International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/17-WP/11
5/3/07
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRTD)

SEVENTEENTH MEETING

Montréal, 20 to 22 March 2007

Agenda Item :2 Implementation of ePassports
Agenda Item :2.1 Progress and Issues

EXTENDED ACCESS CONTROL

Presented by the New Technologies Working Group (NTWG)

1. INTRODUCTION

1.1 In its fifteenth meeting in May 2004, the TAG-MRTD endorsed the Technical Report, "PKI for Machine Readable Travel Documents Offering ICC Read-only Access", Version 1.0.

1.2 A Version 1.1 of this Technical Report was prepared for publication, and published on the ICAO website in October 2004.

1.3 The Technical Report has been incorporated as Section IV into the sixth edition of Doc 9303 Part 1, Volume 2, published in September 2006.

1.4 Issues, arising from implementation practices, that come within the scope of the sixth edition of Doc 9303 Part 1, are being addressed in the "Supplement--9303". The purpose of this Supplement is to provide guidance, advice, update, clarification and amplification as a "bridge" between the formal drafting of Standards and Technical Reports and the needs of the Travel Document community to have timely and official direction to rely on. The Supplement is being published on a regular base.

1.5 In its sixteenth meeting in September 2005, the TAG-MRTD approved ongoing efforts in development of second versions of LDS and PKI Technical Reports. The draft table of contents for the second version of the PKI Technical Report identifies Extended Access Control in section 3.2.

2. BACKGROUND

2.1 Section IV of the sixth edition of Doc 9303 Part 1, Volume 2, provides, at a detailed level, specifications that can be used by MRTD-issuing States to implement PKI in securing the authenticity and integrity of electronic data in their travel documents, as well as specifications for additional optional security features that can be adopted to counter threats of skimming and eavesdropping of data from contactless chips and the prevention of chip substitution.

2.2 The detailed specifications of the additional optional security features are intentionally limited to the protection of the Logical Data Structure (LDS), containing only the face being the *primary* biometric. No provisions have been specified in detail to secure additional *secondary* biometrics, such as finger and iris.

2.3 In the sixth edition of Doc 9303 Part 1, the secondary biometrics are recognized as being *more sensitive* personal data than the face. Therefore, access to this data should be more restricted, to be accomplished by Extended Access Control or Data Encryption.

2.4 Implementing and securing secondary biometrics are left to the discretion of States, to be specified for national or bilateral use.

2.5 This Information Paper provides an overview of the presently known initiatives in the development of Extended Access Control specifications.

3. SINGAPORE

3.1 Singapore started the issuance of e-passports, conforming to the ICAO specifications, in April 2006.

3.2 The Singapore e-passport contains the images of the face, and two fingers as biometric features, stored in the contact-less chip.

3.3 The fingers are protected by an Extended Access Control scheme, according to the "Singapore Standard SS 529: 2006, Specifications for SmartCard ID". An overview of the specifications is provided in Appendix 1 to this Information Paper.

4. THE EUROPEAN UNION

4.1 The development of standards for security features and biometrics in passports and travel documents issued by Member States of the European Union, have been formalized in the Council Regulation No 2252/04 of the European Commission, dated 13 December 2004.

4.2 According to EU regulations, its Member States have to implement the finger as secondary biometric in their e-passports, at latest by June 2009. The fingers shall be stored in accordance with ICAO's sixth edition of Doc 9303 Part 1 and must be protected by Extended Access Control.

4.3 Technical specifications of Extended Access Control have been developed and described in a Technical Guideline (TR-03110) "Advanced Security Mechanisms for Machine Readable Travel Documents -

Extended Access Control (EAC)", version 1.01. An overview of the specifications is provided in Appendix 2 to this Information Paper.

5. FEASIBILITY OF EAC IN ICAO STANDARDS

5.1 The sixth edition of Doc 9303 Part 1 specifies that secondary biometrics need to be protected under the issuing State's responsibility. Both schemes have implemented this requirement by means of an authorization mechanism for inspection systems under control of the MRTD issuer.

5.2 Both schemes result from a preference for Extended Access Control above Data Encryption, because of the vulnerability of an encryption scheme to brute force attacks.

5.3 Extended Access Control is already operational in Singapore. In the EU the first interoperability tests have been performed in December 2006 and implementations are expected to commence between end 2007 and mid 2009.

5.4 The Singapore approach is limited to the extension of the ICAO specifications with restricted access to the secondary biometrics only, while the EU scheme beside that also offers a strong communications encryption and an implicit alternative to Active Authentication.

5.5 Both schemes are backwards compatible; they do not affect compliancy to the existing ICAO LDS and PKI specifications.

