nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

antel

nCipher le permite a Antel desarrollar una identidad digital y una infraestructura de firma para Uruguay

Antel, la empresa estatal de telecomunicaciones de Uruguay, administra toda la telefonía fija y es el operador líder de telefonía móvil y datos en el país, además de contribuir activamente al desarrollo de la sociedad digital del país. Antel desarrolló y lanzó un servicio de firma digital seguro para uso de más de 1 millón de ciudadanos uruguayos y no uruguayos. Cumpliendo con las regulaciones locales y reflejando el modelo de Identificación electrónica, autenticación y servicios de confianza (eIDAS) de la Unión Europea, los servicios de identidad y firma digital no solo se integrarán con los sistemas y procesos de Antel, sino con los de la mayoría de las instituciones públicas y privadas en Uruguay. Los servicios de identidad y firma digital les permitirán a los suscriptores:

- Crear una identidad digital segura y certificada en la nube
- Utilizar múltiples autenticadores, incluida una aplicación móvil y datos biométricos, para alcanzar su identidad digital y certificados en centros de datos basados en la nube
- Utilizar de forma segura servicios en línea públicos y privados mediante la autenticación y firma digital de transacciones desde diferentes dispositivos

NEGOCIOS

El objetivo principal del proyecto era construir una identidad electrónica segura a nivel nacional y una infraestructura de firma en la que los uruguayos pudieran confiar y usar. Esto requería que el sistema fuera:

- Seguro
- Estable
- Confiable
- Fácil de usar y de acceder

Antel vio dos desafíos principales:

- Identificar usuarios humanos en el contexto digital y confiar en que el usuario era quien dijo ser (identificar y autenticar)
- Fomentar la adopción masiva del sistema a través de la facilidad de uso y establecer la confianza en la identificación digital reemplazando la presencia física y las firmas electrónicas como alternativas válidas y viables a las firmas tradicionales de pluma y tinta

Identificar y autenticar

La solución al primer desafío fue construir un servicio de identificación electrónica (mapeado a estándares locales e internacionales) que pudiera autenticar la identidad del solicitante y generar una identidad digital. Debido a que algunas formas de solicitar estas credenciales digitales son más seguras que otras, el sistema podría otorgar credenciales con diferentes niveles de seguridad. Por ejemplo, una persona puede presentar una solicitud en persona con credenciales en papel, como un pasaporte y proporcionar una huella digital electrónica. El sistema otorgaría a este tipo de aplicación el más alto nivel de seguridad, lo que permitiría el equivalente en línea de firmar un documento frente a un notario público. Otra persona puede solicitar en línea y autenticarse utilizando su tarjeta de identificación nacional y una fotografía simultánea generada por computadora. Esto recibiría un nivel de seguridad más bajo.

Fomentar la adopción

Según Daniel Fuentes, vicepresidente de Antel, cuando comenzó el proyecto, la firma electrónica avanzada ya estaba legislada en Uruguay y bajo la consideración seria de la mayoría de las organizaciones públicas y privadas que interactúan digitalmente entre sí y con sus partes interesadas. Sin embargo, los usuarios no querían usar dispositivos físicos como tarjetas inteligentes con lectores, ni descargar controladores y complementos para realizar una firma digital. En cambio, querían un proceso más simple y directo usando su computadora, teléfono inteligente o tableta para la firma digital en múltiples lugares y situaciones sin instalar nada.

Para abordar esto, el sistema incorpora la firma electrónica con custodia centralizada de claves. Las claves no están alojadas en un dispositivo físico, sino en la nube por un proveedor de servicios de confianza (TSP). Los TSP, según lo definido por la ley de Uruguay y eIDAS, son responsables de asegurar la identificación electrónica de los firmantes y servicios mediante el uso de mecanismos sólidos para la autenticación, los certificados digitales y las firmas electrónicas. El TSP utiliza las claves criptográficas para aplicar firmas autorizadas, siempre que el propietario las solicite expresamente. El acceso a este sistema de firma altamente seguro requiere la identificación electrónica de la persona que desea firmar y esto depende del sistema de identificación verificado descrito anteriormente.

