Infraestructura de clave pública (PKI) Caso de Uso

Planifique la implementación o actualización de su PKI empresarial

CARACTERÍSTICAS PRINCIPALES

- El análisis experto de sus requisitos, anhelos, limitaciones y prioridades define un enfoque práctico y rentable para la implementación o actualización de su PKI
- Décadas de experiencia con PKIs le permiten a Entrust ofrecer opciones y recomendaciones bien estudiadas para el diseño, la política y la gobernanza de PKIs, así como una hoja de ruta de implementación para satisfacer sus necesidades comerciales y de seguridad.
- Seguridad mejorada a través del diseño en los módulos de seguridad de hardware (HSMs) de Entrust comprobados en miles de unidades implementadas a nivel mundial

Muchas empresas cuentan con una infraestructura de clave pública (PKI) para proporcionar certificados digitales y así proteger sus activos más importantes, La PKI se utiliza para una amplia variedad de fines, tales como la autenticación, la firma digital y el cifrado.

La dependencia de la PKI empresarial generalmente aumenta con el tiempo, a menudo se expande más allá de los propósitos para los que se creó originalmente y surgen nuevos requisitos para la PKI. Es importante que la PKI pueda proporcionar el nivel de garantía necesario para cumplir con su función de seguridad crucial y que sea capaz de sustentar los requisitos actuales y futuros esperados de la organización.

La actualización de la PKI empresarial o la implementación de una nueva PKI empresarial requiere del análisis de los casos de uso, los requisitos de seguridad, la compatibilidad de sistemas, los planes y deseos corporativos, así como los requisitos en materia de cumplimiento.

Embarcarse en un proyecto PKI puede resultar abrumador debido a la variedad de opciones y posibilidades. El equipo de servicios profesionales (PS) de Entrust puede ayudarlo a determinar los requisitos de seguridad, técnicos y operativos para planificar su proyecto de implementación o actualización.

Caso de Uso de la PKI

Características principales

Un consultor de Servicios Profesionales (PS) de Entrust realizará las siguientes funciones como parte del Estudio de alcance de la PKI

- Analizar sus casos de uso de la PKI
- Comprender los requisitos y las limitaciones de su PKI y su PKI empresarial actual (de ser el caso)
- Evaluar los riesgos de seguridad de los sistemas que dependen de la PKI y, por lo tanto, el nivel de seguridad necesario para la PKI.
- Analizar los requisitos y las opciones de transición de la PKI
- Elecciones recomendadas
- Desarrollar un diseño de PKI con un alto nivel de recomendaciones
- Crear una hoja de ruta para un proyecto (o proyectos) de implementación de la PKI

El proceso de estudio de alcance de la PKI

Antes del comienzo del estudio, Entrust establecerá un Acuerdo de no divulgación (NDA) mutuo para proteger su información y la de Entrust para permitir una discusión abierta detallada.

El estudio de alcance de PKI se lleva a cabo en tres fases.

Fase 1: Recopilación de información

El consultor visitará su sitio para recopilar información a través de reuniones y talleres con sus principales interesados. Esto se guiará por los cuestionarios detallados de Entrust. La experiencia muestra que esto es más efectivo que proporcionar cuestionarios para que las organizaciones los completen en ausencia de discusiones y explicaciones.

Como opción, los cuestionarios se pueden proporcionar por adelantado, para luego revisarlos en detalle con su equipo y el consultor de Entrust en reuniones.

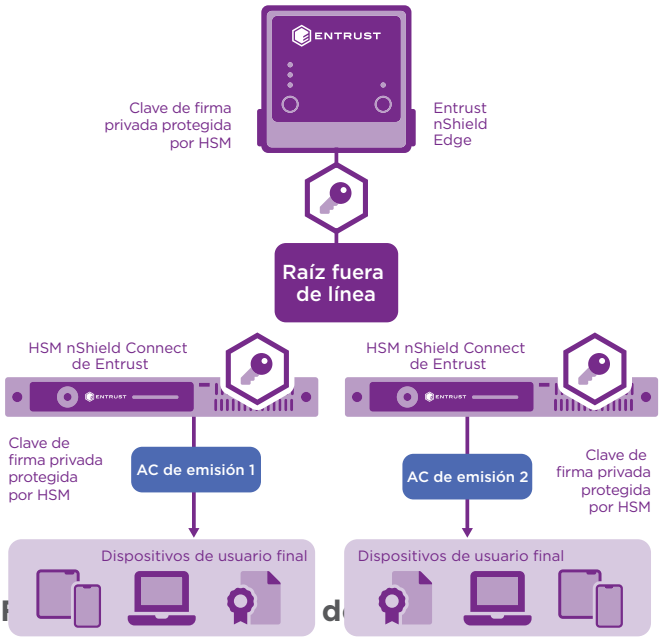
Finalmente, toda la información recabada durante esta fase irá incluida en el informe que le dará su asesor.

Fase 2 - Análisis e informe

El consultor analizará los datos recopilados durante la Fase 1, realizará un seguimiento con correos electrónicos y llamadas telefónicas para cualquier aclaración necesaria, luego producirá un informe que detalla:

- Casos de uso de la PKI
- Entornos actuales
- Requisitos para la PKI
- Diseño y recomendaciones de PKI de alto nivel
- Hoja de ruta de implementación

La solución se diseñará en función de la opción más adecuada de software de PKI y utilizando HSMs de Entrust para la protección de las claves privadas.



Caso de Uso de la PKI

El consultor presentará los hallazgos del estudio de alcance en una presentación de gestión en el sitio, luego finalizará el informe teniendo en cuenta los comentarios.

HSMs de Entrust

Los HSMs nShield® de Entrust se encuentran entre las soluciones de HSMs de mayor rendimiento, más seguras y fáciles de integrar que se encuentran disponibles, lo cual facilita el cumplimiento normativo y ofrece los niveles más altos de seguridad de datos y aplicaciones para organizaciones empresariales, financieras y gubernamentales.

Nuestra exclusiva arquitectura de administración de claves Security World proporciona controles sólidos y granulares sobre el acceso y uso de claves.

Más información

Para saber más sobre los HSMs nShield de Entrust visite **entrust.com/HSM**. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Para saber más sobre los HSMs nShield de Entrust

HSMinfo@entrust.com

entrust.com/HSM

SOBRE ENTRUST CORPORATION

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