's (EBA) newest regulatory directive to ensure customer security in the payments space, is upon us. In order to comply with these new regulations, you first need to ensure you have a good understanding of what they are, why they exist, and how they will affect your organization's business strategy moving forward.

Don't let the potential business impact of PSD2 hang over your head. PSD2 can actually be a catalyst for your digital transformation. With the right solution, you can provide a more secure, better user experience for your customers. If you are able to capitalize on PSD2 and implement a forward-thinking strategy, you can ultimately differentiate your brand from emerging competition like neobanks, fintechs, and wallet providers and retain customer trust and loyalty.

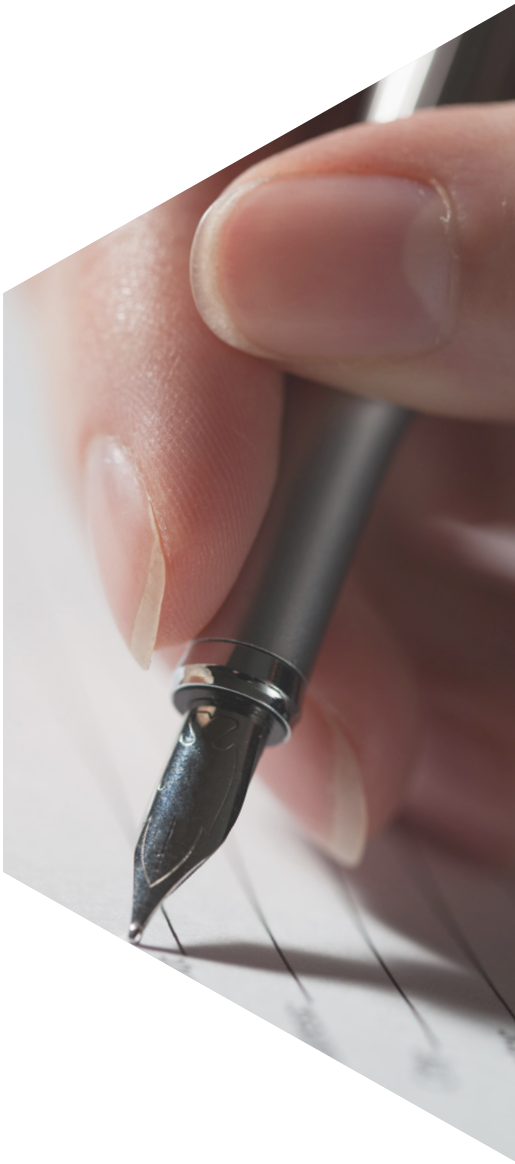
"Companies that are bold — building new products inhouse when possible, partnering when necessary, and even acquiring when feasible — in delivering innovation to the market will be rewarded."

- PSD2 and Fintech: Delivering Innovation

James West, IDC

Revised payment services directive

A general overview



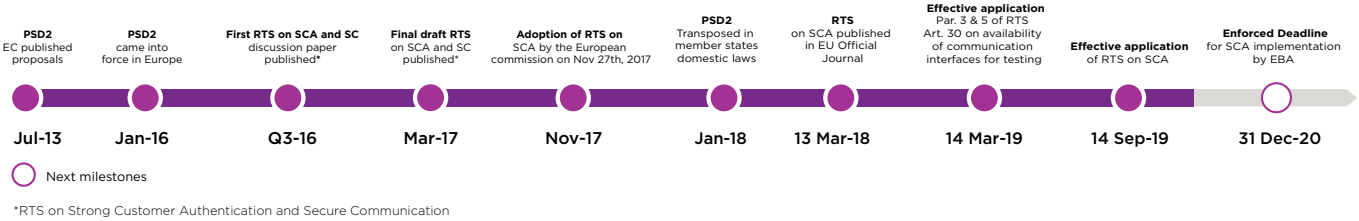
Payment Services Directive (PSD): the foundation for PSD2

In 2007, as a reflection of the growing e-commerce industry, the European Commission (EC), the European Banking Authority (EBA), and their advisory bodies recognized a need to offer consumers a wider choice of payment services by encouraging non-bank financial institutions to enter the market for consumers while enabling faster payments and increasing consumer protections and transparency. This led to the publication of the first Payment Services Directive (PSD).

