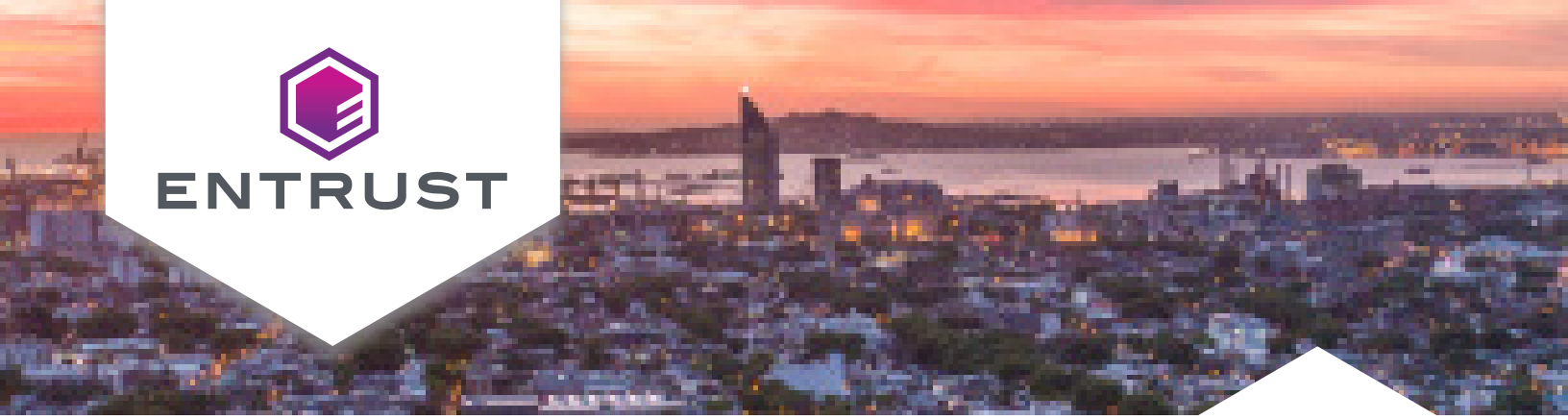

Entrust Enables Antel to Build Digital Identity and Signing Infrastructure for Uruguay

Challenge

In order to construct a secure nationwide electronic identity and signing infrastructure that would be easy for Uruguayans to use and access from different devices, Antel needed a technology partner to help design the architecture necessary to guard and control the digital identities of users throughout their lifecycle; and generate, protect, and manage cryptographic keys used for digital certificates and signatures.

Solution

Using Entrust Remote Signing Server and Public Key Infrastructure (PKI) solutions with Entrust nShield Hardware Security Modules (HSMs), Antel developed secure digital identity and signature services integrated with its own systems and processes, as well as those of most public and private institutions in Uruguay.

Results

- New system called TuID (an abbreviation that corresponds to "Your Digital Identity") was deployed for use by more than 1 million Uruguay citizens and non-Uruguayans.
- Antel was accredited by the local regulatory entity of Uruguay as a trust service provider (TSP) for advanced digital signature services, with centralized custody of keys and digital identification.

CUSTOMER PROFILE

Antel, Uruguay's state-owned telecommunications company, manages the country's entire landline telephony and is its leading mobile and data operator.

Objectives

- Confidently identify human users in the digital context
- Implement identification and authentication processes across combined technologies
- Encourage mass adoption of digital identification system and establish trust in electronic signatures

Technology

- Entrust Remote Signing Server
- Entrust PKI solutions
- Entrust nShield HSMs

LEARN MORE AT ENTRUST.COM

Antel Case Study

ELEMENTS OF SUCCESS

Creating a safe, easy-to-use system for identification and authentication

The primary objective of the project was to construct a secure nationwide electronic identity and signing infrastructure that Uruguayans would trust and use. This required the system to be safe, secure, reliable, and easy to use and access.

Antel saw two main challenges:

- Identifying human users in the digital context and being confident the user was whom they said they were (identify and authenticate)
- Encouraging mass adoption of the system through ease of use, and establishing trust in digital identification replacing physical presence and electronic signatures as valid and viable alternatives to traditional pen and ink signatures

The solution to the first challenge was to build an electronic identification service (mapped to local and international standards) that could authenticate the identity of the applicant and generate a digital identity.

Because some ways of applying for digital credentials are more secure than others, the electronic identification service Antel deployed is able to grant credentials with different security levels. For example, a person might apply in person with paper credentials, such as a passport, and provide an electronic fingerprint. The system would grant this kind of application the highest level of security, which would enable the online equivalent of signing a document in front of a public notary. Another individual might apply online and authenticate using their national ID card and a simultaneous computer-generated photograph. This would receive a lower security level.