DESAFÍO TÉCNICO

Existen muchos desafíos técnicos involucrados en la creación de una infraestructura de firma digital a nivel nacional. Entre los cuales se incluyen:

- Diseñar la arquitectura necesaria para proteger las identidades de los usuarios y garantizar que mantengan un control exclusivo sobre ellos.
- Generar, proteger y administrar de forma segura el ciclo de vida de los datos de creación de firmas y las claves de los certificados digitales.
- Permitirles a los usuarios firmar sin exponer las claves del certificado digital
- Implementación segura de procesos de identificación y autenticación de usuarios en tecnologías combinadas, tales como aplicaciones móviles, biometría y claves de un solo uso, entre otras
- Firma desde múltiples dispositivos
- Integración con cualquier aplicación que deba utilizar estos servicios.
- Escalado tanto en rendimiento de capacidad como en funcionalidad

SOLUCIÓN

El desafío central para todo este proyecto fue construir un proveedor de servicios de confianza (TSP) en la nube donde los uruguayos pudieran establecer y autenticar sus identidades y luego usar esas identidades para acceder a servicios digitales y firmar documentos digitales.

Los gerentes y consultores de proyectos de Antel sabían que este TSP requeriría el uso de Módulos de Seguridad de Hardware (HSMs) para proteger las claves y crear firmas. Eligieron los HSMs nShield de nCipher, debido a su larga reputación de calidad, valor y soporte y porque los HSMs de nCipher no solo cumplen con todos los requisitos para TSP en Uruguay (PSCo), sino que también están certificados como QSCD (dispositivos de creación de firma calificados) según las normas eIDAS, además de ser utilizados en numerosos TSP en la UE.

- Los HSMs nShield son dispositivos de hardware reforzados y resistentes a las manipulaciones indebidas que fortalecen las prácticas de cifrado al generar claves, cifrar y descifrar datos así como crear y verificar firmas digitales. Además de estar certificados como QSCD bajo el estándar eIDAS, los HSMs nShield Connect que emplea Antel también están certificados para FIPS 140-2 Nivel 3 y Common Criteria EAL4+. El uso de HSMs se considera una práctica recomendada entre los profesionales de seguridad, lo que permite a las organizaciones cumplir y superar los estándares regulatorios establecidos para la seguridad cibernética. HSM:

a. Logran altos niveles de seguridad de datos y confianza

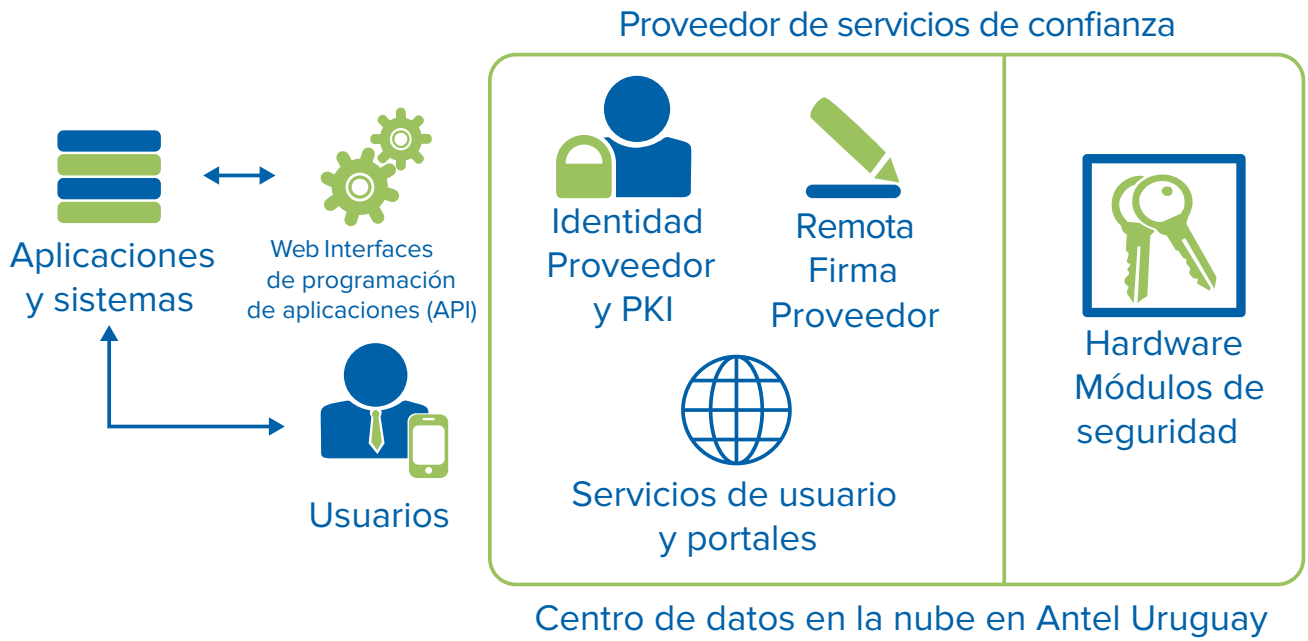
b. Mantienen altos niveles de servicio y agilidad empresarial

