INFOTECH
secure identity and payments

X Infotech Government:

Soluciones De Infraestructura De Clave Publica (PKI)

- X Infotech Country Signing Certification Authority (CSCA)
- X Infotech Document Signer (DS)
- X Infotech Country Verifying Certification Authority (CVCA)
- X Infotech Document Verifier (DV)
- X Infotech Terminal Control Center (TCC)
- X Infotech Single Point of Contact (SPOC)
- X Infotech National Public Key Directory (nPKD)

INFOTECH
secure identity and payments

Términos Y Definiciones

PKI (Infraestructura de Clave Pública) - es un conjunto de políticas y procedimientos necesarios para crear, administrar, distribuir, utilizar, almacenar y revocar los certificados digitales y administrar el cifrado de clave pública.

BAC (Control de Acceso Básico) - es un mecanismo específico para garantizar que sólo las partes autorizadas puedan leer de forma inalámbrica información personal de los pasaportes con un chip RFID. Permite que el sistema de chips compruebe que el documento está abierto para su inspección. Los datos sensibles (por ejemplo, biométricos) en este documento no están protegidos.

EAC (Control de Acceso Ampliado) - es un conjunto de características avanzadas de seguridad para pasaportes electrónicos que protegen y restringen el acceso a datos personales sensibles (por ejemplo, biométricos) contenidos en el chip RFID. Permite al chip comprobar que el Sistema de Inspección (IS) se encuentra autorizado a leer datos confidenciales.

ICAO (Organización de Aviación Civil Internacional) - es un organismo especializado de las Naciones Unidas. La OACI normaliza los pasaportes legibles por máquina en todo el mundo. El Documento 9303 contiene las especificaciones actuales de la OACI para los pasaportes, visados y tarjetas de identificación legibles por máquina ("documentos de viaje") utilizados para cruzar las fronteras.

Los lineamientos técnicos BSI especifican los mecanismos de seguridad para los Documentos de Viaje Electrónicos de Lectura Mecánica (eMRTD). Estas especificaciones constituyen la base técnica de los pasaportes electrónicos europeos y de las licencias de conducir electrónicas, y figuran en el Informe Técnico 03110 elaborado por la Oficina Federal Alemana de Seguridad de la Información (BSI).

Soluciones PKI De X Infotech

Las soluciones de Infraestructura de Clave Pública de X Infotech son componentes que facilitan la producción segura y verificación fiable de documentos eID en las fronteras, asegurando una integración fluida con diferentes componentes y sistemas de terceros. Las soluciones se pueden adaptar fácilmente a los cambios actuales o futuros en los negocios.

X Infotech proporciona una gama completa y segura de soluciones EAC-PKI según sea necesario para la emisión y verificación de documentos electrónicos ePassport o eID de la OACI.
Los procesos de infraestructura PKI pueden segmentarse de forma lógica en fases:

1. Producción de documentos
2. Identidad y verificación de documentos
3. Gestión de certificación entre países

Con el fin de producir y verificar de forma segura pasaportes electrónicos, se necesita una infraestructura de clave pública confiable. Para la producción de documentos, la solución consta de los siguientes módulos: Firmante Documentario (Document Signer (DS)), Country Signing Certification Authority (Autoridad de Certificación de Firma de País (CSCA)) y Country Verifying Certification Authority (Autoridad de Certificación de Verificación de País (CVCA)). Otros componentes de Infraestructura de Clave Pública, Document Verifier (Verificador de Documentos (DV)) y Terminal Control Centre (Centro de control de terminales (TCC)), permiten la creación de un entorno seguro para el acceso a datos de documentos en modo EAC (por ejemplo, lectura de huellas dactilares de ePassort o eID durante la verificación de identidad en zonas fronterizas). Con el fin de proporcionar la gestión de certificados entre países, se utilizan los componentes National Public Key Directory (Directorio Nacional de Claves Públicas (nPKD)) y Terminal Control Center (Punto de Contacto Único (SPOC)).

Produccion Documentaria

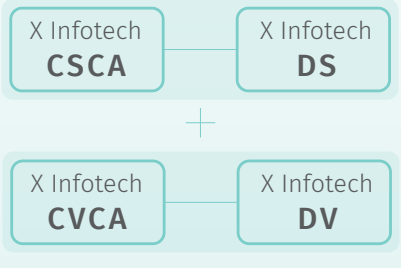
Los componentes PKI proporcionados por X Infotech crean un entorno confiable para la producción de documentos ePassport y eID en conformidad con OACI y habilitados con EAC (Control de Acceso Ampliado) para asegurar la información biométrica de un individuo almacenada en el chip.
Document Signer (Firmante Documentario (DS)) firma documentos con certificados emitidos por CSCA - la autoridad de certificación madre para la verificación de autenticidad de documentos. CSCA emite certificados del firmante de documentos y delega la firma de documentos a un firmante de documentos. El chip del ePassport también almacena el certificado de Country Verifying Certification Authority (Autoridad de Certificación de Verificación de País (CVCA)), que se utiliza para la Autenticación de Terminal.

