ICAO

MACHINE READABLE TRAVEL DOCUMENTS GUIDANCE DOCUMENT

DOC 9303 CRYPTOGRAPHIC KEY LENGTH REVIEW

Version – 0.04 | November 2024

ISO/IEC JTC1 SC17 WG3/TF5 FOR THE NEW TECHNOLOGIES WORKING GROUP

FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION

Release Control

Release	Date	Description
0.01	Jul 2024	Initial Draft
0.02	Jul 2024	Resolution of comments from ad-hoc group to v0.01
0.03	Jul 2024	Resolution from discussion in ad-hoc group
0.04	Nov 2024	Comment resolution from v0.03

Michael Hoppe	Germany	DIN
Alban Feraud	France	AFNOR

Table of contents

1. Scope

This document provides an inventory of all currently allowed cryptographic algorithms, domain parameters and key lengths in ICAO Doc 9303 (part 11, 12 and 13). These are mapped to their security strength *n*, which is modelled by the bit-length *n* of an equivalent perfect block cipher. Hereby, the number n also refers to the number of 2^n operations an attacker would have to perform to break it.

Based on the inventory, the document provides guidance on which algorithms, parameters or key lengths are recommended depending on their security strength. The following table indicates recommendations for certain security strengths, whereby the color highlighting is applied throughout the document.

Security strength [bits]	Recommendation for newly issued documents
< 100	Not recommended for future deployments
100 – 109	Should be phased out as soon as possible
110 – 119	Acceptable (Security strength >= 120 bits should be considered for future proofness)
>= 120	Recommended

Table 1: Security strength recommendations

The recommendations currently only applies to newly issued documents. However, any document that implements the currently allowed algorithms, domain parameters and key lengths must be considered compliant to ICAO Doc 9303. Thus, Inspection Systems must support all algorithms as specified in Doc 9303 Part 11. Furthermore, receiving States must support all algorithms referred to in Doc 9303 Part 12 at points where they wish to validate the signature on eMRTDs.

Regardless of the recommendations provided by this document, selecting algorithms, domain parameters or key-lengths remains at the discretion of the issuing State or organization. They shall choose appropriate key lengths offering protection against attacks for the life time of the eMRTD.

This document is informative and does not supersede the normative requirements from Doc 9303.

2. Executive Summary

Issuing authorities are recommended to regularly assess the cryptographic algorithms currently implemented in their travel documents and, if necessary, to develop a migration strategy for a transition to algorithms that are considered robust against current and emerging threats. This document outlines the current recommendations for cryptographic algorithms and key lengths available in Doc 9303 to maintain state-of-the-art security standards.

Hereby, implementing the symmetric cipher 3DES is no longer recommended. Also, asymmetric algorithms based on RSA or Finite Field (DH/DSA) with key lengths less than 2048 bits are not recommended for new deployments, except for Active Authentication. It is advisable to replace these algorithms in existing deployments to enhance security.

To be prepared for potential future advances in cryptanalysis and ensure future-proof security, algorithms with a security strength greater than 120 bits should be chosen for new deployments were feasible. For existing systems utilizing mechanisms with less than 120-bit security strength, it is recommended to develop a migration strategy towards algorithms with security strength greater than 120 bits as soon as practical.

The threat of compromising a Country Signing key (CSCA) or a Document Signing key used at issuance is far greater than breaking Access Control on an individual eMRTD. The control of a signing key would potentially enable an attacker to certify any data stored on an eMRTD chip as authentic. The risk arising from the compromise of chip-specific keys of an eMRTD, on the other hand, would be limited to documents using the same keys. Consequently, a migration strategy should consider addressing the document issuing eMRTD PKI and Passive Authentication first.

By considering these guidelines, issuing authorities can help ensure that their cryptographic protocols remain robust against modern attack vectors, thereby safeguarding the integrity and authenticity of electronic travel documents.

3. Review of currently allowed cryptographic algorithms

The security protocols specified by ICAO Doc 9303 are composed of several cryptographic primitives, each with a certain security level. Hereby, the security level of the entire protocol can never be greater than the security level of the weakest primitive.