Antel creó una plataforma criptográfica utilizando la plataforma TrustedX eIDAS de Entrust Datacard y las soluciones para PKI, con los HSM nShield de nCipher, implementados en varios TSP de EMEA y LATAM. Esta plataforma:

- Incorpora una Infraestructura de clave pública (PKI), que genera certificados digitales y los administra como atributos de identidad
- Valida las identidades de los usuarios utilizando múltiples métodos de autenticación y gestiona los niveles de identidad de confianza de acuerdo con los estándares locales e internacionales (NIST y eIDAS)
- Incluye un proveedor de firma electrónica, que permite a los usuarios firmar documentos de forma remota con su certificado digital y claves en la infraestructura central del HSM
- Proporciona APIs de servicios web para integrar métodos de autenticación y firma electrónica de usuario

Entrust Datacard es un proveedor líder de software de seguridad para la Infraestructura de clave pública (PKI), de autenticación multifactor, firma electrónica, cifrado de datos y de la protección de transacciones electrónicas.

Interfase Uruguay, el integrador de sistemas que implementó la solución con Antel, ha sido apoyado por los ingenieros de sistemas locales certificados por nShield de Neodata que forman parte de la red de socios de distribución profesional y servicios profesionales de nCipher. Juntos, han desarrollado una propuesta de valor única como asesor de seguridad confiable en criptografía HSM aplicada para este tipo de proyecto.



RESULTADOS

Antel fue acreditado por la entidad reguladora local de Uruguay (UCE) como un TSP para servicios de Firma Digital Avanzada con Custodia Centralizada e Identificación digital. El 15 de octubre, Antel presentó el nuevo sistema que se llama "TuID" (una abreviatura que corresponde a "Su identidad digital").

El sistema utiliza varios grupos de HSMs nShield Connect XC de red en su centro de datos primario Tier III de Antel, con entornos de producción, prueba y desarrollo, así como HSM de respaldo en un centro de datos secundario de contingencia.

ACERCA DE NCIPHER SECURITY

nCipher Security, una empresa de Entrust Datacard, lidera el mercado de Módulos de Seguridad de Hardware (HSMs) de propósito general y con ello fortalece a las organizaciones líderes en el mundo al brindarles confianza, integridad y control sobre la información y las aplicaciones críticas de sus negocios. El rápido entorno digital de hoy en día mejora la satisfacción del cliente, proporciona una ventaja competitiva y mejora la eficiencia operativa. Y también multiplica los riesgos en seguridad. Nuestras soluciones criptográficas protegen las tecnologías emergentes, tales como la nube, el IoT, el blockchain, los pagos digitales y ayudan a cumplir con las nuevas exigencias en materia de cumplimiento. Esto lo llevamos a cabo utilizando la misma tecnología comprobada de la que dependen las organizaciones globales en la actualidad para protegerse contra las amenazas a sus datos confidenciales, las comunicaciones de red y la infraestructura empresarial. Le ofrecemos confianza para las aplicaciones críticas de su negocio, aseguramos la integridad de sus datos y le damos el control completo, hoy, mañana y en todo momento. www.ncipher.com

ACERCA DE ENTRUST DATACARD

Los consumidores, ciudadanos y empleados esperan cada vez más experiencias en cualquier lugar y en cualquier momento, ya sea que estén haciendo compras, cruzando fronteras, accediendo a servicios electrónicos del gobierno o iniciando sesión en redes corporativas. Entrust Datacard ofrece la identidad confiable y tecnologías de emisión seguras que hacen que esas experiencias sean confiables y seguras. Las soluciones van desde el mundo físico de las tarjetas financieras, pasaportes y tarjetas de identificación hasta el ámbito digital de autenticación, certificados y comunicaciones seguras. Con más de 2,000 colegas de Entrust Datacard en todo el mundo y una red de socios globales fuertes, la compañía presta servicios a clientes en 150 países de todo el mundo. Para más información, visite www.entrustdatacard.com

Necesidad del negocio

Construir una identidad electrónica segura en todo el país y la infraestructura de firma en que los uruguayos confiarán y usarán.

Necesidad tecnológica

- Diseñar la arquitectura necesaria para proteger y controlar las identidades digitales de los usuarios a lo largo de su ciclo de vida
- Generar, proteger y administrar claves criptográficas utilizadas para certificados y firmas digitales.

Solución

Plataforma criptográfica que utiliza TrustedX y PKI de Entrust Datacard, con HSM nShield de nCipher.

Resultado

- Se está implementando la solución TuID (su identidad digital)
- Proveedor de servicios de confianza para firmas digitales avanzadas
- Acreditado por la entidad reguladora local en Uruguay

Buscar: nCipherSecurity