

EXTENDED ACCESS CONTROL

► Security for Electronic Passports

► A new chapter in Electronic Passport's technology

With the new threats to homeland security, global border controls need to be enhanced. This security requirement can be achieved through the usage of Electronic Passports which currently avoid skimming, eavesdropping and misuse, while protecting the identity and privacy of the holder. The second generation of Electronic Passports capitalizes on existing technology (digital identity, biometrics and PKI), adding new and stronger security mechanisms (Extended Access Control), that reinforce the protection of digital imaging and fingerprint scan biometrics placed on the contactless chip, creating an unrivaled level of security and protection against counterfeit and fraudulent identification papers.

► First Generation Electronic Passports

To assist the efforts for stronger border security, ICAO specified the first generation Electronic Passport, an extremely secure document that provides reliable protection against forgery and misuse, meets high data protection requirements and ensures that information about the holder stored in the electronic passport chip cannot be acquired illegally.

MULTICERT developed the "**MULTICERT CSCA out-of-the-box solution**" and the "**MULTICERT DS Object Signer Service**" integrated with the first generation Portuguese Electronic Passport (PEP).

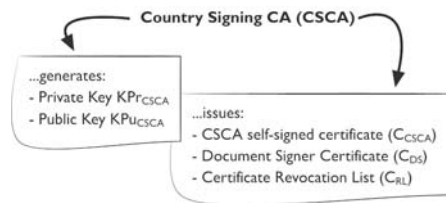


Figure 1 - MULTICERT CSCA out-of-the-box solution

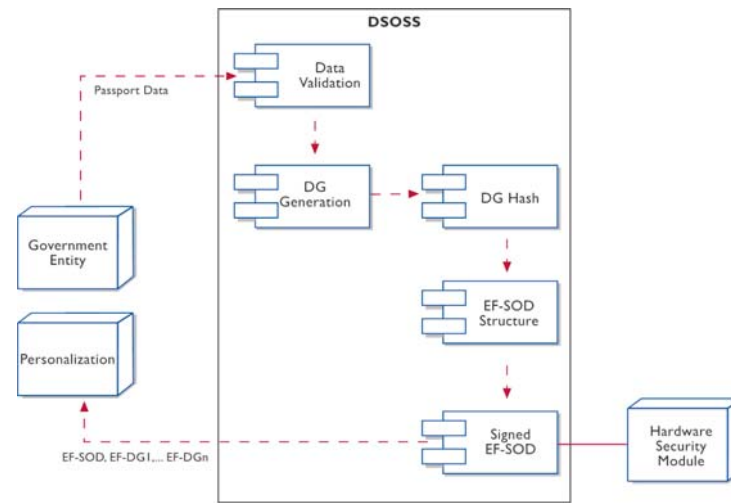


Figure 2 - MULTICERT DS Object Signer Service

MULTICERT CSCA out-of-the-box solution includes hardware, software, HSM, documentation (CPS, CP, ceremonies, policies,...) and added value integration services.

Standard Compliance:

- ICAO PKI for MRTD offering ICC Read-Only Access;
- Council Regulation (EC) No 2252/2004 of 13 December 2004;
- RFC 3369 CMS Signed Data Structure;
- PKCS #7 Cryptographic Message Syntax Standard;
- Directive 1999/93/EC of the European Parliament on a Community framework for electronic signatures.

After the request reception from the Government Entity to the DSOSS (Figure 2), the Passport data is verified, Data Groups are generated (according to ICAO specification) and, for each Data Group, a hash is computed. Data Group's hash, DS digital certificate and other information are stored in EF-SOD structure. Signed EF-SOD (signed with the DS private key, stored in a Hardware Security Module (HSM)) and Data Groups are sent

to Passport/chip Personalization Service.

► Second Generation Electronic Passports

As we move towards a more digitally secure world, technology advancements will also impact the way we travel. Today's newest generation of electronic passports capitalize on existing technology (digital, biometrics and PKI) to enhance global border control and homeland security.

Second Generation Electronic Passports establishes additional data protection requirements for introduction of biometric data, creating an unrivaled level of security

and protection against counterfeit and fraudulent identification papers:

- EAC strongly protects the retrieval of biometric data;
- Only authorized Passport readers can retrieve the stored biometric data.

Joining the development efforts of Second Generation Electronic Passports, MULTICERT has been participating in conformity tests with PEP, using the "**MULTICERT CSCA out-of-the-box solution**", "**MULTICERT EAC DS Object Signer Service**", and the "**MULTICERT EAC PKI out-of-the-box solution**".

