PKD Machine Readable Error Codes

PKD Machine Readable Error Codes
-
PKD Board Discussion Paper

Forwarded by: Netrust

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/26 dated 27.06.2011 - PKD Upload Contents Checks
7. B-Tec/39 dated 08.02.2011 - Procedure for Non Conformant PKD Contents

Introduction

1. The PKD Board installed a mechanism for accepting non-conformant entries and their publishing in the PKD.

2. For all entries published in the PKD, a description field will be added detailing the non-conformance of the entry. This would be a human readable list of messages that detail the non-conformance.

3. The PKD Board requested that along with a human readable description, a mechanism be proposed for publishing machine readable descriptions that can be used for automated processing of the entries by downloading entities.

Principles

4. The machine readable error codes will have the following components.

5. An identifier marking whether this is an acceptable deviation or a non-acceptable deviation from the standards. Acceptable deviations will be identified as "WARN" and non-acceptable deviations will be identified as "ERR". (DevID)

6. An identifier stating the type of entry i.e. CSCA Certificate, DSC or CRL. (TypeID)

7. An identifier that states the element within the CSCA Certificate, DSC or CRL that has the deviation. A complete list is provided in Attachment A. (ElementID)

8. An identifier stating the non-conformance. A complete list is provided in Attachment B. (non-conformanceID)

9. Attachment C maps the non-conformance identifiers to the contents of CSCA Certificates, DSC and CRL.

10. Attachment D gives some worked out examples of the error code that will be published based on the three components.

Additional Considerations

11. Since an entry may have both acceptable and non acceptable variations, all the variations will be listed and delimited by the sign ":". All the warnings will be listed together, followed by the errors.

12. An entry (DSC or CRL) may have been issued by a non-conformant CSCA Certificate. The CSCA Certificate non-conformance will be included in the description for the entry.

13. The machine readable error codes will take the following form: DevID:TypeID.ElementID.non-conformanceID

Attachment A

A-I. Certificates

Field	Identifier
Version	VER
Serial Number	SER
Issuer	ISS
Validity	VAL
Subject	SUB
Unique Identifiers	UID
Extensions	EXT
Authority Key Identifier	AKI
Subject Key Identifier	SKI
Key Usage	BKU
Private Key Usage Period	PKU
Certificate Policies	CEP
Policy Mappings	POM
Subject Alternate Name	SAN
Issuer Alternate Name	IAN
Subject Directory Attributes	SDA
Basic Constraints	BAC
Name Constraints	NAC
Policy Constraints	POC
Extended Key Usage	EKU
CRL Distribution Point	CDP
Inhibit Any Policy	IAP
Freshest CRL	FCR
Private Internet Extensions	PIE
Netscape Certificate Extensions	NCE

A-II. Certificate Revocation Lists

Field	Identifier
Version	VER
Issuer	ISS
This Update	TUP
Next Update	NUP
Revoked Certificates	REC
Extensions	EXT
Authority Key Identifier	AKI
Issuer Alternate Name	IAN
CRL Number	CRN
Delta CRL indicator	DCR
Issuing Distribution point	IDP
Freshest CRL	FCR
CRL Entry Extensions: Reason Code	REA
CRL Entry Extensions: Hold Instruction code	HIC

Field	Identifier
CRL Entry Extensions: Invalidity Date	IND
CRL Entry Extensions: Certificate Issuer	CEI

Attachment B

Error	**Numeric Code**
Integer_Not_Positive	0
Integer_Not_2scomplement_Encoded	1
Integer_Not_Smallest_Octet_Encoded	2
Integer_Largerthan_20Octets	3
Date_Lessthan_2050_Encodedas_GenTime	4
Date_Greaterthan_2049_Encodedas_UTC_Time	5
GenTime_has_Fractional_Seconds	6
UTCTime_Wrong_Encoding	7
GenTime_Wrong_Encoding	8
Not_Encodedas_GenTime	9
Country_Code_Not_Present	10
Invalid_String_Encoding	11
Version_Not_3	12
Version_Not_2	13
Field_Not_Present	14
Field_Present	15
Is_Present_But_Empty	16
Is_Present_But_NotBefore_and_NotAfter_Missing	17
Is_Critical	18
Is_Not_Critical	19
Bit_Otherthan_crlSign_and_keyCertSign_Set	20
Bit_Otherthan_DigSig_Set	21
Default_Value_Encoded	22
KeyID_Missing	23
CA_Bit_Not_Asserted	24
Path_Length_Not_Zero	25