PSD2 goals and requirements

As the payments space continued to evolve with rapidly increasing mobile and internet payments, the EC reviewed the initial PSD and acknowledged that it required critical improvements and clarifications to keep pace and ensure customer security. As a result, PSD2 came into effect on January 13, 2018. Similar to PSD, PSD2 is a significant step forward in payment industry regulations. Beyond renewed support for the existing goals of PSD — promoting increased competition and cost-effective choices for the consumer by opening up the payment market to new entrants — PSD2 aims to:

- Better protect consumer financial data with stricter security requirements such as stronger authentication
- Require banks to provide open communication interfaces (APIs) that allow access to third-party providers (TPPs)
- Enact specific rules for access to customer accounts
- Make the conditions and information requirements for payment services more transparent
- Redefine user and provider rights and obligations for payment services
- Clarify the criteria and scope of exemptions

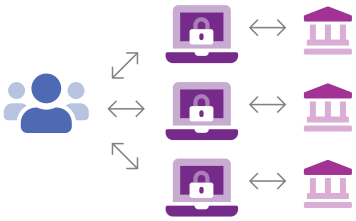


*RTS on Strong Customer Authentication and Secure Communication

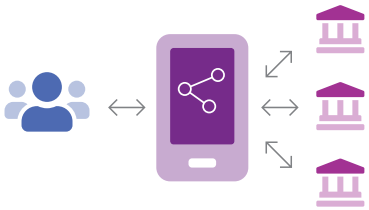
PSD2 role and responsibility definitions

While PSD encouraged new market competition, it did not take into account rules and regulations for new payment service providers such as Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs). PSD2 more clearly defines roles and responsibilities.