El nivel básico de protección (control de acceso básico, BAC) permite a las entidades autorizadas acceder y leer datos no sensibles.

Ambiente BAC
(Control de Acceso Básico)

El nivel de protección ampliado (control de acceso ampliado, EAC) permite a las entidades acceder y leer datos sensibles, incluyendo datos biométricos (huellas digitales, escaneo del iris, etc.)

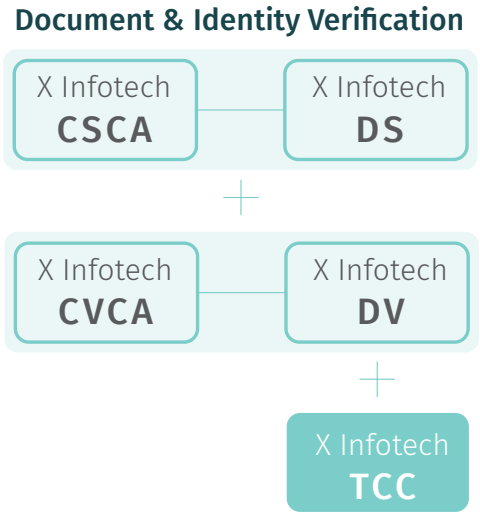
Ambiente EAC
(Control de Acceso Ampliado)



Verificacion Documentaria Y De Identificacion

ICAO PKD (Directorio de Claves Públicas de la OACI) es la plataforma central para la gestión del intercambio global de certificados y listas de revocación de certificados. Estos certificados y listas de revocación de certificados se utilizan para verificar la firma electrónica de los datos contenidos en el chip RFID de los ePassports y otros eMRTD.

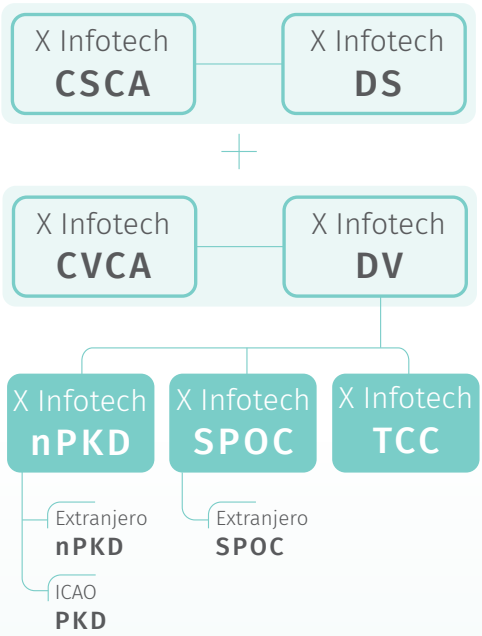
Durante la verificación del documento, el Sistema de Inspección (IS) envía un Certificado de Inspección del Sistema, proporcionado por Document Verifier (Verificador de Documentos (DV)), al chip del ePassport, permitiendo así al chip verificar el Certificado de Inspección del Sistema. Para asegurar que el certificado enviado por el Sistema de Inspección es genuino, el chip envía un número al azar al sistema.
El número es firmado por el Sistema de Inspección y devuelto al chip, el cual luego verifica este número. Cuando todos los pasos logran completarse con éxito, el ePassport autoriza el acceso a los datos protegidos por EAC.



Gestion De Certificacion Entre Paises

El componente nPKD establece una infraestructura confiable para la gestión de certificados entre países para ePassports y eID. National Public Key Directory (Directorio Nacional de Claves Públicas (nPKD)) se comunica con el ICAO PKD (Directorio de Claves Públicas de la OACI), luego recoge y almacena certificados de CSCA y DS además de listas de revocación de países de todo el mundo. nPKD distribuye estos certificados a las terminales de verificación de documentos, permitiéndoles verificar la autenticidad de los documentos emitidos por las autoridades locales u otros países.

