International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/18-WP/6
22/4/08
English only

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

EIGHTEENTH MEETING

Montréal, 5 to 8 May 2008

Agenda Item 1: Activities of the NTWG
Agenda Item 1.6: Basic Access Control/Extended Access Control in e-Passports

BASIC ACCESS CONTROL/EXTENDED ACCESS CONTROL IN E-PASSPORTS

Presented by the New Technologies Working Group (NTWG)

1. INTRODUCTION

1.1 The sixth edition of Doc 9303 Part 1, Volume 2, published in September 2006, contains the technical specifications of the Logical Data Structure (LDS) in Section III, and the Public Key Infrastructure (PKI) in Section IV.

1.2 Issues that arise within the scope of the sixth edition of Doc 9303 are being addressed in the "Supplement to Doc 9303". The purpose of this Supplement is to provide guidance, advice, update, clarification and amplification to the Travel Document community to have timely and official direction with respect to the standard. The Supplement is being published on a regular base.

1.3 Section IV of the sixth edition of Doc 9303 Part 1, Volume 2, provides 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 features that can be adopted to detect the copying of chip contents and to counter threats of skimming and eavesdropping.

1.4 In Doc 9303 no provisions have been specified in detail to secure additional *secondary* biometrics, such as finger and iris. Since these biometrics are recognized as being more privacy sensitive than the face, access to it should be more restricted, for which Extended Access Control is seen as the most appropriate method.

1.5 A Working Paper (WP-11) on Extended Access Control was presented at the seventeenth meeting of the TAG in May 2007. Comparison of existing EAC schemes lead to the conclusion that the EU specifications seem to be the most suitable basis for global use of Extended Access Control.

1.6 In its seventeenth meeting in March 2007, the TAG-MRTD approved the continuation of the study to a global standard for Extended Access Control. This Working Paper provides an overview of the existing security and privacy features, as well as Extended Access Control specifications, present status and possible use on a global level.

2. SECURITY FEATURE – PASSIVE AUTHENTICATION

2.1 **Passive Authentication** enables an inspection system to verify if the information in the eMRTD's chip is authentic, stored on the chip by the issuer of the eMRTD, and has not been change since it was stored.

2.2 For this purpose the data is electronically signed. The electronic signature is generated by cryptographic calculations, using a Private Key from the eMRTD's issuer, and stored on the chip. Successful verification of this electronic signature by the inspection system (using the Public Key corresponding to this Private Key) proves the authenticity and integrity of the data.

2.3 Distribution of Public Keys to inspection systems to enable these to verify the digital signatures on eMRTDs is realized through a Public Key Infrastructure (PKI).

2.4 The mechanism is called *Passive* Authentication because it does not require the eMRTD's chip to actively perform calculations. The chip only carries the data and the signature; signature verification is performed by the inspection system.

2.5 According to Doc 9303 Passive Authentication is a mandatory feature.

3. SECURITY FEATURE - ACTIVE AUTHENTICATION

3.1 **Active Authentication** enables the inspection system to check if the data is read from the genuine chip it was stored on by the issuer, and is not a copy ('clone') of the original data.

3.2 An eMRTD that supports Active Authentication contains two corresponding Keys, forming the "Active Authentication Key Pair". The Private Key is stored in a secure area in the chip; it can not be read out, only the chip can use it for internal calculations. The corresponding Public Key is stored as part of the eMRTDs data; an inspection system can therefore read it and verify its authenticity through Passive Authentication.

3.3 In Active Authentication the inspection system checks if chip and data belong to each other by offering a random number to the chip, to be signed (encrypted) by the chip using the Active Authentication Private Key, and verifying the result with the Active Authentication Public Key. If this verification is successful it proves that both keys belong to each other, e.g. that the data comes from a genuine chip.

3.4 Since both Keys are stored on the chip itself, no distribution of keys is required for Active Authentication.

3.5 The mechanism is called *Active* Authentication because the chip actively performs cryptographic calculations, signing the random number from the inspection system.