Before PSD2



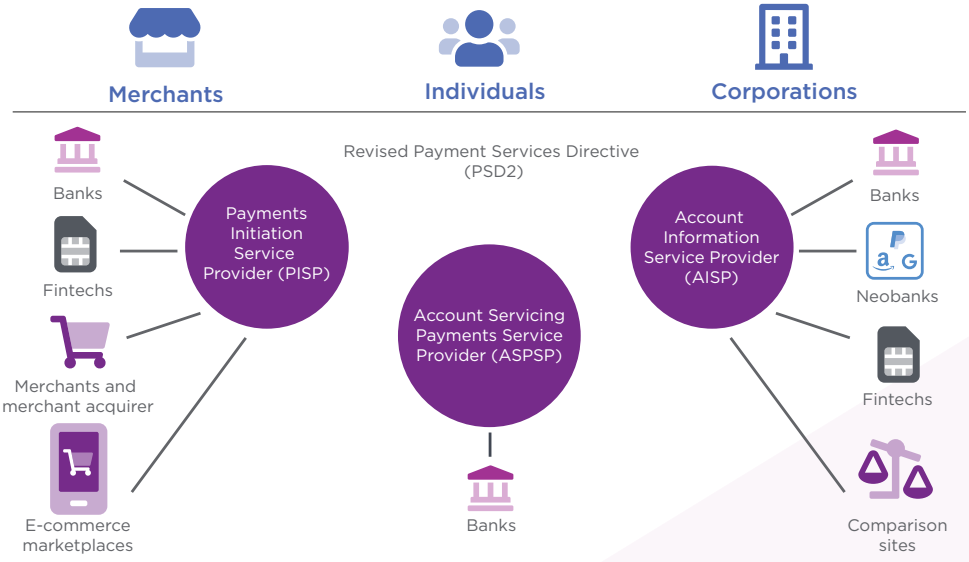
After PSD2



PSD2 PAYMENT SERVICES PROVIDER ROLES AND RESPONSIBILITIES

Financial Institution Type	Description	Example
Payment Service Provider (PSP)	Catchall term for payment service providers without specifications on services	Banks, wallet providers
Account Servicing Payment Service Provider (ASPSP)	Payment service provider that offers payment accounts (current accounts, credit cards) with online access	Banks, neobanks
Account Information Service Provider (AISP)	A third-party provider that acts as an account aggregator for a consumer or payment service user (PSU) who has one or more accounts. They provide consolidated information, helping consumers to better track and analyze their financial accounts data. AISPs must have user consent before accessing an account.	Banks, neobanks, fintech providers, comparison sites
Payment Initiation Service Provider (PISP)	A third-party provider that initiates payments on behalf of the consumer (PSU) with respect to a payment account held by another PSP or ASPSP. PISPs must have consumer consent prior to initiating the payment.	Banks, neobanks, merchants & merchant acquirers, e-commerce, fintech providers

Because of the emergence of new players, entrants beyond traditional banks — including fintechs, wallet providers, neobanks, e-commerce marketplace players, and comparison sites — now factor into a more complex ecosystem, creating more choices for customers and increased competition for banks.



Regulatory Technical Standards

A general overview

On the 27th of November, 2017, the EC also adopted the long awaited Regulatory Technical Standards (RTS), which specify requirements and exemptions for strong customer authentication (SCA) and common and secure communication between banks and TPPs. The RTS were scrutinized for three months by European Parliament and Council before they were published to the EU Official Journal on March 13, 2018. The RTS on SCA came into effect September 14, 2019. However, as per paragraphs three and five of Article 30, the open communication interfaces (APIs) became available for testing purposes by March 14, 2019.

The RTS provide additional guidance on SCA and common and secure communication in line with PSD2 guidelines that both traditional and new third-party payment service providers will be required to abide by.

Secure communication (access to account — XS2A)

Secure communication focuses on communication exchanges between AISPs, PISPs, PSPs that issue card-based payment instruments, and ASPSPs. RTS specify that any of these that offer a payer a payment account accessible online must meet the following requirements:

- AISPSs, PISPs, and PSPs that issue card-based payment instruments must identify themselves to the ASPSPs
- AISPs must communicate securely to request/receive information on designated payments accounts and associated payments transactions
- PISPs must communicate securely to initiate a payment order from the payer's payment account and receive all information on the initiation and execution of the payment transaction
- Communication between ASPSPs, PISPs, AISPs, payers, payees, and other PSPs must be identified by a certificate issued by an eIDAS-qualified trust service provider

ASPSPs are also required to offer TPPs at least one interface to access customer data. Most of the industry is preparing to move toward dedicated interfaces by using open APIs because screen scraping, also known as named direct access, will no longer be allowed as of the RTS implementation date. The EBA wants to maintain technical neutrality, so it does not mandate the use of a specific API. Banks can choose between standardized APIs such as Open Banking UK, STET, or the Berlin Group, or they can develop their own in collaboration with other local and regional initiatives.

Verification requirements

PSD2 Qualified Website Authentication Certificates (QWACs) require the applicant to provide the following information before a certificate can be issued:

1. Authorization Number of the third-party payment provider (TPP) found in the public registers of the national competent authorities
2. The role(s) of the TPP Issuing the card-based payment instruments, which may be one or more of the following:
    - ASPSP
    - PSIP
    - AISP
3. Name of the competent authorities where the TPP is registered
4. Name of Qualified Trust Service Provider (QTSP)
5. The traditional certificate requirements, which include:
    - Name of certificate owner
    - Organization identity
    - Legal identity of organization controlling the website
    - Domain verification
    - Validity period

Verification requirements

Regulatory requirements for third-party providers to access bank accounts or bank account data
A third-party provider that wants to access customer bank accounts within the EU or their associated data needs to obtain a license and unique PSD identifier from its National Competent Authority (NCA) in the EU member state with regulator authority over the third-party provider. There are different types of licenses that each determine the data access rights or "roles" of the third-party provider in accordance with their business model.

