PKD Upload Contents Checks

PKD Upload Contents Checks

Forwarded by: 2011 Chairperson

Reference Document(s):
1. Doc 9303, Part I, Volume 2, Sixth Edition dated 8/06
2. Doc 9303 Supplement, Release 8, Final, dated 19.03.2010
3. CSCA Countersigning and Master List Issuance, Technical Report, Version 1.0 dated 23.06.2009
4. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280 dated April 2002
5. Machine Readable Travel Documents, GUIDANCE DOCUMENT, PKI for Machine Readable Travel Documents, Version - 1.0 dated 22.06.2011
6. B-Tec/46 dated 27.06.2011 - PKD Machine Readable Error Codes

Introduction

1. The PKD content categories Country Signing Certification Authority (CSCA) Certificates (Self-Signed and Link), Document Signer Certificates, Certificate Revocation Lists and CSCA Master Lists are defined in ICAO Document 9303, the corresponding Supplement and the CSCA Master Lists Technical Report. The reference to RFC 3280 is given for completeness.

2. It is a matter of fact that PKD Participants implement the PKD contents specifications not in exactly the same way. As the efficient and effective PKD operation has the highest priority in accordance with the Rules of Procedure the PKD Operator must handle the resulting deviations from the specifications during up- and download of PKD contents.

3. The term upload for CSCA Certificates is used here for simplicity though there is no possibility for downloading them. (The term import is more appropriate.)

Principle

4. Two different classes of deviations from the PKD contents specifications are distinguished.

5. The first class comprises acceptable deviations, i.e. the deviation is not security or interoperability critical but may require special attention should the PKD content be used for document validation.

6. The second class comprises unacceptable deviations, i.e. the deviation is security or interoperability critical and prevents the prospective PKD content from being uploaded.

Procedure

7. The PKD Operator implements PKD upload contents checks to identify deviations from the PKD contents specifications.

8. A prospective PKD content will be assigned to belong to the class of contents with acceptable deviations should one or more checks contained in Attachment A not be passed. This content will during upload be individually marked with a list of checks not passed. It will be offered for separate download in the PKD.

9. A prospective PKD content will be assigned to belong to the class of contents with unacceptable deviations should one or more checks contained in Attachment B not be passed. This content can only be uploaded with the permission of the PKD Board that includes the obligation of the uploading party to rectify the deviations within six months at the maximum.

10. The checks mentioned in Attachments A and B together with the used error codes are elaborated in greater detail in a separate document given in the list of reference documents (see above).

11. For additional information please also visit the Frequently Asked Questions (FAQ) at the PKD Board web site[1] as well as at the PKD main[2] / backup[3] sites.

---

[1] http://www.icao.int/Security/mrtd/Pages/icaoPKD.aspx
[2] https://pkddownloadsg.icao.int/
[3] https://pkddownloadth.icao.int/

Attachment A

(non standard conformant PKD contents with acceptable variations)

A-I. CSCA Certificates

Field	Variations allowed
Serial Number	May be zero.
Subject	Encoding may be Printable String.
Path Length Constraint	May be 1.

A-II. CSCA Link Certificates

Field	Variations allowed
Serial Number	May be zero.
Subject	Encoding may be Printable String.
Path Length Constraint	May be 1.

A-III. Document Signer Certificates

Field	Variations allowed
Serial Number	May be zero.
Subject	Encoding may be Printable String.
Subject	Country code may be absent.

A-IV. CSCA Master Lists

None

A-V. Certificate Revocation Lists

Field	Variations allowed
Issuer	Encoding may be Printable String.

Attachment B

(non standard conformant PKD contents with unacceptable variations)

B-I. CSCA Certificates

Field	Variations not allowed
Version	Value other than 3.
Serial Number	Is not present.
	Negative Values.
	Not 2's complement encoding.
	Not smallest number of Octets representation.
	Greater than 20 Octets.
Validity	Is not present.
	Dates less than 2050 encoded as Generalised Time.
	Date greater than 2049 encoded as UTCTime.
	Generalised Time having fractional seconds.
	UTCTime encoding is wrong
	Generalised Time encoding is wrong
Subject	Is not present.
	Country code not present.
	Invalid String Encoding. (other than UTF8 and PrintableString)
Unique Identifiers	Is present.
Extensions	Default values are encoded.
AKI	Is critical.
	Does not have Key Identifier.
SKI	Is critical.
	Is not present.
	Does not have Key Identifier.
Key Usage	Is not present.
	Any bit other than crlSign and keyCertSign is set.
	Is not critical.

Field	Variations not allowed
Private Key Usage Period	Is critical.
	Is present, but notBefore and notAfter are missing.
	Is not encoded as generalised Time.
Certificate Policies	Is critical.
Policy Mappings	Is present.
Subject Alternate Name	Is critical.
Issuer Alternate Name	Is critical.
Subject Directory Attributes	Is critical.
Basic Constraints	Is not present.
	Is not critical.
	CA bit is not asserted.
	Path Length is absent or greater than 1.
Name Constraints	Is present.
Policy Constraints	Is present.
EKU	Is present.
CRL DP	Is critical.
Inhibit Any Policy	Is present.
Freshest CRL	Is present.
Private Internet Extensions	Is critical.
Netscape Certificate Extensions	Is present.

B-II. CSCA Link Certificates

Field	Variations not allowed
Version	Value other than 3.
Serial Number	Is not present.
	Negative Values.
	Not 2's complement encoding.
	Not smallest number of Octets representation.
	Greater than 20 Octets.
Validity	Is not present.

