MACHINE READABLE TRAVEL DOCUMENTS

(Logo)

TECHNICAL REPORT

PKI for Machine Readable Travel Documents offering ICC Read-Only Access

Version - **1.1**
Date - October 01, 2004

Published by authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

File	: TR-PKI for MRTDs offering ICC Read-Only Access V1.1.doc
Author	: Tom A.F. Kinneging for ICAO-NTWG, PKI Task Force

Release Control

Release	Date	Description
0.1	15-12-2003	First draft for TF-PKI
0.2	05-01-2004	Results meeting in London (December 17/18) incorporated
0.31	12-01-2004	Comments "London 17/18 group" incorporated
0.4	13-02-2004	Comments PKI Task Force & Task Force leaders incorporated; published on NTWG website
1.0	21-04-2004	Results NTWG meeting February 24-27 incorporated; version for TAG 15.
1.1	01-10-2004	Clarifications on specs included (see release note)

Release note

Changes, made on version 1.0, resulting in this version 1.1:

Subject	Description	Reference
Basic Access Control	References to CWA 14890 removed. Detailed description of the protocol added.	3.2.2 Annex E Annex F
Active Authentication	Detailed description of the protocol.	3.2.2 3.3.1 Annex D
Certificate profile	PathLengthConstraint specified '0 for New Country Signing CA Certificate' and '1 for Linked Country Signing CA Certificate'.	Annex A
Data Group 15	Textual clarification.	2.3.2 3.2.2
Signature generation	Clarification on references for signing Certificates and the $SO_{D,}$ as opposed to the signing of the challenge in the active Authentication.	3.3.2 Annex F
Basic access Control	Expanded specification of EXTERNAL AUTHENTICATE command.	Annex F
Optional features	Statement added: "In case OPTIONAL features are implemented, they MUST be implemented as described in this Technical Report."	1.3.1
Certificate naming	Country Codes MUST follow the format of two letter	Annex A

Subject	Description	Reference
	country codes as per ISO/IEC 3166.	
Risk Analysis	New text	Annex G
RSA	Changed text in : "RFC 3447 specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED to generate signatures according to RSASSA-PSS, but receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15."	3.3.2
ECC	Text incorporated: "The elliptic curve domain parameters used to generate the ECDSA key pair MUST be described explicitly in the parameters of the public key, i.e. parameters MUST be of type ECParameters (no named curves, no implicit parameters) and MUST include the optional cofactor. ECPoints MUST be in uncompressed format."	3.3.4

Preamble

In the meeting of the ICAO-TAG in May 2003, the TAG endorsed the so-called 'New Orleans Resolution' in which storage of biometrics (images of the face and, optional, finger and/or iris) in contactless chips is recommended.

Related security principles, described in the ICAO-NTWG document [R2] (Technical Report: PKI Digital Signatures for Machine Readable Travel Documents, version 4) have been presented and approved. The Technical Report provided guidance and advice to States and Suppliers regarding the application and usage of modern public key infrastructure (PKI) schemes for the implementation and use of Digital Signatures, and proposed details of a specific infrastructure for that purpose.

In the meeting the TAG stated that the priority for the NTWG should proceed with specifying the PKI scheme for the MRTD community in more detail. As a result of this, the NTWG Task Force PKI & Security has composed a new Technical Report (this Report). The intention of the specifications in this Technical Report is to be as detailed as necessary to enable States to implement the scheme in MRTDs offering ICC read-only access.

For readability purposes relevant parts of the first Technical Report have been repeated in this Technical Report, so some redundancy can be expected.

The aim of the PKI scheme, described in this Technical Report, is mainly to enable MRTD-inspecting authorities (receiving States) to verify the authenticity and integrity of the data stored in the MRTD. It is assumed that this data is stored in the way as described in [R3] (Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies.). However, in favour of the New Orleans Resolution the focus of this Technical Report is based on chip technology. Other storage media, like 2D-Barcode and Optical Memory are left out of consideration.

This Technical Report is the result of the contributions of the members of a sub-group (the "London 17/18 group") of the NTWG PKI Task Force. Without their contributions and input to the various discussions it would not have been possible to create this Technical Report in this short period of time.

NTWG PKI Task Force – London 17/18 group		
John Davies (chairman)	UKPS	United Kingdom
David Clark	Caicos Technologies	Canada
Simon Godwin		United States of America
Simon Johnson	CESG	United Kingdom
Tom Kinneging	Sdu Identification	The Netherlands
Dennis Kügler	BSI	Germany
Richard Martin	US Department of State	United States of America
Bill Perry	ETS	United Kingdom
Uwe Seidel	BKA	Germany

Table of contents

1. Introduction

Regarding the development of biometrics in MRTDs and securing global interoperability ICAO/TAG in it's meeting in Montreal in May 2003 endorsed the so called "New Orleans Resolution", which was prepared by the NTWG in New Orleans in March 2003.
This resolution states the following:

New Orleans Resolution

In order to clarify NTWG resolution N001 of June 28, 2002 (commonly referred to as the "Berlin Resolution"), and taking into account recent developments in data storage technologies, the NTWG hereby resolves:

ICAO TAG-MRTD/NTWG recognizes that Member States currently and will continue to utilize the facial image as the primary identifier for MRTDs and as such endorses the use of standardized digitally-stored facial images as the globally interoperable biometric to support facial recognition technologies for machine assisted identity verification with machine-readable travel documents.

ICAO TAG-MRTD/NTWG further recognizes that in addition to the use of a digitally stored facial image, Member States can use standardized digitally-stored fingerprint and/or iris images as additional globally interoperable biometrics in support of machine assisted verification and/or identification.

Member States, in their initial deployment of MRTDs with biometric identifiers, are encouraged to adopt contactless IC media of sufficient capacity to facilitate on-board storage of additional MRTD data and biometric identifiers.

In line with the New Orleans resolution ICAO/TAG and the NTWG have been active in researching, evaluating, and preparing Technical Reports for two significant initiatives; the deployment of biometrics in MRTDs, and the development and use of contactless/RFI IC chip devices in MRTDs. These initiatives provide significant benefits for authenticating MRTDs and the rightful bearer, and facilitating border crossings and security.

The choice for chip technology as preferred storage media for biometric information, as opposed to 2D barcode or Optical memory, provides States with the means to enhance document security further than the in the previous Technical Report ([R2], *Technical Report: PKI Digital Signatures for Machine Readable Travel Documents, version 4*) described Digital Signatures by applying separate applications in the chip.

1.1 Scope and purpose

The first Technical Report on PKI Digital Signatures provided guidance and advice to States and Suppliers regarding the application and usage of modern public key infrastructure (PKI) schemes for the implementation and use of Digital Signatures and proposed details of a specific infrastructure for that purpose.

Based on this first guidance discussions within the NTWG lead to a proposed authentication scheme, using signed certificates in combination with the Logical Data Structure ([R3], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies.*).

This Technical Report describes this scheme and is intended to provide States and Suppliers with specifications that enable States and Suppliers to implement the proposed authentication scheme for Machine Readable Travel Documents ("MRTDs") offering ICC read-only access.

Based on the premises that effective implementation will have to be possible in 2004, the scheme does not try to prescribe a full implementation of a complicated PKI structure within each country. This Technical Report is intended rather to provide a way of implementation in which States are able to make choices in several areas (like active or passive authentication, anti skimming and access control, automated border crossing, et cetera), thus having the possibility to phase in implementation of additional features without being incompliant to the framework.

1.2 Assumptions

It has been assumed that the reader is familiar with the concepts and mechanisms offered by public key cryptography and public key infrastructures.

It has been assumed that the reader is familiar with the contents of [R2], Technical Report: PKI Digital Signatures for Machine Readable Travel Documents, version 4.

Whilst the use of public key cryptography techniques adds complications to the implementations of passports, they add value in that they will provide front line border control points with an additional measure to determine the authenticity of the passport document. It is assumed that it does not provide the sole measure for determining authenticity and it SHOULD NOT be relied upon as a single determining factor.

The digitally stored image of the face is assumed not to be privacy sensitive information. The face of the MRTD holder is also printed in the MRTD and can be obtained freely anyway.

The digitally stored image of the finger(s) and/or iris are additional biometric features for which States MAY choose, to apply for national use. They are generally considered to be privacy sensitive and therefore need to be protected under the issuing State's responsibility.

It is not feasible that ICAO, or some other single, central organization will assign, maintain or manage secure private keys for any State. Despite many strategic alliances among participants this will not be recognized as being a trusted solution.

In the event that the data from the chip cannot be used, for instance as a result of a certificate revocation or an invalid signature verification, or if the chip was left intentionally blanc (as described in paragraph 3.1.1), it does not necessarily invalidate the MRTD. In that case a receiving State MAY rely on other document security features for validation purposes.

The use of Certificate Revocation Lists (CRLs) is limited to Country Signing CA Certificates. CRLs are not applicable for individual Document Security Objects and document specific Active Authentication Key pairs.

1.3 Terminology

1.3.1 Technical report terminology

The key words "MUST", "SHALL", "REQUIRED", "SHOULD", "RECOMMENDED", and "MAY" in this document are to be interpreted as described in [R4], *RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997*.

In case OPTIONAL features are implemented, they MUST be implemented as described in this Technical Report.

1.3.2 CAs, Keys and Certificates

The following Keys and Certificates are relevant within the scope of this Technical Report:

Name	Abbreviation	Comments
Country Signing CA	CSCA	
Country Signing CA Certificate	C_{CSCA}	Issued by CSCA (self-signed). Carries the Country Signing CA Public Key (KPu_{CSCA}). Stored in the inspection system.
Country Signing CA Private Key	KPr_{CSCA}	Signing the Document Signer Certificate (C_{DS}). Stored in a Issuing State's (highly) secured environment.
Country Signing CA Public Key	KPu_{CSCA}	For verification of the authenticity of the Document Signer Certificate (C_{DS}).
Document Signer	DS	
Document Signer Certificate	C_{DS}	Issued by Country Signing CA (CSCA). Carries the Document Signer Public Key (KPu_{DS}). Stored in the inspection system AND/OR in the MRTD's chip.
Document Signer Private Key	KPr_{DS}	Signing the Document Security Object (SO_D). Stored in a Issuing State's (highly) secured environment.
Document Signer Public Key	KPu_{DS}	For verification of the authenticity of the Document Security Object (SO_D).
Document Security Object	SO_D	A RFC3369 CMS Signed Data Structure, signed by the Document Signer (DS). Carries the hashed LDS Data Groups. Stored in the MRTD's chip.

Name	Abbreviation	Comments
		MAY carry the Document Signer Certificate (C_{DS}).
Active Authentication Private Key	KPr_{AA}	OPTIONAL. Signature calculation in Active Authentication mechanism of the MRTD's chip. Stored in the chip's Secure Memory.
Active Authentication Public Key	KPu_{AA}	OPTIONAL. Signature verification in Active Authentication mechanism of the MRTD's chip.
Document Basic Access Keys	K_{ENC} and K_{MAC}	OPTIONAL. To obtain access to public MRTD data and to secure communications between MRTD's chip and inspection system.

1.3.3 Abbreviations

Abbreviation	
APDU	Application Protocol Data Unit
BLOB	Binary Large OBject
CA	Certificate Authority
CRL	Certificate Revocation List
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
NTWG	New Technologies Working Group
PKI	Public Key Infrastructure
PKD	Public Key Directory
TAG	Technical Advisory Group

1.4 Reference documentation

The following documentation served as reference for this Technical Report:

[R1] *PKI Threat Assess, ICAO-NTWG, Sept 03 Final. October 03, 2003*

[R2] *Technical Report: PKI Digital Signatures for Machine Readable Travel Documents, version 4*

[R3] *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies.*

[R4] *RFC 2119, S. Bradner, "Key Words for Use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997*

[R5] *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*

[R6] *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002*

[R7] *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*

[R8] *FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002*

[R9] *FIPS 186-2, Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000. (Supersedes FIPS PUB 186-1 dated 15 December 1998)*

[R10] *FIPS 186-3, Federal Information Processing Standards Publication (FIPS PUB) 186-3, Digital Signature Standard*

[R11] *X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", January 7, 1999*

[R12] *ISO/IEC 7816-4, Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange, 1994*

[R13] *ISO/IEC 7816-8, Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security architecture and related interindustry commands, 1999*

[R14] *RFC 3369, Cryptographic Message Syntax, August 2002.*

[R15] *ICAO Doc 9303, Machine Readable Travel Documents, Fifth Edition – 2003.*

[R16] *ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997.*

[R17] *ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002.*

2. Overview

2.1 General outline

The principles of PKI schemes have evolved in their use to become highly complex in their application to modern scenarios. Their prime use is in Internet transactions, where keys are to be trusted across a broad range of users and agencies; this has resulted in elaborate systems of key certificates, where public keys are issued in "certificates" which are digitally signed by trusted issuing organizations called Certificate Authorities (CA's). The trust in these CA organizations is further being verified by higher level CA's in a trust hierarchy, each one in the hierarchy issuing the key and signed certificate for the one beneath it in the hierarchy. The highest level in such a hierarchy is the so-called "Root CA". Different hierarchies cross-certify each other to establish trust in the keys issued by each with the other.

A complicating factor is the need for Certificate Revocation Lists (CRL's), indicating where a key (certificate) has lost it's validity for whatever reason. In fact, by revoking a certificate and publishing this revocation in a CRL, the certificate's issuer informs receiving parties that the contents can no longer be trusted. The need to verify certificates for each and every transaction often implies multiple accesses to CA records and to CRL records in different databases. This is a complex requirement.