Technical requirements for third-party providers and banks
A third-party provider that wants to gain access to bank accounts, and a bank that is providing third-parties with access to customer account data, must each identify themselves with one or more PSD2 certificates, which are built on the foundation of Qualified Website Authentication Certificates (QWACs). Entrust will offer both types of certificates.

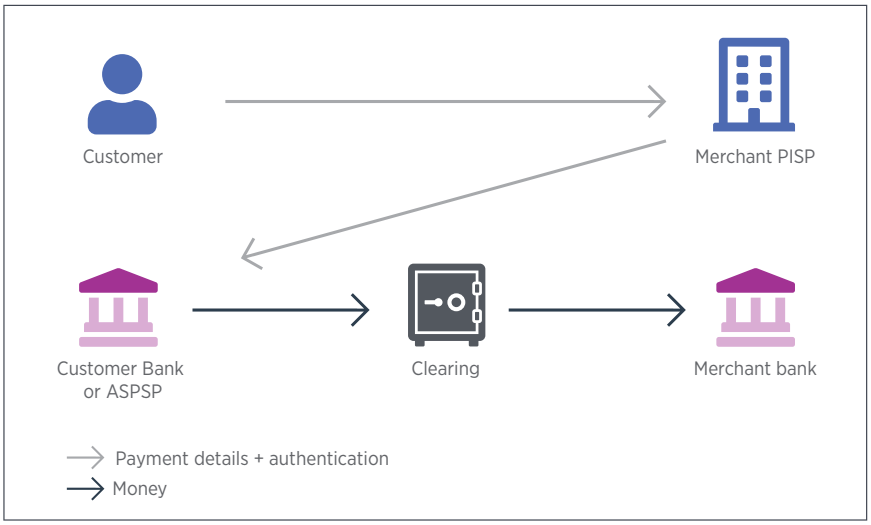
Requirements for banks
Banks must also make an API available to third-party providers that enables access to customer bank accounts or account information. A bank's identity will be confirmed through its own QWAC.

Application process for a PSD2 certificate
Before applying for a PSD2 certificate, a third party must first register as a payment service provider with its National Competent Authority (NCA). After the third party receives its NCA license, Entrust can then complete verification (including all verification required for Extended Validation [EV] certificates) and issue the third party with a PSD2 certificate.

Strong Customer Authentication (SCA)

As fraud methods evolve, PSPs must implement security measures to apply SCA (and its exemptions) and protect the confidentiality and integrity of the consumer's security credentials.

When PSPs apply SCA, in accordance with Article 97(1) of Directive (EU) 2015/2366, the authentication must be based on two or more of the following elements: knowledge (something you know), possession (something you have), and inherence (something you are).



This drawing shows an **embedded model** where SCA is asked by the PISP. Two other models exist — the **redirect model,** in which the PISP redirects the user to ASPSP for SCA, and the **decoupled model,** in which the PISP redirects the user to a registered digital identity provider for SCA.

Dynamic linking

As electronic remote payment transactions are subject to a higher risk of fraud, additional SCA measures are required for online transactions to ensure that SCA elements dynamically link the transaction to an amount and a payee specified by the payer when the transaction is initiated.

Dynamic linking can be achieved via authentication code generation, which is subject to a set of strict security requirements. To remain technologically neutral, a specific technology is not required to implement authentication codes. Therefore, as long as the security requirements are fulfilled, authentication codes can be based on a variety of different solutions, including generating and validating one-time passwords, digital signatures, and other cryptographically underpinned validity assertions that use keys and/or cryptographic material stored in the authentication elements.

SCA exemptions

In order to provide a better user experience — especially for low-value and low-risk payments — a set of exemptions to the principle of SCA were created.

