nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

# Maximice las oportunidades de eIDAS

*Creación de servicios de confianza en HSM de nCipher*

# Resumen Ejecutivo

El Reglamento del sistema europeo de reconocimiento de identidades electrónicas (eIDAS) de la Unión Europea ofrece oportunidades significativas para las organizaciones de toda la UE. Para las agencias gubernamentales y las empresas, eIDAS hace que sea más rápido, más fácil y más seguro apoyar el comercio digital transfronterizo. Para los proveedores de servicios de confianza (TSP), eIDAS establece un entorno empresarial que creará una mayor demanda de soluciones.

Para obtener estos logros, establecer servicios e identidades confiables es un requisito fundamental. Los Módulos de Seguridad de Hardware (HSMs) nShield ofrecen los servicios de seguridad críticos que permiten transacciones digitales confiables. Al utilizar los HSM de nShield, los TSP pueden expandir sus ofertas de servicios con base en una fuerte raíz de confianza y permitir transacciones legalmente vinculantes a través de las fronteras, al tiempo que fortalecen la seguridad.

# La oportunidad

El reglamento eIDAS de la UE ofrece oportunidades convincentes para las organizaciones que prestan servicios de confianza dentro de la UE. La regulación fue desarrollada para ayudar a establecer estándares en toda la UE que faciliten el comercio electrónico seguro y, en última instancia, potencien la economía digital de Europa. Por medio de la regulación, la UE ha establecido un marco para el comercio electrónico que permite transacciones, acuerdos y servicios transfronterizos legalmente vinculantes.

Al adoptar estos estándares comunes, las organizaciones pueden reducir su dependencia de los enfoques tradicionales basados en papel y aprovechar al máximo las ventajas que ofrecen las transacciones digitales, que incluyen:

- Flujos de trabajo y respuesta más rápidos
- Mayor comodidad del usuario
- Mayor seguridad
- Ahorro de costos
- Eficacia operativa

***REGULACIÓN eIDAS***

***La regulación eIDAS representa "un hito para proporcionar un entorno regulatorio predecible que permita interacciones electrónicas seguras y sin problemas entre empresas, ciudadanos y autoridades públicas".***

*Tomado de* ec.europa.eu/digital-single-market/en/trust-services-and-eid.

Más específicamente, la regulación eIDAS proporciona una serie de beneficios a las siguientes organizaciones:

- Empresas. eIDAS permite a las empresas respaldar más transacciones y expandirse más fácilmente a través de las fronteras.
- Entidades gubernamentales. Según la regulación, las entidades pueden brindar más servicios, brindar más conveniencia y valor, atender a más usuarios y reducir costos.
- TSP. Al ofrecer servicios de confianza que cumplen con eIDAS, los TSP pueden expandir sus mercados y ofertas de servicios, así como capitalizar un mercado en rápido crecimiento.

# Los requisitos

Para establecer la confianza en las transacciones digitales transfronterizas y entre organizaciones, deben existir sistemas confiables que garanticen la confiabilidad, visibilidad, auditabilidad y el control. eIDAS ofrece un marco para servicios de confianza, que incluye lo siguiente:

- Emisión de certificados para firmar y sellar documentos e identificar sitios web
- Suministro de sellos de tiempo firmados digitalmente
- Preservación de los datos firmados a largo plazo
- Prestación de servicios de entrega electrónica
- Verificación y validación de firmas y sellos

Para cumplir con el reglamento eIDAS, los servicios de confianza deben usar HSMs certificados; de preferencia, certificados según Common Criteria EAL 4+, aunque la certificación FIPS 140-2 es aceptable en algunos países de la UE, pero, no en todos. Además, al mantener llaves de cliente utilizadas para firmar en el "nivel calificado", el dispositivo debe estar certificado como un dispositivo de creación de firma calificado (QSCD), que cumple con los requisitos específicos para el "control exclusivo" de la llave por parte del firmante. En ambos casos, se requiere de una criptografía sólida que solo se puede realizar cuando las llaves criptográficas que sustentan el proceso de firma están debidamente protegidas en un dispositivo seguro. En el caso de firmas calificadas, se requiere protección adicional de la llave de firma del usuario para garantizar el control exclusivo de la llave por parte de un firmante autenticado. En última instancia, la seguridad del sistema en general solo será tan fuerte como la raíz de la confianza que protege las llaves criptográficas.