5.6 Since the Singapore EAC is based on a MRTD specific EAC key, encrypted for each individual authorized inspection system and stored on the MRTD chip, the necessity could arise that inspection systems must be known at personalization time. This effect has been diminished by the creation of a set of pre-defined key pairs, of which the public keys already are being stored on the chip, while the corresponding private keys are kept for secure delivery to future inspection systems. EAC in the EU scheme is based on inspection systems proving to be authorized through the possession of certificates. These certificates are exchanged via a Public Key Infrastructure.

5.7 As a consequence the Singapore approach is static with respect to the inspection systems being supported by issued MRTDs. The EU approach offers more flexibility.

5.8 The EU PKI offers the possibility for authorization revocation. In Singapore this is not technically supported by the scheme and may be implemented by other means.

5.9 A drawback of the flexibility of the EU scheme is that it requires a rather complex infrastructure and certificates distribution scheme, while the Singapore infrastructure is less complex.

5.10 In accordance with the assumption made in Doc 9303 Part 1 (Volume 2, Section IV, 2.4) the Singapore scheme is used at a national level. Its design seems to be intended that way. The EU specifications are designed to be used unilaterally by the EU Member States.

5.11 In case ICAO specifications for Extended Access Control should be developed the EU scheme seems to be the most feasible starting point to base these specifications on because of its unilateral nature.

6. ACTION BY THE TAG/MRTD

6.1 The TAG/MRTD is invited to:

a) confirm the continuation of the study to EAC and the investigation if EAC should be developed as a global standard.

— — — — — — — —

APPENDIX 1

OVERVIEW OF TECHNICAL SPECIFICATIONS FOR EXTENDED ACCESS CONTROL

SINGAPORE[1]

1. INTRODUCTION

1.1 Extended Access Control enforces that only authorized inspection systems can access sensitive data (LDS Data Group 3 - fingers).

1.2 At all time, communications between the Inspection System and the MRTD chip are protected by the session encryption that is provided by Basic Access Control.

1.3 In the Singapore Extended Access Control access to LDS Data Group 3 (DG3) is protected by a 16-byte triple-DES key (the EAC key), which is used in the context of an EXTERNAL AUTHENTICATE command prior to a read operation. The receiving party (Inspection System) must have the key in order to read DG3.

2. GENERATION, DISTRIBUTION AND STORAGE OF THE EAC KEY

2.1 The EAC key consists of a random number, generated by the MRTD issuer during personalization. This key is different for each MRTD.

2.2 In order to distribute the EAC key to the intended authorized verifier (Inspection System), it is encrypted using an asymmetric cryptographic algorithm and the result is stored in LDS Data Group 13 (DG13).

2.3 For each authorized Inspection System, one copy of EAC key is encrypted with that Inspection System's public key. The authorized Inspection System shall use its matching private key to decrypt its copy of the EAC key before using it to obtain access to DG3.

2.4 As a consequence DG13 contains multiple encrypted EAC keys, one for each authorized Inspection System. A conceptual view of the data in DG13 is as follows:

[1] Based on "Singapore Standard SS 529: 2006, Specifications for SmartCard ID", SPRING Singapore, 2006.

EAC key encrypted using Asymmetric public Key 1 (for IS 1)	EAC key encrypted using Asymmetric public Key 2 (for IS 2)	. . .	EAC key encrypted using Asymmetric public Key n-1 (for IS n-1)	EAC key encrypted using Asymmetric public Key n (for IS n)

2.5 The encryption asymmetric public key in general is delivered to the issuer (personalizer) by the receiving party (the party who wants to read DG3 and is authorized to do so by the passport issuer).

2.6 If this encryption key is not available at the time of production (because no agreement has been reached between the two parties), then the issuing party may generate a key pair, and provide the receiving party with the decryption (private) asymmetric key subsequently via a secure delivery method.

3. DETAILS OF LDS DATA GROUP 13

3.1 The Encrypted EAC Key for each receiving party is a data item with 3 components:

a) The corresponding Subject Distinguish Name of the receiving party.
b) The corresponding public-private key pair ID (SHA-1 of public key) that was used to encrypt the EAC key.
c) The encrypted EAC key that is generated by the issuing party.

```
EncryptedEACKeyInfos ::= SEQUENCE {
                version          INTEGER
                totalCount       INTEGER,
                SEQUENCE OF      EncryptedEACKeyInfo OPTIONAL}

EncryptedEACKeyInfo ::= SEQUENCE {
                subjectDN              PRINTABLE STRING,
                subjectKeyIdentifier   OCTET STRING,
                EncryptedEACKey        OCTET STRING}
```

3.2 The EAC key is encrypted using 1024-bit RSA, the size of the data items is given as follows:

SN	***Name***	***Fixed/Var.***	***Number of Bytes***
1	SubjectDN	V	96 Max
2	subjectKeyIdentifier	F	20
3	EncryptedEACKey	F	128

3.2.1 The EncryptedEACKeyInfo for each receiving party may be up to 256 bytes (96 + 20 + 128 + ASN.1 tags). Therefore if there are 10 intended recipients, the total size required for EF.DG13 can be 2 kilobytes.