3.1 Asymmetric domain parameters:

Asymmetric cryptographic primitives are algorithm that leverage either the

- RSA/integer factorization problem,
- the finite field discrete logarithm problem or,
- the elliptic curve discrete logarithm problem

In the case of the RSA algorithm, its strength primarily depends on the size of the RSA modulus, indicated by its bit size or key length. In case of the two discrete logarithm problems the security strength of the respective algorithms depends on the chosen domain parameters. The following two tables map RSA key lengths or the domain parameters for Finite Field or Elliptic Curve cryptographic algorithms to their respective security strength.

Algorithm	Key length [bits]	Security strength [bits]	Applicable Algorithms in Doc 9303
RSA	1024	≤80[1,2,3,4]	PA (RSA), AA (RSA)
RSA	1536	≤89[2]	PA (RSA), AA (RSA)[a]
RSA	2048	≤112[1,2,3,4]	PA (RSA), AA (RSA), TA-RSA
RSA	3072	≤128[1,2,3,4]	PA (RSA), AA (RSA), TA-RSA
RSA	4096	≤142[2]	PA (RSA), AA (RSA)
RSA	7680	≤192[2,3,4]	PA (RSA)
RSA	15360	≤256[2,3,4]	PA (RSA)

Table 2: Security strength of RSA keys
1=[JTC1/SC27 cd12], 2=[NIST 800-57 P1], 3=[BSI TR-02102-1], 4=[ECRYPT II 2014]

Type	Name	Size [bits]	Security strength [bits]	Applicable Algorithms in Doc 9303
Finite Field	1024-bit MODP Group with 160-bit Prime Order Subgroup	1024/160	≤80[1,2,3,4]	PA (DSA), PACE-DH, CA-DH
Finite Field	2048-bit MODP Group with 224-bit Prime Order Subgroup	2048/224	≤112[1,2,3,4]	PA (DSA), PACE-DH, CA-DH
Finite Field	2048-bit MODP Group with 256-bit Prime Order Subgroup	2048/256	≤112[1,2,3,4]	PA (DSA), PACE-DH, CA-DH
Finite Field	3072-bit MODP Group with 256-bit Prime Order Subgroup	3072/256	≤128[1,2,3,4]	PA (DSA)
EC	NIST P-192 (secp192r1)	192	96[4]	PA (ECDSA), PACE-ECDH, CA-ECDH, AA (ECDSA), TA-ECDSA,
EC	BrainpoolP192r1	192	96[4]	
EC	NIST P-224 (secp224r1)	224	112[1,2,4]	PA (ECDSA), PACE-ECDH, CA-ECDH, AA (ECDSA),TA-ECDSA
EC	BrainpoolP224r1	224	112[1,2,4]	

[a] Specific recommendation for AA RSA-keys apply. C.f. section 3.5

EC	NIST P-256 (secp256r1)	256	128[1,2,3,4]	PA (ECDSA), PACE-ECDH, CA-ECDH, AA (ECDSA) ,TA-ECDSA
EC	BrainpoolP256r1	256	128[1,2,3,4]	
EC	BrainpoolP320r1	320	160[4]	
EC	NIST P-384 (secp384r1)	384	192[1,2,3,4]	
EC	BrainpoolP384r1	384	192[1,2,3,4]	
EC	BrainpoolP512r1	512	256[2,3,4]	
EC	NIST P-521 (secp521r1)	521	260[4]	

Table 3: Security strength of asymmetric domain parameters
1=[JTC1/SC27 cd12], 2=[NIST 800-57 P1], 3=[BSI TR-02102-1], 4=[ECRYPT II 2014]

Note: The safety strength of EC domain parameters depends not only on the size of the underlying cyclic group, but also on the choice of a suitable elliptic curve. Unsuitable curves can lead to a small subgroup with weak cryptographic properties. Therefore, only recommended domain parameters like in Doc 9303 Part 11 should be used.

3.2 Digital Signatures

Digital signatures are cryptograhic algorithms which allow to verify that digital data originated from a signer is authentic and has not been altered.

Digital signatures are utilised extensively by entities of the Digital Signature/eMRTD PKI as specified in ICAO Doc 9303 Part 12 to sign certificates like Signer Certificates or issued data object like Document Security Objects or Visible Digital Seals. The same applies to entities from the Authorization PKI.

