# Servicios en la nube seguros de grado federal con ORC y Entrust

PIVotal ID™ de ORC, una solución de identidad federada utilizada por el gobierno de los EE. UU., muestra la manera en que la identidad como servicio (IDaaS) basada en la nube y respaldada por criptografía reforzada ofrece una seguridad sólida y una amplia interoperabilidad.

Para muchas empresas que piensan en trasladar datos confidenciales a la nube, los problemas de seguridad siguen siendo una preocupación importante. Pero una empresa, Operational Research Consultants Inc. (ORC), está demostrando que la nube realmente se puede hacer tan segura o incluso más segura que las implementaciones locales, incluso para organizaciones tan centradas en la seguridad como el gobierno federal de EE. UU.

## ORC - UN PIONERO EN GESTIÓN DE IDENTIDAD FEDERAL

ORC ha sido un socio de confianza del gobierno de EE. UU. desde mediados de la década de 1990, cuando la compañía lanzó la Infraestructura de clave pública de adquisición de la Armada para respaldar interacciones seguras con contratistas y proveedores. A medida que el énfasis del gobierno en la garantía de la información se expandió durante las siguientes dos décadas, ORC se convirtió en un socio de referencia para las soluciones de seguridad y una de las primeras empresas autorizadas para proporcionar soluciones de gestión de identidad que cumplen con las normas gubernamentales.

En la actualidad, ORC administra más de tres millones de identidades y ha emitido más de 10 millones de certificados digitales que cumplen con las normas federales a una variedad de empleados, contratistas, aliados, veteranos y ciudadanos que realizan negocios con el gobierno.

# ORC

## LA NECESIDAD DE IDENTIFICACIÓN Y AUTENTICACIÓN SEGURAS E INTEROPERABLES

En agosto de 2004, la administración Bush emitió una Directiva Presidencial de Seguridad Nacional (HSPD-12) para asegurar las instalaciones y los recursos federales mediante el establecimiento de un estándar para todo el gobierno para formas seguras y confiables de identificación. Más allá de la simple emisión de credenciales de identificación a los empleados del gobierno, esta iniciativa se centraba en los procesos necesarios para emitir credenciales personales seguras, en los métodos para validar esos procesos de emisión y credenciales, así como en la gestión del riesgo y la calidad durante todo el ciclo de vida de las credenciales.

El programa de verificación de identidad personal (PIV) implementa estos procesos y FIPS (Estándar federal de procesamiento de información) 201 especifica la interfaz y los elementos de datos de la tarjeta inteligente PIV. Entre los elementos de datos de una tarjeta PIV se encuentran una o más claves criptográficas privadas asimétricas. Los departamentos y agencias deben utilizar una infraestructura de clave pública (PKI) compatible para emitir certificados digitales a los usuarios. La iniciativa PIV también ha generado otras credenciales de alta seguridad que admiten transacciones específicas de empresa a gobierno, de ciudadano a gobierno y de ciudadano a empresa, al mismo tiempo que respaldan la interoperabilidad federada entre las credenciales emitidas. Estas incluyen varias variantes de PIV-Interoperable (PIV-I) y PIV, tales como: Credencial de identificación de trabajador de transporte (TWIC®), Credenciales de autenticación de personal de primera respuesta (FRAC), Verificación de identidad comercial (CIV) y Autoridad de certificación externa (ECA) PI -I que abordan varios requisitos regulatorios y están diseñados para escalar globalmente. Los procesos y políticas para la emisión de certificados y las protecciones otorgadas a la raíz crítica y las claves de la autoridad certificadora emisora en esa PKI se constituyen como factores críticos en el nivel de garantía general del sistema.

## LOS RETOS: CERTIFICACIÓN, INTEROPERABILIDAD Y CONFIANZA

Los sistemas tradicionales de gestión de identidades locales no se extienden fácilmente a la nube. Al reconocer que la seguridad era un diferenciador importante para que la gestión de identidades basada en la nube fuera confiable en todo el gobierno federal, ORC sabía que la criptografía de alta seguridad era la única forma de cumplir con los requisitos de seguridad de NIST. En el contexto de la PKI, esto significaba que la raíz y las claves de la autoridad certificadora emisora debían generarse y protegerse en hardware de alta seguridad con certificación FIPS. Las razones iban más allá de la simple seguridad sólida: el impacto operativo de comprometer una de estas claves sería que todos los certificados emitidos bajo la PKI tendrían que ser revocados y todas las credenciales deberían volver a emitirse.

