SIGNIUS Harmony - harmonising local and remote signing with Entrust nShield GP HSM and nShield QSCD with SAM

White Paper

Bridging the gap between local applications and centrally managed keys for large organisations and Qualified Trust Service Providers

Local and remote desktop signing

While today's generation of Qualified Electronic Signatures traditionally require desktop applications for use with local smart cards or USB tokens, recent eIDAS regulation has introduced Remote Signature protocols which are designed to support and enable remote digital services.

As these two concepts are fundamentally different, users will now have to choose a solution which supports either local or remote signing, but not both.

SIGNIUS Harmony is addressing the challenges and requirements that organizations are facing with the introduction of remote signing services. Harmony enables all applications with smart card functionality to access remote keys through API, a device-independent cryptographic.

Qualified certificates are hosted by a TSP/QTSP, along with a Remote Signing Server, which can be utilized by millions of legacy applications to sign documents locally on a desktop, and in turn providing the best possible user experience for remote and locally-qualified signing.

Smart card applications

Today there is barely a single desktop application that is capable of signing and encryption, and can utilize Remote Signing Services where the keys are being managed centrally by the organization or through a QTSP.

This is not going to change in the future, as all application developers would have to develop and maintain custom integration components for all available Remote Signing Services in the market.

As QTSPs are pushing towards being eIDAS compliant (an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market), and with centrally managed Remote Signing Services, smart card-based Digital Signatures are becoming less relevant and eventually obsolete in with next five years.

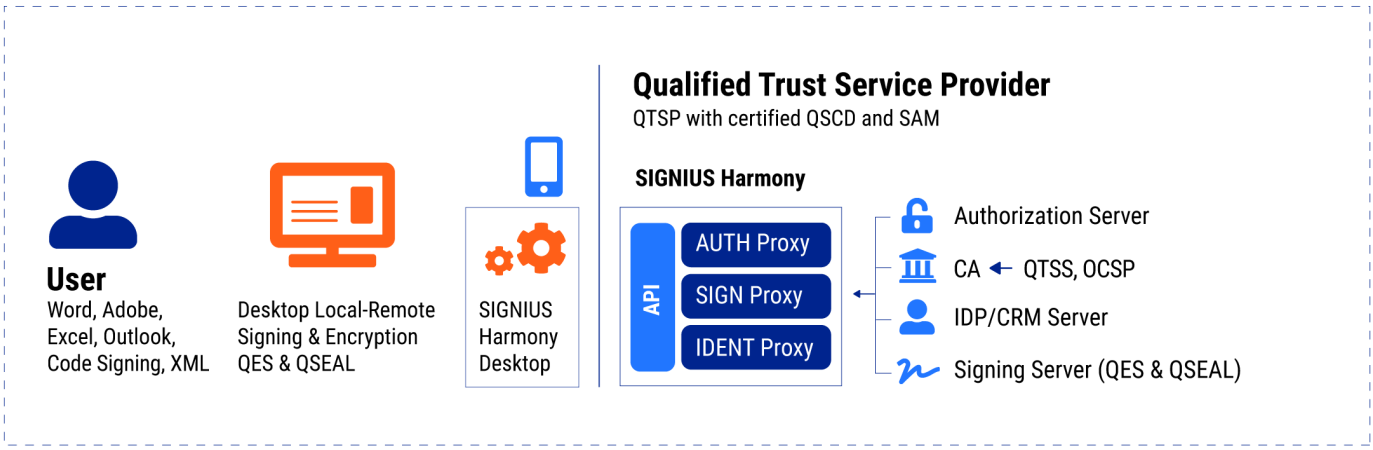
Main disadvantages of using legacy technologies

- A card reader and smart card are required at all times
- Cards can get easily lost, the PIN easily forgotten
- Card reader drivers and middleware need to be updated frequently
- Card readers and cards are exposed to physical damage
- For web applications, custom applets need to be developed and maintained continuously
- There is a wide range of card dependencies, services and complex updates on each Desktop system

Designed for QTSPs and large organizations

Enterprise deployment	QTSP deployment
• GP HSM or QSCD with QSeal or AdES • HSM • 2FA • On-premises • Centrally managed • PKI • Integrating signing & encryption (Office, Outlook, Acrobat, etc.) • Authentication (SSL/TLS Client Authentication based, web applications) • Mail encryption with self-signed and WebTrust certificates • Easy management and user roll out of digital identities • Windows log-on • PIN Caching • Automated log-on • GPO based rollout • Full audit log	• QSCD for AdES+QES+QSeal • SAM • 2FA • Cloud, hosted by QTSP • Centrally managed • Remote signing AdES+QES+QSeal • Integrated signing with Office, Acrobat, etc. • Authentication (SSL/TLS Client Authentication based, web applications) • Mail encryption with self-signed and WebTrust certificates • Easy management and user roll out of digital identities • Full audit log

SIGNIUS Harmony – QTSP based deployment



QES & QSeal hosted remotely by a Qualified Trust Service Provider (QTSP)

QTSPs can address end users with their remote QES & QSeal offering for local-remote QTSP user & QES rollout process:

- ✔ RSS account setup
- ✔ Identity verification
- ✔ 2FA/MFA token roll out
- ✔ SIGNIUS Harmony installation and initialization
- ✔ Signature generation with all desktop applications and RSS
- ✔ Sole control with 2FA/MFA OTP

SIGNIUS Harmony components

- **Harmony Client**
- **Harmony CSP, PKCS#11**
- **Harmony Server with**
  - Certificate Manager
  - Authentication Manager
  - Server API
  - IdP/CRM Connector
  - CA Connector
  - 2FA Connector

