



NATIONAL SECURITY AUTHORITY

Version 1.0

Trusted List Management

7 July 2009

This English version of the Slovak document No. 6644/2008/IBEP-001 is for reference purposes only. In case of conflict between the English translation and the original Slovak version, the Slovak version shall prevail and supersedes the English translation as the original version. Therefore, only the NSA Deliverables published by NSA in their original language shall be used for evaluation of products and technical judgement.

NATIONAL SECURITY AUTHORITY

Information Security and Electronic Signature Department

Budatinska 30, P.O. BOX 16, 850 07 Bratislava 57

<http://www.nbusr.sk/>

E-mail: sep@nbusr.sk

Content

1	Introduction	4
2	Scope	4
3	References	5
4	Abbreviations	6
5	Management and life cycle of TL	7
5.1	Adding the references to approved SPs and trusted certificates	7
5.2	Prolonging the validity of approved SP	7
5.3	SP and trusted certificate revocation.....	8
5.4	Trusted publication of TL	8
6	TL format and procedures of its creation and verification	9
7	The Qualified Electronic Signature validity of the document	10
	Annex A (informative) Examples of approved SPs and trusted certificates in TL	11
A.1	The example of signed TXT file in TL	11
A.2	Examples of revocation of approved SPs with OID 1.1.5 in TL	11
	Annex B (informative) Revisions made since previous version	12
B.1	Additional requirements	12
B.2	Updated requirements.....	12
B.3	Clarifications	12
B.4	Editorial	12
	Annex C (informative) Bibliography	13
	Annex D History	15

1 Introduction

Verification of the Qualified Electronic Signature (hereinafter referred to as QES) validity is realized not only in the time of the qualified certificate or maintenance certificate validity period, but also in later time when e.g. all certificates used for QES verification have expired. The majority of certification service providers, after the certificate expiration, do not continue with providing the information about the potential revocation in CRL or OCSP. In order to ensure the **correct verification of QES** also in the time when the certificates are already expired and the trusted certificate is already expired too and cannot be found in the trusted repository of applications, it is required to provide **a trusted publication of information containing the history of expired trusted certificates** as well as the history of **rules** used in the past which are **verifiable by the currently trusted certificate**. The publication of such information is most frequently realized by means of trusted list containing the current and historic data too. While verifying the QES there is also a need of checking the attributes and properties which are not usually required for ordinary electronic signatures [1, 6] but they are essential for QES to ensure the required level of trust in QES, for example whether in the time of the signature creation were used algorithms from the set of permitted secure algorithms and their parameters for the QES creation and verification [4, 5, 9, 11]. In order to realize the signing and verification process of the QES validity automatically also in the QES verification with already expired certificates with the least interactions possible between the signer and verifier, it is necessary to define automatic procedures and data structures which shall enable such verification.

2 Scope

The standard “Trusted List Management” is issued pursuant to Article 4 (6) of the Decree of the National Security Authority (hereinafter referred to as the Authority) No. 135/2009 Coll. on the format and method of creating the qualified electronic signature, the method of publishing the public key of the National Security Authority, the conditions of validity for the qualified electronic signature, procedure during the verification and verification conditions of the qualified electronic signature, format of the time stamp and method of creating it, requirements on the source of time data and requirements for keeping time stamp documentation (on the creation and verification of the electronic signature and time stamp).

The present standard defines rules for trusted publishing the lists of different types of electronic documents for example the list of approved signature policies or current as well as expired trusted certificates which are required for the qualified electronic signature creation and verification and also for publishing the trusted certificates for the signature verification of the trusted list which was issued according to Commission Decision 2009/767/EC. While the trusted list according to CD 2009/767/EC is mainly used as a source of information if the certificate was issued by accredited/supervised provider in EU, the trusted list (hereinafter referred to as TL) according to this standard is a starting point for subsequent verification by TL according to CD 2009/767/EC.

To enable the automatic verification of current and historic information on the validity of approved signature policies (SPs) and trusted certificates, the list of approved signature policies is published on the web page of the Authority according to Article 4 (6) of the NSA Decree No. 135/2009 Coll. by means of the signed TL of references on approved SPs and trusted certificates.

The format of the attribute content and the manner of usage of such TL are defined in the present document. In further chapters the present document defines the management, the method of publishing, the end of validity, validity prolonging, early revocation and adding new approved SPs and trusted certificates for technical specification of requirements laid down in Article 4 of the NSA Decree No. 135/2009 Coll.

Requirements of the present document are adequately used for publishing the trusted lists of other types of electronic documents than signature policies and certificates.

3 References

References to documents defining used types and methods.