SPOC establece una infraestructura confiable en la gestión de certificados entre países para ePassports y eID. SPOC facilita el intercambio entre el Verificador Documentario (DV) nacional y Verificador Documentario (DV) extranjero, otorgando autorización para acceder a la biometría compatible con la OACI para autenticación de terminal (necesaria para el acceso a un documento en modo EAC) en puntos de control fronterizo y otros dispositivos de verificación biométrica de identidad.



Terminos Y Definiciones

Autenticación Pasiva - es un protocolo BAC diseñado contra manipulación y falsificación de documentos. El Sistema de Inspección lee el código MRZ del documento y firma electrónica, confirmando que los datos del chip son auténticos y no han sido cambiados.

Autenticación de Terminal - es un protocolo EAC que se utiliza para determinar si el sistema de inspección (IS) se encuentra autorizado a leer datos confidenciales del pasaporte electrónico. El mecanismo se basa en certificados digitales que vienen en un formato de certificados verificables por tarjeta.

Sistema de inspección (IS) - es un o un grupo de dispositivos de hardware diseñados para la verificación de documentos (por ejemplo, lectoras y escáners de ePassport / eID en control de fronteras, eGates, etc.)

HSM (Módulo de Seguridad Hardware) es un dispositivo de hardware que almacena y gestiona claves digitales para la autenticación, así mismo proporciona criptoprocesamiento.

INFOTECH
secure identity and payments

Descripcion De Soluciones De Infraestructura De Clave Publica (PKI) X Infotech

X Infotech
CSCA

Country Signing Certification Authority (Autoridad de Certificación de Firma de País (CSCA)) proporcionado por X Infotech establece un punto de confianza de PKI nacional en el contexto de documentos electrónicos. La CSCA emite certificados de clave pública para uno o más firmantes de documentos y, opcionalmente, para otras entidades como los Firmantes de Listas Maestras. Así también, almacena las claves privadas en el dispositivo criptográfico HSM y opera en un entorno altamente protegido de cualquier acceso externo o no autorizado al entorno de la red.

Características:
- Certificados CSCA y perfiles clave de conformidad con la especificación IOACI 9303
- Generación y protección de pares de claves por dispositivos criptográficos HSM
- Interfaz gráfica de usuario para la configuración, gestión y auditoría
- Soporta varios CSCA especiales para diferentes tipos de documentos
- Políticas flexibles de control de acceso de usuario (m-of-n)

X Infotech
DS

Document Signer (Firmante Documentario (DS)) es un componente de solución PKI que firma digitalmente los datos de documentos electrónicos. La firma digital DS asegura la integridad y autenticidad del documento. A su vez, se valida mediante un certificado CSCA durante la autenticación pasiva para confirmar que los datos del chip son auténticos para el estado emisor.

Características:
- Los certificados DS y perfiles clave cumplen plenamente con la especificación OACI 9303
- Generación y protección de pares de claves por dispositivos criptográficos HSM
- Interfaz gráfica de usuario para la configuración, gestión y auditoría
- Integración con la solución de personalización para simplificar la infraestructura y reducir costos

---

X Infotech
CVCA

Country Verifying Certification Authority (Autoridad de Certificación de Verificación de País (CVCA)) es un punto de confianza PKI nacional que autoriza a Document Verifiers (Verificador de Documentos (DV)) tanto nacional como extranjero a acceder a los datos sensibles de los documentos electrónicos como huellas digitales o biometría del iris.
CVCA almacena las claves privadas en el dispositivo criptográfico HSM y opera en un entorno fuera de línea altamente protegido de cualquier acceso externo o no autorizado.

Características:
- Los certificados y perfiles claves CVCA cumplen en su totalidad con los lineamientos técnicos BSI TR03110.
- Generación y protección de pares de claves por dispositivos criptográficos HSM
- Interfaz gráfica de usuario para la configuración, gestión y auditoría
- Políticas flexibles de control de acceso de usuario (m-of-n)

X Infotech
DV

Document Verifier (Verificador de Documentos (DV)) es el componente de solución PKI que determina qué Sistema de Inspección (IS) obtendrá autorización para leer datos sensibles como huellas dactilares o biometría de iris de los documentos electrónicos con protección Control de Acceso Ampliado (EAC).
Document Verifier solicita y obtiene estos certificados de la CVCA de cada país para cuyos documentos electrónicos el Verificador Documentario está autorizado a acceder.
DV emite certificados del Sistema de Inspección en respuesta a las solicitudes de certificación de los Sistemas de Inspección.
Estos certificados autorizan al Sistema de Inspección a acceder a los datos confidenciales protegidos en los chips de documentos electrónicos.