3.6 According to Doc 9303 Active Authentication is an optional feature.

4. PRIVACY FEATURE - BASIC ACCESS CONTROL

4.1 **Basic Access Control** protects against unauthorised reading information from the eMRTD's chip through skimming or eavesdropping.

4.2 Skimming is the form of unauthorized reading by powering the chip and communicating with it, using a contactless chip reader, without the eMRTD bearer's notice. As opposed to a conventional MRTD, of which the contents can not be read as long as the book is closed, the technology of the specified proximity chip in an eMRTD makes reading the chip contents possible from a short distance.

4.3 Eavesdropping is the unauthorized interception of the communications between the eMRTD's chip and the authorized inspection system. In this case the chip has already been powered by the authorized reader with the consequence that eavesdropping can be performed from a greater distance than skimming.

4.4 An eMRTD that supports Basic Access Control does not grant access to the data, stored on its chip, unless the inspection system offers the proper access key to it. In the Basic Access Control protocol the inspection system calculates this key from information that is stored in the Machine Readable Zone. As a consequence the eMRTD has to be opened and offered to the inspector before its contents can be read, which eliminates the difference to the conventional MRTD, set out in 4.2.

4.5 The same information, read from the Machine Readable Zone, is used to calculate keys that encrypt the communications between the chip and the inspection system. As a result the data obtained from eavesdropping these communications cannot be read without knowledge of these keys.

4.6 The Basic Access Control keys are derived from the fields 'document number', 'date of birth', and 'date of expiry' in the Machine Readable Zone. Due to the limited amount of digits the entropy of the keys derived from it is relatively low. In principle an attacker might record the encrypted communications, calculate the keys by brute force and decrypt the recorded information. However, since such an attack currently still requires a considerable effort compared to obtaining the data from other sources and the data consists of the same information as printed on the data page, Basic Access Control is suitable for its goal presently.

4.7 As a result of the continuous and fast increase of computer power and calculation speed the efforts necessary to successfully calculate Basic Access Keys from eavesdropped communications will decrease. As a consequence Basic Access Control will at a certain point in time not be an effective measure against such attacks. An alternative means to protect against unauthorised reading information from the eMRTD's chip through skimming or eavesdropping will need to be investigated and specified.

4.8 According to Doc 9303 Basic Access Control is a recommended feature.

5. PRIVACY FEATURE - EXTENDED ACCESS CONTROL

5.1 **Extended Access Control** provides a stricter protection against unauthorized reading of sensitive data, like finger print and iris images, than Basic Access Control does for the less sensitive data (the face).

5.2 Through Extended Access Control (EAC) an inspection system can only access areas on the eMRTD's chip to which it has been authorized by the eMRTD's issuer. This is accomplished by the Terminal Authentication protocol. A strong encryption of the communications between the eMRTD's chip and the inspection system is achieved through the Chip Authentication protocol.

5.3 The Extended Access Control procedure starts with performing Basic Access Control. Under protection of the Basic Access Control communications encryption **Chip Authentication** is performed.

5.3.1 Through the Chip Authentication protocol the Basic Access Control low entropy session keys are exchanged for stronger keys, with which the communications are restarted.

5.3.2 The key agreement protocol with which the new keys are derived is based on the presence of a key pair in the eMRTD's chip, of which the private key is stored in secure memory and the corresponding public key in Data Group 14, verifiable through Passive Authentication. As a consequence a successful restart of the communications with the new session keys also proves that the chip and the information on it are genuine and not a copy (clone).

5.3.3 Chip Authentication can be performed as a protocol on itself, without performing Terminal Authentication. It then provides a strong protection of the communications against eavesdropping and protection against copying as an alternative to Active Authentication.

5.4 To obtain access to data, protected by Extended Access Control, after Chip Authentication the **Terminal Authentication** protocol must be executed.

