DATASHEET

Using GlobalSign Qualified Certificates to Support PSD2 Compliance

What Is PSD2?

The revised Payment Services Directive (PSD2) applies to all member states of the European Union (EU) and mandates that financial institutions (such as banks) must open access to their customer information and payment networks to Third Party service Providers (TPPs).

The goal of the directive is to remove the monopoly financial institutions have on their users' data, increase competition, and encourage new, innovative financial solutions, while at the same time establishing standards to ensure interoperability and the security of user data.

The Regulatory Technical Standards (RTS) for Strong Customer Authentication (SCA) and Common and Secure Open Standards of Communication (CSC)

The RTS for SCA and CSC detail the specific security measures and implementation requirements that financial institutions and TPPs must meet to comply with PSD2. The RTS goes into effect in September 2019.

A core principle of the RTS is common and secure communication between all parties involved. All transactions between payment service providers and financial institutions must take place over secured channels and ensure authenticity and integrity of the data.

Meeting PSD2 RTS Service Provider Identity Requirements with Qualified Certificates for Electronic Seals

As specified by PSD2 RTS, payment service providers shall rely on qualified certificates for the purpose of identification and securing communications.

Qualified certificates for electronic seals:

- Uniquely identify the payment service provider, including their authorization number, PSD2 role, and name of National Competent Authority with whom they've registered.
- Protect the contents of data or documents originating from the payment service provider, ensuring their integrity and authenticity.

Qualified Certificates for Electronic Seals from GlobalSign

Qualified certificates can only be issued by a Qualified Trust Service Provider (QTSP) recognized under eIDAS. GlobalSign is recognized across all EU and EEA countries as a QTSP and has undergone the appropriate eIDAS conformity assessments in order to be able to provide qualified certificates that can be used to create electronic seals. View GlobalSign on the EU Trust List here.

Qualified certificates for electronic signatures and seals are available to individuals and organizations through GlobalSign's token-based deployment. In keeping with eIDAS requirements, each signing identity, whether individual or corporate body, is verified and issued a qualified certificate stored on a Qualified Signature Creation Device (QSCD) - the token.

PSD2 Roles

PSD2 establishes defined roles for the various parties involved in maintaining and/or transacting with user account and payment information.

- AISP (ACCOUNT INFORMATION SERVICE PROVIDER)
  Aggregates online information from multiple payment accounts (e.g., a customer can see all financial information from multiple banks in one place)
- PISP (PAYMENT INITIATION SERVICE PROVIDER)
  Can initiate online payments directly from the individual's bank on the individual's behalf (e.g., a customer shopping online can allow the e-retailer to initiate the payment right from their bank, without having to give their account details to the e-retailer)
- ASPSP (ACCOUNT SERVICING PAYMENT SERVICE PROVIDER)
  Provides and maintains the customer's payment account and in the Open Banking ecosystem, publishes standards-based APIs to give third party providers access to customer transaction data in order to provide account information or payment initiation services. Only financial institutions (e.g., banks) can be ASPSPs and they can also be AISPs or PISPs.
- TPP (THIRD PARTY PROVIDER)
  Does not hold payment accounts for their customers and uses the AISPS-provided APIs to access these accounts to provide account information or payment initiation services. TPPs can only be AISPs and/or PISPs since they do not have access to the payment accounts.

GlobalSign®
GMO INTERNET GROUP

Other GlobalSign PKI Solutions

GlobalSign is an identity services company providing cloud-based, highly scalable PKI solutions for enterprises needing to conduct safe commerce, communications, content delivery, and community interactions. Our identity and security solutions enable businesses, large enterprises, cloud-based service providers and IoT innovators around the world to conduct secure online communications, manage millions of verified digital identities, and automate authentication and encryption.

- **STRONG DEVICE IDENTITY**
  IoT providers need to address critical security concerns including authentication, privacy and integrity. GlobalSign's cloud scale PKI service can issue and manage identification and authentication credentials for devices enabling manufacturers to build and deploy a robust and strong identity strategy into their products and ecosystems.

- **WEB AND SERVER SECURITY**
  Prove your public and private sites and servers are legitimate, protect data submissions and provide the best browser experience with the strongest SSL/TLS available. Private hierarchies, internal, and special use case certificates support dynamic server environments to ensure critical networked communications and services remain secure and uninterrupted.

- **USER AND DEVICE AUTHENTICATION**
  Implement strong authentication without burdening end users with hardware tokens or applications and ensure only approved machines and devices can operate on corporate networks.

- **DOCUMENT SIGNING**
  Digital signatures authenticate the signer's identity and create a tamper-evident seal to protect document contents and meet compliance requirements. GlobalSign offers a range of deployment options, including a highly scalable cloud-based service for direct integration into existing workflows.

- **ENTERPRISE MANAGED PKI**
  GlobalSign's cloud-based Managed PKI platform centralizes all certificates across multiple business entities under one account. Automated deployment, flexible APIs for integration with enterprise systems, and comprehensive lifecycle management save time and money while keeping enterprises more secure.

- **SECURE EMAIL**
  Digitally signing and encrypting all internal emails mitigates phishing and data loss risks by clearly verifying message origin so recipients can identify legitimate versus phishing emails and ensuring only intended recipients can access email contents.

- **MOBILE SECURITY**
  Support BYOD (bring your own device) and secure corporate devices with mobile PKI, SCEP support, and integrations with popular MDM/EMM platforms, including AirWatch and MobileIron.

- **CODE INTEGRITY**
  Assure end users that code is legitimate and comes from a verified source, while protecting code from tampering and the threat of malware injections.

- **CUSTOM SUBORDINATE/ISSUING CAs**
  A custom public or private issuing CA for your enterprise maintained by GlobalSign.

About GlobalSign

GlobalSign is the leading provider of trusted identity and security solutions enabling businesses, large enterprises, cloud service providers and IoT innovators around the world to secure online communications, manage millions of verified digital identities and automate authentication and encryption. Its high-scale Public Key Infrastructure (PKI) and identity solutions support the billions of services, devices, people and things comprising the Internet of Everything (IoE).

US: +1 877 775 4562
UK: +44 1622 766766
EU: +32 16 89 19 00
sales@globalsign.com
www.globalsign.com

GlobalSign
GMO INTERNET GROUP