Attachment C

C-I. CSCA Certificates

Field	Variations allowed	Error Code
Serial Number	May be zero.	Integer_Not_Positive
Subject	Encoding may be Printable String.	Invalid_String_Encoding
Path Length Constraint	May be 1.	Path_Length_Not_Zero

C-II. CSCA Link Certificates

Field	Variations allowed	Error Code
Serial Number	May be zero.	Integer_Not_Positive
Subject	Encoding may be Printable String.	Invalid_String_Encoding
Path Length Constraint	May be 1.	Path_Length_Not_Zero

C-III. Document Signer Certificates

Field	Variations allowed	Error Code
Serial Number	May be zero.	Integer_Not_Positive
Subject	Encoding may be Printable String.	Invalid_String_Encoding
Subject	Country code may be absent.	Country_Code_Not_Present

C-IV. Certificate Revocation Lists

Field	Variations allowed	Error Code
Issuer	Encoding may be Printable String.	Invalid_String_Encoding

C-V. CSCA Certificates

Field	Variations not allowed	Error Code
Version	Value other than 3.	Version_Not_3
Serial Number	Is not present.	Field_Not_Present
	Negative Values.	Integer_Not_Positive
	Not 2's complement encoding.	Integer_Not_2scomplement_Encoded
	Not smallest number of Octets representation.	Integer_Not_Smallest_Octet_Encoded
	Greater than 20 Octets.	Integer_Largerthan_20Octets

Field	Variations not allowed	Error Code
Validity	Is not present.	Field_Not_Present
	Dates less than 2050 encoded as Generalised Time.	Date_Lessthan_2050_Encodedas_GenTime
	Date greater than 2049 encoded as UTCTime.	Date_Greaterthan_2049_Encodedas_UTC_Time
	Generalised Time having fractional seconds.	GenTime_has_Fractional_Seconds
	UTCTime encoding is wrong	UTCTime_Wrong_Encoding
	Generalised Time encoding is wrong	GenTime_Wrong_Encoding
Subject	Is not present.	Field_Not_Present
	Country code not present.	Country_Code_Not_Present
	Invalid String Encoding. (other than UTF8 and PrintableString)	Invalid_String_Encoding
Unique Identifiers	Is present.	Field_Present
Extensions	Default values are encoded.	Default_Value_Encoded
AKI	Is critical.	Is_Critical
	Does not have Key Identifier.	KeyID_Missing
SKI	Is critical.	Is_Critical
	Is not present.	Field_Not_Present
	Does not have Key Identifier.	KeyID_Missing
Key Usage	Is not present.	Field_Not_Present
	Any bit other than crlSign and keyCertSign is set.	Bit_Otherthan_crlSign_and_keyCertSign_Set
	Is not critical.	Is_Not_Critical
Private Key Usage Period	Is critical.	Is_Critical
	Is present, but notBefore and notAfter are missing.	Is_Present_But_NotBefore_and_NotAfter_Missing
	Is not encoded as generalised Time.	Not_Encodedas_GenTime
Certificate Policies	Is critical.	Is_Critical

Field	Variations not allowed	Error Code
Policy Mappings	Is present.	Field_Present
Subject Alternate Name	Is critical.	Is_Critical
Issuer Alternate Name	Is critical.	Is_Critical
Subject Directory Attributes	Is critical.	Is_Critical
Basic Constraints	Is not present.	Field_Not_Present
	Is not critical.	Is_Not_Critical
	CA bit is not asserted.	CA_Bit_Not_Asserted
	Path Length is absent or greater than 1.	Path_Length_Not_Zero
Name Constraints	Is present.	Field_Present
Policy Constraints	Is present.	Field_Present
EKU	Is present.	Field_Present
CRL DP	Is critical.	Is_Critical
Inhibit Any Policy	Is present.	Field_Present
Freshest CRL	Is present.	Field_Present
Private Internet Extensions	Is critical.	Is_Critical
Netscape Certificate Extensions	Is present.	Field_Present

