e-book

10 things you need to know about the PSD2

InfoCert
TINEXTA GROUP

infocert.it Infocert.digital

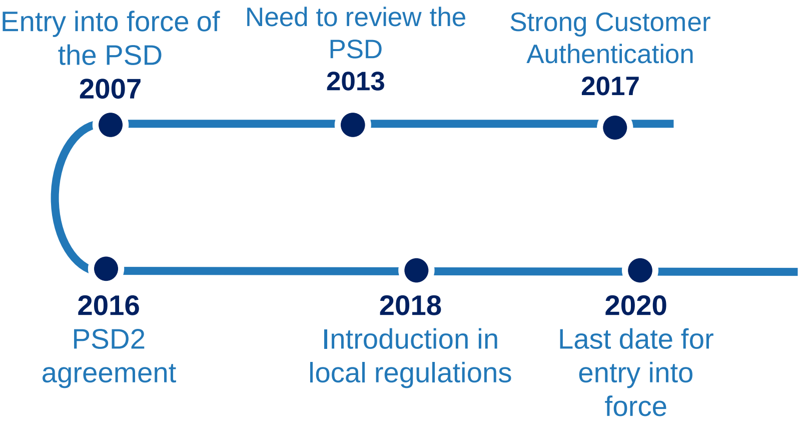
What is the PSD2? 1

The Payment Services Directive (**PSD2**) is the second **European Payment Services Directive** , which came into force in **2016** and was transposed into national law by Member States two years later.

Driven by the growth of digital commerce, the European Commission (EC), the European Banking Authority (EBA) and their advisory bodies recognised the need to revise the structure of the **first European Payment Services Directive (PSD)**, which entered into force in 2007, to further expand the spread of these services within the EU single market and encourage competition among sector players while guaranteeing the **security** and **protection of final consumers**.

In particular, growth and innovation in electronic payment services poses new challenges with regard to payment security and to protecting consumers against the risk of fraud and abuse.

Therefore, these risks must be mitigated if such services are to be fully diffused on the market.



Entry into force of the PSD
2007

Need to review the PSD
2013

Strong Customer Authentication
2017

2016
PSD2 agreement

2018
Introduction in local regulations

2020
Last date for entry into force

What are its objectives? 2

The main purpose of the Second Payment Service Directive (**PSD2**) is to **promote development and innovation in digital payments** within the European Union, while **increasing consumer security** and protection.

OPEN BANKING

Under the PSD2, banks are obliged to guarantee access to their customers' accounts to Third-Party Providers (TPP) authorised to provide Payment Initiation (PISP) or Account Information (AISP) services.

NEW PLAYERS: NEW SERVICES

The PSD2 sets the authorisation and market access rules for Third-Party Providers (TPP) of account access and payment services;

SECURITY REQUIREMENTS

The PSD2 introduces new security requirements to better protect users making online electronic payments (Strong Customer Authentication (SCA)).

CLEAR RULES

New and clearer rules for cases where payment service providers are not required to apply the Directive.

Who it is for? 3

The PSD2 applies to **payment service** providers such as banks, electronic money institutions (EMI), payment institutions, and Third-Party Providers (TPP).
It protects the users of payment services i.e., consumers, micro-enterprises and other parties involved in transactions as beneficiaries and/or payers.

ASPSP — **ACCOUNT SERVICING PAYMENT SERVICE PROVIDER:** A payment services provider provides and administers payment accounts for payers

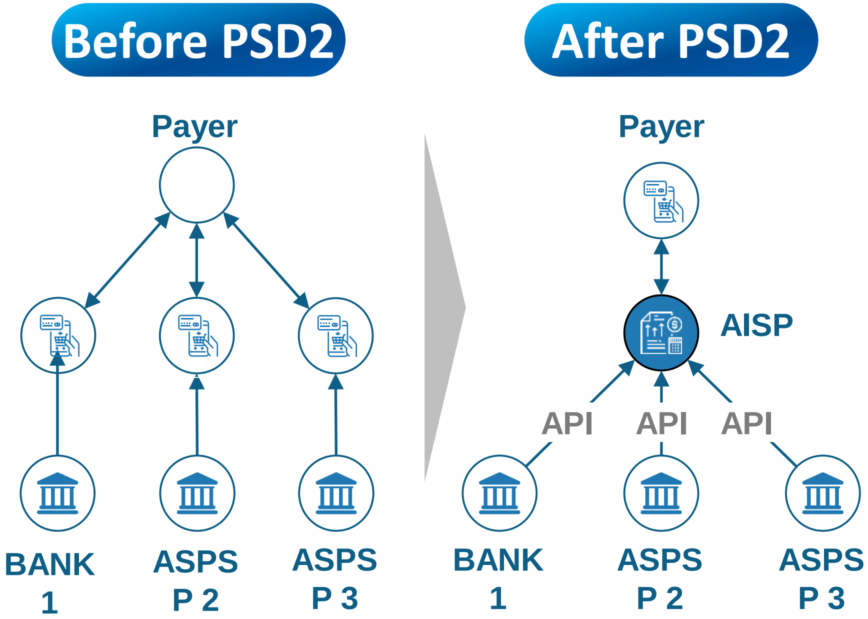
CISP — **CARD ISSUER SERVICE PROVIDER**: A company that issues debit or credit cards linked to a bank account