The ICAO operating environment is different from the above mentioned commercial environments, where the question of public key revocation does apply in a different way (compared to individual users), since the unlikely event of a compromise of any State's private key used during some period to sign many MRTDs cannot deny that documents were indeed signed using that key. These (valid) documents are still in use by there holders for travel purposes. The Digital Signatures applied are meant to last for the validity period of the MRTD and are not intended for every day transaction purposes. In the case of key compromise, a caution mechanism MUST be used to warn States to view those documents more closely.

As a consequence, this Technical Report presents a customized approach that will enable the MRTD community to fast-track implementation of this application for MRTDs with ICC read-only access, and take advantage of its benefits without attempting to address larger PKI policy issues and complex hierarchies. Certificates are used for security purposes, along with a proposed methodology for public key (certificate) circulation to member States and the infrastructure is customized for ICAO purposes.

2.2 Responsibilities

The ICAO PKI application operates in a completely peer-based user environment, with each State independent and autonomous in the matter of MRTDs and security.

Nonetheless it is integral to the program to have an efficient and commonly accepted means of sharing and updating the set of public keys in effect for all non-expired MRTDs in existence for all participating countries at any time.

2.2.1 Issuing States

Each participating State SHALL install its own secure facilities to generate key sets for different periods of time, these SHALL be used to compute the Digital Signatures to be

applied for signing Certificates. These systems or facilities SHALL be well protected from any outside or unauthorized access through inherent design and hardware security facilities.

Country Signing CA.
The CA hierarchy, in which the key generation will be embedded, is only relevant to this Technical Report as far as it involves the Certificates that are distributed to receiving States. The highest level certificate that is distributed SHALL act as the trust point for the receiving State. In this Technical Report this certificate is referenced to as the Country Signing CA Certificate (C_{CSCA}). The Country Signing CA Certificate (C_{CSCA}) SHALL be self-signed and issued by the Country Signing CA (CSCA).

It is RECOMMENDED that Country Signing CA Key Pairs (KPu_{CSCA}, KPr_{CSCA}) are generated and stored in a highly protected, off line CA infrastructure by the issuing State.

Country Signing CA Certificates (C_{CSCA}) MUST distributed by strictly secure diplomatic means (out-of-band distribution).

Each Country Signing CA Certificate (C_{CSCA}) generated by each State MUST also be forwarded to ICAO (for the purpose of validation of Document Signer Certificates (C_{DS})).

The Country Signing CA Private Key (KPr_{CSCA}) is used to sign Document Signer Certificates (C_{DS}).

Annex A specifies the Certificate Profiles.

Document Signer.
It is RECOMMENDED that Document Signer Key Pairs (KPu_{DS}, KPr_{DS}) are generated and stored in a highly protected CA infrastructure by the issuing State.

Each Document Signer Certificate (C_{DS}) generated by each State MUST be forwarded to ICAO, and MAY be stored in the MRTD's chip.

The Document Signer Private Key (KPr_{DS}) is used to sign Document Security Objects (SO_D).

Each Document Security Object (SO_D) generated by each State MUST be stored in the corresponding MRTD's chip.

Annex A specifies the Certificate Profiles.

Certificate Revocation.
Issuing States can revoke certificates in case of an incident (like a key compromise). Such a revocation MUST be communicated bilaterally to all other participating States and to the ICAO Public Key Directory within 48 hours.

In case of absence of incidents issuing States SHOULD distribute 'routine' CRLs bilaterally and to the ICAO Public Key Directory at least every 90 days.

2.2.2 ICAO Public Key Directory (PKD)

In order to efficiently share the Document Signer Certificates (C_{DS}) of all States, ICAO will develop and provide a Public Key Directory (PKD) Service to all participating States. This

service SHALL accept information on public keys from all States, store them in a directory, and make this information accessible to all other States.

Access for updating the PKD SHALL be restricted to member States.

There SHALL NOT be access control for reading the PKD (e.g. for the purpose of downloading PKD information).

Country Signing CA Certificates.
Country Signing CA Certificates (C_{CSCA}) are not part of the ICAO PKD service. The PKD however SHALL use Country Signing CA Certificates (C_{CSCA}) to verify the authenticity and integrity of the Document Signer Certificates (C_{DS}) received from participating States, before publishing.

ICAO does not allow access to the Country Signing CA Certificate (C_{CSCA}).

Document Signer Certificates.
The ICAO PKD is intended as the repository for all Document Signer Certificates (C_{DS}) used by all participating States at any time. This includes certificates actively being used at any time for signing purposes as well as those no longer being used but still in effect for issued MRTDs.

The ICAO PKD will be the primary distribution mechanism for all these Document Signer Certificates (C_{DS}) and so MUST be populated and maintained up-to-date by all participating States.

Public Key information from a certain Issuing State, stored in the PKD SHALL also be available for other parties (not being participating States) that need this information for validating the authenticity of digitally stored MRTD data.

Certificate Revocation Lists.
The PKD will also be a repository for all Certificate Revocation Lists (CRLs) issued by each participating State. Although States SHALL primarily distribute CRLs bilaterally, they MUST also be communicated to the PKD. As such the ICAO PKD will be the secondary distribution mechanism for CRLs.

2.2.3 Receiving States

Members of the PKD service SHALL access the ICAO PKD service on a regular basis and download new key certificate information for storage and use by their internal border systems.

Similarly, it is a relying State's responsibility to maintain a current CRL cache, namely a current set of CRLs, which SHALL be part of the downloaded information from the ICAO PKD.

Each receiving State SHALL take care of the internal distribution of Country Signing CA Certificates (C_{CSCA}), Document Signer Certificates (C_{DS}) and CRLs to it's inspection systems.

It is a State's responsibility to store the Country Signing CA Certificates (C_{CSCA}), as being trust points, in a secure way in their border inspection systems.

2.2.4 Other parties

Everyone who has the appropriate equipment is able to read the chip contents of the MRTD, but only the parties that are provided with the appropriate public key certificates and certificate revocation lists will be able to verify the authenticity and integrity of the chip contents. These parties MAY obtain this information from the ICAO Public Key Directory, although they will have to obtain the set of Country Signing CA Certificates (C_{CSCA}) by other means as these are not published in the ICAO PKD.

2.3 Data Authentication

2.3.1 Passive authentication

In addition to the LDS Data Groups, the chip also contains a Document Security Object (SO_D). This object is digitally signed by the issuing State and contains hash representations of the LDS contents (see Section 3).

An inspection system, containing the Document Signer Public Key (KPu_{DS}) of each State, or having read the Document Signer Certificate (C_{DS}) from the MRTD, will be able to verify the Document Security Object (SO_D). In this way, through the contents of the Document Security Object (SO_D), the contents of the LDS is authenticated.

This verification mechanism does not require processing capabilities of the chip in the MRTD. Therefore it is called 'passive authentication' of the chip contents.

Passive authentication proves that the contents of the Document Security Object (SO_D) and LDS are authentic and not changed. It does not prevent exact copying of the chip content or chip substitution.

Therefore a passive authentication system SHOULD be supported by an additional physical inspection of the MRTD.

Passive authentication is specified in 3.2.2.

2.3.2 Active authentication

An issuing State MAY choose to protect it's MRTDs against chip substitution. This can be done by implementing an active authentication mechanism.

If supported, the active authentication mechanism MUST ensure that the chip has not been substituted, by means of a challenge-response protocol between the inspection system and the MRTD's chip.

For this purpose the chip contains it's own Active Authentication Key pair (KPr_{AA} and KPu_{AA}). A hash representation of Data Group 15 (Public Key (KPu_{AA}) info) is stored in the Document Security Object (SO_D) and therefore authenticated by the issuer's digital signature. The corresponding Private Key (KPr_{AA}) is stored in the chip's secure memory.

By authenticating the visual MRZ (through the hashed MRZ in the Document Security Object (SO_D)) in combination with the challenge response, using the MRTD's Active Authentication Key Pair (KPr_{AA} and KPu_{AA}), the inspection system verifies that the Document Security Object (SO_D) has been read from the genuine chip, stored in the genuine MRTD.

Active authentication requires processing capabilities of the MRTD's chip.

Active authentication is specified in 3.2.2.

2.4 Access control

Comparing a MRTD that is equipped with a contactless chip with a traditional MRTD shows two differences:

- The data stored in the chip can be electronically read without opening the document (skimming).
- The communication between a chip and a reader, that is unencrypted, can be eavesdropped in a distance of several meters.

While there are physical measures possible against skimming these don't address eavesdropping. Therefore, it is understood that States MAY choose to implement a Basic Access Control mechanism, i.e. an access control mechanism that requires the consent of the bearer of the MRTD that the data stored in the chip to be read in a secure way. This Basic Access Control Mechanism prevents skimming as well as eavesdropping.

This access control mechanism is OPTIONAL. Descriptions and specifications in this Technical Report on Basic Access Control and Secure Messaging only apply for MRTDs and Inspection Systems that support this option. If supported, this mechanism MUST ensure that the contents of the chip can only be read after the bearer has willingly offered his MRTD.

A chip that is protected by the Basic Access Control mechanism denies access to it's contents unless the inspection system can prove that it is authorized to access the chip. This proof is given in a challenge-response protocol, where the inspection system proves knowledge of the chip-individual Document Basic Access Keys (K_{ENC} and K_{MAC}) which are derived from information from the MRZ.

The inspection system MUST be provided with this information prior to reading the chip. The information has to be retrieved optically/visually from the MRTD (e.g. from the MRZ). It also MUST be possible for an inspector to enter this information manually on the inspection system in case machine-reading of the MRZ is not possible.

Additionally, after the inspection system has been authenticated successfully, it is REQUIRED that the chip enforces encryption of the communication channel between the inspection system and the MRTD's chip by Secure Messaging techniques.

Assuming that the Document Basic Access Keys (K_{ENC} and K_{MAC}) cannot be obtained from a closed document (since they are derived from the optically read MRZ), it is accepted that the passport was willingly handed over for inspection. Due to the encryption of the channel, eavesdropping on the communication would require a considerable effort.

The access control mechanism is specified in 3.2.2.

2.5 Security for additional biometrics

The personal data stored in the chip as defined to be the mandatory minimum for global interoperability are the MRZ and the digitally stored image of the bearer's face. Both items can also be seen (read) visually after the MRTD has been opened and offered for inspection.

Beside the digitally stored image of the face as the primary biometrics for global interoperability, ICAO also has endorsed the use of digitally stored images of fingers and/or irises in addition to the face. For national or n-lateral use States MAY choose to store templates and/or MAY choose to limit access or encrypt this data, as to be decided by States themselves.

Access to this, more sensitive, personal data SHOULD be more restricted. This can be accomplished in two ways: Extended Access Control or Data Encryption. Although these options are mentioned in this Technical Report ICAO is not proposing or specifying any standards or practices in these areas at this time.

2.5.1 Extended Access Control

The OPTIONAL Extended Access Control mechanism is similar to the Basic Access Control mechanism described before, however for Extended Access Control a Document Extended Access Key set is used instead of the Document Basic Access Keys (K_{ENC} and K_{MAC}).

Defining the (chip-individual) Document Extended Access Key set is up to the implementing State. The Document Extended Access Key set MAY consist of either symmetric keys, e.g. derived from the MRZ and a National Master key, or an asymmetric key pair with a corresponding card verifiable certificate.

Extended Access Control requires processing capabilities of the MRTD's chip.

2.5.2 Encryption

Restricting access to the additional biometrics MAY also be done by encrypting them. To be able to decrypt the encrypted data, the inspection system MUST be provided with a decryption key. Defining the encryption/decryption algorithm and the keys to be used is up to the implementing State and is outside the scope of this Technical Report.

2.6 Securing electronic data in MRTDs (Summary)

Beside Passive Authentication by Digital Signatures, States MAY choose additional security, using more complex ways of securing the chip and its data. The options given in the table can be suitably combined to achieve additional security according to existing ISO/IEC standards.

BASELINE SECURITY METHOD				
Method	**Issuer**	**Insp. System**	**Benefits**	**Deficiencies**
Passive Authentication (2.3.1)	**M**	**M**	Proves that the contents of the SO_D and the LDS are authentic and not changed.	Does not prevent an exact copy or chip substitution. Does not prevent unauthorized access. Does not prevent skimming.
ADVANCED SECURITY METHODS				
Comparison of conventional MRZ(OCR-B) and chip-based MRZ(LDS)	N/A	O	Proves that chip content and physical MRTD belong together	Adds (minor) complexity. Does not prevent an exact copy of chip AND conventional document.
Active Authentication (2.3.2)	O	O	Prevents copying the SO_D and proves that it has been read from the authentic chip. Proves that the chip has not been substituted.	Adds complexity. Requires processor-chips.
Basic Access Control (2.4)	O	O	Prevents skimming and misuse. Prevents eavesdropping on the communications between MRTD and inspection system (when used to set up encrypted session channel).	Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Adds complexity. Requires processor-chips.
Extended Access Control (2.5.1)	O	O	Prevents unauthorized access to additional biometrics. Prevents skimming of additional biometrics.	Requires additional key management. Does not prevent an exact copy or chip substitution (requires also copying of the conventional document). Adds complexity. Requires processor-chips.
Data Encryption (2.5.2)	O	O	Secures additional biometrics. Does not require processor-chips.	Requires complex decryption key management. Does not prevent an exact copy or chip substitution. Adds complexity.