Características:
- Los certificados y perfiles claves DV cumplen con los lineamientos establecidos por BSI-EAC y BSI TR-03139
- Funciona de acuerdo con los protocolos BSI TR-03129
- Generación y protección de pares de claves por dispositivos criptográficos HSM
- Interfaz gráfica de usuario para la configuración, gestión y auditoría

INFOTECH
secure identity and payments

X Infotech TCC

Terminal Control Center (Centro de control de terminales (TCC)) automatiza la verificación de documentos de viaje legibles por mecanismos nacionales y extranjeros (MRTD) tanto por sistemas de inspección de control de fronteras manuales como totalmente automatizados.

TCC proporciona un servicio de Autenticación de Terminal de Documentos (TA) que permite a los Sistemas de Inspección acceder a los datos personales sensibles (huellas dactilares, iris) en el chip de documentos y utilizar mecanismos avanzados de autenticación biométrica. El mecanismo se basa en la integración con el sistema de Document Verifier (Verificador de Documentos), que emite certificados verificables de tarjeta que son válidos sólo por un período corto, por lo general entre 1 día y 1 mes.
Además, la solución de tipo TCC proporciona el servicio de autenticación de documento pasivo para verificar la autenticidad del documento comparando el certificado del documento con los certificados recibidos del ICAO PKD (Directorio de Claves Públicas del ICAO) o de PKD nacional (Directorio de Claves Públicas Nacional).

La solución cumple con los estándares y lineamientos ICAO y BSI, permitiendo una fácil integración con los sistemas particulares. Apoya el despliegue centralizado, cuando un TCC actúa como punto central de distribución de certificados en todo el país, o cuando las instancias de TCC se encuentran descentralizadas y localizadas en lugares remotos como aeropuertos, puertos marítimos o puntos fronterizos.

X Infotech SPOC

Single Point of Contact (Punto de Contacto Único (SPOC)) proporcionado por X Infotech gestiona el intercambio de certificados CVCA entre diversos países con el fin de conceder acceso a datos biométricos sensibles en los Documentos EAC en conformidad con la OACI en los puntos de control fronterizos.
La arquitectura en base a PKI de Control de Acceso Ampliado (EAC) es actualmente el estándar más avanzado en documentos de viaje seguro.
SPOC implementa estándares internacionales, protocolo y gestión de certificación para los pasaportes electrónicos EAC con el fin de intercambiar certificados de Document Verifier (Verificador de Documentos (DV)) entre países. La solución cumple con los estándares y lineamientos de la OACI y BSI, lo que facilita la operación e integración con sistemas particulares.

Características:
- Integración en línea y manual con los sistemas de Document Verifier (Verificador de Documentos (DV)) PKI para la gestión de certificados DV.
- Integración con los Sistemas de Country Verifying Certification Authority (Autoridad de Certificación de Verificación de País (CVCA) PKI ara firma de certificados DV.
- Integración completa con los productos X Infotech
- Comunicación en línea con los Sistemas SPOC extranjeros para intercambio de datos
- La interfaz con el sistema SPOC extranjero se encuentra protegida bajo certificación SPOC CA
- Protección TLS para interfaces de sistema
- Cumplimiento de las normas internacionales BSI TR-03129, ICOA 9303 y CSN 36 9791: 2009
- Control de Acceso a través de perfiles de usuario (Operador, Administrador, Auditor, Autoridad de Registro)
- Registro de auditoría para eventos del sistema.