AISP — **ACCOUNT INFORMATION SERVICE PROVIDER**: provides consolidated information on one or more payment accounts held by users with another or several ASPSPs

PISP — **PAYMENT INITIATION SERVICE PROVIDER**: provides payment order initiation services

NEW SERVICES

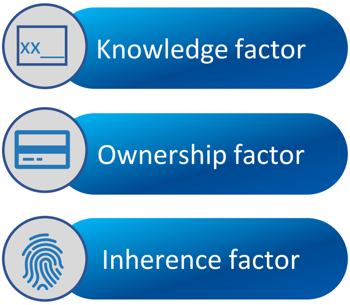
The services introduced by the PSD2 for **payment order initiation** (PISPs), **account information** (AISPs), **and payment card provider** (CISPs) depend on **access to customers' online account data**. Banks or other entities **directly managing a user's current account** (ASPSPs) need to make the data available via an **Application Programming Interface** (API).



What security measures have been introduced? 5

STRONG CUSTOMER AUTHENTICATION (SCA)

The PSD2 introduces an obligation for banks and other payment service providers to implement **authentication systems** containing **at least two distinct and mutually independent factors**.



Knowledge factor	Something the customer knows
Ownership factor	Something the customer owns
Inherence factor	Something the customer is (biometrics)

SECURITY IN COMMUNICATIONS

Exchanges of **information** between TPPs and ASPSPs must meet the **following security requirements**:

- **AISPs, PISPs and PSPs** that issue card-based payment instruments must **be identified with ASPSP**.
- **AISPs and PISPs** must **communicate securely** to request/receive information on accounts and related payment transactions or to issue a payment order from those accounts.
- Communication between ASPSPs, PISPs, AISPs, payers, beneficiaries and other PSPs must be **identified by a certificate** issued by an **eIDAS** qualified trust service provider.

What are PSD2 certificates? 6

To guarantee the security of sensitive financial transactions, the **European Banking Authority** (EBA) has issued new **Regulatory Technical Standards** (RTS) that introduce the use of qualified electronic identification authentication and signature (**eIDAS**) certificates issued by **Qualified Trust Service Providers** (QTSP).

Qualified PSD2 certificates, Qualified Website Authentication Certificates (QWAC) and **Qualified Seals** (QSeal) are used to **identify** PSPs and banking institutions, verify their authorised roles, **encrypt** communications, and provide **tamper-proof seals** for transactions or data.

	QWAC *Qualified Website Authentication Certificate*	**QSealC** *Qualified electronic Seal Certificate*
What is it for?	It identifies the parties and protects data during communication	It identifies the origin of the document or data and protects against tampering.
Security characteristics	Confidentiality, authenticity and integrity	Authenticity and integrity
Probative legal value	No	Yes

What is the QWAC for? 7

The Qualified Website Authentication Certificate (QWAC) is a special type of Transport Layer Security (TLS) certificate that is necessary to **guarantee a secure channel between third parties** and financial institutions in the context of payment services. It confirms the identity and role of the service provider providing payment services for its customers and companies.

It makes communications secure

- It authenticates a client (person or system) to a server to be certain who “owns” the communication channel end point.
- It authenticates a server to a client when a TLS protocol is used to be certain who “owns” the communication channel end point.

It validates identity

- It guarantees the confidentiality, integrity and authenticity of all data transferred on the channel.
- It guarantees that the data have not been changed between endpoints and that no one else can read it along the way.

What is the QSealC for? 8

The **Qualified electronic Seal Certificate** (QSealC) **guarantees the origin and integrity of the data.** The electronic seal certifies that the digitally transferred data did indeed come from the organisation that sent them, and that the document has not been altered along the way.

Data authenticity and integrity

- A Qualified electronic Seal Certificate lets the party using it validate the identity of the certificate’s subject, as well as the authenticity and integrity of the sealed data, and to prove it to third parties.

Data origin

- The electronic seal provides strong evidence, having legal effect, that the data provided originates from the legal entity identified in the certificate.

Who issues them? 9

Regulatory Technical Standards (RTS) require that digital certificates for PSD2 comply with **eIDAS** standards, which means that they can only be issued by **Qualified Trust Service Providers** (QTSP).

WHAT IS A QTSP?

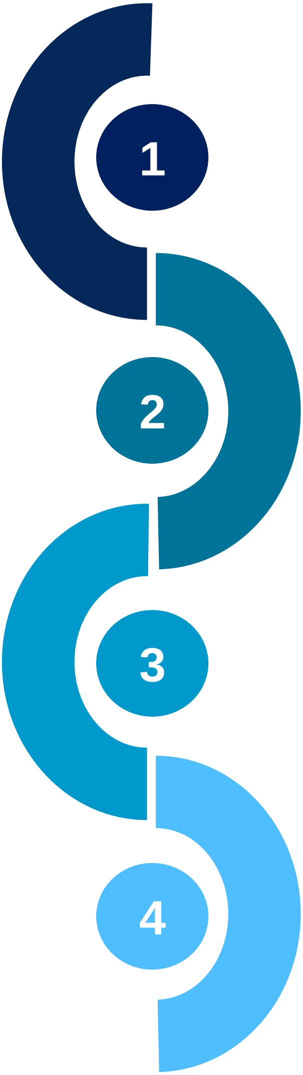
A **Qualified Trust Service Provide**r is a trust service provider that has been granted qualified status by a government supervisory body and has been authorised to provide its **services under eIDAS**. QTSPs use strong authentication mechanisms, digital certificates and electronic signatures to certify the electronic identification of signatories and services.