— — — — — — — —

APPENDIX 2

OVERVIEW OF TECHNICAL SPECIFICATIONS FOR EXTENDED ACCESS CONTROL

EUROPEAN UNION[1]

1. INTRODUCTION

1.1 Extended Access Control enforces that only authorized inspection systems can access sensitive data (like fingers and/or iris).

1.2 Since the data to be accessed by an inspection system, once granted by the MRTD's chip, is considered sensitive, communications are protected by a stronger session encryption than provided by Basic Access Control.

1.3 The EU Extended Access Control consists of two advanced security mechanisms, *Chip Authentication*, providing strong session encryption and enabling the inspection system to verify that the chip is genuine, and *Terminal Authentication*, enabling the chip to verify that the inspection system is entitled to access sensitive data.

1.4 An EAC compliant MRTD chip supports a non EAC compliant inspection system with respect to access to less sensitive data (like MRZ and face) in full compliancy with ICAO Doc 9303. Inspection procedures to be used are defined as 'Standard' (non EAC) and 'Advanced' (EAC):

Inspection system	**MRTD chip**	
	compliant	**non-compliant**
compliant	Advanced	Standard
non-compliant	Standard	Standard

Standard inspection procedure
1. Basic Access Control (O - conditional)
2. Passive Authentication started (M)
3. Active Authentication (M)
4. Reading of less sensitive data (O)

Advanced inspection procedure
1. Basic Access Control (M)
2. Chip Authentication (M)
3. Passive Authentication started (M)
4. Reading of less sensitive data (O)
5. Terminal Authentication (O - conditional)
6. Reading of sensitive data (O)

[1] Based on "Technical Guideline TR-03110, Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC)", version 1.01, Bundesamt für Sicherheit in der Informationstechnik, 2006-11-02.

2. CHIP AUTHENTICATION

2.1 Chip Authentication is an ephemeral-static Diffie-Hellmann key agreement protocol. By use of this protocol the chip and the inspection system agree on (strong) session keys to encrypt their communications.

2.2 The exchange of information between chip and inspection system, in order to generate a shared secret and derive session keys is protected by the secure messaging, provided by Basic Access Control.

2.3 Once Chip Authentication is performed successfully, Secure Messaging is restarted using the new (strong) session keys.

2.4 For this protocol the chip contains a Chip Authentication key pair, of which the private key is stored in the chip's secure memory, and the public key is stored in LDS Data Group 14. Therefore the authenticity of the public key can be verified by the inspection system through Passive Authentication.

2.5 The genuineness of the chip is implicitly verified by its ability to perform secure messaging using the new session keys, proving that the chip's private and public key belong together, and performing Passive Authentication on the chip's public key, proving its authenticity and integrity. Therefore Chip Authentication can be used as an alternative to Active Authentication.

3. TERMINAL AUTHENTICATION

3.1 Terminal Authentication enables the chip to verify that the inspection system is authorized by the MRTD's issuing State to access sensitive data.

3.2 Terminal Authentication is based on the presence, in the inspection system, of a certificate chain, which starts with a certificate, signed by a MRTD issuer. By signing this certificate, the issuing State authorizes the inspection systems using it. The public key to verify this certificate is stored on the MRTD chip.

3.3 In the Terminal Authentication protocol the MRTD chip verifies the signature chain, and if the protocol is successfully performed, grants access to the stored sensitive data, according to an effective authorization level, determined by the MRTD issuer.