- [1] ETSI TS 101 733 Electronic Signature Formats
- [2] ETSI TR 102 272 ASN.1 format for signature policies
- [3] RFC 5280 X.509 PKI Certificate and Certificate Revocation List May 2008
- [4] RFC 3739 Qualified Certificates Profile March 2004
- [5] RFC 5126 CMS Advanced Electronic Signatures (CAAdES) February 2008
- [6] RFC 5652 Cryptographic Message Syntax (CMS) September 2009
- [7] RFC 3161 Time-Stamp Protocol (TSP) August 2001
- [8] RFC 2560 X.509 PKI Online Certificate Status Protocol June 1999
- [9] NSA Qualified Electronic Signature Formats
- [10] EN 14890 Application Interface for Smart Cards used as Secure Signature Creation Devices
Part 1: Basic Services; Part 2: Additional Services
- [11] RFC 2044 UTF-8, a transformation format of Unicode and ISO 10646 October 1996
- [12] ETSI TS 102 231 V3.1.1 Provision of harmonized Trust-service status information
- [13] NSA Decree No. 135/2009 Coll. on the format and method of creating the qualified electronic signature, the method of publishing the public key of the National Security Authority, the conditions of validity for the qualified electronic signature, procedure during the verification and verification conditions of the qualified electronic signature, format of the time stamp and method of creating it, requirements on the source of time data and requirements for keeping time stamp documentation (on the creation and verification of the electronic signature and time stamp)
- [14] NSA Decree No. 136/2009 Coll. on the method and procedure of using the electronic signature in business and administrative relations

4 Abbreviations

ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CAdES	CMS Advanced Electronic Signature
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
SP	Signature Policy
QC	Qualified Certificate
QES	Qualified Electronic Signature
SHA-1	Secure Hash Algorithm 1
SSCD	Secure-Signature-Creation Device
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
TL	Trusted list of references on electronic documents e.g. approved SPs and trusted certificates
NSA	National Security Authority of the Slovak Republic

5 Management and life cycle of TL

Pursuant to Act No. 215/2002 Coll. on Electronic Signature and on the amendment and supplementing of certain acts as amended (hereinafter referred to as the Act), Article 10 (2), letter d) the Authority publishes its own public key and pursuant to Article 4 of the NSA Decree No. 135/2009 Coll. the Authority publishes approved SPs.

All the information is published on the web page of the Authority in the form of TL. TL is regularly updated by the Authority, in case any of used components in TL or any of used components for the TL verification has changed its status [3] (e.g. validity) or in case new SPs were approved or new trusted certificates were issued. The certificate which was used to sign TL shall not be revoked immediately. It shall be valid also after the time of new TL publication so that the applications verifying the signature validity of old TL could continue with verification without the threat of the overall malfunctioning of verification and the need of manual setting of the new TL. If the application for QES finds out that the data (e.g. the signature policy or the trusted certificate) is not found in current TL application, it shall display a warning about the need for downloading and setting a new TL in the application by updating from the web page of the Authority.

The certificate which was used to sign TL can be revoked in the critical situation which might cause a serious harm to QES trustworthiness.

5.1 Adding the references to approved SPs and trusted certificates

The Authority after the approval of SP for the qualified electronic signature creation and verification will publish the approved SP on its web page and similarly, when issuing a new trusted certificate pursuant to Article 10 (2) letter d) of the Act No.215/2002 Coll. the Authority will publish this certificate on its web page. After publishing this information on the web page of the Authority, the Authority will include this data in TL, which will be signed by the certificate intended for TL signing.

The approved SP is valid in the time period indicated in the signature policy (validity notBefore - notAfter), if the signature policy was not revoked earlier. Similarly, the trusted certificate is valid according to data indicated in the trusted certificate (validity notBefore - notAfter) if the trusted certificate was not revoked earlier (for the reason that the selfsigned certificate revocation is not published in CRL).

Information mentioned above is published on the web page of the Authority and recorded in TL which is also published and signed by the Authority.

5.2 Prolonging the validity of approved SP

The signature policy due to algorithm ageing must not be issued for unlimited period of time. The validity of approved signature policy is automatically prolonged before its end by issuing a new signature policy with changed data concerning the date of SP issuing, SP validity beginning and end and OID identifier of SP (and a hash value in DER SP [2]), if defects unacceptable for further validity period were not found in the approved SP.

After the validity of approved SP is prolonged by the Authority, the approved SP will be published pursuant to the procedure described in part 5.1.

5.3 SP and trusted certificate revocation

Approved SPs are revoked by the Authority on request of the applicant who applied for SP approval. The Authority can revoke the approved SP on request of other physical person or legal entity but also in case of circumstances occurring after the approval under which mentioned SP would not be approved.

In case of the approved SP revocation, this SP will be published on the web page of the Authority as revoked and because this SP was a part of TL, its validity in TL is shortened up to the time of its revocation.

If the Authority revokes the trusted certificate earlier, the information about this event will be published on the web page of the Authority. In case of trusted certificate validity revocation, its validity in TL will be shortened up to the time of its revocation.

After the revocation of the approved SP or trusted certificate a new TL will be issued. The new TL containing the reference to revoked SP or revoked trusted certificate whose validity period (notBefore - notAfter) was shortened, will be signed by a new certificate intended for TL signing. The certificate intended for signing the old TL can be, in critical situation which might cause a serious harm to QES trustworthiness, revoked before the time of the SP revocation or the trusted certificate revocation.