Encouraging adoption

According to Daniel Fuentes, Vice President at Antel, when the project began, the advanced electronic signature was already legislated in Uruguay and under serious consideration by the majority of public and private organizations that interact digitally with each other and their stakeholders. However, users did not want to use physical devices like smart cards with readers, nor download drivers and plugins to perform a digital signature. Instead, they wanted a more simple and straightforward process using their computer, smartphone, or tablet for digital signing in multiple places and situations without installing anything.

To address this, the system incorporates the electronic signature with centralized custody of keys. The keys are housed, but in the cloud by a TSP. TSPs, as defined by Uruguay law and eIDAS, are responsible for assuring the electronic identification of signatories and services by using strong mechanisms for authentication, digital certificates, and electronic signatures. The TSP uses the cryptographic keys to apply authorized signatures whenever they are expressly requested by the owner. Access to this highly secure signing system requires the electronic identification of the individual who wishes to sign, and this relies on the verified identification system described above.

Antel Case Study

Navigating technical challenges

Creating a nationwide digital signing infrastructure involves technical challenges such as:

- Designing the architecture necessary to guard the identities of the users, and ensure they maintain exclusive control over them
- Generating, guarding, and managing the lifecycle of the signature creation data – the keys of the digital certificates – in a secure way
- Enabling users to sign without exposing digital certificate keys
- Securely implementing user identification and authentication processes across combined technologies, such as mobile applications, biometrics, and one-time keys, among others
- Signing from multiple devices
- Integrating with any application that should use these services
- Scaling in both capacity performance and functionality

Building a cloud-based TSP

The central challenge for this entire project was to build a trust service provider (TSP) in the cloud where Uruguayans could establish and authenticate their identities and then use those identities to access digital services and sign digital documents.

Antel project managers and consultants knew this TSP would require the use of hardware security modules (HSMs) to protect the keys and create signatures. They chose Entrust Remote Signing Server with Entrust nShield HSMs because of their long-standing reputation for quality, value, and support. In addition, the Entrust Remote Signing Server complies with all the requirements for TSPs in Uruguay (PSCo, by its Spanish acronym), and is also a qualified signature creation device (QSCD). It uses Entrust nShield HSM devices as cryptographic modules for the generation and protection of the signature creation data (SCD) under the European Union's electronic Identification, Authentication, and Trust Services (eIDAS) standards.

Entrust nShield HSMs are hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures. Besides being certified as QSCDs under the eIDAS standard, the Entrust nShield Connect HSMs that Antel employs are also certified to FIPS 140-2 Level 3 and Common Criteria EAL4+. The use of HSMs is considered a best practice among security professionals, enabling organizations to meet and exceed established regulatory standards for cybersecurity. HSMs achieve higher levels of data security and trust. They also maintain high service levels and business agility.

Antel created a cryptographic platform using Entrust's Remote Signing Server and PKI solutions, deployed in several EMEA and LATAM TSPs. This platform:

- Incorporates a public key infrastructure (PKI), which generates digital certificates and manages them as identity attributes
- Validates user identities using multiple authentication methods and manages trust identity levels according to local and international standards (NIST and eIDAS)

Antel Case Study

- Includes an electronic signature provider, allowing the users to remotely sign documents with their digital certificate and keys in the central HSM infrastructure
- Provides web services APIs for integrating authentication and electronic signature user methods

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

Interfase Uruguay, the system integrator that implemented the solution based on Entrust Remote Signing Server and PKI with Antel, has been supported by Neodata local nShield certified systems engineers. Together, they have developed a unique value proposition as a trusted security adviser in applied HSM cryptography for this type of project.

MEASURES OF SUCCESS

Launching a secure digital signing service

Antel developed and launched a secure digital signing service for use by more than 1 million Uruguay citizens and non-Uruguayans. Adhering to local regulations and mirroring the European Union's electronic Identification, Authentication, and Trust Services (eIDAS) model, the digital identity and signature services will not only be integrated with Antel's systems and processes, but with those of most public and private institutions in Uruguay. The digital identity and signature services will enable subscribers to:

- Create a secure, certified digital identity in the cloud
- Use multiple authenticators, including a mobile application and biometrics, to reach their digital identity and certificates in cloud-based data centers
- Securely use public and private online services by authenticating and digitally signing transactions from different devices

Gaining accreditation

Antel was accredited by the local regulatory entity of Uruguay as a TSP for advanced digital signature services with centralized custody and digital identification. On Oct. 15, 2019, Antel presented the new system, which is called "TuID" (an abbreviation that corresponds to "Your Digital Identity").

Entrust Remote Signing Server is deployed in several clusters that use network Entrust nShield Connect XC HSMs in their primary Tier III data center of Antel with production, testing, and development environments, and backup HSMs in a secondary contingency data center.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
EMEA Phone: +44 (0) 118 953 3000