www.ncipher.com

nCipher Security enables itAgile to create trust in a paperless world

BUSINESS OPPORTUNITY

As a provider of digital document and signature solutions, itAgile recognized the opportunity to help its customers become Trusted Service Providers (TSPs) by creating a product that would enable them to meet the Electronic Identification, Authentication and Trust Services (eIDAS) regulation TSP certification requirements and get to market more quickly.

eIDAS was designed to establish a framework for electronic transactions that enables legally binding cross-border business throughout the European Union (EU). It creates standards for which electronic signatures are given the same legal standing as their "wet-ink" equivalents, and sees the regulation of Trust Service Providers (TSPs) by supervisory bodies within their respective member states.

Businesses operating in the EU will benefit from using trust services that comply with the regulation: any signed documents and agreements will be valid throughout the EU. Banks in particular are beginning to make use of the eIDAS regulations to ensure the identity of their customers and the validity of their agreements. As governments extend their digital services to their citizens, they are also requiring the use of eIDAS compliant services and signatures.

TECHNICAL CHALLENGE

itAgile's solution would include a Certificate Authority (CA), a core component of a Public Key Infrastructure (PKI), which is responsible for establishing a hierarchical chain of trust. PKIs include the hardware, software, policies, procedures, and processes needed to ensure that a signatory is who they claim to be.

CAs issue the digital credentials used to certify the identity of users and underpin the security of a PKI and the services they support. CAs therefore can be the focus of sophisticated targeted attacks. In order to mitigate the risk of attacks against CAs, physical and logical controls as well as hardening mechanisms, such as hardware security modules (HSMs), are used to ensure the integrity of a PKI.

As Gianni Sandrucci, chief executive officer for itAgile, notes, "It is quite challenging to build a certification authority that meets the eIDAS TSP requirements. To achieve TSP certification, you must satisfy 360 requirements. Among the requirements is the use of HSMs that are certified at Common Criteria EAL4, security standard for cryptographic solutions. Suitable HSMs are not easily found on the market. Moreover, cryptography itself is not a clear and simple matter.

SOLUTION

As experts in digital signatures, itAgile selected nCipher's nShield Solo HSMs, which are Common Criteria EAL4+ certified and recognized as Qualified Signature Creation Devices (QSCDs). TSPs are required to use QSCDs employing strong cryptography to protect the security of their signatures.

"We know the nShield Solo; it's a foundational component of the system. The system is successful, and it's been a positive experience working with the nCipher team and its nShield HSM, allowing us to achieve a short time to market and to recover our costs."

"...our service needs to be very reliable, which is matched by the reliability of the nCipher HSM. This is one of the reasons we chose nCipher. Their HSMs are dependable and last for many years."

– Gianni Sandrucci, chief executive officer, itAgile

According to Sandrucci, “HSMs are the core of the process. We need one HSM to provide the root of trust; two for PKI operations, such as issuing and validating digital certificates and signatures; and one for disaster recovery. This architecture provides a double level of security, because it separates the root key and the CA. One HSM creates the root of trust, and the other creates the certificates.

Beyond that, our service needs to be very reliable, which is matched by the reliability of the nCipher HSM. This is one of the reasons we chose nCipher. Their HSMs are dependable and last for many years.”

RESULTS

itAgile’s PrimeCert TSP provides customers with a turnkey solution that enables them to become a qualified TSP. The PrimeCert customer is still required to achieve eIDAS certification, but all the pieces for certification are in place. And one of the essential pieces is nCipher’s nShield Solo HSM, which is not only certified at Common Criteria EAL4+, but also at FIPS 140-2 Level 3.

Mr. Sandrucci observes, “The EU is heavily regulated. When one of our customers wants to go paperless, they must first satisfy the EU that their system is compliant with the eIDAS regulation. With nCipher nShield Solo HSMs, our product satisfies all the current rules as well as what we expect the next generation of rules to be.”

“We know the nShield Solo; it’s a foundational component of the system. The system is successful, and it’s been a positive experience working with the nCipher team and its nShield HSM, allowing us to achieve a short time to market and to recover our costs.”

ABOUT ITAGILE

itAgile specializes in agile digital document and signature solutions in Italy and the rest of the European Union (EU). Founded in 2008, the company offers its customers and partners:

- Best of breed products
- A thorough knowledge of legislation and standards
- Technical support
- Application development to integrate products efficiently into customer processes

Certified ISO 27001 and ISO 9001, itAgile operates with a nimble, light organizational model focused on customer service and based on the use of cloud technologies and innovative collaborative tools.

Business need

- Create a turnkey solution to enable digital signing customers to achieve eIDAS TSP certification and get to market more quickly

Technology need

- Create a replicable process that satisfies numerous, rigorous technical requirements needed to achieve eIDAS qualified TSP status. These include CAs governed by Common Criteria EAL4+ certified HSMs

Solution

- nCipher nShield Solo HSMs

Result

- Faster time to market for itAgile customers whose strategy includes being a TSP

ABOUT NCIPHER SECURITY

Today’s fast moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency. It also multiplies the security risks. nCipher Security, a leader in the general purpose hardware security module (HSM) market, empowers world-leading organizations by delivering trust, integrity and control to their business critical information and applications.

Our cryptographic solutions secure emerging technologies – cloud, IoT, blockchain, digital payments – and help meet new compliance mandates, using the same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensuring the integrity of your data and putting you in complete control – today, tomorrow, at all times. **www.ncipher.com**