ORC también enfrentó múltiples requisitos de certificación y acreditación, incluidos Federal Bridge, PIV/PIV-I, DoD y FISMA y la necesidad de respaldar la certificación cruzada en múltiples niveles, lo que requiere una solución que pueda respaldar una gama flexible de niveles y políticas de garantía. La solución también necesitaba ser comprobada y basada en estándares de sistemas abiertos para asegurar una amplia interoperabilidad. Finalmente, ORC reconoció la importancia de brindar alta disponibilidad y confiabilidad para los servicios criptográficos en un entorno de nube.

# ORC

## LA SOLUCIÓN: ORC PIVOTAL ID™ Y ENTRUST

Con el fin de proporcionar altos niveles de garantía para los servicios federales en la nube,  ORC ofrece un conjunto de soluciones llamado PIVotal ID™. PIVotal ID™ incluye servicios administrados certificados y acreditados para emitir credenciales de identidad sólidas que son confiables en todo el gobierno federal y pueden federarse a nivel mundial, incluida la emisión de certificados digitales de PKI respaldados por módulos de seguridad de hardware (HSMs) nShield® de Entrust de alta confianza. ORC ha emitido y gestiona millones de credenciales compatibles que permiten transacciones seguras para las agencias federales de los EE. UU. (Civil y Defensa), sus empleados, la comunidad de contratación global, socios comerciales, veteranos y ciudadanos que necesitan realizar negocios con cualquier faceta del gobierno de EE. UU. y las industrias reguladas. PIVotal ID™ incluye:

- Verificación de identificación personal (PIV)
- Emisor no federal PIV-Interoperable (NFI PIV-I)
- Autoridad de certificación externa (ECA)
- Certificados de acceso para servicios electrónicos (ACES)
- Autoridad de fabricación certificada TWIC
- PIVotal Commercial™ (PIV-CIV)
- PIVotal Validation™

ORC reconoció que la familia nShield de HSMs de Entrust ofrecía una protección superior y capacidades de aceleración criptográfica, así como la flexibilidad y escalabilidad para proteger y gestionar las claves raíz y todas las claves subordinadas dentro de su infraestructura segura de servicios en la nube.

## SOLUCIONES RENTABLES PARA CRIPTOGRAFÍA ROBUSTA

Los HSMs nShield de Entrust se basan en una plataforma reforzada y resistente a manipulaciones indebidas que protege y gestiona las claves confidenciales utilizadas para el cifrado y la firma digital para admitir prácticamente cualquier aplicación, desde la gestión de identidades, los servicios web y el cifrado de bases de datos hasta la tokenización, los servicios de PKI y la autenticación sólida. Los HSMs nShield ofrecen la forma más rentable de establecer los niveles adecuados de controles físicos y lógicos para los sistemas en los que la seguridad que ofrece la criptografía basada en software se considera inadecuada.

# ORC

## CONFIAR EN HSMs NSHIELD LE PERMITE A LAS EMPRESAS:

- Lograr una flexibilidad operativa, alta disponibilidad y escalabilidad inigualables en entornos virtualizados y en la nube.
- Reducir el coste de cumplimiento con la normativa y las tareas cotidianas de gestión de claves, tales como las copias de seguridad y la gestión remota.
- Obtener una continuidad empresarial de alta seguridad con una inscripción simplificada a un HSM, un aprovisionamiento eficaz de claves y funciones de hardware totalmente resistentes.
- Mejorar la seguridad para aplicaciones críticas protegiendo las claves criptográficas y las operaciones dentro del hardware a prueba de manipulaciones.
- Establecer una fuerte separación de funciones y controles duales a través de políticas de administración sólidas que incluyen autenticación multifactor basada en roles y la autorización basada en quórum flexible.

## ACERCA DE ORC

ORC, una empresa de WidePoint y socio de confianza del gobierno federal de los EE. UU., ofrece soluciones de seguridad de la información a clientes gubernamentales y empresariales, lo cual garantiza el intercambio y la garantía de la información totalmente compatible y confiable. Como proveedor de élite de servicios de autenticación y garantía de la información para empresas a gobiernos, de gobiernos a gobiernos y de ciudadanos a gobiernos, las soluciones de ORC son interoperables con los sistemas heredados y se integran a la perfección con todas las aplicaciones de software líderes en el mercado. ORC aprovecha los HSMs nShield de Entrust para proporcionar servicios de administración de identidad en la nube con seguridad de grado federal.

## ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Aprenda más en
**entrust.com/HSM**

ENTRUST

**Contacte con nosotros:**
**HSMinfo@entrust.com**