nCipher AN ENTRUST DATACARD COMPANY

www.ncipher.com

## Ensure end user identity via authentication with Mobile ID app and eSignature integrated services

- Two factor authentication and e-signature across entire application ecosystem
- Trust and convenience across multiple user devices
- FIPS 140-2 Level 3 and Common Criteria EAL 4+ root of trust
- EU eIDAS Regulation and Payment Services Directive (PSD2)

SAFELAYER

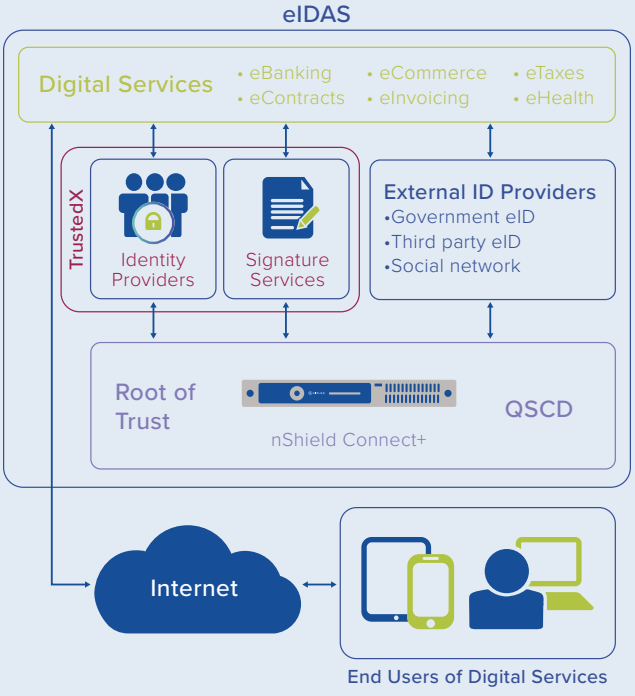
# Safelayer and nCipher provide an integrated solution for deploying eIDAS trust services

### THE PROBLEM: ONLINE AUTHENTICATION AND ESIGNATURE SERVICES CONTINUE TO POSE A BURDEN ON USERS, REQUIRING THEM TO CONSTANTLY USE AND VALIDATE CREDENTIALS

Adoption of online services has become ubiquitous, and the convenience they offer has driven users to increasingly conduct more everyday business using portable smart devices. Yet control mechanisms to securely access online services have not evolved at the same pace. They continue to be highly segmented, requiring users to independently re-authenticate to different services, even after having been authenticated and given access to other applications.

### THE CHALLENGE: ENABLING INDEPENDENT APPLICATIONS TO DELEGATE USER AUTHENTICATION AND ESIGNATURE TO FEDERATED PROVIDERS IN A TRUSTED MANNER

Federated identity providers across applications and services identify and authenticate end users. The process enables subsequent access requests to other applications and services to leverage the initial validation, without the user having to re-authenticate. Preforming this in a trusted manner, across different applications and services, requires a common cryptographic root of trust.




nCipher nShield HSMs integrate with Safelayer TrustedX to protect the PKI key attributes.

# Safelayer and nCipher provide an integrated solution for deploying eIDAS trust services

## THE SOLUTION: SINGLE POINT FOR DATA INCORPORATION, AUDIT, REPORTING, AND INTELLIGENCE ANALYSIS ON THE USE OF CREDENTIALS FOR AUTHENTICATION AND E-SIGNING

TrustedX from Safelayer Secure Communications S.A. is an eIDAS compliant platform for identification, authentication, and electronic signature. The solution guarantees the identity of web service users via adaptive authentication and recognition of government, third party, and social network electronic identities. Providing authentication, single sign-on, and identity federation functions, TrustedX verifies individuals' identities based on context and through one-time keys, digital certificates, and mobile devices. The platform is complemented through the incorporation of public key infrastructure (PKI) identity attributes for developing electronic signature. Along with the authentication mobility solution called Mobile ID, TrustedX provides server and mobile device signatures for deploying eIDAS trust services.

TrustedX integrates with nCipher nShield Connect+ hardware security modules (HSMs) to establish a root of trust for the entire identity management system. nShield HSMs provide a secure container for protecting sensitive PKI attributes and using them to develop electronic signatures for end user identification and authentication. As a Common Criteria EAL4+ qualified signature creation device (QSCD), nShield provides digital signing, web authentication, and other trust services.

## WHY USE NCIPHER NSHIELD HSMs WITH THE SAFELAYER TRUSTEDX PLATFORM?

Cryptographic keys handled outside the protected boundary of a certified HSM are vulnerable to attacks, which can lead to security breaches. HSMs offer a proven and auditable way to secure valuable cryptographic material. nCipher nShield Connect+ HSMs integrate with Safelayer TrustedX to provide comprehensive logical and physical protection of the PKI key attributes. The combined solution delivers an auditable method for enforcing security policies which:

- Enable customers and service providers to meet EU cross-border standards
- Generate and manage sensitive cryptographic keys in a certified, tamper-resistant hardware environment
- Deliver a root of trust for all derived digital services

Providing a mechanism to enforce security policies, and a secure tamper resistant environment, nCipher nShield Connect+ HSMs enables customers to:

- Secure keys within a carefully designed cryptographic boundary that uses a robust access control mechanism, so keys are only used for their authorized purpose
- Ensure key availability by using sophisticated management, storage, and redundancy features to guarantee they are always accessible when needed
- Deliver superior performance to support the most demanding applications

## NCIPHER - AN ENTRUST DATACARD COMPANY

nCipher nShield Connect+ HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nCipher HSMs you can:

- Provide a tightly controlled tamper resistant environment for safekeeping and managing encryption keys
- Enforce key use policies, separating security functions from administrative tasks
- Interface with applications using industry-standard APIs (PKCS#11, OpenSSL, JCE, CAPI, and CNG)

## SAFELAYER

Safelayer is a leading provider of security software for PKI, multi-factor authentication, electronic signature, data encryption, and for the protection of electronic transactions.

The purpose built TrustedX platform provides:

- eIDAS compliant advanced electronic signatures solution
- Single platform for authentication and e-signature across end user devices
- Identity federation services enabling the usage of cloud-based applications
- Increase user security and convenience with Mobile ID, a 2FA identification system based on integrated authentication and electronic-signature services.

For more detailed technical specifications, please visit www.ncipher.com or www.safelayer.com

Search: nCipherSecurity





nCipher AN ENTRUST DATACARD COMPANY