INFOTECH
secure identity and payments

X Infotech Government: PKI Solutions

- 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

Terms and Definitions

PKI (Public Key Infrastructure) – is a set of policies and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

BAC (Basic Access Control) – is a mechanism specified to ensure only authorized parties can wirelessly read personal information from passports with an RFID chip. Enables the chip system to verify that the document is opened for inspection. The sensitive (e.g. biometric) data of a document holder is not protected.

EAC (Extended Access Control) – is a set of advanced security features for electronic passports that protects and restricts access to sensitive (e.g. biometric) personal data contained in the RFID chip. Enables the chip to verify that the Inspection System (IS) is authorized to read sensitive data.

ICAO (The International Civil Aviation Organization) – is a specialized agency of the United Nations. ICAO standardizes Machine-Readable Travel Documents (MRTDs) worldwide. The Document 9303 contains ICAO specifications for machine-readable passports, visas and ID cards ("travel documents") used in crossing the borders.

BSI – Electronic Machine-Readable Travel Documents (eMRTDs) refer to BSI technical guidelines describing security mechanisms. These specifications are the technical basis for European ePassports and electronic Driving Licenses, and are listed in the Technical Report 03110 developed by German Federal Office for Information Security, BSI.

PKI solutions of X Infotech

X Infotech PKI solutions are infrastructure components that facilitate the secure production and reliable verification of eID documents on borders, ensuring smooth integration with different third-party components and systems. The solutions can be easily adapted to ongoing or future changes in business.

X Infotech provides a full, secure range of EAC-PKI solutions as required for ICAO compliant ePassport or eID document issuance and verification.

The PKI infrastructure processes can be logically segmented into phases:
1. Document Production
2. Identity and Document Verification
3. Inter-country Certificate Management

In order to securely produce and verify e-Passports, reliable Public Key Infrastructure is needed. For document production the solution comprises the following modules: Document Signer (DS), Country Signing Certification Authority (CSCA) and Country Verifying Certification Authority (CVCA). Other PKI infrastructure components, Document Verifier (DV) and Terminal Control centre (TCC), enable the creation of a secure environment for document data access in EAC mode (e.g. fingerprint reading from ePassort or eID during identity verification at the Border). In order to provide inter-country certificate management, National Public Key Directory (nPKD) and Single Point of Contact (SPOC) components are used.

Document Production

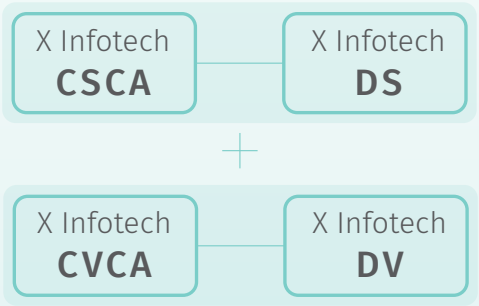
PKI components provided by X Infotech create a reliable environment for ICAO compliant ePassport and eID document production with enabled EAC (Extended Access Control) for securing an individual's biometric information stored on the chip. Document Signer signs documents with certificates issued by CSCA – the root certification authority for document authenticity verification. CSCA issues Document Signer certificates and delegates signing of documents to a Document Signer. The ePassport chip also stores the Country Verifying Certification Authority (CVCA) certificate, which is used for Terminal Authentication.

The **basic protection level** (basic access control, BAC) permits authorized entities to access and read non-sensitive data.

BAC environment
(Basic Access Conrol)

The **extended protection level** (extended access control, EAC) permits entities to access and read sensitive data, including biometrics (fingerprints, iris scans, etc.)

EAC environment
(Extended Access Conrol)



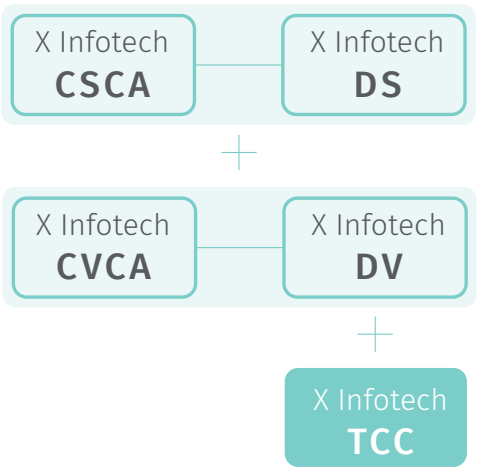
INFOTECH
secure identity and payments

Document and Identity Verification

The ICAO PKD is the central platform for management of global exchange of certificates and certificate revocation lists. These certificates and certificate revocation lists are used to verify the electronic signature of data contained in the RFID chip of ePassports and other eMRTD.