MRTDs issued by States choosing to use advanced security methods will be fully ICAO compliant and deem to meet global interoperability standards.

3. Specifications

3.1 MRTD

3.1.1 MRTD personalisation

MRTD production and personalisation are the States' responsibility and therefore out of the scope of this Technical Report.

However, it is RECOMMENDED that States implement measures to secure transport and storage of chips, the embedding of the chips in MRTDs and the personalisation process.

This version of the Technical Report is based on the assumption that MRTDs will not be written to after personalisation. Therefore the personalisation process SHOULD lock the chip as a final step.

In the event of a State's PKI infrastructure not being available to sign MRTD data as part of personalisation, and the issuance of the document(s) can not be delayed, it is RECOMMENDED that the MRTD's chip is left blanc and be locked. The passport book SHOULD contain an appropriate endorsement on this. This is expected to be an exceptional circumstance.

3.1.2 Information stored in the chip

Schematically, the contents of the MRTD's chip is as follows:

MF	
|	
|---------DF – LDS	REQUIRED
|	
|---------K_{ENC}	OPTIONAL
|	
|---------K_{MAC}	OPTIONAL
|	
|---------KPr_{AA}	OPTIONAL
|	
|---------EF – COM	REQUIRED
|	
|---------EF – SO_D	REQUIRED
|	
|---------EF – Datagroup_1 (MRZ)	REQUIRED
|	
|---------EF – Datagroup_2 (Encoded Face)	REQUIRED
//	
|---------EF – Datagroup_n	OPTIONAL

K_{ENC} , K_{MAC}

The (OPTIONAL) Document Basic Access Keys (K_{ENC} and K_{MAC}) are stored in the DF. Derivation of these keys from the MRZ is described in paragraph 3.2.2.

KPr_{AA}
The (OPTIONAL) Active Authentication Private Key (KPr_{AA}) is stored in the DF.

EF-COM
See [R3], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies.*.

EF-Data Group 1-n
See [R3], *Technical Report: Development of a Logical Data Structure – LDS for optional capacity expansion technologies.*.

EF-SO_D
The EF-SO_D contains the Document Security Object (SO_D). The Document Security Object (SO_D) contains the hash values of the LDS Data Groups that are being used (this structure is called the LDS Security Object (SO_{LDS}). The specification of the Document Security Object (SO_D), including an ASN.1 formatted example of the LDS Security Object (SO_{LDS}) can be found in Annex C.

3.2 Inspection

3.2.1 Inspection system

In order to support the required functionality and the defined options that can be implemented on MRTDs, that will be offered, the inspection system will have to meet certain pre-conditions.

For MRTD Basic Access Control.
Although the described Basic Access Control is OPTIONAL, inspection systems supporting it MUST meet the following pre-conditions:

- The inspection system is equipped with a MRZ reader or a form of manual input device (f.i. a keyboard) to derive the Document Basic Access Keys (K_{ENC} and K_{MAC}) from the MRTD.
- The inspection system's software supports the protocol described in paragraph 3.2.2, in the case that a MRTD with Basic Access Control is offered to the system, including the encryption of the communication channel with Secure Messaging.

For Passive Authentication.
To be able to perform a passive authentication of the data, stored in the MRTD's chip, the inspection system needs to have knowledge of key information of the issuing States:

- Of each participating issuing State the Country Signing CA Certificate (C_{CSCA}) MUST be stored in the inspection system.
- Of each participating issuing State the Document Signer Certificate (C_{DS}) MUST be stored in the inspection system.

For Active Authentication.
Support of Active Authentication by inspection systems is OPTIONAL.

If the inspection system supports the OPTIONAL Active Authentication it is REQUIRED that the inspection system has the ability to read the visual MRZ.

If the inspection system supports the OPTIONAL Active Authentication the inspection system's software SHALL support the Active Authentication protocol described in paragraph 3.2.2.

For Extended Access Control to additional biometrics.
The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilateral agreed specifications between States, sharing this information.

For Decryption of additional biometrics.
The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilateral agreed specifications between States, sharing this information.

3.2.2 Inspection process flow

This section describes the flow of the inspection process steps in order of occurrence. Both OPTIONAL and REQUIRED steps are described.

MRTD Basic Access Control (OPTIONAL)
When a MRTD with OPTIONAL Basic Access Control mechanism is offered to the inspection system optically or visually read information is used to derive the Document Basic Access Keys (K_{ENC} and K_{MAC}) to gain access to the chip and to set up a Secure Channel for communications between the MRTD's chip and the inspection system.

A MRTD chip that supports Basic Access Control MUST respond to unauthenticated read attempts (including *selection* of (protected) files in the LDS) with 'Security status not satisfied' (0x6982). To authenticate the inspection system the following steps MUST be performed:

1. The inspection system reads the 'MRZ_information' consisting of the concatenation of Document-Number, Date-of-Birth and Date-of-Expiry, including their respective checkdigits, as described in [ref to ICAO doc 9303] from the MRZ using an OCR-B reader. Alternatively, the required information can be typed in, in this case it SHALL be typed in as it appears in the MRZ. The most significant 16 bytes of the SHA-1 hash of this 'MRZ_information' is used as key seed to derive the Document Basic Access Keys using the key derivation mechanism described in Annex E.1.
2. The inspection system and the MRTD chip mutually authenticate and derive session keys. The authentication and key establishment protocol described in Annex E.2 MUST be used.
3. After successful authentication, subsequent communication MUST be protected by Secure Messaging as described in Annex E.3.

Passive Authentication (REQUIRED)
The inspection system performs the following steps:
1. The Document Security Object (SO_D) (OPTIONALLY containing the Document Signer Certificate (C_{DS})) is read from the chip.
2. The Document Signer (DS) is read from the Document Security Object (SO_D).
3. The digital signature of the Document Security Object (SO_D) is verified by the inspection system, using the Document Signer Public Key (KPu_{DS}). The Document

Signer Certificate (C_{DS}) for this key is stored in the inspection system as downloaded from the ICAO PKD and MAY also be stored in the MRTD's chip. This ensures that the Document Security Object (SO_D) is authentic, issued by the authority mentioned in the Document Security Object (SO_D) and unchanged. So the contents of the Document Security Object (SO_D) can be trusted and SHOULD be used in the inspection process.

4. The inspection system reads relevant data groups from the LDS.
5. By hashing the contents and comparing the result with the corresponding hash value in the Document Security Object (SO_D) it ensures that the contents of the data group is authentic and unchanged.

The biometric information can now be used to perform the biometrics verification with the person who offers the MRTD.

Active Authentication (OPTIONAL)
When a MRTD with the OPTIONAL Data Group 15 is offered to the inspection system, the Active Authentication mechanism MAY be performed to ensure that the data is read from the genuine chip and that the chip and data page belong to each other.

The inspection system and the chip perform the following steps:

1. The entire MRZ is read visually from the MRTD's data page (if not already read as part of the Basic Access Control procedure) and compared with the MRZ value in Data Group 1. Since the authenticity and integrity of Data Group 1 have been checked through Passive Authentication similarity ensures that the visual MRZ is authentic and unchanged.
2. Passive Authentication has also proved the authenticity and integrity of Data Group 15. This ensures that the Active Authentication Public Key (KPu_{AA}) is authentic and unchanged.
3. To ensure that the Document Security Object (SO_D) is not a copy the inspection system uses the MRTD's Active Authentication Key pair (KPr_{AA} and KPu_{AA}) in a challenge-response protocol with the MRTD's chip as described in D.2.

After a successful challenge-response protocol it is proven that the Document Security Object (SO_D) belongs to the data page, the chip is genuine and chip and data page belong to each other.

Extended Access Control to additional biometrics (OPTIONAL)
The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilateral agreed specifications between States, sharing this information.

Decryption of additional biometrics (OPTIONAL)
The implementation of the protection of the OPTIONAL additional biometrics depends on the State's internal specifications or the bilateral agreed specifications between States, sharing this information.

3.2.3 Additional command set

The minimum command set (defined by the NTWG Task Force 'LDS and Related') MUST at least contain the commands:
SELECT FILE (See ISO7816-4)
READ BINARY (See ISO7816-4)

Implementation of the recommendations, defined as OPTIONAL, in this Technical Report requires support of the following additional commands:
EXTERNAL_AUTHENTICATE (See ISO7816-4)

INTERNAL_AUTHENTICATE (See ISO7816-4)
GET_CHALLENGE (See ISO7816-4)

3.3 Algorithms

3.3.1 Overview

States MUST support the same algorithm for use in their Country Signing CA, Document Signing keys and where applicable Document Security Objects, although different key sizes may be required depending on the algorithm selected.

States MUST support all algorithms at points where they wish to validate the signature on passport documents and where they exchange key management with other States.

The recommendations on key sizes here assume the maximum recommendations for key issuing periods and a ten-year maximum document validity.

For signature generation in the Active Authentication mechanism States SHALL use ISO9796-2 Digital Signature scheme 1 ([R17], *ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002.*).

For use in their Country Signing CA, Document Signing keys and where applicable Document Security Objects States SHALL support one of the algorithms below.

3.3.2 RSA

Those States implementing the RSA algorithm for signature generation and verification of Certificates and the Document Security Object (SO_D) SHALL use RFC3447 ([R7], *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*). RFC 3447 specifies two signature mechanisms, RSASSA-PSS and RSASSA-PKCS1_v15. It is RECOMMENDED to generate signatures according to RSASSA-PSS, but receiving States MUST also be prepared to verify signatures according to RSASSA-PKCS1_v15.

It is RECOMMENDED that the minimum size of the modulus, n, for Country Signing CA Keys using RSA is *3072 bits*.

It is RECOMMENDED that the minimum size of the modulus, n, for Document Signer Keys using RSA is *2048 bits*.

It is RECOMMENDED that the minimum size of the modulus, n, for Active Authentication Keys using RSA is *1024 bits.*

3.3.3 DSA

Those States implementing the DSA algorithm for signature generation or verification SHALL use FIPS 186-2 ([R9], *FIPS 186-2, Federal Information Processing Standards Publication (FIPS PUB) 186-2 (+ Change Notice), Digital Signature Standard, 27 January 2000. (Supersedes FIPS PUB 186-1 dated 15 December 1998)*).
The current specification for DSA FIPS186-2 only supports 1024 key lengths. A new version of the standard FIPS186-3 is being trialled but no date for its availability could be ascertained at this point in time.

It is RECOMMENDED that the minimum size of the moduli, p and q, for Country Signing CA Keys using DSA is *3072 and 256 bits respectively.*

It is RECOMMENDED that the minimum size of the moduli, p and q, for Document Signer Keys using DSA is *2048 and 224 bits respectively*.

It is RECOMMENDED that the minimum size of the moduli, p and q, for Active Authentication Keys using DSA is *1024 and 160 bits respectively.*

3.3.4 Elliptic Curve DSA

Those States implementing the ECDSA algorithm for signature generation or verification SHALL use X 9.62 ([R11], *X9.62, "Public Key Cryptography For The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", January 7, 1999*). The elliptic curve domain parameters used to generate the ECDSA key pair MUST be described explicitly in the parameters of the public key, i.e. parameters MUST be of type ECParameters (no named curves, no implicit parameters) and MUST include the optional cofactor. ECPoints MUST be in uncompressed format.

It is RECOMMENDED that the minimum size for the base point order for Country Signing CA Keys using ECDSA is *256 bits*.

It is RECOMMENDED that the minimum size for the base point order for Document Signer Keys using ECDSA is *224 bits*.

It is RECOMMENDED that the minimum size for the base point order for Active Authentication Keys using ECDSA is *160 bits*.

3.3.5 Hashing Algorithms

SHA-1, SHA-224 (Draft), SHA-256, SHA-384 and SHA-512 are all permitted hashing algorithms. See [R8], *FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB) 180-2, Secure Hash Standard, August 2002*.

An appropriately sized hashing algorithm SHOULD be selected for the signature algorithm chosen. For example:

- SHA-1 with RSA 1024
- SHA-224 with ECDSA 224

3.4 Key management

3.4.1 Overview

Issuing States SHALL have at least two key types, we call them:

- Country Signing CA Keys
- Document Signer Keys

Issuing States MAY have additional key types:

- Active Authentication Keys

The Country Signing CA Keys and the Document Signer Keys are issued using X.509 certificates (RFC3280, see [R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet*

X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002) and the public keys contained within them are used to validate Document Signer Keys (in the case of Country Signing CA Keys) or Document Security Objects (SO_D) issued by that State (in the case of Document Signer Keys).

All certificates issued by States MUST conform to the certificate profile in Annex A.

States MUST issue a Certificate Revocation List on a periodic basis, see section 3.4.5 on revocation.

3.4.2 Active Authentication Keys

The OPTIONAL Active Authentication Key Pairs (KPr_{AA} and KPu_{AA}) SHALL be generated in a secure way.

Both the Active Authentication Public Key (KPu_{AA}) and the Active Authentication Private Key (KPr_{AA}) are stored in the MRTD's chip. After that, no Key Management is applicable for these keys.

3.4.3 Document Signer Keys

Document Signer Certificates (C_{DS}) are used to verify the validity of Document Security Objects (SO_D). Therefore, to accept an electronic passport from another State, the receiving State MUST already have placed into some form of trust store a copy of the originating States Document Signer Certificates (C_{DS}).

It is RECOMMENDED that the Document Signer Certificate (C_{DS}) is stored in the Document Security Object (SO_D). See Annex C for details.

The Document Signer Certificate (C_{DS}) could be read from the MRTD's chip if the issuing State supports the storage of this certificate in the chip.