USE CASE	EXEMPTION CRITERIA
Payment account information	Viewing the balance or payment transactions executed in the last 90 days through one or more designated accounts
Contactless transaction at the point of sale	• Under €50 • Cumulative amount doesn't exceed €150 or five consecutive individual payment transactions
Transport and parking fares	Payment transaction initiated at unattended payment terminal for paying a transport or parking fare
Trusted beneficiaries and recurring transactions	When the payer initiates: • A payment where the payee is included in a list of trusted beneficiaries previously confirmed by the payer through their ASPSP • A series of payment transactions with the same amount and payee
Payments to self	When the payer initiates a credit transfer where the payer and payee are the same legal person
Low-value transaction	• When the amount of the remote transaction is less than €30 • When the cumulative previous remote electronic payment transactions initiated by the payer since the last application of SCA does not exceed €100 or five consecutive remote electronic payment transactions

PSPs are also exempt from SCA when transaction risk analysis (TRA) is provided with all the parameters described here:

Transaction Risk Analysis (TRA)

Amount of electronic payment transaction does not exceed the exemption threshold value (ETV) corresponding to the PSP reference fraud rate (%):

Reference Fraud Rate %		
ETV	**Remote card base payment**	**Credit transfers**
EUR 100	0,13	0,015
EUR 250	0,06	0,01
EUR 500	0,01	0,005

An electronic payment transaction is identified as low risk only when the following conditions, in combination with the risk analysis, are met:

- No abnormal spending or behavioral pattern of the payer is identified
- No unusual information about the payer's device/ software access is identified
- No malware infection in any session of the authentication procedure is identified
- No known fraud scenario in the provision of payment services is identified
- The location of the payer is not abnormal
- The location of the payee is not identified as high risk

PSD2 exemptions

To ensure an optimal user experience, there are a number of aspects that appear to not be covered by PSD2, including:

- Cash and paper-based payments
- Payment transactions within a settlement system (clearing house, central banks, settlement agents, etc.)
- Existing corporate accounts that are not online and can't be interrogated in real time
- Payments made through telco operators for the purchase of digital services such as music or digital newspapers, electronic tickets that are downloaded onto a digital device, or donations to charity
- Payments made with fuel cards, anonymous prepaid cards, or closed loop store cards
- Cash withdrawal services provided by independent ATM operators. These providers do, however, have to comply with the basic transparency rules of PSD2 regarding information on withdrawal charges and receipt of cash.
- Cryptocurrency payments

In addition, some areas seem to have been insulated with the expectation of further clarification:

- Absence of explanations on the use of eIDAS certificates and authorities
- Lack of technical standards on open API and SC channels (reference to ISO27001 has been removed)
- Need for better consumer (PSU) education
- Use of authentication codes
- Compliance with GDPR — how to define transaction sensitive data
- SCA compliance process and authorities
- TPPs and ASPSPs registration and audit procedures