During document verification, the Inspection System (IS) sends an Inspection System certificate, together with Document Verifier certificate provided by the Document Verifier (DV), to the ePassport chip - thus enabling the chip to verify the Inspection System certificate. To ensure that the Inspection System has an appropriate private key, the chip sends a random number to the IS. The number is signed by the Inspection System and returned to the chip, which then verifies this number. When all steps are successful, the ePassport authorizes access to the EAC protected data.

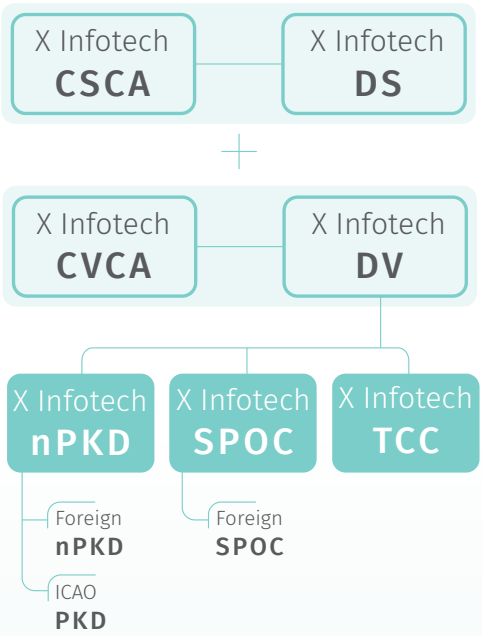
Document & Identity Verification



Inter-country Certificate Management

The component nPKD establishes reliable infrastructure for inter-country certificate management for ePassports and eID. The nPKD certificate directory communicates with ICAO PKD, then collects, stores CSCA and DS certificates and revocation lists from countries all over the world. nPKD distributes these certificates to document verification terminals allowing them to verify the authenticity of documents, issued by local authorities or other countries.

SPOC establishes a reliable infrastructure in inter-country certificate management for ePassports and eID. SPOC facilitates an exchange of EAC certificates, granting authorization to access ICAO compliant biometrics for terminal authentication (required for access to a document in EAC mode) at border control points and other identity biometrical verification devices.



Terms and Definitions

Passive Authentication – is a BAC protocol designed against document counterfeit and manipulation. The Inspection System reads the document MRZ-code and electronic signature, veryfying that the chip data is authentic and has not been changed.

Terminal Authentication – is a EAC protocol which is used to determine whether the inspection system (IS) is allowed to read sensitive data from the electronic document. The mechanism is based on digital certificates which come in the format of card verifiable certificates.

Inspection System (IS) – is one or a group of hardware devices designed for document verification (e.g. border control ePassport/eID readers and scanners, eGates, etc.)

HSM (Hardware Security Module) is a hardware device that stores and manages digital keys for authentication and provides cryptoprocessing.

INFOTECH
secure identity and payments

X Infotech PKI Solutions description

X Infotech **CSCA**

X Infotech Country Signing Certification Authority (CSCA) establishes a national PKI trust point in the context of electronic documents. The CSCA issues public key certificates for one or more Document Signers and optionally for other entities such as Master List Signers. The CSCA stores private keys in HSM cryptographic device and operates in a highly protected from any outside or unauthorized access offline environment.

Features:
- CSCA certificates and key profiles are compliant to ICAO 9303 specification
- Key Pair generation and protection by HSM cryptographic devices
- Graphical User Interface for configuration, management and auditing
- Supports multiple CSCA dedicated to different document types
- Flexible User Access Control policies (m-of-n)

X Infotech **DS**

X Infotech Document Signer (DS) is a PKI solution component that digitally signs data on electronic documents. The DS digital signature ensures integrity and authenticity of the document. In turn it is validated using a CSCA certificate during Passive Authentication to confirm the chip data is authentic to the issuing state.