# La solución

*Los HSMs nShield de nCipher*

## INTRODUCCIÓN A LA SOLUCIÓN

Las mejores prácticas de seguridad requieren el uso de HSM dedicados, que ofrecen una forma certificada y auditable de asegurar material criptográfico valioso. Los HSMs nShield de nCipher generan llaves criptográficas fuertes para realizar la firma digital y el cifrado. Y, debido a su reconocida fortaleza sobre la administración de llaves criptográficas basadas en software, los HSMs se utilizan cada vez más y su uso se acelerará a medida que la adopción de los estándares eIDAS continúe creciendo.

Los HSMs nShield han obtenido las certificaciones Common Criteria EAL4+ y también son reconocidos como QSCD, lo que permite compatibilidad con los requisitos de eIDAS. Con los HSMs nShield, las organizaciones pueden generar y administrar llaves de cifrado y la firma en un hardware certificado y resistente a manipulaciones indebidas.

## MAXIMIZAR EL VALOR DEL CLIENTE A TRAVÉS DE ALIANZAS

Los TSP que emiten certificados digitales, marcas de tiempo o firmas digitales, pueden usar los HSMs nShield como parte de sus soluciones compatibles con eIDAS. nCipher ha desarrollado alianzas tecnológicas con varios TSP y a través de estas alianzas, nCipher ofrece una solución integrada de HSM nShield para el ecosistema eIDAS.

Al adoptar los HSMs nShield, los TSP pueden cumplir con las regulaciones de eIDAS al tiempo que mejoran significativamente la seguridad de sus ofertas. Al ofrecer soluciones integradas y completas, los TSP pueden:

- Establecer servicios confiables de alto valor
- Aprovechar el creciente mercado asociado con eIDAS
- Fortalecer la difusión en el mercado a través del reconocimiento de marca global de nCipher
- Asóciese con un líder en seguridad que pueda ayudar a los TSP a adaptarse a los requisitos dinámicos del mercado

### LOS HSMS NSHIELD

***Los HSMs nShield de nCipher proporcionan un entorno reforzado y resistente a las manipulaciones indebidas para realizar un procesamiento criptográfico seguro, la protección y administración de llaves.***