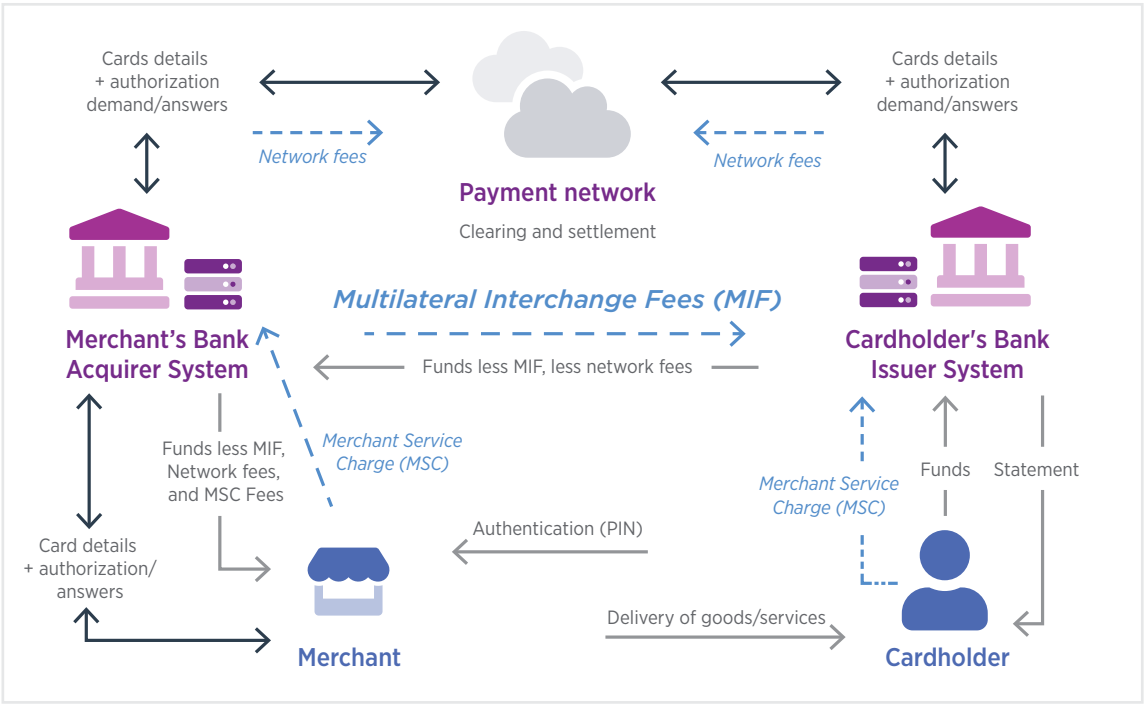
Strategic considerations for banks

As new players emerge and competition increases, strategic planning is key to success. In order to determine the best approach for implementing PSD2, we've gathered a list of potential challenges and considerations for your business:

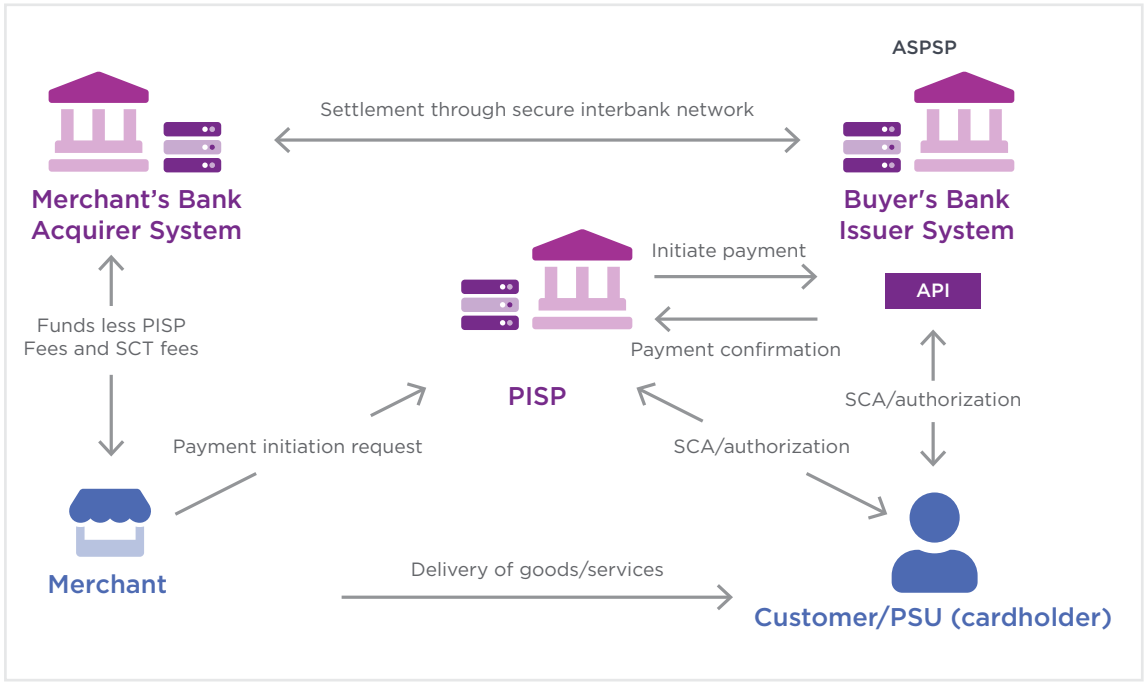
POTENTIAL CHALLENGES WITH PSD2	OPPORTUNITIES FOR BANKS
Will my bank be ready for PSD2 on time?	You have an opportunity to act as an aggregator (AISP) and offer account information services, even providing personal management and financial forecast services.
PSD2 requires mass investment to become compliant. We may have to defer other investments.	You can act as a PISP to: • Propose online payment initiation services from your bank portals • Extend your influence in retail payments
PSD2 seems more like a cost driver than a revenue driver.	You can partner with fintechs to offer a wider range of solutions, becoming a banking platform customers can use as a marketplace
PSD2 encourages such an open market that my bank may be vulnerable to service commoditization or exposed to competitive margination.	If your country has a National Digital Identity program, you can become a digital identity provider.
Will we lose interchange fees from card-based transactions?	You can transform financial services to become a banking as a platform service. You can help customers manage finances, make better purchasing decisions, and cross-sell services as their trusted financial advisor.

