

# nCipher Security le permite a itAgile generar confianza en un mundo digital



## OPORTUNIDAD DE NEGOCIO

Como proveedor de documentos digitales y soluciones de firma, itAgile reconoció la oportunidad de ayudar a sus clientes a convertirse en proveedores de servicios de confianza (TSP) mediante la creación de un producto que les permitiera cumplir con los requisitos de certificación de TSP del Reglamento europeo relativo a la identificación electrónica, autenticación y servicios de confianza (eIDAS) y llegar al mercado más rápido.

eIDAS fue diseñado para establecer un marco para las transacciones electrónicas que permita negocios transfronterizos legalmente vinculantes en todo el territorio de la Unión Europea (UE). Este crea estándares en los que se da la misma capacidad legal a las firmas electrónicas que a sus equivalentes en "tinta fresca" y se ocupa de la regulación de Proveedores de servicios de confianza (TSP) por organismos supervisores dentro de sus respectivos estados miembros.

Las empresas que operen en la UE se beneficiarán al utilizar los servicios de confianza que cumplan con la regulación: cualquier documento o acuerdo firmado tendrá validez en todo el territorio de la UE. Los bancos en particular están comenzando a utilizar las regulaciones de eIDAS a modo de garantizar la identidad de sus clientes, así como la validez de sus contratos. Conforme los gobiernos extienden sus servicios digitales a sus ciudadanos, también requieren del uso de servicios y firmas compatibles con eIDAS.

## DESAFÍO TÉCNICO

La solución de itAgile incluye una entidad de certificación (CA), un componente principal de una Infraestructura de llave pública (PKI) que es responsable de establecer una cadena de confianza jerárquica. Entre las PKI se incluye el equipo, el software, las políticas, los procedimientos y los procesos necesarios para garantizar que un signatario sea quien dice ser.

Las CA emiten las credenciales digitales utilizadas para certificar la identidad de los usuarios y respaldar la seguridad de una PKI y los servicios que prestan. Por lo tanto, las CA pueden ser el centro de sofisticados ataques dirigidos. A fin de mitigar el riesgo de ataques en contra de las CA, se utilizan controles físicos y lógicos, así como mecanismos de fortalecimiento, como los Módulos de Seguridad de Hardware (HSMs), para garantizar la integridad de una PKI.

Tal y como apunta Gianni Sandrucci, director general de itAgile, "Es muy difícil crear una autoridad de certificación que cumpla con los requisitos para TSP de eIDAS. Para obtener una certificación de TSP, se debe cumplir con 360 requisitos. Entre los requisitos se encuentra el uso de los HSMs que cuentan con la certificación EAL4 de Common Criteria para el estándar de seguridad de soluciones criptográficas. No es fácil encontrar los HSMs adecuados en el mercado. Por otro lado, la criptografía no es en sí misma un tema claro y simple.

## SOLUCIÓN

Como expertos en firmas digitales, itAgile eligió los HSMs nShield Solo de nCipher que cuentan con la certificación EAL4+ de Common Criteria y que son reconocidos como dispositivos calificados de creación de firmas (QSCD). Los TSP deben utilizar QSCD que empleen una criptografía sólida para proteger la seguridad de sus firmas.



*"Conocemos el nShield Solo; es un componente fundamental del sistema. El sistema funciona con éxito y ha sido una experiencia positiva trabajar con el equipo de nCipher y su HSM nShield, que nos ha permitido tener éxito en corto tiempo para comercializar y recuperar nuestros costos".*

*"... nuestro servicio debe ser muy confiable, lo que se combina con la confiabilidad del HSM de nCipher. Esta es una de las razones por las cuales elegimos nCipher. Sus HSMs son confiables y duran muchos años".*

– Gianni Sandrucci, director general, itAgile



De acuerdo con Sandrucci, los "HSMs son el núcleo del proceso. Necesitamos un HSM para facilitar la raíz de confianza; dos para operaciones de la PKI, como la emisión y la validación de firmas y certificados digitales, y uno para recuperación en caso de desastres. Esta arquitectura ofrece un nivel doble de seguridad, ya que separa la llave de raíz de la CA. Un HSM crea la raíz de confianza, mientras que el otro crea los certificados.

Además, nuestro servicio debe ser muy confiable, lo que se combina con la confiabilidad del HSM de nCipher. Esta es una de las razones por las cuales elegimos nCipher. Sus HSM son confiables y duran muchos años".

## RESULTADOS

El TSP PrimeCert de itAgile brinda a sus clientes una solución llave en mano que les permite convertirse en TSP calificados. El cliente de PrimeCert debe, de todos modos, obtener la certificación de eIDAS; sin embargo, se han dado todos los pasos para la certificación. Y uno de los pasos esenciales es el HSM nShield Solo de nCipher, el cual no solo cuenta con la certificación EAL4+ de Common Criteria, sino también con la FIPS 140-2 Nivel 3.

El Sr. Sandrucci observa: "La UE está muy regulada. Cuando uno de nuestros clientes elige la vía digital, este debe satisfacer primero a la UE de que su sistema cumple con el Reglamento eIDAS. Con los HSM nShield Solo de nCipher, nuestro producto satisface todas las regulaciones actuales, así como lo que esperamos que sea la siguiente generación de reglamentos".

"Conocemos el nShield Solo; es un componente fundamental del sistema. El sistema funciona con éxito y ha sido una experiencia positiva trabajar con el equipo de nCipher y su HSM nShield, que nos ha permitido tener éxito en corto tiempo para comercializar y recuperar nuestros costos".

## SOBRE ITAGILE

itAgile se especializa en soluciones ágiles para documentos y firmas digitales en Italia, así como en el resto de la Unión Europea (UE). Fundada en 2008, la compañía le ofrece a sus clientes y socios:

- Los mejores productos de su categoría
- Conocimiento profundo sobre estándares y legislación
- Soporte técnico
- Desarrollo de aplicaciones para integrar productos en los procesos del cliente de forma eficiente

Con las certificaciones ISO 27001 e ISO 9001, itAgile funciona con un modelo organizacional ágil y ligero con enfoque en el servicio al cliente y basado en el uso de tecnologías en la nube y herramientas de colaboración innovadoras.

### Necesidad del negocio

- Crear una solución llave en mano que permita la firma digital de manera que los clientes puedan obtener la certificación TSP de eIDAS y salir más rápido al mercado.

### Necesidad tecnológica

- Crear un proceso replicable que cumpla con numerosos y rigurosos requisitos técnicos necesarios para alcanzar el estatus de TSP calificado de eIDAS. Este incluye CA regidos por HSM con la certificación EAL4+ de Common Criteria.

### Solución

- HSM nShield Solo de nCipher

### Resultado

- Plazo más breve de lanzamiento al mercado para clientes de itAgile cuya estrategia incluye ser TSP

## 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](http://www.ncipher.com)

Buscar: nCipherSecurity



nCipher - Marzo de 2020 • itAgile

[www.ncipher.com](http://www.ncipher.com)

