Bit4id enhances Middle Eastern electronic ID card system with eIDAS-compliant online digital ID system using Entrust HSMs

Bit4id develops easy, secure and standardized technologies for authentication, digital signatures, and cryptography. Headquartered in Italy, the company has offices in Ecuador, India, Macau, Peru, Portugal, Spain and the United Kingdom.

Bit4id's philosophy is that just as a person's physical identity is unique and universally recognized, that person's digital identity should be singular and able to safely represent him or her in computer networks and on the internet. It also believes that for digital identity programs to be successful, they must be simple and secure, as well as easy and natural to use – both for the enterprises that manage them and the individuals who use them.

> **Entrust nShield HSMs are the standard around the world. We develop projects based on the extraordinary reliability and availability that Entrust nShield HSMs provide, and we integrate them into all our products. We trust both the Entrust brand and its products implicitly.**
>
> – Pierluigi Pilla, ID Systems and PKI Unit Director at Bit4id

LEARN MORE AT ENTRUST.COM/HSM

Bit4id

BUSINESS CHALLENGE

As part of a joint venture of system integrators, Bit4ID was awarded a contract by the Ministry of Information (MIT) of a Middle Eastern country, to provide a mobile digital identity solution for its entire population, including both citizens and non-citizens of the country. The country already had in place an electronic ID card (microchip) system, but MIT wanted to complement that system with an IT infrastructure to generate and manage digital IDs in cyberspace – modeled on and compliant with the European Union's (EU's) Electronic Identification and Trust Services (eIDAS) Regulation. Using the eIDAS model would not only ensure a best practice approach, but compliance would enable commerce with the EU and other countries adhering to that standard.

TECHNICAL CHALLENGE

PKIs, digital certificates and digital identities

Public key infrastructure (PKI) helps establish the identity of people, devices, and services, enabling controlled access to systems and resources, protection of data, and accountability in online transactions. PKI is the foundation that enables the use of technologies such as digital signatures and encryption across large user populations. Consequently, PKIs are essential for secure and trusted government transactions and e-commerce.

Digital certificates

Digital certificates are the credentials that facilitate the verification of identities between users in a transaction. Much as a passport certifies someone's identity as a citizen of a country, the digital certificate establishes the identity of users within the ecosystem. Because digital certificates are used to verify the identity of the signer of information, protecting the authenticity and integrity of the certificate is imperative to maintain the trustworthiness of the system.

Certificate authorities

A Certificate Authority (CA) is the core component of a PKI responsible for establishing a hierarchical chain of trust. CAs issue the digital credentials used to certify the identity of users and underpin the security of a PKI and the services it supports. The physical and logical controls and hardening mechanisms of a hardware security module (HSM) ensure the integrity of a PKI and mitigate the risk of attack.

eIDAS

eIDAS is an EU regulation that establishes standards for electronic identities, authentication, and signatures. It applies to government bodies and businesses that provide online services to European citizens, and that recognize or use identities, authentication, or signatures. eIDAS also requires the use of Common Criteria EAL4+ (AVA_VAN.5) certified HSMs to issue digital certificates, digital signatures, time stamps, and other transactional data.

System requirements

MIT already had a PKI in place to issue its citizens with electronic ID cards. Bit4id needed to integrate additional capabilities into the PKI that would:

- Allow residents to digitally sign transactions and documents from both desktop and mobile devices, such as digital notebooks, tablets, and smartphones

Bit4id

- Scale easily
- Generate certificates for millions of users
- Process many 1000s of transactions per second

SOLUTION

One reason MIT awarded this project to Bit4id was its proposal that mobile certificates be stored in an Entrust nShield® HSM, certified to Common Criteria EAL4+, rather than on the device itself, such as a mobile phone. This would comply with eIDAS regulations regarding remote digital credentials. Being well-versed in eIDAS compliance, Bit4id knew how to make the system work.

The company custom designed a digital identity system that facilitates traffic between the national PKI, Entrust nShield HSMs, and the residents of the Middle Eastern country using the system. The system securely manages certificate issuance by the national PKI to the HSM, regulates certificate use from the HSM to users and controls certificate life-cycle management (eg, suspension, revocation, renewal). Certificates are required for the users to be identified and authenticated within the system, and then to sign documents in various government applications, such as opening a business, electronically filing income tax or signing and uploading documents for legal correspondence.

The deployment currently uses Bit4id's SignCloud solution together with its ancillary middleware application, Universal Key Chain, and a total of four nShield Connect XC HSMs: one for development, one for testing, and two for production, including a failover mechanism. This provides high availability and load balancing for smooth operation. Bit4id also took advantage of Entrust's unique Security World architecture, which enables storing keys as encrypted and protected files outside the physical confines of the HSM. This provides virtually unlimited key storage.

The current digital ID system is being used primarily for government to citizens applications. However, there are plans in place to replicate the current deployment to enable further use cases that make use of digital signatures in government-to-business and government-to-government applications.

"Bit4id has worked with Entrust and used its nShield HSMs for many years," says Pierluigi Pilla, ID Systems and PKI Unit Director at Bit4id. "Entrust HSMs are the standard around the world. We develop projects based on the extraordinary reliability and availability that Entrust nShield HSMs provide, and we integrate them into all our products. We trust both the Entrust brand and its products implicitly."

Bit4id

Business need

Create an online digital ID system that complements an existing electronic ID card system and is compliant with eIDAS

Technology need

Integrate into existing PKI additional infrastructure that would:

- Allow residents to digitally sign from desktop and mobile devices,such as digital notebooks, tablets, smartphones
- Scale easily
- Generate certificates for millions of users
- Process many 1000s of transactions per second

Solutions

Custom design a digital ID system using:

- Bit4id SignCloud
- Bit4ID Universal Key Chain
- Entrust nShield Connect HSMs
- nShield Security World architecture

Results

- Creation of a national mobile digital ID system
- Satisfied the customer's business, technology and security requirements
- Robust system soon to be duplicated and expanded to other use cases

RESULTS

Bit4id created an eIDAS-compliant mobile digital ID system that complements the Middle Eastern country's existing electronic ID card system. The system:

- Allows residents to digitally sign from both desktop and mobile devices
- Scales easily
- Generates certificates for millions of users
- Processes many 1000s of transactions per second
- Is scheduled to be duplicated and expanded to government-to-business and government-to-government applications

ABOUT ENTRUST

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