C-VI. CSCA Link Certificates

Field	Variations not allowed	Error Code
Version	Value other than 3.	Version_Not_3
Serial Number	Is not present.	Field_Not_Present
	Negative Values.	Integer_Not_Positive
	Not 2's complement encoding.	Integer_Not_2scomplement_Encoded
	Not smallest number of Octets representation.	Integer_Not_Smallest_Octet_Encoded

Field	Variations not allowed	Error Code
	Greater than 20 Octets.	Integer_Largerthan_20Octets
Validity	Is not present.	Field_Not_Present
	Dates less than 2050 encoded as Generalised Time.	Date_Lessthan_2050_Encodedas_GenTime
	Date greater than 2049 encoded as UTCTime.	Date_Greaterthan_2049_Encodedas_UTC_Time
	Generalised Time having fractional seconds.	GenTime_has_Fractional_Seconds
	UTCTime encoding is wrong	UTCTime_Wrong_Encoding
	Generalised Time encoding is wrong	GenTime_Wrong_Encoding
Issuer	Is not present.	Field_Not_Present
	Country code not present.	Country_Code_Not_Present
	Invalid String Encoding. (other than UTF8 and PrintableString)	Invalid_String_Encoding
Subject	Is not present.	Field_Not_Present
	Country code not present.	Country_Code_Not_Present
	Invalid String Encoding. (other than UTF8 and PrintableString)	Invalid_String_Encoding
Unique Identifiers	Is present.	Field_Present
Extensions	Default values are encoded.	Default_Value_Encoded
AKI	Is not present.	Field_Not_Present
	Is critical.	Is_Critical
	Does not have Key Identifier.	KeyID_Missing
SKI	Is critical.	Is_Critical
	Is not present.	Field_Not_Present
	Does not have Key Identifier.	KeyID_Missing
Key Usage	Is not present.	Field_Not_Present
	Any bit other than crlSign and keyCertSign is set.	Bit_Otherthan_crlSign_and_keyCertSign_Set
	Is not critical.	Is_Not_Critical

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

C-VII. Document Signer Certificates

Field	Variations not allowed	Error Code
Version	Value other than 3.	Version_Not_3
Serial Number	Is not present.	Field_Not_Present
	Negative Values.	Integer_Not_Positive
	Not 2's complement encoding.	Integer_Not_2scomplement_Encoded
	Not smallest number of Octets representation.	Integer_Not_Smallest_Octet_Encoded
	Greater than 20 Octets.	Integer_Largerthan_20Octets
Issuer	Is not present.	Field_Not_Present
	Country code not present.	Country_Code_Not_Present
	Invalid String Encoding. (other than UTF8 and PrintableString)	Invalid_String_Encoding
Validity	Is not present.	Field_Not_Present
	Dates less than 2050 encoded as Generalised Time.	Date_Lessthan_2050_Encodedas_GenTime
	Date greater than 2049 encoded as UTCTime.	Date_Greaterthan_2049_Encodedas_UTC_Time
	Generalised Time having fractional seconds.	GenTime_has_Fractional_Seconds
	UTCTime encoding is wrong	UTCTime_Wrong_Encoding
	Generalised Time encoding is wrong	GenTime_Wrong_Encoding
Subject	Is not present.	Field_Not_Present
	Invalid String Encoding. (other than UTF8 and PrintableString)	Invalid_String_Encoding
Unique Identifiers	Is present.	Field_Present
Extensions	Default values are encoded.	Default_Value_Encoded
AKI	Is not present.	Field_Not_Present
	Is critical.	Is_Critical
	Does not have Key Identifier.	KeyID_Missing
SKI	Is critical.	Is_Critical
Key Usage	Is not present.	Field_Not_Present