Document Signer Key Lifetime

The life time, i.e. the certificate validity period, of the Document Signer Key is determined by concatenating the following two periods:

- The length of time the key will be used to issue Passports, with;
- The [longest] validity period of any passport issued under that key. [1]

The Document Signer Certificate (C_{DS}) SHALL be valid for this total period to enable the authenticity of passports to be verified. However the key SHOULD only be used to issue documents for a limited period, once the last document it was used to issue has expired itself the Public Key is no longer required.

Once the last document has been produced it is RECOMMENDED that States erase the private key in an auditable and accountable manner.

Document Signer Key Issuing Period

[1] Some nations may issue passports before they become valid, for instance on a change of name upon marriage. The effect of doing this is to extend the validity period by the longest period it is possible to pre-issue the passport.

When deploying their systems States may wish to take into account the number of documents that will be signed by any one individual Document Signer Key. A State which issues a large number of documents per day, and only uses one Document Signer Key may wish to use a short issuing period in order to minimise business continuity costs in the event of the Document Signer Key being revoked (see section 3.4.5). Alternatively a State may also choose to use a large number of signing keys to reduce the overhead on any single key.

However, if a State issues only a small number of certificates, there is no necessity for the issuing period of the Document Signer Key to be as short and therefore MAY be longer.

It is therefore RECOMMENDED that the maximum period the Document Signer Key is used to sign passport documents is three months. For States that generate large numbers of MRTD's several current document signing keys MAY be issued at any given time.

3.4.4 Country Signing CA Keys

Country Signing CA Certificates (C_{CSCA}) are used to verify the validity of Document Signer Keys. Therefore, to accept an electronic passport from another State, the receiving State MUST already have placed into some form of trust store, accessible by their border control system, a copy of the originating States Country Signing CA Certificate (C_{CSCA}).

Country Signing CA Key Lifetime

The life time, i.e. the certificate validity, of the Country Signing CA Key is determined by concatenating the following periods:

- The length of time the Country Signing CA Key will be used to issue Document Signer Certificates (C_{DS}), and;
- The Key Lifetime of Document Signer Keys, this is made up of:
    - The length of time the key will be used to issue Passports
    - The [longest] validity period of any passport issued under that key.

Country Signing CA Key Issuing Period

The issuing period for the Country Signing CA Key is a delicate balance between:

- In the unlikely event of a State's Country Signing CA Key being compromised, then the validity of all the passports issued using Document Signer Keys issued under the Country Signing CA Key in question are called into doubt. Consequently States MAY wish to keep the issuing period quite short;
- Keeping the issuing period very short, however, leads to having a very large number of Country Signing CA Keys present at any one time. This can lead to a complex certificate management within the border processing systems;
- If Country Signing CA Key rollover is too infrequent it is possible that this will make it more difficult for States due to lack of knowledge or facilities.

It is therefore RECOMMENDED that a State's Country Signing CA Key be replaced every 3 to 5 years.

Country Signing Re-key

Country Signing CA Keys provide the trust points in the whole system and without these the system would collapse. Therefore States SHOULD plan the replacement of their Country Signing CA Key carefully. Once the initial signing period has elapsed a State will always have at least two Country Signing CA Certificates (C_{CSCA}) valid at any one time.

States MUST give 90 days notification that their CSCA certificate is about to change, and then distribute their new CSCA certificate bi-laterally. To authenticate their new certificate States should also confirm their new CSCA certificate using an out-of-band method.

States MAY additionally produce link certificates to support backwards compatibility with previously issued CSCA certificates. Where States choose to issue link certificates they do not have to issue CSCA certificates using an out-of-band method.

States should refrain from using their CSCA certificate for the first 2 days after issuance.

3.4.5 Revocation

All National authorities that issue Document Signer Certificates (C_{DS}) MUST produce periodic revocation information in the form of Certificate Revocation Lists (CRL). Issued CRL's MUST conform to the profile as defined in Annex B.

States MUST produce at least one CRL every 90 days. States MAY choose to produce a CRL more frequently than every 90 days but not more frequently than every 48 hours.

Revocation Notification
When a State wishes to revoke a Document Signer Key, they do not need to wait until the `nextUpdate` period in the current CRL is due to issue a new CRL. It is RECOMMENDED that a new CRL will be issued within a 48 hour period of revocation notification.

Country Signing CA Key Revocation
Revocation of a Country Signing CA Key is both extreme and difficult. Upon informing a relying State that a Country Signing CA Key has been revoked all other keys issued using that key are effectively revoked.

Where a State has used an old Country Signing CA Key to authenticate a new Country Signing CA Key (see "Country Signing re-key" in 3.4.4) revoking the old Country Signing CA Key SHALL also revoke the new Country Signing CA Key.

To issue new documents the issuing State basically MUST revert to bootstrapping their authentication process all over again by establishing bi-laterally the new Country Signing CA Certificates (C_{CSCA}) they issued by using the out-of-band method.

3.5 Certificate and CRL distribution

States need to plan their certificate rollover strategies for both Country Signing CA Keys and Document Signer Keys, in order to enable propagation of certificates and CRL's into receiving States' border control systems in a timely manner. Ideally propagation will occur within 48 hours, but some receiving States may have remote and poorly connected border outposts that may take more time for certificates and CRL's to propagate out to.
Receiving States SHOULD make every effort to distribute these certificates and CRLs to all border stations within 48 hours.

Country Signing CA Certificate distribution
Issuing States should expect that Country Signing CA Certificates (C_{CSCA}) will be propagated by receiving States within 48 hours.

Document Signer Certificate distribution
Issuing States should expect that Document Signer Certificates (C_{DS}) will be propagated within 48 hours.

Issuing States can ensure the timely propagation of Document Signer Certificates (C_{DS}) by including the Document Signer Certificate (C_{DS}) within the Document Security Object (SO_D).

CRL distribution
States SHOULD make every attempt whether electronically or by other means to act upon those CRL's issued under exceptional circumstances.

For CRL distribution, also see section 2.2.2.

3.5.1 Distribution through ICAO PKD

For Document Signer Certificates (C_{DS}) the primary distribution channel will be the ICAO Public Key Directory. For CRLs the PKD is the secondary channel. Country Signing CA Certificates (C_{CSCA}) are not published and not accessible in the PKD, but are used by the PKD to verify Document Signer Certificates (C_{DS}) that are offered to it for publication.

Communications.
All communications with the ICAO Public Key Directory SHALL be based on server side authenticated SSL. For this purpose ICAO SHALL obtain a single server key (per site) from a commercial party.

Directory update.
Public Keys SHALL be sent to the PKD as X.509-format certificates, signed by the issuing State using that State's Country Signing CA Key. These Certificates SHALL meet the requirements in Annex A, Certificate Profile.

Updates SHALL be performed using the LDAP protocol, where the directory is altered by changes forwarded. Since it is essential that ICAO exercises some due diligence over the process, the PKD SHALL consist of a "Write Directory", where proposed certificate and CRL updates are sent, and a "Read Directory" which is used to contain new certificates after the due diligence process and which is accessed by the MRTD community to download this information.

The certificates and CRLs are by nature signed by the issuing State. This signature SHALL be verified by ICAO before the Certificate or CRL is published in the "Read Directory".

Directory download.
The PKD will be set up as a X.500 directory. The estimated size of the PKD will be 15 – 20 MB.

Because the PKD is relatively small it is RECOMMENDED that States download the entire PKD on a daily basis. This enables States to process the information further in their own way.

Read access to the PKD SHALL NOT be limited to participating States. The PKD will be a totally open and Internet-enabled resource, also available for read-only access to it's services (for download) to airlines and the like.

3.5.2 Distribution by bilateral means

For CRLs and Country Signing CA Certificates (C_{CSCA}) the primary distribution channel will be bilateral exchange between relying States.

States generally have bilateral agreements and ways of exchanging information bilaterally (f.i. email, LDAP service, et cetera). States SHOULD use these existing channels for the exchange of Certificates and CRLs.

States that currently do not have bilateral agreements or ways of exchanging information bilaterally SHOULD establish such agreements and communication channels with other participating States.

Annex A Certificate Profile

Those States conforming to the specification MUST issue certificates that conform to this profile. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.
The following profile uses the following terminology for each of the fields in the X.509 certificate:

m mandatory – the field MUST be present
x do not use – the field SHOULD NOT be populated
o optional – the field MAY be present
c critical – the extension is marked critical, receiving applications MUST be able to process this extension.

A.1 Certificate Body

Certificate Component	Section in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
Certificate	4.1.1	m	m	
TBSCertificate	4.1.1.1	m	m	see next part of the table
signatureAlgorithm	4.1.1.2	m	m	value inserted here dependent on algorithm selected
signatureValue	4.1.1.3	m	m	value inserted here dependent on algorithm selected
TBSCertificate	4.1.2			
version	4.1.2.1	m	m	MUST be v3
serialNumber	4.1.2.2	m	m	
signature	4.1.2.3	m	m	value inserted here MUST match the OID in signatureAlgorithm
issuer	4.1.2.4	m	m	see A.6
validity	4.1.2.5	m	m	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
subject	4.1.2.6	m	m	see A.6
subjectPublickKeyInfo	4.1.2.7	m	m	
issuerUniqueID	4.1.2.8	x	x	
subjectUniqueID	4.1.2.8	x	x	
extensions	4.1.2.9	m	m	see next table on which extensions SHOULD be present

A.2 Extensions

Extension name	Section in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
AuthorityKeyIndentifier	4.2.1.1	o	m	mandatory in all certificates accept for self-signed Country Signing CA Certificates
SubjectKeyIdentifier	4.2.1.2	m	o	
KeyUsage	4.2.1.3	mc	mc	This extension MUST be marked CRITICAL
PrivateKeyUsagePeriod	4.2.1.4	o	o	This would be the issuing period of the private key
CertificatePolicies	4.2.1.5	o	o	
PolicyMappings	4.2.1.6	x	x	
SubjectAltName	4.2.1.7	x	x	
IssuerAltName	4.2.1.8	x	x	
SubjectDirectoryAttributes	4.2.1.9	x	x	
BasicConstraints	4.2.1.10	mc	x	This extension MUST be marked CRITICAL
NameConstraints	4.2.1.11	x	x	
PolicyConstraints	4.2.1.12	x	x	
ExtKeyUsage	4.2.1.13	x	x	
CRLDistributionPoints	4.2.1.14	o	o	If States choose to use this extension they MUST include the ICAO PKD as a distribution point. Implementations may also include relative CRL DP's for local purposes, these may be ignored by other nations.
InhibitAnyPolicy	4.2.1.15	x	x	
FreshestCRL	4.2.1.16	x	x	
privateInternetExtensions	4.2.2	x	x	
other private extensions	N/A	o	o	If any private extension is included for national purposes then they MUST NOT be marked. States are discouraged from including any private extensions.

Extension name	Section in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
AuthorityKeyIdentifier	**4.2.1.1**			
keyIdentifier		m	m	If this extension is used this field MUST be supported as a minimum
authorityCertIssuer		o	o	see A.6
authorityCertSerialNumber		o	o	
SubjectKeyIdentifier	**4.2.1.2**			
subjectKeyIdentifier		m	m	
KeyUsage	**4.2.1.3**			
digitalSignature		x	m	
nonRepudiation		x	x	
keyEncipherment		x	x	
dataEncipherment		x	x	
keyAgreement		x	x	
keyCertSign		m	x	
cRLSign		m	x	
encipherOnly		x	x	
decipherOnly		x	x	
BasicConstraints	***4.2.1.10***			
cA		m	x	TRUE for CA Certificates
PathLenConstraint		m	x	0 for New Country Signing CA Certificate, 1 for Linked Country Signing CA Certificate
CRLDistributionPoints	**4.2.1.14**			
distributionPoint		m	x	
reasons		m	x	
cRLIssuer		m	x	
CertificatePolicies				

Extension name	Section in RFC 3280	Country Signing CA Certificate	Document Signer Certificate	Comments
PolicyInformation				
policyIdentifier		m	m	
policyQualifiers		o	o	

A.3 SignatureAlgorithm

The Object Identifiers specified in section 2.2 of [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002* and section A.2 of [R7], *RFC 3447, J. Jonsson, B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", February 2003*, SHALL be used for those algorithms identified in section 3.3 of this document.

A.4 SignatureValue

The signature structures stored in the signatureValue field SHALL be as specified in section 2.2 of [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*, for those algorithms identified in section 3.3 of this document.

A.5 SubjectPublicKeyInfo

The subjectPublicKeyInfo fields for the algorithms specified in section 3.3 of this document SHALL be populated in line with section 2.3 of [R5], *RFC 3279, W. Polk, R. Housley, L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", April 2002*.

A.6 Certificate and Naming conventions

The following naming and addressing convention for Issuer and Subject fields are RECOMMENDED, in both CSCA and DS Certificates, and the Issuer field in Certificate Revocation Lists.

The following Attributes SHOULD be used:

- country. (country codes MUST follow the format of two letter country codes, specified in [R16], *ISO/IEC 3166, Codes for the representation of names of countries and their subdivisions – 1997*.)
- organization.
- organizational-unit.
- common name.

Additionally some countries MAY use:

- serial number.

States wishing to use existing PKI infrastructures to support their passport issuing systems may be bound by existing naming conventions.

Annex B CRL Profile

The following profile uses the following terminology for each of the fields in the X.509 certificate revocation list:

m mandatory – the field MUST be present
x do not use – the field SHOULD NOT be populated
o optional – the field MAY be present
c critical – the extension is marked critical, receiving applications MUST be able to process this extension.