As an example, the following two diagrams represent the risk of disintermediation of the traditional card schemes with one of the possible new payment models resulting from PSD2.

Traditional pre-PSD2 payment model



Possible post-PSD2 payment model



How to best prepare for PSD2

PSD2 implementation is mandated for December 31, 2020. You'll want to consider vendors that can help enable PSD2 and provide solutions that will grow with you as your business evolves and future regulations are enacted. We've gathered critical criteria that will help your financial institution expand its reach and use PSD2 as an opportunity to attract and retain customers:

- **A noncompromising approach:** With the rapid growth of digital banking, it is critical to provide users a secure, frictionless user experience. Look for solutions that provide high assurance and low complexity and offer mobile-centric approaches that are transparent to the end user.
- **Innovation:** Organizations need to ensure they exceed customer demands and expectations. With innovative technologies, banks can differentiate their brand while reducing costs.
- **Financial market expertise:** Look for a provider that has proven financial market experience, understands your customers' pain points, and can lean in as your trusted advisor.

"Through 2023, organizations that can instill digital trust will be able to participate in 50% more ecosystems to expand revenue generation opportunities."

— Digital Trust Drives Customer Satisfaction and Business Results, Gartner, 2020

How Entrust solutions can help enable PSD2 and beyond

Entrust can help financial institutions meet PSD2 and other compliance standards while enabling their digital business — setting them apart from the competition. We provide a variety of secure solutions and features, including:

Strong customer authentication — user authentication, adaptive authentication, mobile solutions:

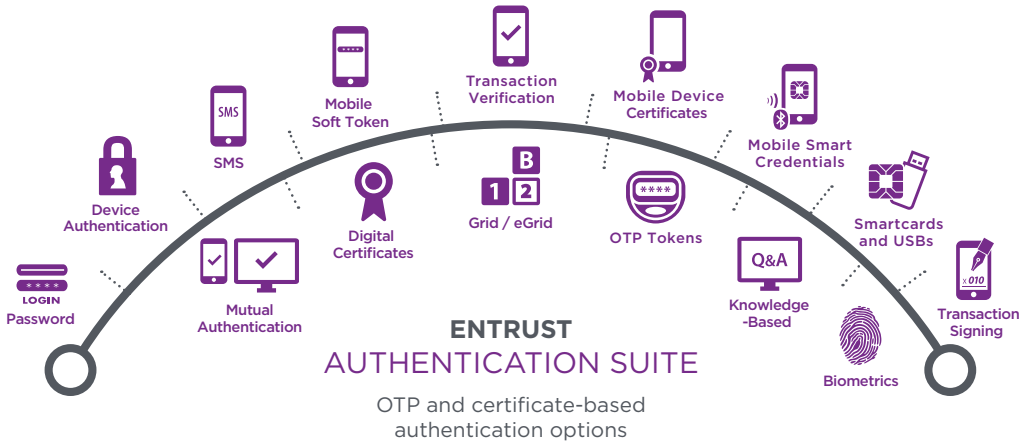
Entrust offers modern SCA solutions to help redefine the user experience and increase security. Our next-gen mobile capabilities and adaptive authentication enable increased security and transparency.

