

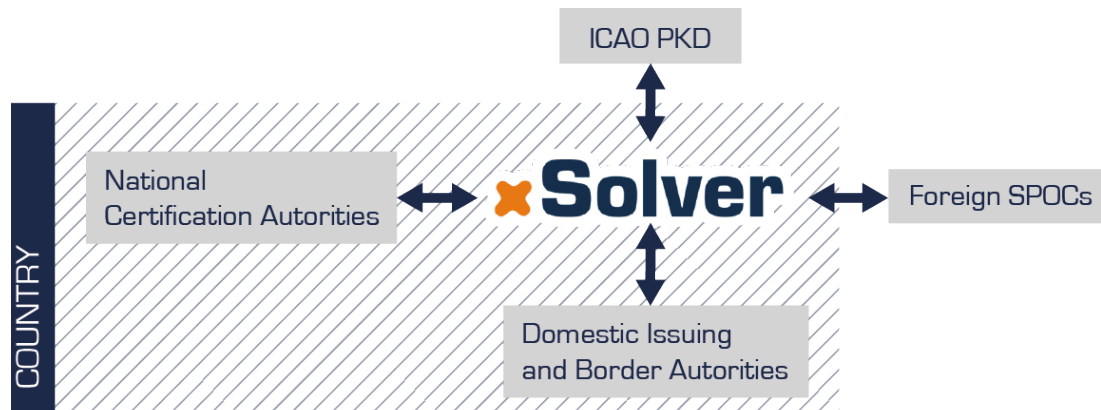


Solution for exchange of e-travel document security

WHAT IS xSOLVER?

Electronic travel documents with biometric data (e-passports and e-residence permits) became one of the significant pillars for European Union security policy.

The infrastructure implemented for issuance and verification of travel documents with biometric data imposes high requirements on the management of biometric data exchange in the vast international environment. As a result of this challenge MONET+ developed (as one of the first countries) a product xSolver, that meets all mentioned prerequisites but also it makes the communication systems operations easy with high level of automation.



The development of xSolver followed the technical and security standards defined by international specifications given by International Civil Aviation Organization and EC Decisions, as Extended Access Control, Single Point of Contact (SPOC) and Common Certificate Policy for the Extended Access Control Infrastructure for Passports and Travel Documents Issued by EU Member States.

WHAT THE xSOLVER DOES?

+ **Established and manages all necessary trusted on-line and off-line communication channels both for international purposes (ICAO PKD, SPOC) and domestic purposes (issuing and verification border authorities).**

Both these functionalities enable equip the border authority (e.g. Foreign police) with all necessary data and certificates for full international e-travel document verification with biometric data.

+ **Manages, distributes and stores all PKI data for the country.**

+ **Enables trust management of CSCA certificates coming form ICAO-PKD via masterlists.**

+ **Works as registration authority for National CVCA.**

WHAT IS A SUBJECT OF MONET+' OFFER?

1. **Delivery of xSolver system. Three environments, which are connected together by communication interfaces, are following:**

- + National certification authorities for e-travel documents (CSCA, CVCA) - guarantees security of e-travel document (and other electronic documents with biometric data) on the national level.
- + Foreign systems (ICAO PKD and SPOC) – foreign communication partners for e-travel document data exchange
- + Domestic issuing and verification authorities - utilize secure data for issuing and border verification of e-travel document and other electronic documents.

2. Delivery of additional components necessary for e-travel documents PKI

- + ISSUER – xSolver interface for certification of issuing DV/DS. Subsystem consist of:
 - + SPOC ISSUER server (part of xSolver BORDER) and remote client application for communication with issuing authorities (DV and DS).
 - + SPOC ISSUER client, which is implemented as working station at possible remote DV/DS premises.
- + SPOC CA – mandatory additional external certification authority for the SPOC security.
- + xSolver BATCH – SW module for parsing/assembling of request/certificate batch for certification authorities (CVCA), which will not be able to process standard xSolver request/certificate batches.