Having the DSOSS of the current PEP as a basis, EAC mechanism added new requirements to the infra-structure: Data Group 3 (Encoded Fingers) and Data Group 14 (Active Authentication Public Key) are inserted. Figure 3, MULTICERT EAC DS Object Signer Service, shows that Active Authentication key pair is obtained from DSOSS#2 and Data Group 14 is generated from

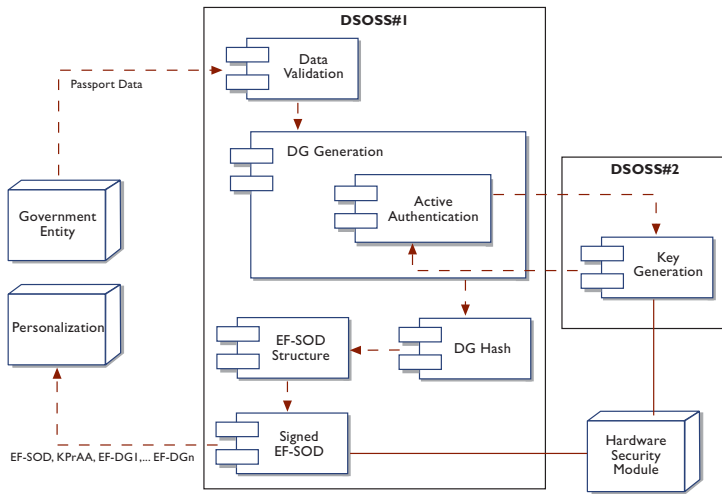


Figure 3 - MULTICERT EAC DS Object Signer Service

Public Key data. To complete the system, EF-SOD, private Active Authentication key and Data Groups are sent to Personalization Service.

The Country Verifying Certification Authority (CVCA) enhances the Document Verifiers (DV) to issue certificates for national Passport checker and reader units. Inspection Systems (IS) allow sensitive biometric data to be read. This complex security infra-structure is shown in Figure 4 and provides reliable protection against the incorrect use and counterfeiting of the second generation Electronic Passports.

Standard Compliance:

- ICAO PKI for MRTD offering ICC Read-Only Access;
- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Basic Access Control;
- Common Criteria Protection Profile for Machine Readable Travel Document with "ICAO Application", Extended Access Control;
- Advanced Security Mechanisms for MRTD – EAC, German Federal Office for Information Security.

Conformity Compliance:

- Brussels Interoperability Group, Terms of Reference;
- EU council decision on June 28th, 2006: Phase 2: Fingerprints must be protected using EAC.

► **Get involved**

From the innovating solutions MULTICERT has successfully deployed in the past, we are building new solutions based on emerging and mature technologies (PKI, chip, biometrics) that increase data and transaction security and enable strong authentication for public and private e-services.

Based on the development experience of the first generation Portuguese Electronic Passports and on the participation in the interoperability tests of the second generation Electronic Passports and reading devices, MULTICERT is your best partner for delivering and integrating the security solution of your first generation and/or second generation Electronic Passport. Contact us!

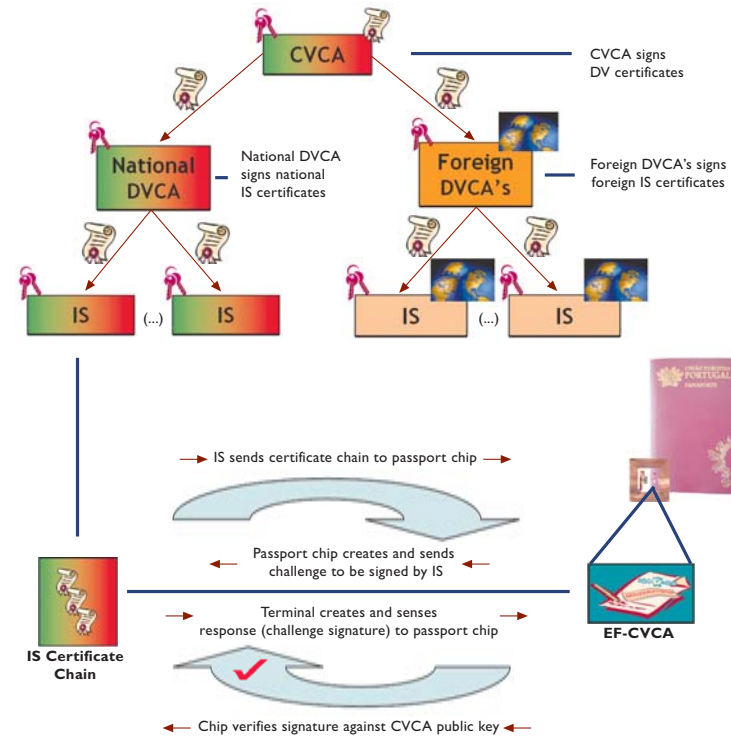


Figure 4 - MULTICERT EAC PKI out-of-the-box solution

About MULTICERT

MULTICERT - Serviços de Certificação Eletrónica S.A. is a company broadly connected to the new information and communication technologies, focused in electronic certification and electronic communication/transaction security. Company's core lies in its larger projects/solutions: besides the Portuguese Citizen Card, the Portuguese Electronic Passport and the Electronic Vote, the company retains an integral part of the EMV/CAP Authentication Platform and of the Electronic Postmark (MDDE) and Electronic Invoice services/solutions.

Telephone: +351 217 123 010
 Fax: +351 217 123 011
 info@multicert.com
 www.multicert.com

MULTICERT Contacts
 Polo Tecnológico de Lisboa
 CID - Lote 1, Sítio 101
 1600-546 Lisboa
 Portugal



All rights reserved © MULTICERT S.A. Produced by MULTICERT Team. The information contained in this document has been carefully checked and is believed to be accurate. MULTICERT logo is a registered trademark in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are property of their respective owners.