Solution Brochure

Maximizing eIDAS opportunities

Building trust services on nShield HSMs

ENTRUST

SECURING A WORLD IN MOTION

Executive summary

The European Union's Electronic Identification and Trust Services (eIDAS) regulation offers significant opportunities for organizations across the EU. For government agencies and businesses, eIDAS makes it faster, easier and more secure to support cross-border digital commerce. For trust service providers (TSPs), eIDAS establishes a business environment that creates expanded demand for solutions.

To realise these gains, establishing trusted services and identities is a bedrock requirement. Entrust nShield® hardware security modules (HSMs) offer the critical security services that enable trusted digital transactions. Using nShield HSMs, TSPs can expand their service offerings based on a strong root of trust, and enable legally binding transactions across borders, while strengthening security.

The opportunity

The EU's eIDAS regulation offers compelling opportunities for organizations delivering trust services within the EU. The regulation was developed to help establish EU-wide standards that facilitate secure electronic commerce and ultimately advance Europe's digital economy. Through the regulation, the EU has established a framework for electronic commerce that enables legally binding, cross-border transactions, agreements and services.

By adopting these common standards, organizations are able to reduce their reliance on traditional, paper-based approaches and more fully capitalize on the advantages that digital transactions provide, including:

- Faster workflows and response
- Improved user convenience
- Stronger security
- Cost savings
- Operational efficiencies

Specifically, the eIDAS regulation provides a number of benefits to these organizations:

- Businesses. eIDAS enables businesses to support more transactions and more readily expand across borders.
- Government agencies. Under the regulation, agencies can deliver more services, provide more convenience and value, serve more users and reduce costs.
- TSPs. By delivering trust services that are compliant with eIDAS, TSPs can expand their markets and service offerings, and capitalize on a rapidly growing market.

eIDAS regulation

The eIDAS regulation represents "a milestone to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities."

From **ec.europa.eu/digital-single-market/en/trust-services-and-eid**

The requirements

To establish confidence in cross-border, cross-organization digital transactions, there must be trustworthy systems that guarantee reliability, visibility, auditability and control. eIDAS offers a framework for trust services, which include the following:

- Issuing certificates for signing and sealing documents and identifying web sites
- Supplying digitally signed time stamps
- Preserving signed data on a long-term basis
- Providing electronic delivery services
- Verifying and validating signatures and seals

To be eIDAS compliant, trust services must use certified HSMs—preferably certified under Common Criteria EAL 4+, although FIPS 140-2 certification is acceptable in some, but not all, EU countries. Further, when holding client keys used to sign at the "qualified level" the device must be certified as a qualified signature creation device (QSCD), which meets specific requirements for "sole control" of the key by the signatory. In both cases, strong cryptography is required which can only be realised when the cryptographic keys underpinning the signature process are properly safeguarded in a secure device. In the case of qualified signatures, additional protection of the user's signing key is required to ensure sole control of the key by an authenticated signatory. Ultimately, the security of the overall system will only be as strong as the root of trust that protects cryptographic keys.

The solution

Entrust nShield HSMs

Solution introduction

Security best practices call for the use of dedicated HSMs, which offer a certified and auditable way to secure valuable cryptographic material. Entrust nShield HSMs generate strong cryptographic keys for performing digital signing and encryption. And, because of their recognised strength over software-based cryptographic key management, HSMs are increasingly used, and their use is set to accelerate as adoption of eIDAS standards continues to grow.

nShield HSMs have earned Common Criteria EAL4+ certifications and are also recognised as QSCDs, enabling support of eIDAS requirements. With nShield HSMs, organizations can generate and manage encryption and signing keys in certified, tamper-resistant hardware.

Maximising customer value through partnerships

TSPs who issue digital certificates, time stamps or digital signatures can use nShield HSMs as a part of their eIDAS-compliant solutions. Entrust has developed technology partnerships with a number of TSPs, and through these partnerships, Entrust offers an integrated nShield HSM solution for the eIDAS ecosystem.