Certificate List Component	Section in RFC 3280	Country Signing CA CRL	COMMENTS
CertificateList	5.1.1	m	
tBSCertList	5.1.1.1	m	see next part of the table
signatureAlgorithm	5.1.1.2	m	value inserted here dependent on algorithm selected
signatureValue	5.1.1.3	m	value inserted here dependent on algorithm selected
tBSCertList	5.1.2		
version	5.1.2.1	m	MUST be v2
signature	5.1.2.2	m	value inserted here dependent on algorithm selected
issuer	5.1.2.3	m	UTF8 Encoding REQUIRED
thisUpdate	5.1.2.4	m	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
nextUpdate	5.1.2.5	m	Implementations MUST specify using UTC time until 2049 from then on using GeneralisedTime
revokedCertificates	5.1.2.6	m	
extensions	5.1.2.7	m	

Extension Name	Section in RFC 3280	Country Signing CA CRL	Comments
authorityKeyIdentifier	5.2.1	m	This MUST be the same value as the subjectKeyIdentifier field in the CRL Issuer's certificate.
issuerAlternativeName	5.2.2	x	
cRLNumber	5.2.3	m	
deltaCRLIndicator	5.2.4	x	
issuingDistributionPoint	5.2.5	x	
freshestCRL	5.2.6	x	
CRL Entry Extensions			
reasonCode	5.3.1	x	
holdInstructionCode	5.3.2	x	
invalidityDate	5.3.3	x	
certificateIssuer	5.3.4	x	

Note:

It is possible that the CRL contains other revocation information, for example concerning system operator or registration authority certificates.

Annex C Document Security Object

The Document Security object is implemented as a SignedData Type, as specified in [R14] *RFC 3369, Cryptographic Message Syntax, August 2002.* All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

C.1 SignedData Type

The processing rules in RFC3369 apply.

m mandatory – the field MUST be present
x do not use – the field SHOULD NOT be populated
o optional – the field MAY be present
c choice – the field contents is a choice from alternatives

Value		Comments
SignedData		
version	m	Value = v3
digestAlgorithms	m	
encapContentInfo	m	
eContentType	m	id-icao-ldsSecurityObject
eContent	m	The encoded contents of an ldsSecurityObject
certificates	o	Nations may choose to include the Document Signer Certificate (C_{DS}) which can be used to verify the signature in the signerInfos field.
crls	x	It is recommended that States do not use this field
signerInfos	m	It is recommended that states only provide 1 signerinfo within this field.
SignerInfo	m	
version	m	The value of this field is dictated by the sid field. See RFC3369 Section 5.3 for rules regarding this field
sid	m	
issuerandSerialNumber	c	It is recommended that nations support this field over subjectKeyIdentifier.
subjectKeyIdentifier	c	
digestAlgorithm	m	The algorithm identifier of the algorithm used to produce the has value over encapsulatedContent and SignedAttrs.
signedAttrs	m	Producing nations may wish to include additional attributes for inclusion in the signature, however these do not have to be processed by receiving nations except to verify the signature value.
signatureAlgorithm	m	The algorithm identifier of the algorithm used to produce the signature value, and any associated parameters.
signature	m	The result of the signature generation process.

Value		Comments
unsignedAttrs	o	Producing States may wish to use this field, but it is not recommended and receiving nations may choose to ignore them.

C.2 ASN.1 Profile LDS Security Object

```
LDSSecurityObject {iso(1) identified-organization(3) icao(ccc) mrtd(1)
security(1) ldsSecurityObject(1)}

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- Imports from RFC 3280 [PROFILE], Appendix A.1
AlgorithmIdentifier FROM
PKIX1Explicit88 { iso(1) identified-organization(3) dod(6)
internet(1) security(5) mechanisms(5) pkix(7)
mod(0) pkix1-explicit(18) }

-- Constants

ub-DataGroups INTEGER ::= 16

-- Object Identifiers

id-icao                   OBJECT IDENTIFIER ::= {1.3.ccc }
id-icao-mrtd              OBJECT IDENTIFIER ::= {id-icao 1}
id-icao-mrtd-security     OBJECT IDENTIFIER ::= {id-icao-mrtd 1}
id-icao-ldsSecurityObject OBJECT IDENTIFIER ::= {id-icao-mrtd-security 1}

-- LDS Security Object

LDSSecurityObjectVersion ::= INTEGER {V0(0)}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier

LDSSecurityObject ::= SEQUENCE {
      version                 LDSSecurityObjectVersion,
      hashAlgorithm           DigestAlgorithmIdentifier,
      dataGroupHashValues     SEQUENCE SIZE (2..ub-DataGroups) OF
DataGroupHash }

DataGroupHash ::= SEQUENCE {
      dataGroupNumber         DataGroupNumber,
      dataGroupHashValue      OCTET STRING }

DataGroupNumber ::= INTEGER {
      dataGroup1   (1),
      dataGroup2   (2),
      dataGroup3   (3),
      dataGroup4   (4),
      dataGroup5   (5),
      dataGroup6   (6),
      dataGroup7   (7),
      dataGroup8   (8),
      dataGroup9   (9),
      dataGroup10 (10),
      dataGroup11 (11),
      dataGroup12 (12),
      dataGroup13 (13),
```

```
      dataGroup14 (14),
      dataGroup15 (15),
      dataGroup16 (16)}
END
```

Notes:
The 'ccc' in `id-icao` defines the ICAO organization. The value of this field (defined by the Registration Authority for ISO 6523) to be published by ICAO.

The field `dataGroupValue` contains the calculated hash over the ***complete*** contents of the Data group EF, specified by dataGroupNumber.

Annex D Active Authentication Public Key Info

D.1 Active Authentication Public Key Info

The OPTIONAL Active Authentication Public Key is stored in the LDS Data Group 15. The format of the structure (SubjectPublicKeyInfo) is specified in [R6], *RFC 3280, R. Housley, W. Polk, W. Ford, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002*. All security objects MUST be produced in Distinguished Encoding Rule (DER) format to preserve the integrity of the signatures within them.

ActiveAuthenticationPublicKeyInfo ::= SubjectPublicKeyInfo

```
SubjectPublicKeyInfo ::= SEQUENCE {
      algorithm         AlgorithmIdentifier,
      subjectPublicKey  BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
      algorithm         OBJECT IDENTIFIER,
      parameters        ANY DEFINED BY algorithm OPTIONAL }
```

D.2 Active Authentication Mechanism

Active Authentication is performed using the ISO7816 INTERAL AUTHENTICATE command. The input is a nonce (RND.IFD) that MUST be 8 bytes. The ICC computes a signature, when an integer factorization based mechanism is used, according to ISO9796-2 Digital Signature scheme 1 ([R17], *ISO/IEC 9796-2, Information Technology – Security Techniques – Digital Signature Schemes giving message recovery – Part 2: Integer factorisation based mechanisms, 2002.*).

M MUST consist of M1 and M2, where M1 MUST be a nonce of length c – 4 bits and M2 is RND.IFD. The trailer option 1 MUST be used in case of SHA-1, if not SHA-1 then option 2 MUST be used.
The result of the signature computation MUST be signature ∑ without the non-recoverable message part M2.

In more detail, IFD (inspection system) and ICC (MRTD's chip) perform the following steps:

1) The IFD generates a nonce RND.IFD and sends it to the ICC using the INTERNAL AUTHENTICATE command.
2) The ICC performs the following operations:
    a) Create the header.
    b) Generate M1.
    c) Calculate h(M)
    d) Create the trailer
    e) Calculate the message representative F.
    f) Compute the signature ∑ and send the response to the IFD.
3) The IFD verifies the response on the send INTERNAL AUTHENTICATE command and checks if the ICC returned the correct value.

Annex E Basic Access Control and Secure Messaging

E.1 Key Derivation Mechanism

The computation of 2 key 3DES keys from a key seed (K_{seed}) is used in both the establishment of the Document Basic Access Keys (K_{ENC} and K_{MAC}) and the establishment of the Session keys for Secure Messaging.

A 32 bit counter c is used to allow for deriving multiple keys from a single seed. Depending on whether a key is used for encryption or MAC computation the following values MUST be used:

- c = 1 (i.e. '0x 00 00 00 01') for encryption.
- c = 2 (i.e. '0x 00 00 00 02') for MAC computation.

The following steps are performed to derive 2 key 3DES keys from the seed K_{seed} and c:

1. Let D be the concatenation of K_{seed} and c ($D = K_{seed} \| c$).
2. Calculate H = SHA-1(D) the SHA-1 hash of D.
3. Bytes 1..8 of H form key K_a and bytes 9..16 of H form key K_b.
4. Adjust the parity bits of keys K_a and K_b to form correct DES keys.

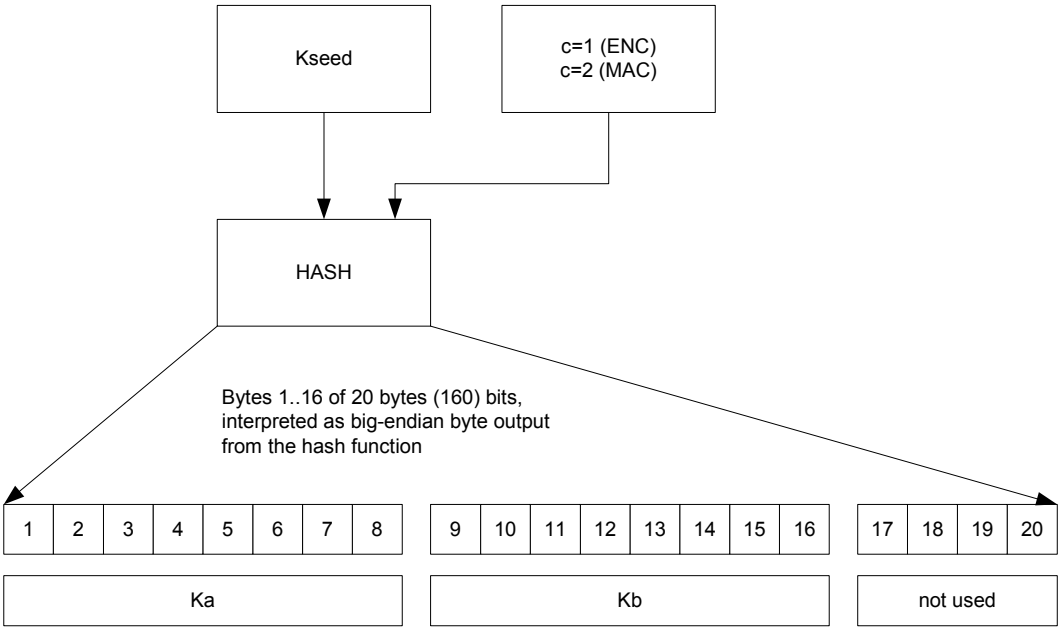


Figure 1: Compute keys from key seed scheme

E.2 Authentication and Key Establishment

Authentication and Key Establishment is provided by a three pass challenge-response protocol according to ISO 11770-2 Key Establishment Mechanism 6 using 3DES as block cipher. A cryptographic checksum according to ISO/IEC 9797-1 MAC Algorithm 3 is calculated over and appended to the ciphertexts. The modes of operation described in Annex E.4 MUST be used. Exchanged nonces MUST be of size 8 bytes, exchanged keying material MUST be of size 16 bytes. Distinguishing identifiers MUST NOT be used.

In more detail, IFD and ICC perform the following steps:

1) The IFD requests a challenge RND.ICC by sending the GET CHALLENGE command. The ICC generates and responds with a nonce RND.ICC.
2) The IFD performs the following operations:
   a) Generate a nonce RND.IFD and keying material K.IFD.
   b) Generate the concatenation S = RND.IFD || RND.ICC || K.IFD
   c) Compute the cryptogram E_IFD = E[K_ENC](S).
   d) Compute the checksum M_IFD = MAC[K_MAC](E_IFD).
   e) Send a MUTUAL AUTHENTICATE command using the data E_IFD || M_IFD.
3) The ICC performs the following operations:
   a) Check the checksum M_IFD of the cryptogram E_IFD.
   b) Decrypt the cryptogram E_IFD.
   c) Extract RND.ICC from S and check if IFD returned the correct value.
   d) Generate keying material K.ICC.
   e) Generate the concatenation R = RND.ICC || RND.IFD || K.ICC
   f) Compute the cryptogram E_ICC = E[K_ENC](R).
   g) Compute the checksum M_ICC = MAC[K_MAC](E_ICC).
   h) Send the response using the data E_ICC || M_ICC.
4) The IFD performs the following operations:
   a) Check the checksum M_ICC of the cryptogram E_ICC.
   b) Decrypt the cryptogram E_ICC.
   c) Extract RND.IFD from R and check if ICC returned the correct value.

E.3 Secure Messaging

After a successful execution of the authentication protocol both the IFD and the ICC compute session keys KS_ENC and KS_MAC using the key derivation mechanism described in Annex E.1 with (K.ICC xor K.IFD) as key seed. All further communication MUST be protected by Secure Messaging in MAC_ENC mode.

E.3.1 Message Structure of SM APDUs

The SM Data Objects MUST be used according to Table 1 in the following order:

- Command APDU: [DO‘87’] [DO‘97’] DO’8E’.
- Response APDU: [DO’87’] DO’99’ DO’8E’.