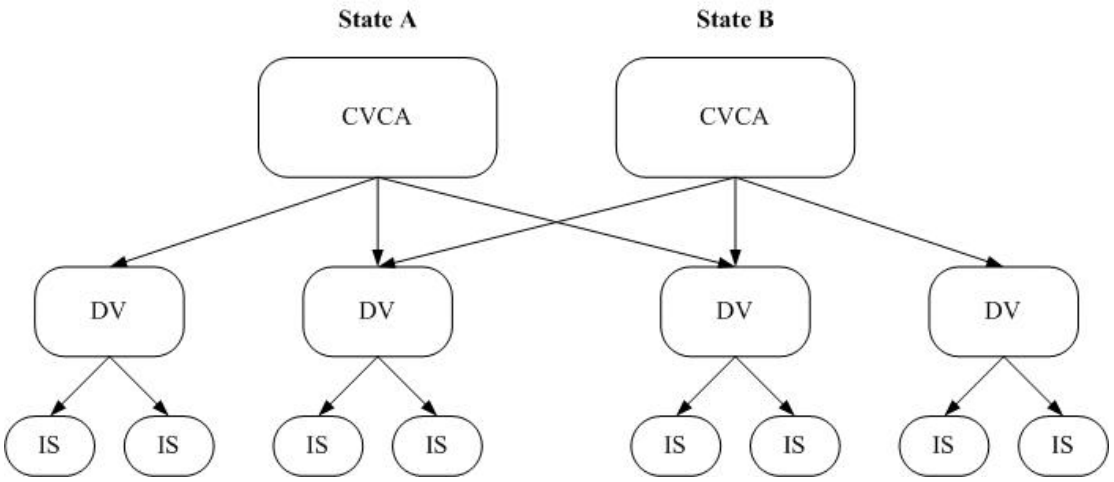
4. PUBLIC KEY INFRASTRUCTURE

4.1 The PKI, required for Terminal Authentication, providing Extended Access Control, consists of the following entities:

a) Country Verifying CAs (CVCA), issuing Document Verifier Certificates.

b) Document Verifiers (DV), issuing Inspection System Certificates.

c) Inspection Systems, accessing MTRD chips.



4.2 **Country Verifying CA (CVCA)**

4.2.1 The CVCA acts as the single trust-point of an issuing State, determining access rights to the MRTD chips issued by that State for Document Verifiers. These access rights are granted to a Document Verifier by issuing a Document Verifier Certificate to it. The Document Verifier Certificate contains the Document Verifier's public key and is signed by the CVCA.

4.2.2 The conditions under which a CVCA grants a Document Verifier access should be stated in a certificate policy published by the CVCA.

4.2.3 The public key to verify the Document Verifier Certificate is stored on the MRTD chip in secure memory.

4.2.4 The Document Verifier Certificate contains access information, such as which data a certain Document Verifier is entitled to access. This information may differ depending on the Document Verifier the certificate is issued to.

4.3 **Document Verifier (DV)**

4.3.1 A DV manages inspection systems by issuing Inspection System Certificates, and is therefore a CA authorized by the national CVCA.

4.3.2 If a DV requires its inspection systems to access sensitive data stored on other States' MRTD chips, it needs to obtain the required Document Verifier Certificate from that issuing State by sending a Certification request (containing the Document Verifier's public key).

4.3.3 Besides issuing Inspection system Certificates, a DV ensures that all received Document Verifier Certificates are forwarded to the Inspection Systems within its domain.

4.4 **Inspection System**

4.4.1 An Inspection System is authorized to access sensitive data stored on a State's MRTD chip through the certificate chain, starting with the Document Verifier Certificate, issued by the MRTD issuer's CVCA and ending with the Inspection System Certificate.

4.4.2 As a consequence, an Inspection System contains a certificate chain for each State, for which MRTD chips it has been authorized to access sensitive data. The Inspection System Certificates in these chains encode the public key of the Inspection System's private/public key pair and access rights.

4.4.3 The certificates in the certificate chain are card verifiable certificates. Therefore the chain can be verified by the MRTDs chip, containing its CVCA public key.

5. CERTIFICATE VALIDITY

5.1 To diminish the potential risk of lost or stolen Inspection Systems the Document Verifier Certificates will have a relatively short validity period assigned by the CVCA.

5.2 As a consequence CVCA link certificates need to be produced and propagated to the Inspection Systems. This enables the MRTD chip to internally update its trust-point (the actual public key to verify the Document Verifier Certificate) at moments it communicates with an Inspection System.

5.3 The validity period of a certificate is identified by two dates, the *certificate effective date*, which is the date of certificate generation, and the *certificate expiration date*, indicating the end of the certificate's validity period.

5.4 A certificate is valid if the *current date*, at the moment that the certificate's validity is being verified, is in between the certificate effective date and the certificate expiration date.

5.5 Since the MRTD has no internal clock, but still has to validate the certificate's validity, the current date is approximated and used as described below:

5.5.1 Initially the current date is stored on the chip during personalization, being the personalization date.

5.5.2 For each received certificate in an inspection procedure the MRTD chip verifies the signature. If the signature is incorrect, the verification fails.

5.5.3 The MRTD chip compares the certificate expiration date to the MRTD chip's current date. If the expiration date is before the current date, the certificate has expired and the verification fails.

5.5.4 The MRTD chip compares the certificate effective date to the MRTD chip's current date. If the current date is before the effective date, apparently the Inspection System has received a new link certificate, and the current date is updated to the effective date. If the effective date is before the current date, apparently this Inspection System did not receive a new link certificate, while an earlier visited Inspection System did (chip's current date has been updated). This could mean that the Inspection System is no longer in the infrastructure, and might be a stolen one.

— END —