SIGNIUS Harmony API

REST API with support for various controllers:

- Administration
- Authentication
- Signing
- Logging

Supported Identity Provider

- ActiveDirectory
- LDAP
- DB
- Custom IdP

Support for different signature formats

- PAdES
- CAdES
- XAdES

Host operating system

- Windows 7
- Windows 10
- MacOS

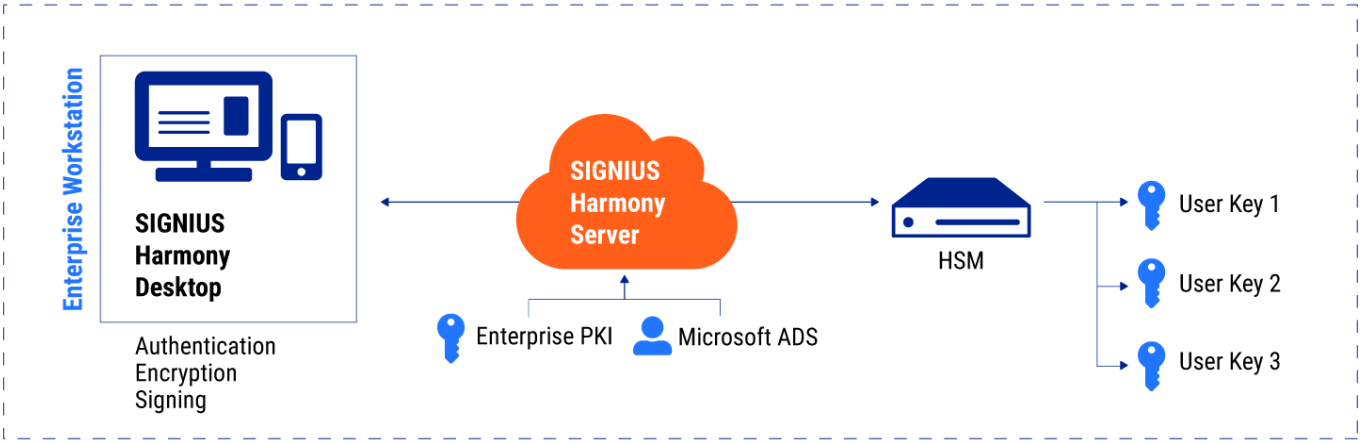
Integrations available with

- Alfresco Document
- Management System
- Microsoft Sharepoint

Solution benefits
Entrust nShield and SIGNIUS Harmony

- ✔ Eliminating the burden of managing physical devices like smart cards and card readers
- ✔ Extending desktop applications with signing capabilities to use remote signatures and utilize modern web technologies
- ✔ Reduce manual work and costs needed for issuance, maintenance, replacement and management of smart cards
- ✔ Documents not leaving the workstation/desktop
- ✔ Out-of-the-box support for all popular applications like Acrobat and Microsoft Office through CSP/CNG and PKCS#11 support
- ✔ Fastest enrolment and remote updates
- ✔ Instant availability without complex software and hardware setup & configuration
- ✔ Desktop applications remain untouched
- ✔ Consistent user experience

SIGNIUS Harmony - Enterprise PKI based deployment



Harmony client specifications

Signature as RAW data

- TSP dedicated installer
- TLS certificate build-in
- RA confirmation process with IdP/CRM
- IdP/CRM integration for
  - Binding user with token in IdP/CRM
  - Authorization details in IdP/CRM
- Middleware
  - CNG
  - PKCS#11
  - Supported OS: Windows, Linux, iOS
- Intuitive and simple GUI
- 2FA: CRM authorization, authorization with assigned tokens
- Server based UI manager

Technical specifications of Entrust QSCD

Security compliance

- Connect XC: eIDAS and Common Criteria EAL4 + AVA_VAN.5 and ALC_FLR.2 certification against EN 419 221-5 Protection Profile, under the Dutch NSCIB scheme
- Connect+: Common Criteria EAL4+ (AVA_VAN.5) certified
- Connect+ recognized as a QSCD
- Connect XC: BSI AIS 20/31 compliant
- IPv6 certified and USGv6 Ready compliant

Supported cryptographic algorithms

- Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, ElGamal, KCDSA, ECDSA (including NIST, Brainpool & secp256k1curves), ECDH, Edwards (Ed25519, Ed25519ph), X25519
- Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, SHA-224 HMAC, SHA256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
- Hash/message digest: SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Full NIST Suite B implementation

Available models and performance

nShield Connect Models	XC Base	1500+	6000+	XC Mid	XC High
RSA signatures per second					
Key length 2048 bit	430	450	3,000	3,500	8,600
Key length 4096 bit	100	190	500	850	2,025

Contact us for a DEMO or a chat with our eIDAS experts!

About SIGNIUS

SIGNIUS S.A. offers a wide range of eIDAS-compliant solutions for trusted services: electronic signatures and seals for individual and corporate clients, remote customer video identification as well as local mass sealing, timestamping and archiving of documents. We create innovative technologies that drive digital transformation, cover a huge number of processes and add significant value to your organization. Our HQ is based in Poznań, Poland. Our sales offices are located in Warsaw, Prague and Berlin.

About ENTRUST

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection around the globe. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, or accessing corporate networks. With our unmatched breadth of digital security and credential issuance solutions, it's no wonder the world's most entrusted organizations trust us.

www.entrust.com

https://signius.eu **connect@signius.eu** **+48 61 415 22 12**