Digital signatures rely on a

- cryptographic hash function and
- an asymmetric cryptographic algorithm that leverages either the
  - RSA/integer factorization problem,
  - the finite field discrete logarithm problem or,
  - the elliptic curve discrete logarithm problem.

The security strength associated with a digital signature is no greater than the minimum of the security strength of the asymmetric cryptographic algorithm and the security strength of the hash function that is employed[b].

3.2.1 eMRTD PKI / Passive Authentication (PA)

The eMRTD Public Key Infrastructure (PKI) enables the creation and subsequent verification of digital signatures on eMRTD objects, including the Document Security Object (SOD) and LDS of an eMRTD or the signed content of a Visible Digital Seal to ensure the signed data is authentic and has not been modified.

These signature are issued by Signers like Document Signer or Bar Code Signer, for which a Signer certificate has been issued and digitally signed by the single CA (CSCA) of the respective issuing State/Authority.

The digital signature algorithm for signing Signer Certificates or eMRTD objects must comply with one of the asymmetric signature algorithms listed in Table 4 and the Hash algorithms listed in Table 5.
(c.f. ICAO Doc 9303 Part 12 section 4.1.6)

[b] Example: RSA-2048 with SHA-256 provides an asymmetric algorithm strength of ≤112 bits and a hash algorithm strength of 128 bits. Thus, the overall security strength is ≤112 bits.

Signature algorithm	Security strength
RSA *RFC 4055: RSASSA-PSS or RSASSA-PKCS1 v1*	See Table 2
DSA *FIPS 186-4*	See Table 3
ECDSA *X9.62 or ISO/IEC 15946*	See Table 3

Table 4: Security strength of signature algorithms

DSA has been deprecated in FIPS 186-5 which supersedes FIPS 186-4, and will be deprecated in BSI [BSI TR-02102-1] after 2029. Since DSA is not known to be used in any current deployment of eMRTDs it could be removed from the list of allowed signature algorithms in Doc 9303 Part 12 without any transition period.

Newly issued documents should not implement DSA.

Hash algorithm:	Security strength [bits]
SHA-224	112
SHA-256	128
SHA-384	192
SHA-512	256

Table 5: Security Strength of Hash algorithms

3.2.2 Authorization PKI / Terminal Authentication (TA)

The algorithm used for Terminal Authentication in the authorization PKI is determined by the CVCA of the eMRTD and either RSA or ECDSA may be used. The allowed combination of asymmetric signature algorithms and the Hash algorithms for Terminal Authentication are grouped into cipher suites which are identified by specific TA protocol Object Identifiers (OIDs) as indicated in Table 6.

The RSA key length or the ECDSA domain parameters can be chosen independently from the cipher suite. The security strength of Terminal Authentication is no greater than the security strength stemming from the RSA key length or the EC domain and the security strength of the hash algorithm.
(c.f. ICAO Doc 9303 Part 11 section 7.1.4)

OID	Hash Algorithm	Hash Algorithm Security strength [bits]	Asymmetric signature algorithm strength
id-TA-ECDSA-SHA-224	SHA-224	112	See Table 3
id-TA-RSA-PSS-SHA-256	SHA-256	128	See Table 2
id-TA-ECDSA-SHA-256			See Table 3
id-TA-ECDSA-SHA-384	SHA-384	192	See Table 3
id-TA-RSA-PSS-SHA-512	SHA-512	256	See Table 2
id-TA-ECDSA-SHA-512			See Table 3

Table 6: Terminal Authentication cipher suites

3.3 Access Control

3.3.1 Basic Access Control (BAC)

Basic Access Control (BAC) offers no choice of algorithms and requires implementation of the primitives indicated in the following table.