By adopting nShield HSMs, TSPs can become compliant with eIDAS regulations while significantly improving the security of their offerings. By delivering integrated, complete solutions, TSPs can:

- Establish compliant, high-value trust services
- Capitalise on the growing market associated with eIDAS
- Strengthen market awareness through Entrust's global brand recognition
- Partner with a leader in security that can help TSPs adapt to dynamic market requirements

nShield HSMs

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

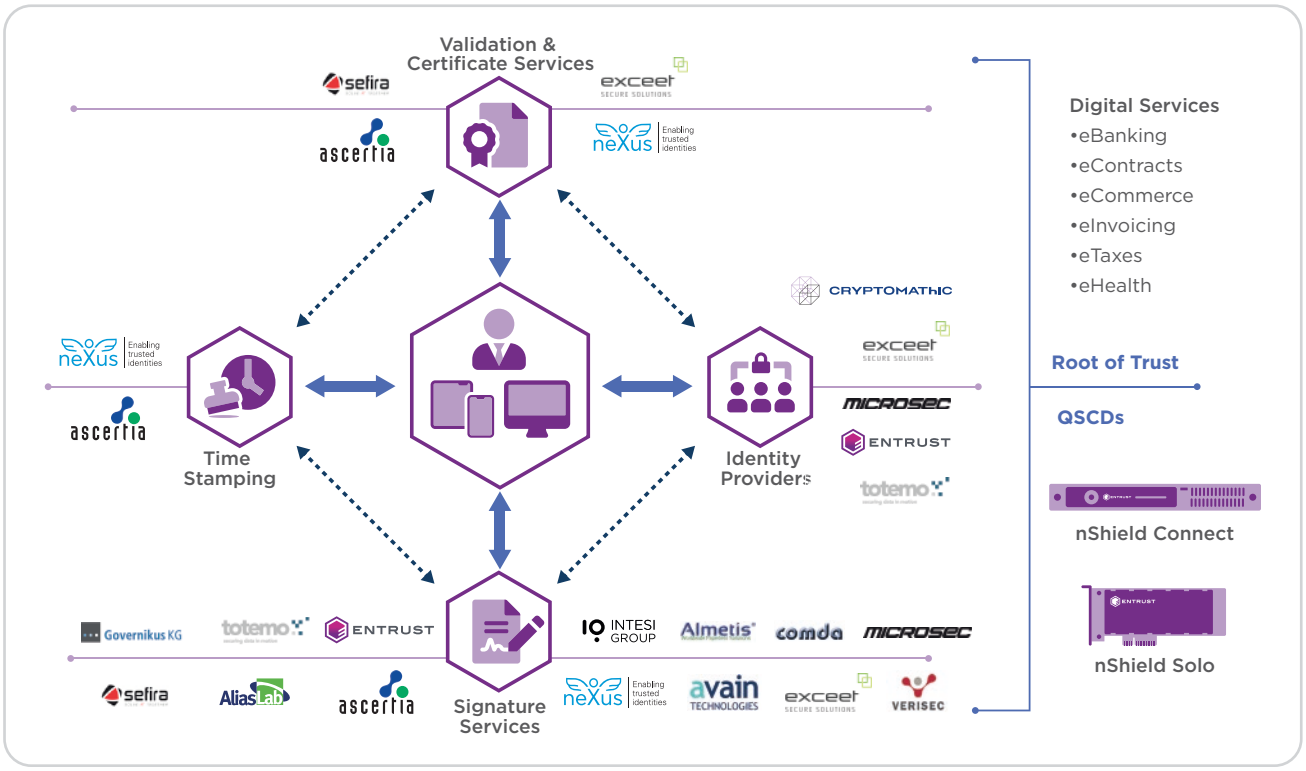

Figure 1: Entrust has established partnerships with an extensive range of solution and service providers.

Today, Entrust's partners strengthen security in four key areas:

- Validation and certificate services
- Identity providers
- Signatures services
- Time stamping

Customer benefits

When combined with integrated partner solutions, nShield HSMs offer government agencies and businesses a number of compelling benefits:

- Conduct legally binding business transactions across borders
- Expand the digitisation of services, while minimising risks and costs
- Employ proven, integrated solutions that minimise deployment time

Conclusion

To maximize the opportunities that the eIDAS regulation presents, businesses, government agencies and TSPs need to establish digital services that are trusted and secure. By adopting Entrust nShield HSMs, organizations establish strong safeguards around the cryptographic keys that are the bedrock of secure digital transactions.

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/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com