3. Service and support of 2nd level for delivered systems.

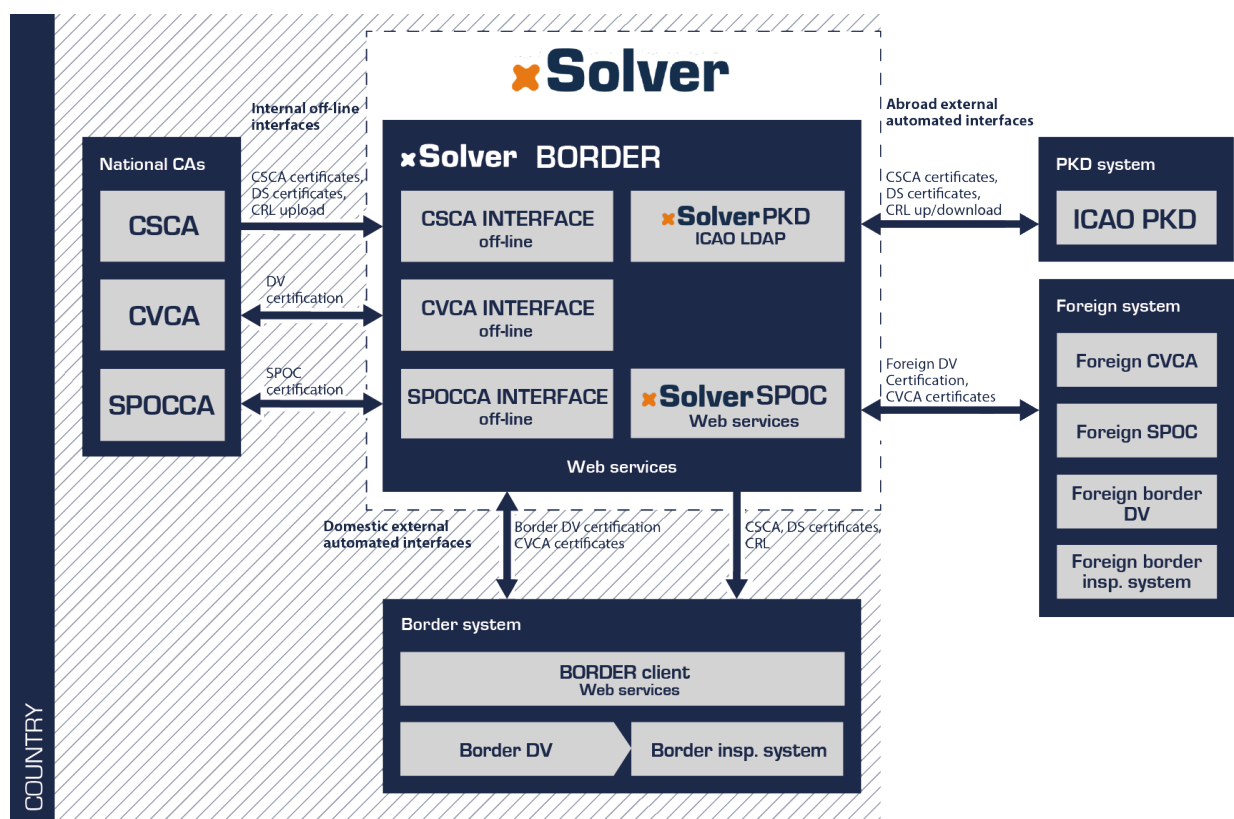
4. Testing services performed from the Czech republic for delivered xSolver system or already implemented SPOC systems. xSolver was already successfully tested with several countries incl. reading of e-travel document.

WHAT IS XSOLVER INTEGRATION AND ARCHITECTURE?

The xSolver product consists of a mandatory component xSolver BORDER serving as a product base and two optional modules xSolver PKD and xSolver SPOC:

1. **xSolver BORDER** – mandatory core of the system, which implements interfaces to domestic issuer and border systems and domestic certification authorities. Contains in addition to application a database for storing of all data, registration authority for domestic CVCA, security component (HSM), user and operational support.
2. **xSolver PKD** – optional interface to ICAO-PKD. This subsystem is dedicated for distribution of country signing data (CSCA, DS certificates and CRLs).
3. **xSolver SPOC** (Single Point of Contact) – optional interface for international DV certification exchange among EU states. This subsystem operates connection with other SPOCs of other countries for certificate exchange for e-travel document verification infrastructure

This picture introduces integration of xSolver into national PKI for e-travel documents.



WHAT ARE KEY ADVANTAGES OF xSOLVER?

- + **xSolver** represents unique solution, which covers all both SPOC and NPKD communication requirements for both domestic and international distribution. It covers all national communication channels among the three key sides: national certification authorities (CSCA, CVCA), foreign communication systems (SPOCs, ICAO-PKD) and domestic systems (border verification and issuing system).
- + **Batch processing** – the batch processing of xSolver converts an automated foreign communication into off-line communication with national CAs (strict separation of national CAs from outer world is supposed). This enables interaction of operator on daily basis for all certification processes (especially CVCA).
- + **Modularity and configurability** – The solution is modular and configurable to customer requirements.
- + **Interface to border system** – the solution implements the central side of border interface for both DV certification and ICAO-PKD data forwarding (CSCA masterlists, DS certificates, CRLs). Using xSolver the border authority can be equipped with all data necessary for e-document verification.
- + **Operational and user conditions** – The system database, high availability according to specification requirements, comfortable and secure user access support could be tuned into robust (clustered), reliable and easily operated system. The system can be easily operated by a graphic user interface based on wizards.
- + **High security** – all possible cryptographic verifications during request processing are performed in HSM. User access is based on roles, users are authenticated by smart cards to the system, all operations are audited, database has a cryptography guaranty of data integrity.
- + **Multi document facility** – the xSolver enables certification of e-residence permits or other documents using EAC technology.
- + **xSolver** was used in the Czech republic as one of the first among EU countries. Czech rep. successfully tested this solution with several countries and following tests with other countries are running. The Czech rep. and Germany started the first live certification data exchange using this system in the EU.
- + **Monet+ experiences** – This xSolver system core was continually equipped by adding functionality (CVCA, SPOC) since 2006, when communication requirements for the state were identified. Monet+ built the whole PKI and personalization system of e-passport for the Czech rep, was active at BIG negotiations from the beginning, organized PKI interoperability test in Prague at 2008, participated at edition of SPOC specification and offers a lot of valuable experiences and the best practices collected for many years.

xSolver

Ing. Břetislav Hofbauer

Project Manager

M +420 603 197 047

T +420 577 110 411

E bretislav.hofbauer@monetplus.cz

Headquarters

MONET+, a. s.,

Za Dvorem 505, 763 14 Zlín – Stipa
(Czech Republic)

www.monetplus.cz

xsolver@monetplus.cz

Office address

Office Center, Venceslas Square 33
110 00 Prague (Czech Republic)