All SM Data Objects MUST be encoded in BER TLV as specified in ISO/IEC 7816-4. The command header MUST be included in the MAC calculation, therefore the class byte CLA = 0x0c MUST be used.

The actual value of Lc will be modified to Lc’ after application of Secure Messaging. If required, an appropriate data object may optionally be included into the APDU data part in order to convey the original value of Lc. In the protected command APDU the *new Le* byte MUST be set to ‘00’.

	DO’87’	**DO‘97’**	**DO‘99’**	**DO‘8E’**
Meaning	Padding-content indicator byte (‘01’ for ISO-Padding) followed by the cryptogram	Le (to be protected by CC)	Processing status (SW1-SW2, protected by MAC)	Cryptographic checksum (MAC)
Command APDU	Mandatory if data is send, otherwise absent.	Mandatory if data is requested, otherwise absent.	Not used	Mandatory

Response APDU	Mandatory if data is returned, otherwise absent.	Not used	Mandatory, only absent if SM error occurs.	Mandatory if DO‘87’ and/or DO‘99’ is present.

Table 1: Usage of SM Data Objects

Figure 2 shows the transformation of an unprotected command APDU to a protected command APDU in the case *Data* and *Le* are available. If no *Data* is available, leave building DO ’87’ out. If *Le* is not available, leave building DO ‘97’ out.

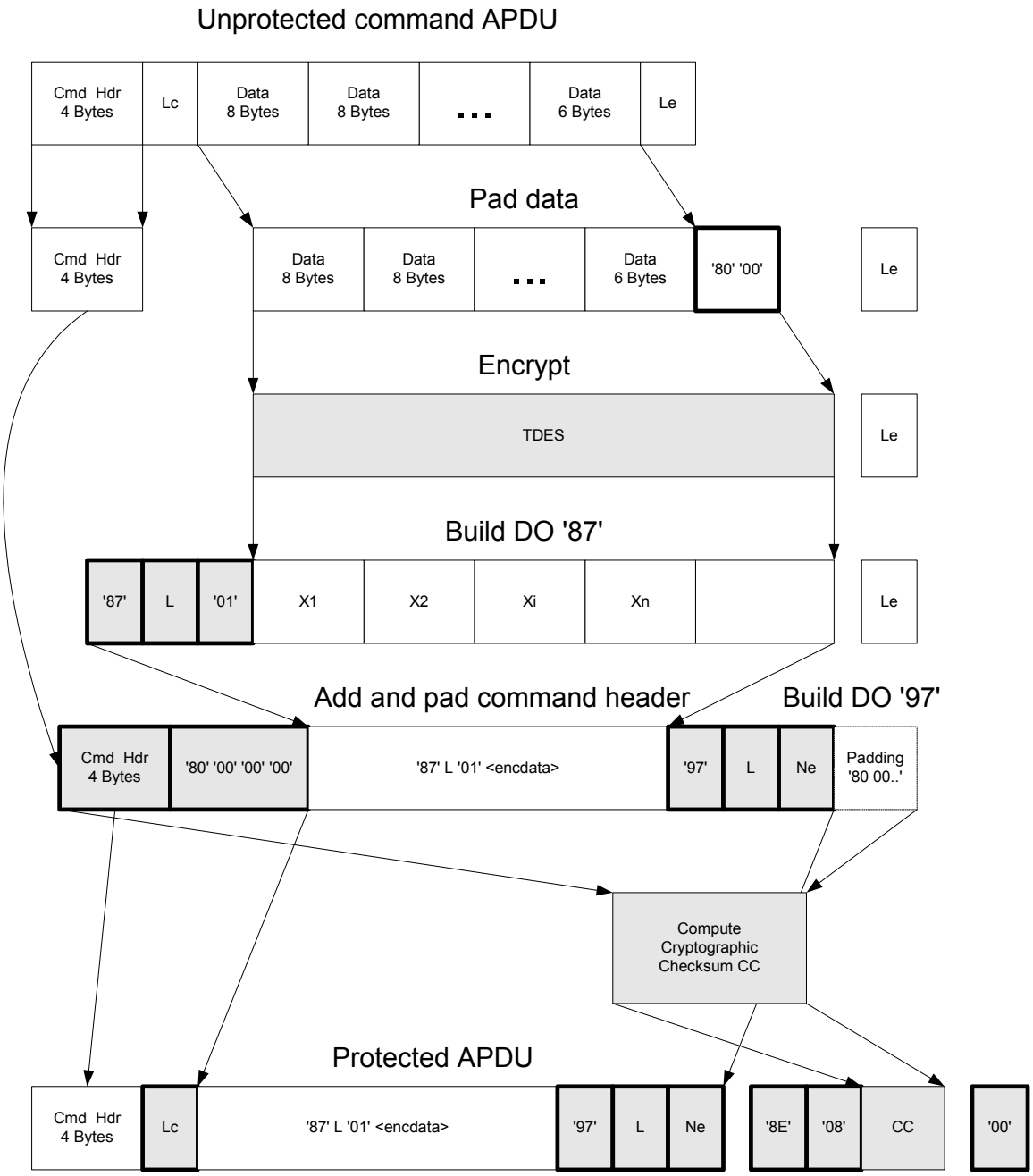


Figure 2: Computation of a SM command APDU

Figure 3 shows the transformation of an unprotected response APDU to a protected response APDU in case *Data* is available. If no *Data* is available, leave building DO ’87’ out.

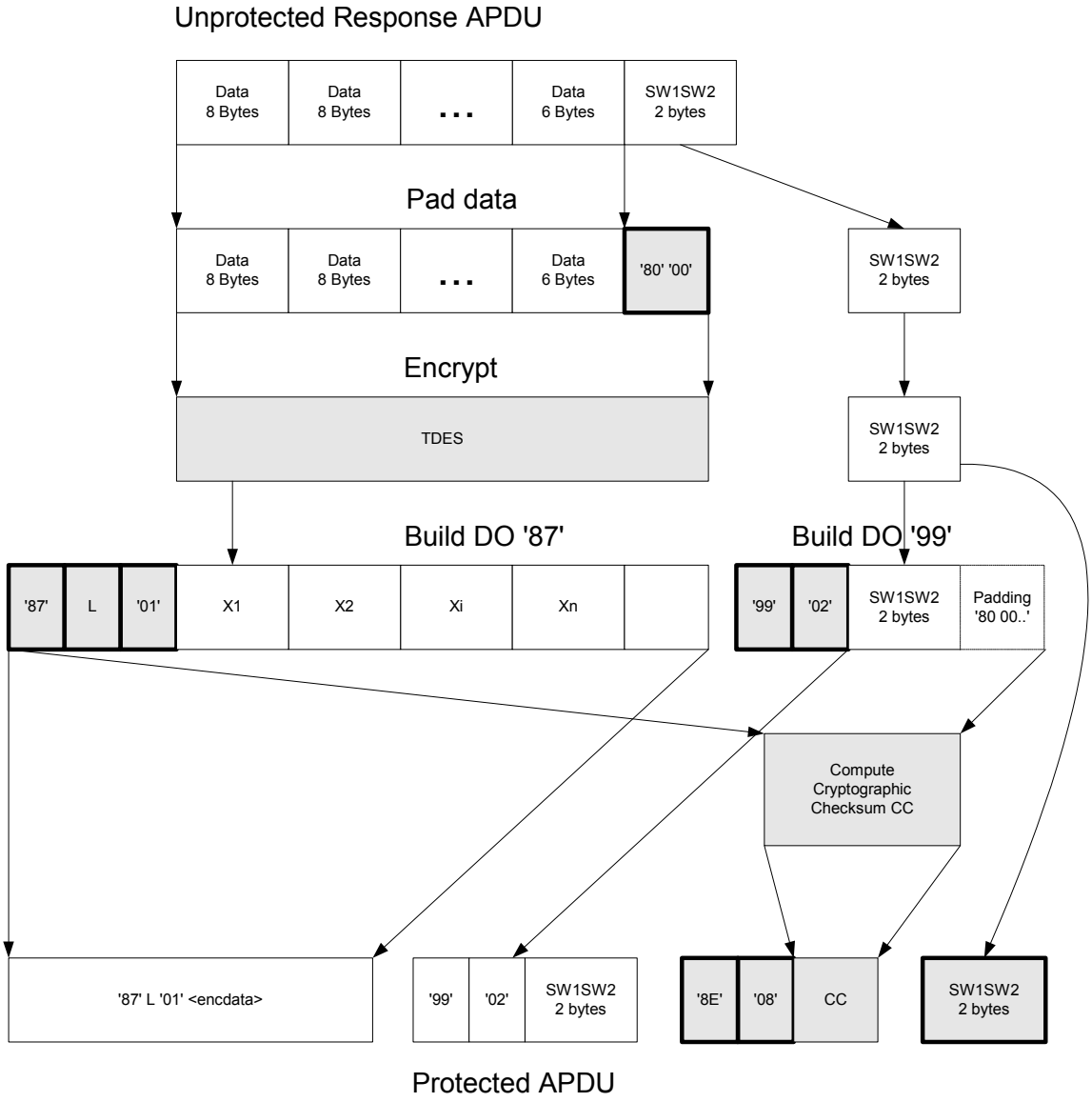


Figure 3: Computation of a SM response APDU

E.3.2 SM errors

When the ICC recognizes an SM error while interpreting a command, then the status bytes must be returned without SM. In ISO/IEC 7816-4 the following status bytes are defined to indicate SM errors:

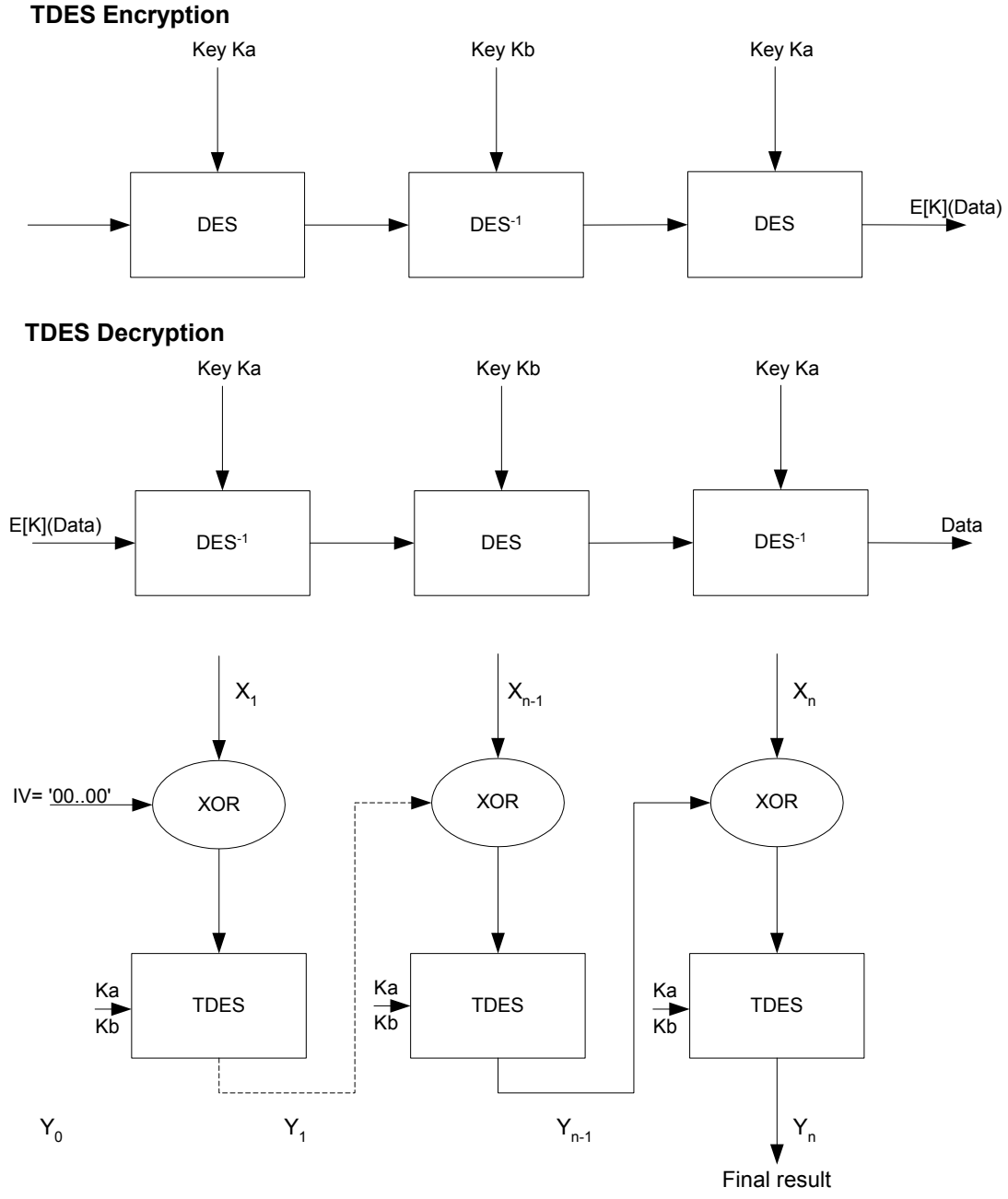
- ´6987´: Expected SM data objects missing
- ´6988´: SM data objects incorrect

Note: Further SM status bytes can occur in application specific contexts. When the ICC returns status bytes without SM DOs or with an erroneous SM DO the ICC deletes the session keys. As a consequence the secure session is aborted.