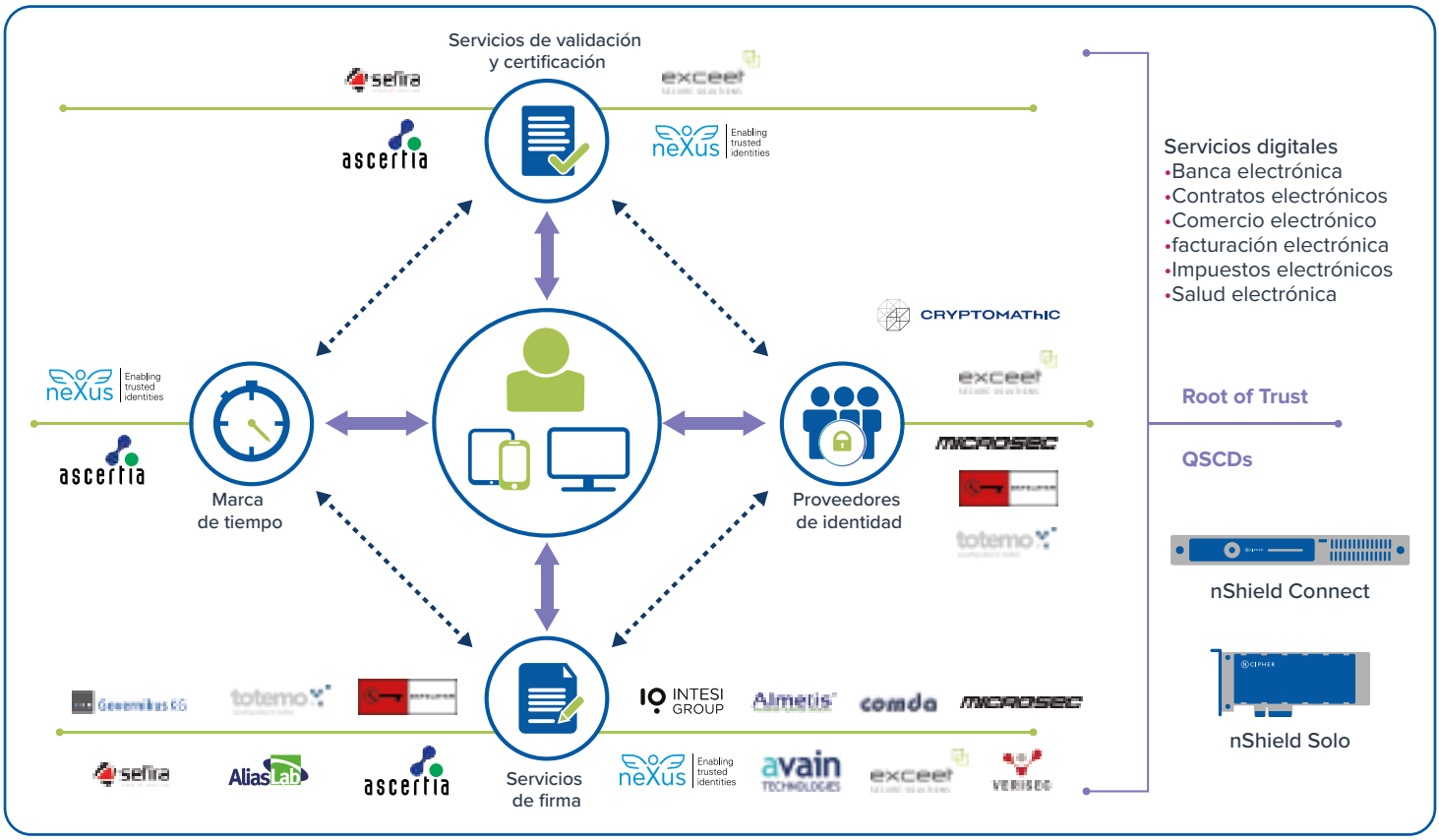



Figura 1: nCipher ha establecido alianzas con una amplia gama de proveedores de soluciones y servicios.

Hoy en día, los socios de nCipher fortalecen la seguridad en cuatro áreas clave:

- Servicios de validación y certificación
- Proveedores de identidad
- Servicios de firma
- Marca de tiempo