Protocol	Key Establishment	Block Cipher for Session Encryption	Message Authentication Code	Security strength [bits]
BAC	ISO/IEC 11770-2 Key Establishment Mechanism 6 with Two Key 3DES	Two Key 3DES	ISO/IEC 9797-1 MAC algorithm 3 with DES	80[1,2]

Table 7: BAC cipher suite
1=[JTC1/SC27 cd12], 2=[NIST 800-57 P1]

Furthermore, the security strength provided by Basic Access Control is limited by the entropy of the BAC password, which is generated from MRZ data with very limited randomness. The maximum entropy of the MRZ stems from the:

- date of birth: 15 bits (365*100, assuming a maximum age of 100), and
- expiry date: 12 bits (assuming a validity period of 10 years), and
- serial number:
  - 46 bits (36^9 possibilities, assuming 9 alphanumeric random digits), or
  - 29 bits (10^9, assuming 9 numeric random digits)

In conclusion, BAC can never exceed a security strength of 73 bits. Since birthdates are not evenly distributed and the document's serial number is often not randomly generated, the security level will generally be even lower.
(c.f. ICAO Doc 9303 Part 11 section 4.3.3)

3.3.2 PACE

The Password Authenticated Connection Establishment (PACE) relies on the following cryptographic primitives:

- Symmetric block cipher for the initial encryption of the nonce,
- Finite Field (DH) or Elliptic Curve Diffie-Hellman (ECDH) for Generic Mapping or,
- Symmetric block cipher for Integrated Mapping,
- Finite Field (DH) or Elliptic Curve Diffie-Hellman (ECDH) for Key Agreement,
- Message Authentication Code (MAC) for Authentication Token,
- Symmetric block cipher and Message Authentication Code (MAC) for Secure Messaging,
- (conditional) Elliptic Curve Diffie-Hellman (ECDH) and symmetric block cipher for Chip Authentication Mapping (CAM).

Symmetric block ciphers and Message Authentication Codes (MACs) permitted for the implementation of the PACE protocol are grouped into PACE cipher suites, which are identified by specific PACE protocol Object Identifiers (OIDs). Each cipher suite specifies a set of block ciphers and MACs with matching security strengths. Consequently, the security strength of these cryptographic components can be indicated for each cipher suite and are provided in Table 8.

Furthermore, the security strength of the PACE protocol also depends on the strength of the Finite Field Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) algorithm, which is determined by the domain parameters and can be selected independently from the block ciphers and MACs within the cipher suite. The respective security strength is provided by Table 3

The security strength of the PACE protocol is influenced by both the selected cipher suite (Table 8) and the chosen domain parameters (Table 3), whereby the lower of the two values indicates the overall security strength.

(c.f. ICAO Doc 9303 Part 11 section 4.4.3)

OID	Block Cipher for Session and Nonce Encryption	Message Authentication Code	Security strength [bits]
id-PACE-DH-GM-3DES-CBC-CBC id-PACE-DH-IM-3DES-CBC-CBC id-PACE-ECDH-GM-3DES-CBC-CBC id-PACE-ECDH-IM-3DES-CBC-CBC	Two Key 3DES	ISO/IEC 9797-1 MAC algorithm 3 with DES	80[1,2]
id-PACE-DH-GM-AES-CBC-CMAC-128 id-PACE-DH-IM-AES-CBC-CMAC-128 id-PACE-ECDH-GM-AES-CBC-CMAC-128 id-PACE-ECDH-IM-AES-CBC-CMAC-128 id-PACE-ECDH-CAM-AES-CBC-CMAC-128	AES-128	CMAC with AES-128	128[1,2,3,4]
id-PACE-DH-GM-AES-CBC-CMAC-192 id-PACE-DH-IM-AES-CBC-CMAC-192 id-PACE-ECDH-GM-AES-CBC-CMAC-192 id-PACE-ECDH-IM-AES-CBC-CMAC-192 id-PACE-ECDH-CAM-AES-CBC-CMAC-192	AES-192	CMAC with AES-192	192[1,2,3,4]
id-PACE-DH-GM-AES-CBC-CMAC-256 id-PACE-DH-IM-AES-CBC-CMAC-256 id-PACE-ECDH-GM-AES-CBC-CMAC-256 id-PACE-ECDH-IM-AES-CBC-CMAC-256 id-PACE-ECDH-CAM-AES-CBC-CMAC-256	AES-256	CMAC with AES-256	256[1,2,3,4]

Table 8: PACE cipher suites
1=[JTC1/SC27 cd12], 2=[NIST 800-57 P1], 3=[BSI TR-02102-1], 4=[ECRYPT II 2014]

3.4 Chip Authentication (CA)

The Chip Authentication (CA) protocol relies on the following cryptographic primitives:

- Finite Field (DH) or Elliptic Curve Diffie-Hellman (ECDH) for Key Agreement,
- Symmetric block cipher and Message Authentication Code (MAC) for Secure Messaging.