E.4 3DES Modes of Operation

E.4.1 Encryption

Two key 3DES in CBC mode with zero IV (i.e. 0x00 00 00 00 00 00 00 00) according to ISO 11568-2 is used (see diagrams below). No padding for the input data is used when performing the MUTUAL AUTHENTICATE command. During the computation of SM APDUs, padding according to ISO 9797-1 padding method 2 is used.



IV = zero initialization vector
'$X_1||....||X_n$' = plain text (message to encrypt) where each block X_i is 64-bit long
'$Y_1||....||Y_n$' = resulting cryptogram (encrypted message) where each block Y_i is 64-bit long

Figure 4: 3DES Encryption/Decryption in CBC Mode

E.4.2 Message Authentication

Cryptographic checksums are calculated using ISO/IEC 9797-1 MAC algorithm 3 with block cipher DES, zero IV (8 bytes), and ISO9797-1 padding method 2. The MAC length MUST be 8 bytes.

After a successful authentication the datagram to be MACed MUST be prepended by the Send Sequence Counter. The Send Sequence Counter is computed by concatenating the four least significant bytes of RND.ICC and RND.IFD respectively:

SSC = RND.ICC (4 least significant bytes) || RND.IFD (4 least significant bytes).

The Send Sequence Counter is increased every time before a MAC is calculated, i.e. if the starting value is x, in the next command the value of SSC is x+1. The value of the first response is then x+2.

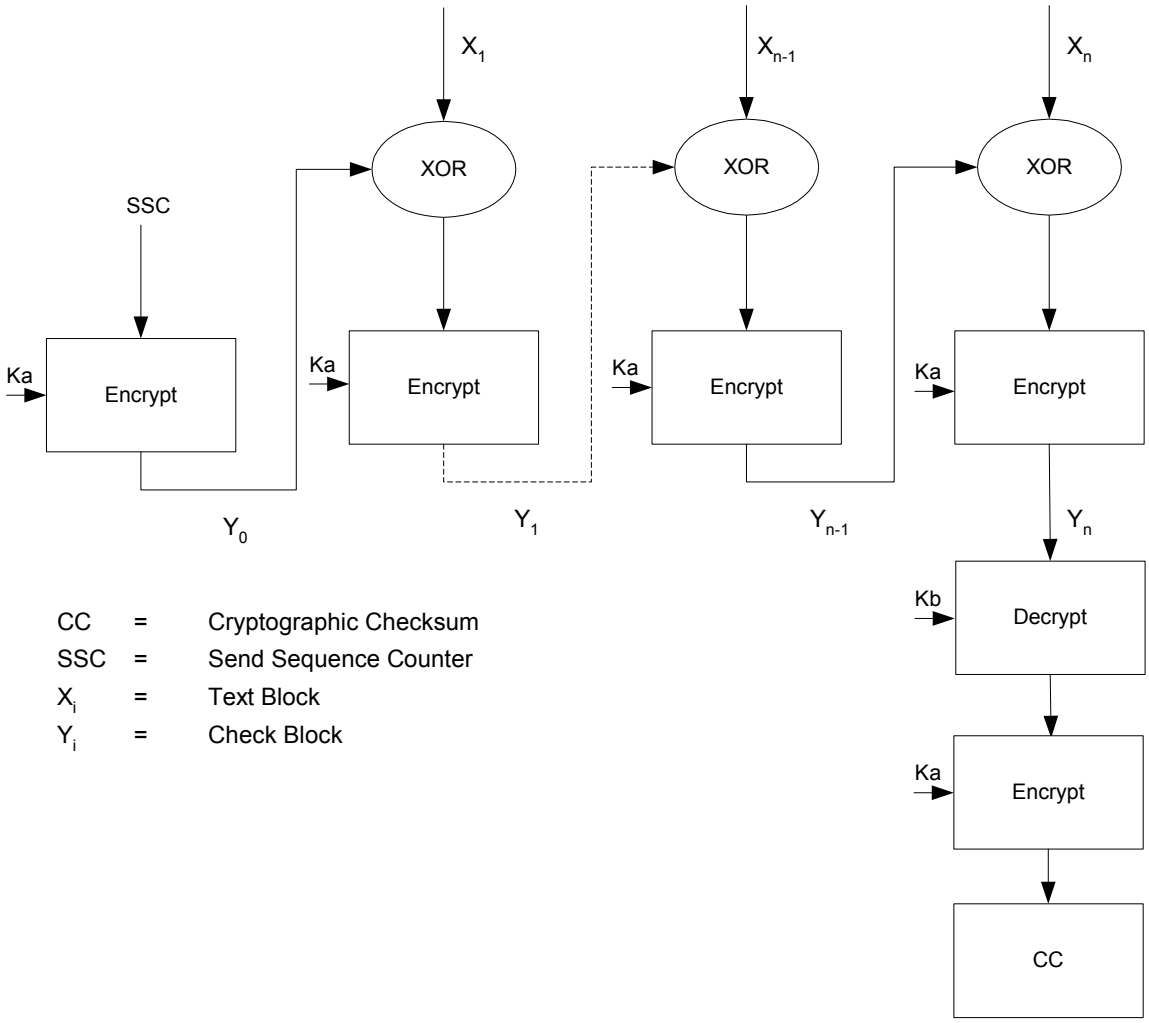


Figure 5: Retail MAC calculation

Annex F Worked Examples

F.1 Command sequences

F.1.1 MRZ based Basic Access Control and Secure Messaging

Compute keys from key seed (K_{seed})

Input:

K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

Compute Encryption key (c = '00000001'):

1. Concatenate K_{seed} and c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000001'

2. Calculate the SHA-1 hash of D:
   $H_{SHA-1}(D)$ = 'AB94FCEDF2664EDFB9B291F85D7F77F27F2F4A9D'

3. Form keys K_a and K_b:
   K_a = 'AB94FCEDF2664EDF'
   K_b = 'B9B291F85D7F77F2'

4. Adjust parity bits:
   K_a = 'AB94FDECF2674FDF'
   K_b = 'B9B391F85D7F76F2'

Compute MAC computation key (c = '00000002'):

1. Concatenate K_{seed} and c:
   D = '239AB9CB282DAF66231DC5A4DF6BFBAE00000002'

2. Calculate the SHA-1 hash of D:
   $H_{SHA-1}(D)$ = '7862D9ECE03C1BCD4D77089DCF131442814EA70A'

3. Form keys K_a and K_b:
   K_a = '7862D9ECE03C1BCD'
   K_b = '4D77089DCF131442'

4. Adjust parity bits:
   K_a = '7962D9ECE03D1ACD'
   K_b = '4C76089DCE131543'

Derivation of Document Basic Access Keys (K_{ENC} and K_{MAC})

1. Read the MRZ:
   MRZ = P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
   L898902C<3UTO6908061F9406236ZE184226B<<<<<14

2. Construct the 'MRZ_information' out of the MRZ:
   Document number = L898902C<, check digit = 3
   Date of Birth = 690806, check digit = 1
   Date of Expiry = 940623, check digit = 6

MRZ_information = L898902C<369080619406236

3. Calculate the SHA-1 hash of 'MRZ_information':
   H_{SHA-1}(MRZ_information) = '239AB9CB282DAF66231D
   C5A4DF6BFBAEDF477565'

4. Take the most significant 16 bytes to form the K_{seed}:
   K_{seed} = '239AB9CB282DAF66231DC5A4DF6BFBAE'

5. Calculate the Basic Access Keys (K_{ENC} and K_{MAC}) using Annex E.1:

   K_{ENC} = 'AB94FDECF2674FDFB9B391F85D7F76F2'
   K_{MAC} = '7962D9ECE03D1ACD4C76089DCE131543'

Authentication and Establishment of Session Keys

Inspection system:

1. Request an 8 byte random number from the MRTD's chip:
   Command APDU:

CLA	INS	P1	P2	LE
00h	84h	00h	00h	08h

   Response APDU:

Response data field	SW1SW2
RND.ICC	9000h

   RND.ICC = '4608F91988702212'

2. Generate an 8 byte random and a 16 byte random:
   RND.IFD = '781723860C06C226'
   K_{IFD} = '0B795240CB7049B01C19B33E32804F0B'

3. Concatenate RND.IFD, RND.ICC and K_{IFD}:
   S = '781723860C06C2264608F91988702212
   0B795240CB7049B01C19B33E32804F0B'

4. Encrypt S with TDES key K_{ENC} as calculated in Annex E.2:
   E_{IFD} = '72C29C2371CC9BDB65B779B8E8D37B29
   ECC154AA56A8799FAE2F498F76ED92F2'

5. Compute MAC over E_{IFD} with TDES key K_{MAC} as calculated in Annex E.2:
   M_{IFD} = '5F1448EEA8AD90A7'

6. Construct command data for MUTUAL AUTHENTICATE and send command APDU to the MRTD's chip:
   cmd_data = '72C29C2371CC9BDB65B779B8E8D37B29ECC154AA
   56A8799FAE2F498F76ED92F25F1448EEA8AD90A7'

   Command APDU:

CLA	INS	P1	P2	LC	Command data field	LE

00h	82h	00h	00h	28h	cmd_data	28h

MRTD's chip:

7. Decrypt en verify received data and compare RND.ICC with response on GET CHALLENGE.

8. Generate a 16 byte random:
   K_{ICC} = '0B4F80323EB3191CB04970CB4052790B'

9. Calculate XOR of K_{IFD} and K_{ICC}:
   K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

10. Calculate Session Keys (KS_{ENC} and KS_{MAC}) using Annex E.1:
    KS_{ENC} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
    KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

11. Calculate Send Sequence Counter:
    SSC = '887022120C06C226'

12. Concatenate RND.ICC, RND.IFD and K_{ICC}:
    R = '4608F919887022127817238 60C06C226
    0B4F80323EB3191CB04970CB4052790B'

13. Encrypt R with TDES key K_{ENC} as calculated in Annex E.2:
    E_{ICC} = '46B9342A41396CD7386BF5803104D7CE
    DC122B9132139BAF2EEDC94EE178534F'

14. Compute MAC over E_{ICC} with TDES key K_{MAC} as calculated in Annex E.2:
    M_{ICC} = '2F2D235D074D7449'

15. Construct response data for MUTUAL AUTHENTICATE and send response APDU to the inspection system:
    resp_data = '46B9342A41396CD7386BF5803104D7CEDC122B91
    32139BAF2EEDC94EE178534F2F2D235D074D7449'

    Response APDU:

Response data field	SW1SW2
resp_data	9000h

Inspection system:

16. Decrypt and verify received data and compare received RND.IFD with generated RND.IFD.

17. Calculate XOR of K_{IFD} and K_{ICC}:
    K_{seed} = '0036D272F5C350ACAC50C3F572D23600'

18. Calculate Session Keys (KS_{ENC} and KS_{MAC}) using Annex E.1:
    KS_{ENC} = '979EC13B1CBFE9DCD01AB0FED307EAE5'
    KS_{MAC} = 'F1CB1F1FB5ADF208806B89DC579DC1F8'

19. Calculate Send Sequence Counter:

SSC = '887022120C06C226'

Secure Messaging

After authentication and establishment of the session keys, the inspection system selects the EF.COM (File ID = '011E') and reads the data using Secure Messaging. The calculated KS_{ENC}, KS_{MAC} and SSC (previous steps 18 and 19) will be used.

First the EF.COM will be selected, then the first 4 bytes of this file will be read so that the length of the structure in the file can be determined and after that the remaining bytes are read.

1. Select EF.COM

   Unprotected command APDU:

CLA	INS	P1	P2	LC	Command data field
00h	A4h	02h	0Ch	02h	01h 1Eh

   a. Mask class byte and pad command header:
      CmdHeader = '0CA4020C80000000'
   b. Pad data:
      Data = '011E800000000000'
   c. Encrypt data with KS_{ENC}:
      EncryptedData = '6375432908C044F6'
   d. Build DO'87':
      DO87 = '8709016375432908C044F6'
   e. Concatenate CmdHeader and DO87:
      M = '0CA4020C8000000087090163754329 08C044F6'
   f. Compute MAC of M:
      i. Increment SSC with 1:
         SSC = '887022120C06C227'
      ii. Concatenate SSC and M and add padding:
         N = '887022120C06C2270CA4020C80000000
         8709016375432908C044F68000000000'
      iii. Compute MAC over N with KS_{MAC}:
         CC = 'BF8B92D635FF24F8'
   g. Build DO'8E':
      DO8E = '8E08BF8B92D635FF24F8'
   h. Construct and send protected APDU:
      ProtectedAPDU = '0CA4020C158709016375432908C0
      44F68E08BF8B92D635FF24F800'

   i. Receive response APDU of MRTD's chip:
      RAPDU = '990290008E08FA855A5D4C50A8ED9000'
   j. Verify RAPDU CC by computing MAC of DO'99':
      i. Increment SSC with 1:
         SSC = '887022120C06C228'
      ii. Concatenate SSC and DO'99' and add padding:
         K = '887022120C06C2289902900080000000'
      iii. Compute MAC with KS_{MAC}:
         CC' = 'FA855A5D4C50A8ED'
      iv. Compare CC' with data of DO'8E' of RAPDU.

'FA855A5D4C50A8ED' == 'FA855A5D4C50A8ED' ? YES.