Features:
- DS certificates and key profiles are in full compliance with ICAO 9303 specification
- Key Pair generation and protection by HSM cryptographic devices
- Graphical User Interface for configuration, management and auditing
- Integration with Personalisation Solution to simplify infrastructure and reduce cost

---

X Infotech **CVCA**

X Infotech Country Verifying Certification Authority (CVCA) is a national PKI trust point that authorises domestic and foreign Document Verifiers (DVs) to access the sensitive data from the electronic documents like fingerprints or iris biometrics to which access is protected via Extended Access Control (EAC).

The CVCA stores private keys in HSM cryptographic device and operates in an offline environment highly protected from any outside or unauthorized access.

Features:
- CVCA certificates and key profiles are in full compliance with BSI TR03110 technical guidelines
- Key Pair generation and protection by HSM cryptographic devices
- Graphical User Interface for configuration, management and auditing
- Flexible User Access Control policies (m-of-n)

X Infotech **DV**

X Infotech Document Verifier (DV) is the PKI solution component that determines which Inspection System (IS) will get authorization to read sensitive data like fingerprints or iris biometrics from the electronic documents with Extended Access Control (EAC) protection.

Document Verifier requests and obtains Document Verifier certificates from the CVCA of each country whose electronic documents the Document Verifier is authorised to access.

DV issues Inspection System certificates in response to certificate requests from Inspection Systems. These certificates authorise the Inspection System to access protected sensitive data on electronic document chips.

Features:
- DV certificates and key profiles are in compliance with BSI-EAC and BSI TR-03139
- Operates in compliance with BSI TR-03129 protocols
- Key Pair generation and protection by HSM cryptographic devices
- Graphical User Interface for configuration, management and auditing

INFOTECH
secure identity and payments

X Infotech TCC

X Infotech Terminal Control Centre (TCC) solution automates the verification of National and Foreign Machine Readable Travel Documents (MRTD) both by manual and fully automated Border Control Inspection Systems.

TCC provides Document Terminal Authentication (TA) service that allows Inspection Systems to access the sensitive personal data (fingerprints, iris) on the documents chip and to use advanced mechanisms of biometric authentication. The mechanism is based on the integration with Document Verification (DV) system, that issues card verifiable certificates that are valid only for a short time period, typically between 1 day and 1 month.

Additionally, TCC solution provides Document Passive Authentication service to verify the authenticity of the document by comparing the Document Signer certificate to certificates received from the ICAO PKD or National PKD.
The solution is compliant with ICAO and BSI standards and guidelines, allowing easy integration with third party systems. Supports centralised deployment, when one TCC acts as a central certificate distribution point all over the country, or when TCC instances are decentralised and located at remote locations like Airports, Seaports or Border points.

X Infotech SPOC

X Infotech Single Point of Contact (SPOC) manages the exchange of CVCA certificates between various countries in order to grant access to sensitive biometric data on ICAO compliant EAC Documents at border control points.
Extended Access Control (EAC) PKI architecture is currently the most advanced standard in secure travel documents.

SPOC implements international standards, protocol and certificate management for EAC ePassports in order to exchange Document Verifying (DV) in order to exchange Document Verifying (DV) and Country Signing Certification Authority (CVCA) certificates between countries. The solution is compliant with ICAO and BSI standards and guidelines, allowing ease operation and integration with third party systems.