In the same way as for the PACE protocol, symmetric block ciphers and Message Authentication Codes (MACs) permitted for the implementation of the CA protocol are grouped into CA cipher suites. Their CA protocol Object Identifiers (OIDs) and their respective security strength are provided in Table 9.

Also CA allows to choose the domain parameters for the Finite Field Diffie-Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) algorithm independently from the cipher suite. Thus, the security strength of the CA protocol is influenced by both the selected cipher suite (Table 9) and the chosen domain parameters (Table 3), whereby the lower of the two values indicates the overall security strength.
(c.f. ICAO Doc 9303 Part 11 section 6.2.3)

OID	Block Cipher for Session Encryption	Message Authentication Code	Security strength [bits]
id-CA-DH-3DES-CBC-CBC id-CA-ECDH-3DES-CBC-CBC	Two key 3DES	ISO/IEC 9797-1 MAC algorithm 3 with DES	80[1,2]
id-CA-DH-AES-CBC-CMAC-128 id-CA-ECDH-AES-CBC-CMAC-128	AES-128	CMAC with AES-128	128[1,2,3,4]
id-CA-DH-AES-CBC-CMAC-192 id-CA-ECDH-AES-CBC-CMAC-192	AES-192	CMAC with AES-192	192[1,2,3,4]
id-CA-DH-AES-CBC-CMAC-256 id-CA-ECDH-AES-CBC-CMAC-256	AES-256	CMAC with AES-256	256[1,2,3,4]

Table 9: CA cipher suites
1=[JTC1/SC27 cd12], 2=[NIST 800-57 P1], 3=[BSI TR-02102-1], 4=[ECRYPT II 2014]

3.5 Active Authentication (AA)

Active Authentication (AA) relies on a hash value and a digital signature, which must be generated using the ECDSA or RSA ([ISO/IEC 9796-2] Digital Signature scheme 1) algorithm. In case of AA, the following hash algorithms are allowed for the respective signature algorithm:
(c.f. ICAO Doc 9303 Part 11 section 6.1.2)

Signature algorithm	Allowed hash algorithms
RSA *[ISO/IEC 9796-2] Digital Signature scheme 1*	SHA-1, SHA-224, SHA256, SHA-384, SHA-512
ECDSA *plain signature format according to [BSI TR-03111]*	SHA-224, SHA256, SHA-384, SHA-512

Table 10: Allowed signature and hash algorithms for Active Authentication

As these digital signature algorithms provide equivalent security strength as the signature algorithms allowed for Passive Authentication, the security strengths specified there in Table 4 and Table 5 also apply for Active Authentication. The security strength of the Active Authentication algorithm is influenced by the security strength of the selected signature algorithm and the security strength of the chosen hash algorithm, whereby the lower of the two values indicates the overall security strength.

The threat severity of a successful attack on an eMRTD's AA private key is limited to the respective document. Therefore, with regard to the operational performance of RSA calculations on chip cards, the following RSA key lengths are also considered acceptable:

Algorithm	Key length [bits]	Recommendation for newly issued documents
AA with RSA	1024	Not recommended for future deployments
AA with RSA	1536	Acceptable
AA with RSA	2048	Acceptable
AA with RSA	3072	Recommended
AA with RSA	4096	Recommended

Table 11: Key-length recommendations for Active Authentication (AA) RSA-keys

In addition to the Hash algorithms listed in Table 5, Active Authentication also allows using the RSA signature algorithm with SHA-1. However, using SHA-1 is no longer considered secure, as successful collision attacks have been demonstrated and only a security strength of less than 63 bits can be assumed. Consequently, newly issued documents should not implement Active Authentication based on RSA with SHA-1.

4. Analysis of extensibility of eMRTD protocols to larger key sizes

This section analyses the protocols defined in ICAO doc 9303 part 11 to identify whether the technical specification remains valid regardless the key size at stake, or whether some limitations are imposed (e.g. APDU size…). The purpose is to check whether the technical specification remains valid regardless the key size and thus is scalable at will, if needed.

