nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

antel

nCipher enables Antel to build digital identity and signing infrastructure for Uruguay

Antel, the state-owned telecommunications company of Uruguay, manages the entire landline telephony and is the leading mobile and data operator in the country, and actively contributes to the development of the country's digital society. Antel developed and launched a secure digital signing service for use by more than 1 million Uruguay citizens and non-Uruguayans. Adhering to the 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 datacenters
- Securely use public and private online services by authenticating and digitally signing transactions from different devices

BUSINESS

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
- 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

Identify and authenticate

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 these digital credentials are more secure than others, the system would be 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 notary public. 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.

Encourage 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 smartcards 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 not housed in a physical device but in the cloud by a trusted service provider (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.

TECHNICAL CHALLENGE

There are many technical challenges involved in creating a nationwide digital signing infrastructure. They include

- Designing the architecture necessary to guard the identities of the users, and ensure they maintain exclusive control over them
- Generating, guarding, and managing the life cycle 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

SOLUTION

The central challenge for this entire project was to build a trusted 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 nCipher's nShield HSMs, because of their long-standing reputation for quality, value, and support, and because nCipher HSMs not only comply with all the requirements for TSPs in Uruguay (PSCo) but also are certified as QSCDs (Qualified Signature Creation Devices) under eIDAS standards, and used in numerous TSPs in the EU.

- 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 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:

a. Achieve higher levels of data security and trust

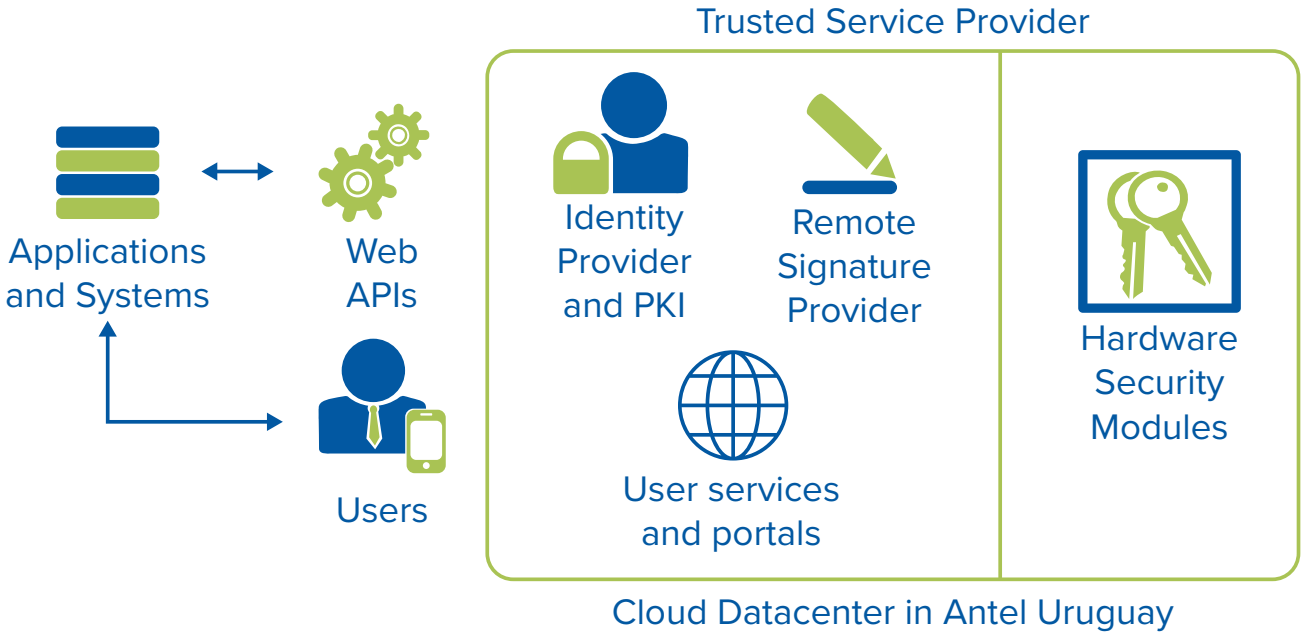
b. Maintain high service levels and business agility

Antel created a cryptographic platform using Entrust Datacard's TrustedX eIDAS Platform and PKI solutions, with nCipher's nShield HSMs, 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)
- 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 Datacard is a leading provider of security software for public key infrastructure (PKI), multi-factor authentication, electronic signature, data encryption and for the protection of electronic transactions.

Interfase Uruguay, the system integrator that implemented the solution with Antel, has been supported by Neodata local nShield certified systems engineers that are part of nCipher's selective distribution and professional services partner network. Together they have developed a unique value proposition as a trusted security advisor in applied HSM cryptography for this type of project.



RESULTS

Antel was accredited by the local regulatory entity of Uruguay (UCE) as a TSP for Advanced Digital Signature services with Centralized Custody and Digital Identification. On October 15, Antel presented the new system which is called “TuID“ (an abbreviation that corresponds to “Your Digital Identity”).

The system uses several clusters of network nShield Connect XC HSMs in their primary Tier III datacenter of Antel with production, testing and development environments, and backup HSMs in a secondary contingency datacenter.

ABOUT NCIPHER SECURITY

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today’s fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our 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, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com

ABOUT ENTRUST DATACARD

Consumers, citizens, and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services, or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure issuance technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports, and ID cards to the digital realm of authentication, certificates, and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide. For more information, visit www.entrustdatacard.com

Business need

Build a secure nation-wide electronic identity and signing infrastructure Uruguayans would trust and use.

Technology need

- Design architecture necessary to guard and control the digital identities of users throughout their lifecycle
- Generate, protect, and manage cryptographic keys used for digital certificates and signature.

Solution

Cryptographic platform using Entrust Datacard’s TrustedX and PKI, with nCipher’s nShield HSMs.

Result

- TuID (Your Digital Identity) solution being deployed
- Trusted service provider for Advanced Digital Signatures
- Accredited by the local regulatory entity in Uruguay

Search: nCipherSecurity