Field	Variations not allowed	Error Code
	Any bit other than Digital Signature is set.	Bit_Otherthan_DigSig_Set
	Is not critical.	Is_Not_Critical
Private Key Usage Period	Is critical.	Is_Critical
	Is present, but notBefore and notAfter are missing.	Is_Present_But_NotBefore_and_NotAfter_Missing
	Is not encoded as generalised Time.	Not_Encodedas_GenTime
Certificate Policies	Is critical.	Is_Critical
Policy Mappings	Is present.	Field_Present
Subject Alternate Name	Is critical.	Is_Critical
Issuer Alternate Name	Is critical.	Is_Critical
Subject Directory Attributes	Is critical.	Is_Critical
Basic Constraints	Is present.	Field_Present
Name Constraints	Is present.	Field_Present
Policy Constraints	Is present.	Field_Present
EKU	Is present.	Field_Present
CRL DP	Is critical.	Is_Critical
Inhibit Any Policy	Is present.	Field_Present
Freshest CRL	Is present.	Field_Present
Private Internet Extensions	Is critical.	Is_Critical
Netscape Certificate Extensions	Is present.	Field_Present

C-VIII. Certificate Revocation Lists

Field	Variations not allowed	Error Code
Version	Value other than 2.	Version_Not_2

Field	Variations not allowed	Error Code
Issuer	Is not present.	Field_Not_Present
	Country code not present.	Country_Code_Not_Present
	Invalid String Encoding. (other than UTF8 and PrintableString)	Invalid_String_Encoding
This Update	Is not present.	Field_Not_Present
	Dates less than 2050 encoded as Generalised Time.	Date_Lessthan_2050_Encodedas_GenTime
	Date greater than 2049 encoded as UTCTime.	Date_Greaterthan_2049_Encodedas_UTC_Time
	Generalised Time having fractional seconds.	GenTime_has_Fractional_Seconds
	UTCTime encoding is wrong	UTCTime_Wrong_Encoding
	Generalised Time encoding is wrong	GenTime_Wrong_Encoding
Next Update	Is not present.	Field_Not_Present
	Dates less than 2050 encoded as Generalised Time.	Date_Lessthan_2050_Encodedas_GenTime
	Date greater than 2049 encoded as UTCTime.	Date_Greaterthan_2049_Encodedas_UTC_Time
	Generalised Time having fractional seconds.	GenTime_has_Fractional_Seconds
	UTCTime encoding is wrong	UTCTime_Wrong_Encoding
	Generalised Time encoding is wrong	GenTime_Wrong_Encoding
Revoked Certificates	Is present but empty.	Is_Present_But_Empty
Extensions	Default values are encoded.	Default_Value_Encoded
AKI	Is not present.	Field_Not_Present
	Is marked critical.	Is_Critical
	Does not have Key Identifier.	KeyID_Missing
Issuer Alternate Name	Is critical.	Is_Critical
CRL Number	Is not present.	Field_Not_Present

Field	Variations not allowed	Error Code
	Not 2's complement encoding.	Integer_Not_2scomplement_Encoded
	Not smallest number of Octets representation.	Integer_Not_Smallest_Octet_Encoded
	Greater than 20 Octets.	Integer_Largerthan_20Octets
	Negative values.	Integer_Not_Positive
	Is critical.	Is_Critical
Delta CRL indicator	Is present.	Field_Present
Issuing Distribution point	Is present.	Field_Present
Freshest CRL	Is present.	Field_Present
CRL Entry Extensions: Reason Code	Is critical.	Is_Critical
CRL Entry Extensions: Hold Instruction code	Is critical.	Is_Critical
CRL Entry Extensions: Invalidity Date	Is critical.	Is_Critical
	Is not generalised time.	Not_Encodedas_GenTime
CRL Entry Extensions: Certificate Issuer	Is present.	Field_Present

Attachment D

Example I:

If a CSCA Certificate has the following non-conformance:

a) In Subject field, encoding for the country code is in PrintableString (Acceptable)
b) Path Length is not set (Not-Acceptable)
c) Extended Key Usage has been set (Not-Acceptable).

The machine readable code would be constructed as follows:

WARN:CSCA.SUB.11:ERR:CSCA.BAC.25:CSCA.EKU.15

Example II:

If a DSC has the following non-conformance:

a) Serial Number has negative value (Not-Acceptable).
b) Subject does not have country code (Acceptable).

And, it is issued by the CSCA Certificate in the previous example, then the machine readable error code would be constructed as follows:

WARN:CSCA.SUB.11:DSC.SUB.10:ERR:CSCA.BAC.25:CSCA.EKU.15:DSC.SER.0