Indeed, the support of these protocols with large key size will still require the eMRTD to support such features (cryptographic capacity, memory size...). The impact on operational performance when migrating to longer key lengths must be taken into account, hereby considering the trade-offs between incremental security and travel facilitation performance.

4.1 Chip Access Procedure

Currently, extended length APDU support of an eMRTD's chip is indicated either in the eMRTD chip's ATR/ATS or in EF.ATR/INFO (c.f. Doc 9303 Part 10 sec. 3.6.4.1). However, only EF.ATR.INFO, which is currently optional, provides information on the maximum number of bytes supported by the chip in command and response APDUs. This file is needed so that Inspection System can (1) know whether the eMRTD supports extended length, and if yes, (2) the size limitation for incoming and outgoing data APDU.

For this reason, it is worth considering to change to specification in Doc 9303 and to mandate that EF.ATR/INFO shall be present and shall provide the maximum number of bytes supported in a command or response APDU in the template with tag '0x7F66' if extended length APDUs are supported.

4.2 Impact on PACE and CA

All key lengths and domain parameters currently allowed in Doc 9303 Part 11 for the PACE and the CA protocol do not require support for extended length APDUs.

ICAO Doc 9303 does not provide for finite field domain parameters greater than 2048 bits for the use of PACE with Finite Field Diffie-Hellman (DH). Consequently, PACE with DH cannot exceed a security strength of 112 bits with the parameters currently permitted in Doc 9303.

4.3 Impact on AA

Doc 9303 Part 11 already states, that Extended Length APDUs must be supported by the eMRTD chip if RSA key lengths exceeding the limit of 1792 bits (if Secure Messaging with AES is used)[c] in Active Authentication are used.

These key lengths are only relevant when using AA with RSA, as EC keys with the allowed domain parameters do not exceed that limit.

[c] 1848 bits if Secure messaging with 3DES is used, whereby implementing 3DES is not recommended by this document.

4.4 Impact on TA

Currently, the RSA key size to be used for TA is explicitly limited to 2048 bits or 3072 bits by ICAO Doc 9303 Part 11. Thus, TA with RSA cannot exceed a security strength of 128 bits with the parameters currently permitted in Doc 9303.

5. References

[JTC1/SC27 cd12] ISO/IEC JTC 1/SC 27 committee document 12 on the Assessment of Cryptographic Techniques and Key Lengths 6th edition, 2023

[ECRYPT II 2014] CRYPT – II, Algorithms, Key Size and Protocols Report, 2012, https://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf

[NIST 800-57 P1] NIST Special Publication 800-57 Part 1 (Revision 5), Recommendation for key management – Part 1: General, National Institute of Standards and Technology, 2020

[NIST SHA1Depr] NIST Transitioning Away from SHA-1 for All Applications, https://csrc.nist.gov/news/2022/nist-transitioning-away-from-sha-1-for-all-apps

[BSI TR-02102-1] BSI – Technical Guideline: Cryptographic Mechanisms: Recommendations and Key Lengths, Federal Office for Information Security (BSI), 2024

[ANSSI] Guide de sélection d'algorithmes cryptographiques, National Cybersecurity Agency of France (ANSSI), 2021, https://cyber.gouv.fr/sites/default/files/2021/03/anssi-guide-selection_crypto-1.0.pdf

[SOG-IS] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

[RFC3526] IETF RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003

[RFC7919] IETF RFC 7919, Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS), 2016

Annex A: Abbreviations

Abbreviation	
3DES	Triple DES
AA	Active Authentication
AES	Advanced Encryption Standard
BAC	Basic Access Control
CA	Chip Authentication
CSCA	Country Signing Certification Authority
CVCA	Country Verifying Certificate Authority
DES	Data Encryption Standard
DH	Diffie Hellmann
DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie Hellmann
ECDSA	Elliptic Curve Digital Signature Algorithm
eMRTD	Electronic Machine Readable Travel Document
ICAO	International Civil Aviation Organization
LDS	Logical Data Structure
MAC	Message Authentication Code
MRZ	Machine Readable Zone
OID	Object Identifier
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PKI	Public Key Infrastructure
RSA	Rivest, Shamir and Adleman
SHA	Secure Hashing Algorithm
SO_D	Document Security Object
TA	Terminal Authentication