2. Read Binary of first 4 bytes:

   Unprotected command APDU:

CLA	INS	P1	P2	LE
00h	B0h	00h	00h	04h

   a. Mask class byte and pad command header:
      CmdHeader = '0CB0000080000000'
   b. Build DO'97':
      DO97 = '970104'
   c. Concatenate CmdHeader and DO97:
      M = '0CB0000080000000970104'
   d. Compute MAC of M:
      i. Increment SSC with 1:
         SSC = '887022120C06C229'
      ii. Concatenate SSC and M and add padding:
         N = '887022120C06C2290CB00000
         8000000097010480000000000'
      iii. Compute MAC over N with KS_{MAC}:
         CC = 'ED6705417E96BA55'
   e. Build DO'8E':
      DO8E = '8E08ED6705417E96BA55'
   f. Construct and send protected APDU:
      ProtectedAPDU = '0CB000000D9701048E08ED6705417E96BA5500'

   g. Receive response APDU of MRTD's chip:
      RAPDU = '8709019FF0EC34F992265199029000
      8E08AD55CC17140B2DED9000'
   h. Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':
      i. Increment SSC with 1:
         SSC = '887022120C06C22A'
      ii. Concatenate SSC, DO'87' and DO'99' and add padding:
         K = '887022120C06C22A8709019F
         F0EC34F99226519902900080'
      iii. Compute MAC with KS_{MAC}:
         CC' = 'AD55CC17140B2DED'
      iv. Compare CC' with data of DO'8E' of RAPDU:
         'AD55CC17140B2DED' == 'AD55CC17140B2DED' ? YES.
   i. Decrypt data of DO'87' with KS_{ENC}:
      DecryptedData = '60145F01'
   j. Determine length of structure:
      L = '14' + 2 = 22 bytes

3. Read Binary of remaining 18 bytes from offset 4:

   Unprotected command APDU:

CLA	INS	P1	P2	LE
00h	B0h	00h	04h	12h

a. Mask class byte and pad command header:
   CmdHeader = '0CB0000480000000'
b. Build DO'97':
   DO97 = '970112'
c. Concatenate CmdHeader and DO97:
   M = '0CB0000480000000970112'
d. Compute MAC of M:
   i. Increment SSC with 1:
      SSC = '887022120C06C22B'
   ii. Concatenate SSC and M and add padding:
      N = '887022120C06C22B0CB00004
      8000000097011280000000000'
   iii. Compute MAC over N with KS_{MAC}:
      CC = '2EA28A70F3C7B535'
e. Build DO'8E':
   DO8E = '8E082EA28A70F3C7B535'
f. Construct and send protected APDU:
   ProtectedAPDU = '0CB000040D9701128E082EA28A70F3C7B53500'

g. Receive response APDU of MRTD's chip:
   RAPDU = '871901FB9235F4E4037F2327DCC8964F1F9B8C30F42
   C8E2FFF224A990290008E08C8B2787EAEA07D749000'
h. Verify RAPDU CC by computing MAC of concatenation DO'87' and DO'99':
   i. Increment SSC with 1:
      SSC = '887022120C06C22C'
   ii. Concatenate SSC, DO'87' and DO'99' and add padding:
      K = '887022120C06C22C871901FB9235F4E4037F232
      7DCC8964F1F9B8C30F42C8E2FFF224A99029000'
   iii. Compute MAC with KS_{MAC}:
      CC' = 'C8B2787EAEA07D74'
   iv. Compare CC' with data of DO'8E' of RAPDU:
      'C8B2787EAEA07D74' == 'C8B2787EAEA07D74' ? YES.
i. Decrypt data of DO'87' with KS_{ENC}:
   DecryptedData = '04303130365F36063034303030305C026175'

RESULT:

EF.COM data = '60145F0104303130365F36063034303030305C026175'

F.1.2 Passive Authentication

Step 1. Read the Document Security Object (SO_D) (optionally containing the Document Signer Certificate (C_{DS})) from the chip.
Step 2: Read the Document Signer (DS) from the Document Security Object (SO_D).
Step 3: The inspection system verifies SO_D by using Document Signer Public Key (KPu_{DS})
Step 4: The inspection system verifies C_{DS} by using the Country Signing CA Public Key (KPu_{CSCA}).

If both verifications in step 3 and 4 are correct, then this ensures that the contents of SO_D can be trusted and SHOULD be used in the inspection process.

Step 5: Read the relevant data groups from the LDS.
Step 6: Calculate the hashes of the relevant data groups.
Step 7: Compare the calculated hashes with the corresponding hash values in the SO_D.

If the hash values in step 7 are identical, then this ensures that the contents of the data group is authentic and unchanged.

F.2 Life Times

The following examples demonstrate the explanations on how to calculate the key life times as described in section 3.4.

F.2.1 Example 1

The first demonstrates a system where the State wishes to keep to a minimum the total life time of all their certificates. The State's passports are valid for 5 years, and as the State issues a relatively large number of passports per year they have decided to keep their key issuing periods to a minimum.

Period	Elapsed Time	
Document Signer Key Issuing		1 Month
Passport Validity	5 Years	-
Document Signer Certificate Validity	5 Years	1 Month
Country Signing CA Key Issuing	3 Years	-
Country Signing CA Certificate Validity	8 Years	1 Month

The consequences of this example are by the time the first Country Signing CA Certificate becomes invalid at least 36 document signing keys will have been issued (1 for each 1 month period) and in the last few months of this Country Signing CA Key there will be at least 2 other Country Signing keys valid for signature verification.

F.2.2 Example 2

The second example demonstrates a system where the State takes slightly more relaxed approach. The passports are valid for 10 years; the State has decided to keep to average issuing periods for all keys.

Period	Elapsed Time	
Document Signer Key Issuing		2 Months
Passport Validity	10 Years	-
Document Signer Certificate Validity	10 Years	2 Months

Period	Elapsed Time	
Country Signing CA Key Issuing	4 Years	-
Country Signing CA Certificate Validity	14 Years	2 Months

The consequences of this example are by the time the first Country Signing CA Certificate becomes invalid at least 24 Document Signer Keys, and in the last few months of the Country Signing CA Key there will be at least 3 other Country Signing CA Keys valid for signature verification.

F.2.3 Example 3

The final example demonstrates a system where the State has decided to use the maximum limits advised by this framework. The passports are valid for 10 years, the Country Signing CA Key is replaced every five years and Document Signer Keys are replaced every 3 months.

Period	Elapsed Time	
Document Signer Key Issuing		3 Months
Passport Validity	10 Years	-
Document Signer Certificate Validity	10 Years	3 Months
Country Signing CA Key Issuing	5 Years	-
Country Signing CA Certificate Validity	15 Years	3 Months

The consequences of this example are by the time the first Country Signing CA Certificate becomes invalid at least 20 Document Signer Keys and in the last few months of the Country Signing CA Key there will be at least 3 other Country Signing CA Keys valid for signature verification.

Annex G PKI and Security Threats

G.1 Key Management

G.1.1 Country Signing CA and Document Signer Keys

To protect the private keys it is RECOMMENDED to use secure hardware devices for signature generation (Secure Signature Creation Device – SSCD), i.e. the SSCD generates new key pairs, stores and destroys (after expiration) the corresponding private key securely. To protect against attacks on the SSCD including Side-Channel Attacks (e.g. timing, power consumption, EM emission, fault injection) and attacks against the random number generator it is RECOMMENDED to use SSCDs that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

When distributing self-signed Country Signing CA Certificates by diplomatic means extreme care must be taken to prevent insertion of a rogue Country Signing CA Certificate. Furthermore, it is RECOMMENDED that States store the received Country Singing CA Certificates in secure hardware devices (Card Acceptor Device – CAD) accessible by the reader devices in a secure manner. To protect against attacks on the CAD, it is RECOMMENDED to use CADs that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

G.1.2 Active Authentication Keys

It is RECOMMENDED to generate key pairs for Active Authentication on the chip of the MRTD. As the private key is stored on the chip in secure memory, and the chip hardware has to resist attacks for the whole validity period of the MRTD, it is RECOMMENDED to use chips that are successfully certified/validated under a CCRA-compliant certification body according to a suitable Common Criteria Protection Profile with EAL 4+ SOF-High.

The available chip technology influences the maximum key length of keys used inside the chip for Active Authentication. Many chips currently do not support key lengths that exceed a security level of 80 bits, which was the reason for choosing this value as recommended minimum. This is a relatively low level of security compared to their validity period of the MRTD. Therefore, it is RECOMMENDED to use longer keys, if supported by the chip.

States that make use of the Active Authentication mechanism to validate a foreign MRTD should also be aware that no revocation mechanism has been specified for compromised Active Authentication keys.

G.1.3 Denial of Service Attacks

Denial of Service Attacks have to be considered when States rely on the Directory for distribution of Document Signer Certificates and CRLs. Those attacks cannot be prevented, it is therefore RECOMMENDED that the Document Signer Certificate required to validate the Document Security Object is also included in the Document Security Object itself. Receiving States SHOULD make use of a provided Document Signer Certificate.

To distribute CRLs bilaterally it is RECOMMENDED to establish multiple channels (e.g. internet, phone, fax, mail, etc.) with other States and to confirm reception of received CRLs.

G.2 Cloning Threats

Compared to paper based MRTDs copying the signed data stored on the RF-Chip is easily possible in general. States concerned about the possibility of having data of their citizens copied to another chip SHOULD implement Active Authentication that prevents this to a certain extent.

G.2.1 Passive Authentication

Passive Authentication does not prevent copying the data stored on the chip. As a consequence, it is possible to substitute the chip of a MRTD against a fake chip storing the data copied from the chip of another MRTD. Receiving States SHOULD verify that the data read from the chip indeed belongs to the presented MRTD. This can be done by comparing DG1 stored on the chip to the MRZ printed on the datapage of the MRTD. If DG1 and the MRZ compare and the document security object is valid and the presented MRTD has not been tampered with (is not counterfeited), then the MRTD and the data stored on the chip can be considered to be belonging together.

G.2.2 Active Authentication

Active Authentication makes chip substitution more difficult, but not impossible: The MRTD presented by the attacker to the inspection system could be equipped with a special chip. This chip works as proxy for a genuine chip located in a remote place: the chip communicates with the attacker, the attacker communicates with another attacker, and the other attacker (temporarily) gains access to the genuine chip. The inspection system is not able to notice that it has authenticated a remote chip instead of the presented chip. This attack is called Grandmaster Chess Attack.

G.3 Privacy Threats

G.3.1 No Access Control

The use of proximity chips already minimizes privacy risks as reader devices have to be very close to the chips, therefore skimming is not considered to be a serious threat. However eavesdropping on an existing communication between a chip and a reader is possible in a larger distance. States wishing to address this threat SHOULD implement Basic Access Control.

G.3.2 Basic Access Control

The Basic Access Keys used to authenticate the reader and to setup session keys to encrypt the communication between chip and reader are generated from the 9 digit Document-Number, the Date-of-Birth, and the Date-of-Expiry. Thus, the entropy of the keys is relatively low. For a 10 year valid MRTD the entropy is 56 bits at maximum. With additional knowledge (e.g. approximate age of the bearer, or relations between Document-Number and Date-of-Expiry) the entropy is lowered even more. Due to the relatively low entropy, in principle an attacker might record an encrypted session, calculate the Basic Access Keys by Brute-Force from the authentication, derive the session keys and decrypt the recorded session. However this still requires a considerable effort compared to obtaining the data from other sources.

G.3.3 Active Authentication (Data Traces)

In the challenge-response protocol used for Active Authentication, the chip signs a bit string that has been chosen more or less randomly by the inspection system. If a receiving State uses the current date, time, and location to generate this bit string in an unpredictable but verifiable way (e.g. using secure hardware), a third party can be convinced afterwards that the signer was at a certain date and time at a certain location.

G.4 Cryptographic Threats

The recommended minimal key lengths have been chosen so that breaking those keys requires a certain (assumed) effort, independent of the chosen signature algorithm:

Type of Key	Level of Security
Country Signing CA	128 bits
Document Signer	112 bits
Active Authentication	80 bits

G.4.1 Mathematical advances and non-standard computing

According to Moore's Law computation power doubles every 18 month. However, the security of the signature algorithm is not only influenced by computing power, advances in mathematics (cryptanalysis) and the availability of new non-standard computation methods (e.g. quantum computers) also have to be taken into account.

Due to the long validity periods of keys it is very difficult to make predictions about mathematical advances and the availability of non-standard computing devices. Therefore, the recommendations for key lengths are mainly based on the extrapolated computing power. States SHOULD review the key lengths for their own but also for received MRTDs often for reasons mentioned above.

Generating key pairs of a special form may improve the overall performance of the signature algorithm, but may also be exploited for cryptanalysis in the future. Therefore, such special key pairs SHOULD be avoided.

G.4.2 Hash Collisions

While it is computationally infeasible to find another message that produces the same hash value as a given message, it is considerably easier to find two message that produce the same hash value. This is called the Birthday Paradoxon.

In general all messages to be signed are produced by the Document Signer itself. Therefore, finding hash collisions does not help an attacker very much. However, if photographs provided by the applicant in digital form are accepted by the Document Signer without additional randomized modification, the following attack is possible:

- Two persons share their digital photos. Then they repeatedly flip a small number of bits at randomly in each photo until two photos produce the same hash value.
- Both persons apply for a new MRTD using the manipulated photo. Either person can now use the MRTD of the other person provided that it is possible to replace the digital photo in the chip (e.g. by chip substitution).

The hash function SHA-1 only provides 80 bits of security against hash collisions. Thus, it is considerably easier to find a hash collision than to break the Document Signer Key which provides 112 bits of security. Therefore, whenever hash collisions are of concern (e.g. as described above), it is RECOMMENDED not to use SHA-1 as hash function.