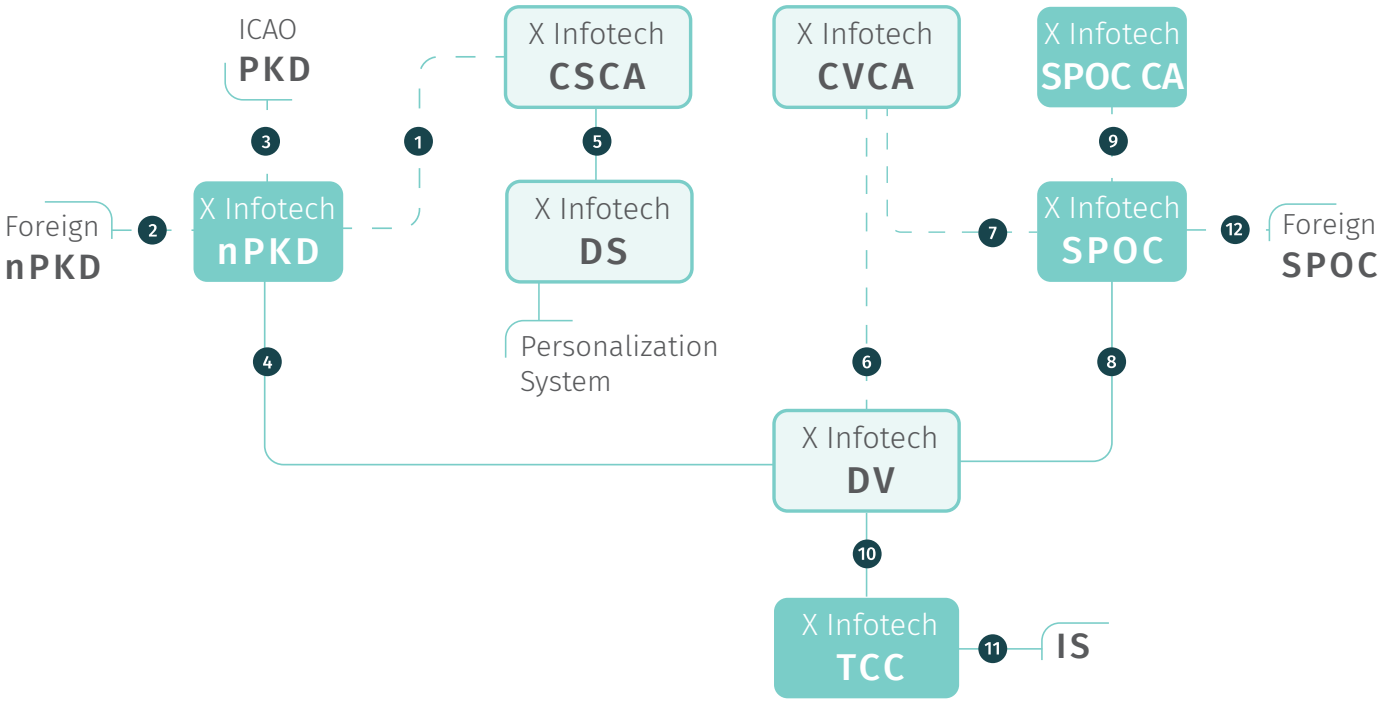
Features:
- Online and manual Integration with the PKI Document Verifier (DV) Systems for management of DV certificates.
- Integration with the PKI Country Verifying Certification Authority (CVCA) Systems for signing DV certificates.
- Complete build-in integration with X Infotech products
- Online communication with Foreign SPOC Systems to exchange the data
- Interface to foreign SPOC system is protected by SPOC CA certificate
- TLS protection for system interfaces
- Compliance with international standards BSI TR-03129, ICOA 9303 and CSN 36 9791:2009
- Access Control through user profiles (Operator, Administrator, Auditor, Registration Authority)
- Audit logging for system events.

X Infotech nPKD

X Infotech National Public Key Directory (nPKD) is a PKI solution component that manages electronic document PKI certificates on national level.
Acts as a central broker to manage the exchange of Document PKI certificates and certificate revocation lists on a country level. It creates a centralised database of document certificates received from multiple sources like Country Signing Cerification Authority (CSCA), ICAO PKD and Foreign nPKD systems.

INFOTECH
secure identity and payments

X Infotech PKI Solutions Workflow



1. nPKD interfaces with CSCA to sign the Master List signing certificate as well as receives the DS and CSCA certificates. Data exchange is carried out in a manual mode.
2. nPKD connects with Foreign nPKD to receive country non ICAO PKD DS and CSCA certificates. Data exchange is carried out in a manual mode.
3. nPKD interfaces with ICAO PKD to receive ICAO PKD Files and send certificates to ICAO PKD.
4. DV interfaces with nPKD to receive Certificates for Passive Authentication.
5. DS interfaces with CSCA to sign DS certificates. Data exchange is carried out in a manual mode.
6. DVCA interfaces with CVCA to sign DV certificates. Data exchange is carried out in a manual mode.
7. SPOC interfaces with CVCA to sign DV and other certificate requests sent and received from Foreign SPOC
8. DV interfaces with SPOC to receive signed DV Certificates.
9. SPOC interfaces with SPOC CA to receive certificate that protects SPOC as well as interfaces with Foreign SPOC. Data exchange is carried out in a manual mode.
10. TCC interfaces with DV to sign IS certificates that are required for Terminal Authentication (TA). In this way, TCC also receives the certificates for Passive Authentication.
11. SPOC interfaces with Foreign SPOC to send/receive messages and certificates.
12. IS interfaces with TCC to perform Passive and Terminal Authentication.