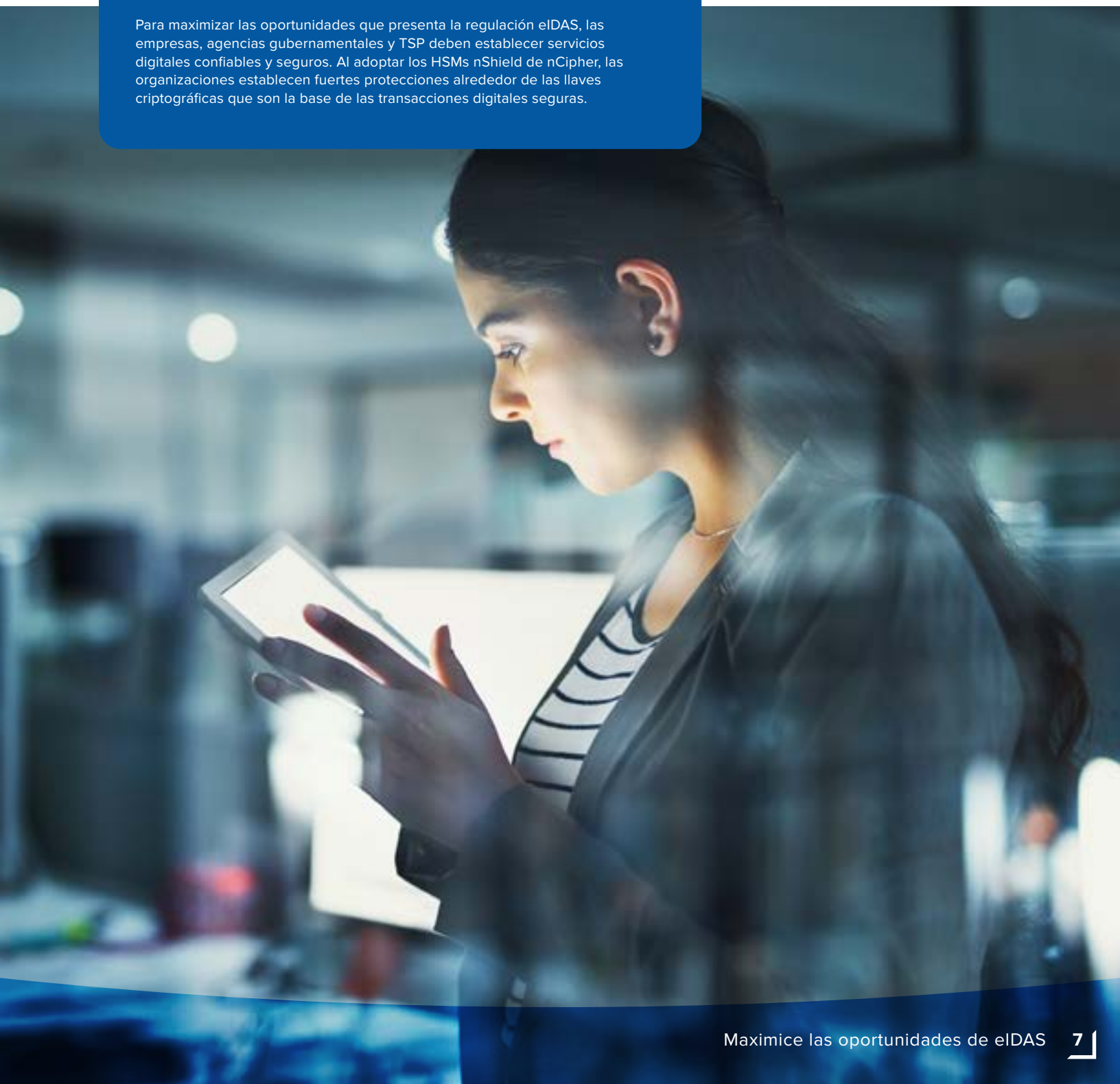
## BENEFICIOS DEL CLIENTE

Cuando se combinan con soluciones integradas para socios, los HSMs nShield ofrecen a las entidades y cuerpos gubernamentales una serie de beneficios convincentes:

- Realizar transacciones comerciales legalmente vinculantes a través de las fronteras
- Extender la digitalización de los servicios, al tiempo que minimiza los riesgos y los costos
- Emplear soluciones integradas y comprobadas que minimicen el tiempo de implementación

# Conclusión

Para maximizar las oportunidades que presenta la regulación eIDAS, las empresas, agencias gubernamentales y TSP deben establecer servicios digitales confiables y seguros. Al adoptar los HSMs nShield de nCipher, las organizaciones establecen fuertes protecciones alrededor de las llaves criptográficas que son la base de las transacciones digitales seguras.



nCipher AN ENTRUST DATACARD COMPANY

www.ncipher.com

## ACERCA DE NCIPHER SECURITY

nCipher Security, una compañía de Entrust Datacard Company, es líder en el mercado de Módulos de seguridad de hardware (HSM) de propósito general, y capacita a las organizaciones líderes a nivel mundial al brindar confianza, integridad y control a sus aplicaciones e información crítica de sus negocios. El entorno digital de rápido movimiento de hoy en día mejora la satisfacción del cliente, brinda una ventaja competitiva y mejora la eficiencia operativa; también multiplica los riesgos de seguridad. Nuestras soluciones criptográficas aseguran tecnologías emergentes como la nube, IoT, blockchain y pagos digitales, y ayudan a cumplir con los nuevos mandatos en materia de cumplimiento. Esto es posible gracias a que usamos la misma tecnología comprobada de la que dependen las organizaciones globales hoy para protegerse contra las amenazas a sus datos confidenciales, comunicaciones de red e infraestructura empresarial. Brindamos confianza para las aplicaciones críticas de su negocio; aseguramos la integridad de sus datos y le damos completo control --hoy, mañana, siempre. www.ncipher.com

Buscar: nCipherSecurity

CONFIANZA. INTEGRIDAD. CONTROL.