Entrust Provides Root of Trust for Ascertia's Signing Solutions

Integration enables eIDAS compliant digital signatures

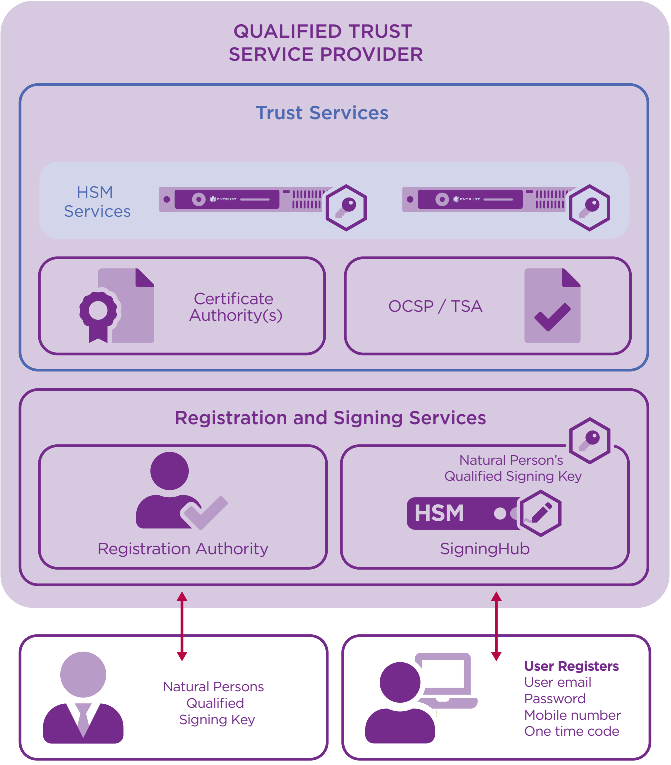
HIGHLIGHTS

- Provide robust solutions for advanced and qualified electronic signatures
- Facilitate advanced document workflow for secure digital signature approval
- Integrate easily for use with business applications across the enterprise
- Enable authentication, traceability, accountability, data integrity, and secure archiving
- Support range of deployments – on-premises, public, private, hybrid, and enterprise cloud
- Compliant to eIDAS, ETSI, SEN, NIST, and Adobe CSC standards

The Problem:

How to enable organizations to conduct electronic business securely?

Organizations from highly regulated sectors including governments, financial services, and telcos need traceability, accountability, and audit services. To meet legislative, regulatory, and internal controls, clear originator authentication, signed approvals, and assured data integrity and provenance are required. Users want ease of use, across devices and applications, giving them confidence and trust.



Entrust nShield® HSMs integrate with Ascertia SigningHub and Advanced Digital Signature Services (ADSS) server to establish a root of trust for underpinning signing keys.

LEARN MORE ABOUT HSM AT ENTRUST.COM

Entrust and Ascertia Integrated Solution

The Challenge:

Supporting organizations to meet legislative, regulatory, and internal control requirements

Ascertia is a global leader in delivering high trust e-security PKI products. Ascertia's SigningHub brings this capability and knowledge together to provide the most secure way to sign and protect documents. It provides the persistent document security required by the high trust sector of the market using existing national and international PKI digital certificate schemes. SigningHub also supports legally enforceable signatures that comply with international regulations, including eIDAS.

The Solution:

Ascertia SigningHub and ADSS server

Ascertia SigningHub delivers a complete signing solution enabling organizations to create seamless workflows for digital signature approval. Whether integrated into core business applications or used as a standalone solution, SigningHub allows businesses to safely migrate paper-intensive processes to the digital world.

Ascertia ADSS server is the cryptographic engine powering SigningHub. ADSS server offers modules for advanced or qualified digital signature creation and verification, together with options for TSA, OCSP, SCVP, XKMS, LTANS as well as CA and RA services.

Together, these products deliver the essential trust services required by public and private organizations to conduct electronic business securely. This includes digital signature creation, verification, timestamping, and long-term evidence archiving services. Ascertia products are device and PKI agnostic, and are available on local, remote, and cloud servers.

Why use Entrust nShield hardware security modules (HSMs) with Ascertia?

Private signing keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise and misuse of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material.

Entrust nShield® HSMs integrate with Ascertia ADSS server to provide comprehensive logical and physical protection of keys for certification authorities, OCSP validation servers, time-stamp authorities, and digital signature services.

Entrust nShield HSMs provide Ascertia ADSS server with centralized HSM services used for remote authorized digital signing, removing the requirement for local smart-cards and readers.

In addition, nShield HSMs are used by Ascertia ADSS server to protect TLS keys used for intercommunications, and provide key storage for the ADSS HMAC service used by business applications to ensure the integrity of data and by the ADSS server audit logs.

Entrust and Ascertia Integrated Solution

Entrust nShield Connect HSMs enable Ascertia customers to:

- Secure keys within carefully designed cryptographic boundaries that use robust access control mechanisms, 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 by the CA, OCSP validation service, and digital signature services
- Deliver superior performance to support demanding applications

nShield Connect HSMs provide a hardened, tamper-resistant environment for performing secure cryptographic processing, key protection, and key management. With nShield HSMs customers 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)

Entrust HSMs

Entrust nShield HSMs are among the highest-performing, most secure, and easy-to-integrate HSM solutions available, facilitating regulatory compliance and delivering the highest levels of data and application security for enterprise, financial, and government organizations.

Our unique Security World key management architecture provides strong, granular controls over access and usage of keys.

Ascertia

Founded in 2001, Ascertia is a privately-owned UK company delivering high trust e-security products. The company focuses on digital signatures and timestamping to help customers securely achieve OCSP validation.

ascertia.com

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications, and data visit **entrust.com**

To find out more about
Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely 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

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

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