WHY IS IT IMPORTANT TO RELY ON A QTSP LIKE INFOCERT?

Because of the more stringent requirements applied to QTSPs, qualified trust services have solid **legal effect** for evidence purposes, and because they are combined with **high security**, they offer **superior guarantees to electronic transactions** and **greater protection** for the business involved.

How can they be requested and/or renewed?

10



Visit the **PSD2 Certificates** section on our **infocert.digital** site or **contact us** for more information.

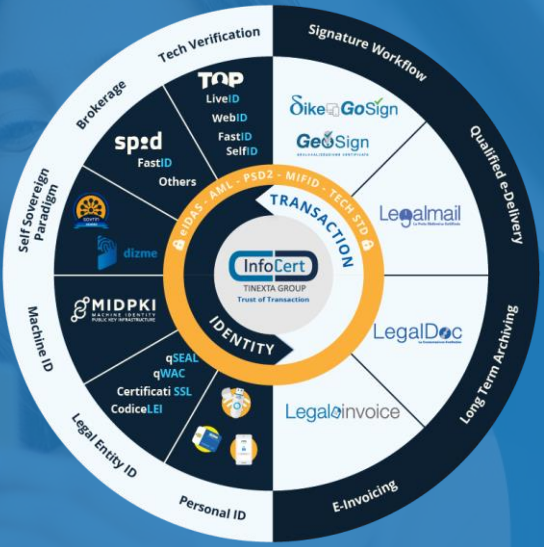
Select the type of PSD2 certificate you need to guarantee maximum security in digital transactions between TPPs.

Digitally complete and sign the **request form and the CSR** (Certificate Signing Request).

Receive the certificate!

InfoCert, the first Pan-European Qualified Trust Provider

InfoCert
TINEXTA GROUP



Product - Solution - API

"We enable companies to innovate their customer interactions and operational processes by leveraging our portfolio of trust-based business solutions and services."

Compliance by design guaranteeing the highest level of innovation

The first pan-European Qualified Trusted Service Provider with solid institutional roots

Trust Solutions to digitise every business process and grow efficiency

Tailor-made solutions to meet specific business needs

infocert.it   Infocert.digital

INFOCERT NUMBERS

2k
Enterprise customers

560 m
Electronic signatures

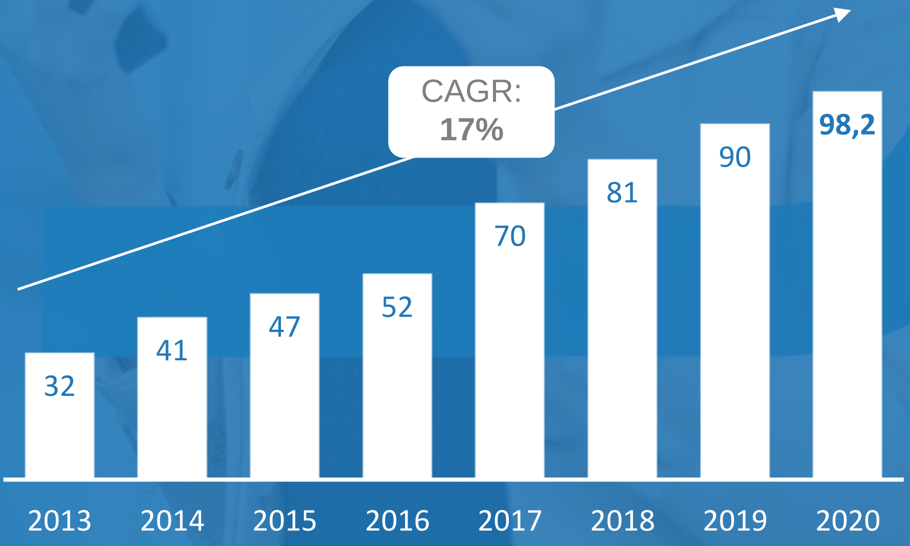
1 bn
Documents stored

17
Countries with enterprise customers

1.5 m
Certified e-mails exchanged daily

605 k
Retail customers

CONSTANTLY GROWING REVENUES



InfoCert revenues: Trend - M€

*InfoCert Group: InfoCert, Sixtema, Camerfirma

InfoCert
TINEXTA GROUP

infocert.it Infocert.digital

GET YOUR QWAC and QSealC PSD2 CERTIFICATE

and

SAVE 50%

SHOW ME THE OFFER >

TINEXTA GROUP

infocert.it Infocert.digital