Independent authentication elements: With more than 17 authenticators, Entrust provides flexibility to provision multiple authentication methods depending on the level of assurance required for your users. Our out-of-band solutions such as mobile push authentication and QR code verification help prevent fraud with independent authentication methods.

Dynamic linking: When it comes to making a payment transaction, we ensure your randomly generated OTP code is linked to your transaction data to create a derived confirmation code — a truly unique code that can only be used to sign a specific transaction.

Replication protection: Our mobile apps protect token and smart credential data by encrypting it with a device's unique characteristics. By encrypting the sensitive data, we prevent decryption and protect against device and application cloning.

Runtime Application Self-Protection (RASP): RASP is a suggested protocol for detecting anomalous app behavior and blocking the app from executing any further operations. With our Entrust Identity Enterprise client-side software, the apps or SDKS act only on requests from the server. If a fraudulent entity tries to fool the app into signing a transaction, the transaction verification fails. We solve much of the areas covered by RASP by deferring the book-keeping to the server, which is run in a protected environment.



Entrust provides a comprehensive range of authenticators and adaptive controls to balance user experience with security.

Fraud detection — transaction verification and monitoring, device reputation, digital signatures, SSL

Detecting fraud is essential. Entrust transaction monitoring capabilities provide real-time fraud analysis tools and alert you when risky behavior occurs. Once fraudulent activity is identified, our solution will enable multiple forms of SCA to ensure a secure experience and reduce fraud for your organization. With high-risk transactions, you can check the reputation of your user's device, easily verify transactions and choose appropriate authentication methods, including PKI-based digital signatures such as mobile smart credentials and mobile push capabilities.

Entrust SSL/TLS certificates provide encrypted transactions and identity assurance for your web applications.

Secure open banking APIs and systems with PKI and certificate services

Providing secure, encrypted data transfers is essential to Secure Communication and a key PSD2 requirement. PSD2 QWACs form the highest level of authentication and will be required to secure the open banking APIs used for transferring private data when making a payment or transferring money. They are meant to bring greater transparency, accountability, and authentication to users in the EU marketplace.

Although open banking provides a better user experience for consumers, it opens the door for fraud. The Entrust PKI solution is an effective way to help ensureyour customers' data is secure and confidential. When sharing customer information to TPPs, certificate-based encryption allows transfers to take place over unsecured networks without compromising the security or integrity of customer data. Entrust offers an end-to-end managed PKI service for a European Member State open banking scheme/API provider for their European ISO 27001 & tScheme certified environments.

Consumer information — instant and central card issuance, mobile push notifications

In today's digital age, consumers want immediate insight into their payments and transactions. In order to exceed customer expectations, you need to provide a solution that ensures instant purchasing power while still maintaining transaction history details. Because our solutions span every customer touch point, Entrust enables you to digitally and instantly issue a credit or debit card to new or existing cardholder accounts. As soon as a cardholder starts making purchases, you can notify them of transaction details while requesting verification at the same time with secure mobile push notifications.

CONCLUSION

Summary

PSD2 introduces a lot of new regulations to the European payments space. While implementing these regulations might seem daunting, they offer financial institutions the opportunity to review their existing digital strategies and find new ways to differentiate themselves from the competition. Financial institutions can not only ensure stronger, more secure digital banking, they can also differentiate their brand by providing a better user experience and more solutions and services for their customers. The most successful organizations will partner with vendors who can provide next-generation technologies that help meet PSD2 regulations within a friendly user experience and help future-proof their business.

For more information

888.690.2424
+1 952 933 1223
info@entrust.com

entrust.com

ABOUT ENTRUST CORPORATION

Entrust secures a rapidly changing world by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com