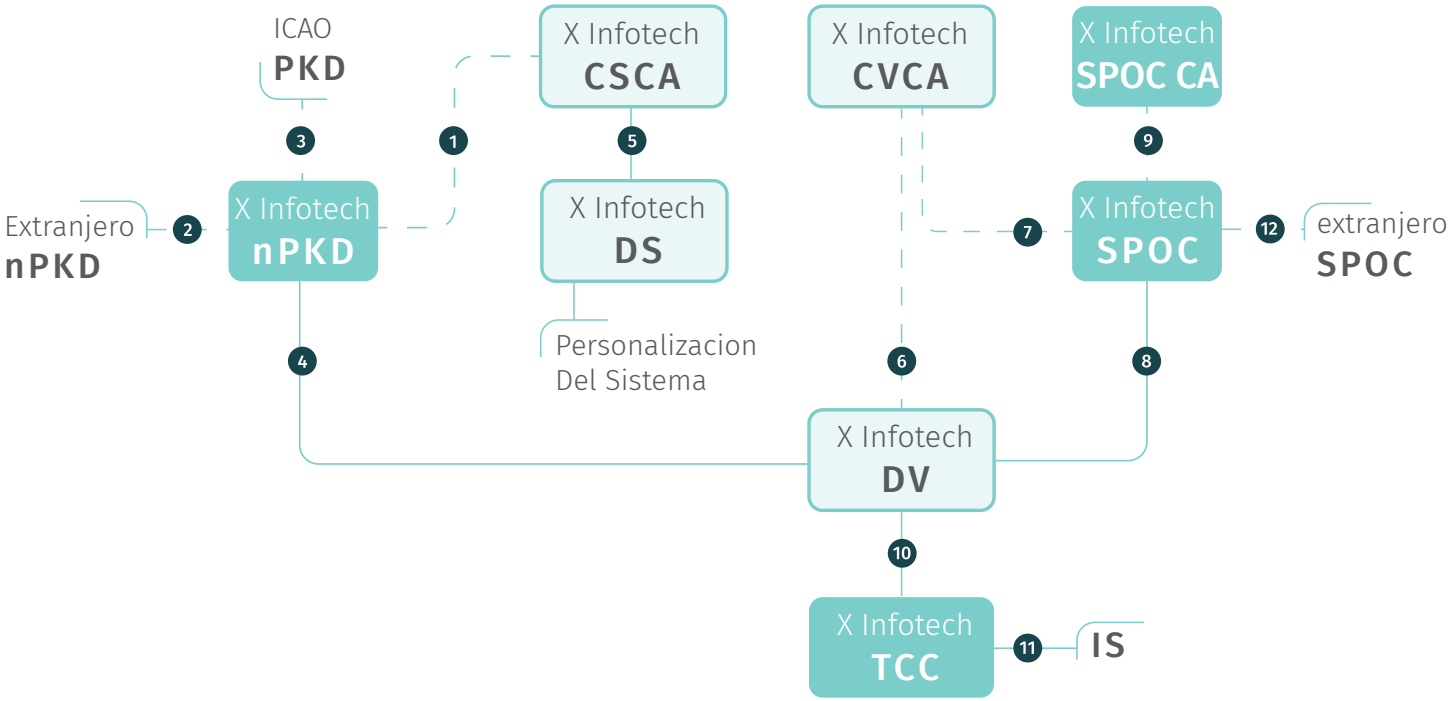
X Infotech nPKD

National Public Key Directory (Directorio Nacional de Claves Públicas (nPKD)) ideado por X Infotech, es un componente de solución PKI que administra certificados electrónicos de documentos PKI a nivel nacional.

Funciona como intermediario central para gestionar el intercambio de certificados de documentos PKI y listas de revocación de certificados a nivel de país. Crea una base de datos centralizada de certificados de documentos recibidos de múltiples fuentes como Country Signing Certification Authority (Autoridad de Certificación de Firma de País (CSCA)), ICAO PKD (Directorio de Claves Públicas de la OACI) y los sistemas nPKD extranjeros.

INFOTECH
secure identity and payments

Flujo De Trabajo Para Soluciones De Infraestructura De Clave Pública (PKI)



1. nPKD se conecta con CSCA para firmar el certificado de la Lista Maestra y recibe los certificados de DS y CSCA. El intercambio de datos se realiza en modo manual.
2. nPKD se conecta con nPKD Extranjero para recibir certificados de PKD DS y CSCA de países no pertenecientes a la OACI. El intercambio de datos se realiza en modo manual.
3. nPKD se conecta con la PKD de la OACI para recibir los Archivos PKD de la OACI y enviar certificados al PKD de la OACI.
4. DV se conecta con nPKD para recibir Certificados para la autenticación pasiva.
5. DS interactúa con CSCA para firmar los certificados DS. El intercambio de datos se realiza en modo manual.
6. DVCA interactúa con CVCA para firmar los certificados DV. El intercambio de datos se realiza en modo manual.
7. SPOC interactúa con CVCA para firmar DV y otras peticiones de certificado enviadas y recibidas de SPOC Extranjero
8 DV se conecta con SPOC para recibir Certificados DV firmados.
9. SPOC interactúa con SPOC CA para recibir el certificado que protege SPOC así mismo se conecta con SPOC Extranjero. El intercambio de datos se realiza en modo manual.
10. TCC se interconecta con DV para firmar certificados IS que se requieren para la autenticación de terminal (TA). De esta manera, TCC también recibe los certificados para la autenticación pasiva.
11. SPOC se interconecta con SPOC Extranjero para enviar / recibir mensajes y certificados.
12. IS se conecta con TCC para realizar la autenticación pasiva y terminal.