Field	Variations not allowed
	Dates less than 2050 encoded as Generalised Time.
	Date greater than 2049 encoded as UTCTime.
	Generalised Time having fractional seconds.
	UTCTime encoding is wrong
	Generalised Time encoding is wrong
Issuer	Is not present.
	Country code not present.
	Invalid String Encoding. (other than UTF8 and PrintableString)
Subject	Is not present.
	Country code not present.
	Invalid String Encoding. (other than UTF8 and PrintableString)
Unique Identifiers	Is present.
Extensions	Default values are encoded.
AKI	Is not present.
	Is critical.
	Does not have Key Identifier.
SKI	Is critical.
	Is not present.
	Does not have Key Identifier.
Key Usage	Is not present.
	Any bit other than crlSign and keyCertSign is set.
	Is not critical.
Private Key Usage Period	Is critical.
	Is present, but notBefore and notAfter are missing.
	Is not encoded as generalised Time.
Certificate Policies	Is critical.
Policy Mappings	Is present.
Subject Alternate Name	Is critical.
Issuer Alternate Name	Is critical.
Subject Directory Attributes	Is critical.
Basic Constraints	Is not present.

Field	Variations not allowed
	Is not critical.
	CA bit is not asserted.
	Path Length is absent or greater than 1.
Name Constraints	Is present.
Policy Constraints	Is present.
EKU	Is present.
CRL DP	Is critical.
Inhibit Any Policy	Is present.
Freshest CRL	Is present.
Private Internet Extensions	Is critical.
Netscape Certificate Extensions	Is present.

B-III. Document Signer Certificates

Field	Variations not allowed
Version	Value other than 3.
Serial Number	Is not present.
	Negative Values.
	Not 2's complement encoding.
	Not smallest number of Octets representation.
	Greater than 20 Octets.
Issuer	Is not present.
	Country code not present.
	Invalid String Encoding. (other than UTF8 and PrintableString)
Validity	Is not present.
	Dates less than 2050 encoded as Generalised Time.
	Date greater than 2050 encoded as UTCTime.
	Generalised Time having fractional seconds.
	UTCTime encoding is wrong
	Generalised Time encoding is wrong
Subject	Is not present.

Field	Variations not allowed
	Invalid String Encoding. (other than UTF8 and PrintableString)
Unique Identifiers	Is present.
Extensions	Default values are encoded.
AKI	Is not present.
	Is critical.
	Does not have Key Identifier.
SKI	Is critical.
Key Usage	Is not present.
	Any bit other than Digital Signature is set.
	Is not critical.
Private Key Usage Period	Is critical.
	Is present, but notBefore and notAfter are missing.
	Is not encoded as generalised Time.
Certificate Policies	Is critical.
Policy Mappings	Is present.
Subject Alternate Name	Is critical.
Issuer Alternate Name	Is critical.
Subject Directory Attributes	Is critical.
Basic Constraints	Is present.
Name Constraints	Is present.
Policy Constraints	Is present.
EKU	Is present.
CRL DP	Is critical.
Inhibit Any Policy	Is present.
Freshest CRL	Is present.
Private Internet Extensions	Is critical.
Netscape Certificate Extensions	Is present.

B-IV. CSCA Master Lists

Field	Variations not allowed
Content Type	Is not signed Data.
Version	Value other than 3.
eContent Type	Is not id-icao cscaMasterlist.
eContent	Is not present.
	Does not include CSCA of MasterList signer.
	Contains data other than x.509 certificates.
Certificates	Is not present.
	Master List Signer is not present.
CRLs	Is present.
SignerInfo: Version	If issuer and Serial number is used, and value is not 1.
	If SKI is used and value is not 3.
SignerInfo: Signer Identifier	Is not present.
SignerInfo: Digest Algorithm	Is not present.
SignerInfo: Signed Attributes	Is not present.
	Does not contain Signing Time.

B-V. Certificate Revocation Lists

Field	Variations not allowed
Version	Value other than 2.
Issuer	Is not present.
	Country code not present.
	Invalid String Encoding. (other than UTF8 and PrintableString)
This Update	Is not present.
	Dates less than 2050 encoded as Generalised Time.
	Date greater than 2049 encoded as UTCTime.
	Generalised Time having fractional seconds.
	UTCTime encoding is wrong
	Generalised Time encoding is wrong

Field	Variations not allowed
Next Update	Is not present.
	Dates less than 2050 encoded as Generalised Time.
	Date greater than 2049 encoded as UTCTime.
	Generalised Time having fractional seconds.
	UTCTime encoding is wrong
	Generalised Time encoding is wrong
Revoked Certificates	Is present but empty.
Extensions	Default values are encoded.
AKI	Is not present.
	Is marked critical.
	Does not have Key Identifier.
Issuer Alternate Name	Is critical.
CRL Number	Is not present.
	Not 2's complement encoding.
	Not smallest number of Octets representation.
	Greater than 20 Octets.
	Negative values.
	Is critical.
Delta CRL indicator	Is present.
Issuing Distribution point	Is present.
Freshest CRL	Is present.
CRL Entry Extensions: Reason Code	Is critical.
CRL Entry Extensions: Hold Instruction code	Is critical.
CRL Entry Extensions: Invalidity Date	Is critical.
	Is not generalised time.
CRL Entry Extensions: Certificate Issuer	Is present.