5.4.1 Terminal Authentication can only be executed after a successful Chip Authentication.

5.4.2 Terminal Authentication is based on the presence, in the inspection system, of a certificate chain, which starts with a certificate, signed by the eMRTD 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 eMRTD's chip.

5.4.3 In the Terminal Authentication protocol the eMRTD's 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.

5.4.4 Since Terminal Authentication enables the eMRTD issuer to authorize inspection systems with various levels of access to the eMRTD's chip it is not only suitable for protection of sensitive data, but also to authorize certain systems to write and/or update data in already issued eMRTDs (e.g. writing visa information, travel records, updating address information, et cetera).

5.5 A more detailed description of Extended Access Control, as it is being introduced in the Europian Union, is described in the Appendix to this Working Paper.

5.6 Since November 2007, Germany is issuing eMRTDs with Extended Access Control. Other EU Member States will implement before June 28, 2009, according to EU regulations. At this moment no practical experiences with more States and the necessary exchange of certificates are available.

6. ACTION BY THE TAG/MRTD

6.1 The TAG/MRTD is invited to:

a) the investigation to alternative means to protect against unauthorised reading information from the eMRTD's chip through skimming or eavesdropping.

b) confirm the continuation of the study to a global standard for Extended Access Control as a Work Item for the next generation of MRTDs.

c) confirm evaluation of implementation experiences within the European Union as part of this study.

d) recognize the feasibility of Chip Authentication as a protocol, which can be used on its own for communications protection and electronic anti copying mechanism.

e) confirm that the study to a global standard for EAC must not just cover the protection of sensitive data, but also its benefits as an authorization mechanism for updates, writing visa information, travel records, et cetera, after issuance.

— — — — — — — —

APPENDIX

OVERVIEW OF TECHNICAL SPECIFICATIONS FOR EXTENDED ACCESS CONTROL

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 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, Part 1, sixth edition. 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 (R - conditional)
2. Passive Authentication started (M)
3. Active Authentication (O)
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)

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.

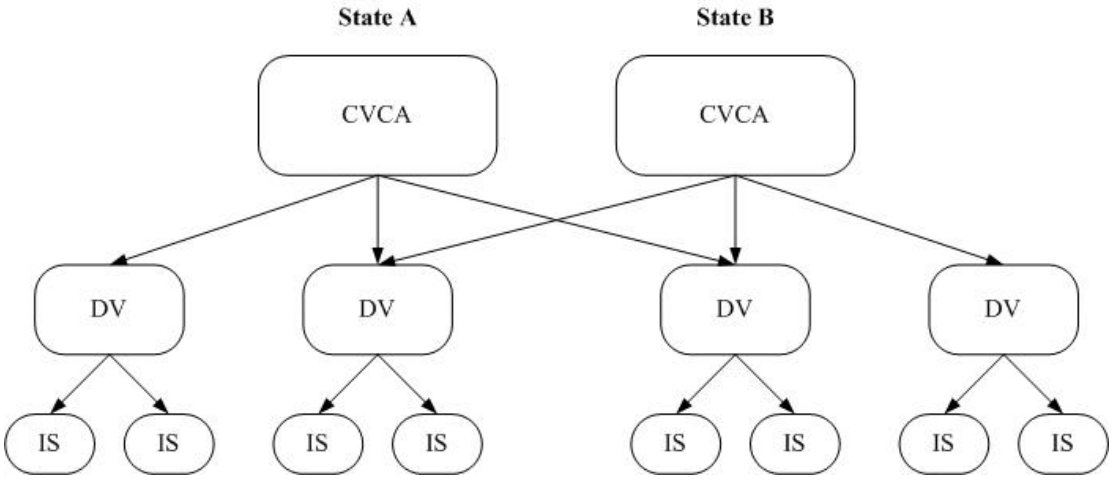
4. PUBLIC KEY INFRASTRUCTURE

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

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

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

4.1.3 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 1nitially 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 —