5.4 Trusted publication of TL

Files of approved SPs and trusted certificates are published on the web page of the Authority and are used to create TL which must be signed by using the integrity signature by authorized employee of the Authority to whom, for that purpose, the certificate, which is verified by the current trusted certificate of the Authority's "Root CA" with the certificate policy and mandatory with the OID value 1.3.158.36061701.0.0.1.10.5.0.1, shall be issued. In addition to requirements for issuing and management of the qualified certificate with OID 1.3.158.36061701.0.0.0.1.2.2 this certificate policy also defines the requirement for its revocation in critical situations, in case of earlier validity revocation of the approved SP or trusted certificate. This OID is unique and must not be found in other types of certificates. The Authority will publish TL on its web page in the format of internal integrity signature [9] but without the time stamp so that the signature is verified to actual time and thus the correct verification in case of revocation of any approved SP or trusted certificate is ensured.

Note 1: Inserting the time stamp could cause the verification to the time of the time stamp what could lead to the use of the approved SP already invalid or invalid trusted certificate.

Note 2: For needs of archiving the content of signed textual file in TL, the text in TL is only supplemented by new information or the data are specified, for example a more secure hash algorithm is used while the old files are not deleted to ensure that it is possible to use the currently valid certificate for the TL verification to verify the validity of the long-time ago expired data on approved SPs and trusted certificates on the web page of the Authority in automatic mode.

6 TL format and procedures of its creation and verification

The structure of TL file is identical with the structure of the integrity signature which is defined in the document [9] "<http://www.nbusr.sk/en/electronic-signature/approved-formats/index.html> Qualified Electronic Signature Formats".

An example of fields of signed TXT document in UTF8 encoding from TL:

```
FILE=http://www.nbusr.sk/archive/20081231230000ZSignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=47599765A2FB493557750039788E6714AE0BFDC3
NOTICE=20091231230000Z NotAfter, OID=1.3.158.36061701.0.0.1.10.4.0.10, FieldOfApplication= Signature policy for QES.
FILE=http://www.nbusr.sk/archive/20040114163833ZTrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)=A6D7D70982CB73BE7FA69470029E7EF9360EEA68
NOTICE=20060114155622Z NotAfter
FILE=http://www.nbusr.sk/archive/20050222161337ZTrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)=4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A
NOTICE=20150222154357Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
```

The content of items in the list:

- FILE must contain the name of the file and may also contain URL of the HTTP type for that file. The name of the file must consist of three parts: the first part must contain the start date and time of the data validity in the format GeneralizedTime 99991231235959Z; the second part contains the name of the file content which in the approved SP being published on the web page of the Authority must be "SignaturePolicy" and in the trusted certificate being published on the web page of the Authority must be "TrustedCertificate"; and the third part contains the file type ".DER" in approved SP and ".CER" in the trusted certificate and in case the file names are identical, the third part may be preceded by distinguishing number;
- HASH must contain the hash value of the file referred to in the item FILE of the approved SP or trusted certificate;
- NOTICE must contain the date and time of the end of the object validity period from the previous item FILE (in the format GeneralizedTime) which is separated by blank space from the string of characters "NotAfter", being followed by other optional parameters. Individual parameters are separated by comma "," and the value is assigned to them by character "=".

The list of parameters:

- "OID" identifier of the object, in SP it is OID of the approved SP.
- "ExplicitPolicy" the list of OID identifiers of explicit certificate policies which are required in building of certification path up to the trusted certificate defined in the previous item FILE. The list of OID certificate policies is in the dot format "1.2.3.4" and separated by character "|".
- "FieldOfApplication" a text from the approved SP from the item FieldOfApplication or description of the application. This parameter is the last one in the line and therefore it can contain any characters except char 0x13 and char 0x10 (CRLF).

The date of end of the signature policy validity or the trusted certificate validity, defined in the item NOTICE must be identical with the date *notAfter* defined in the file whose link is found in the previous item FILE, in the approved SP or trusted certificate whose validity was not shortened.

In case of shortening the validity period of any approved SP or trusted certificate, the item NOTICE must contain the date and time of shortened validity period of the approved SP or trusted certificate and not the date *notAfter* defined in the file whose link is found in the previous item FILE.

TL must be **verified to actual time** and must always contain all approved SPs and trusted certificates, including those which were expired or whose validity was shortened and the date of their revocation must be found in the item NOTICE and the item HASH must contain the value

computed by currently secure algorithm in compliance with the valid legislation. This content of TL is very important for the reason of potential verification of the qualified electronic signature created in the past by using the approved SP being valid in the past and by using the path built to the trusted certificate being valid in the past (which is, in the current time, already substituted by a new trusted certificate in verification applications).

In verification of TL to actual time the verification application tries to obtain the actual CRL [3] (OCSP [8]) which is used to verify the certificate validity of the TL signer. Data included in TL can be declared as valid up to the time thisUpdate as a maximum from the actual CRL (OCSP) for the certificate validity verification of the TL signer which was verified as valid.

Thus, the full validity verification of qualified electronic signatures must be only to the time which is later or the same as thisUpdate from the actual CRL (OCSP) which was used for verification of the certificate validity of the TL signer.

More detailed description of SP items and the control process of individual items in the QES verification, in the applications for QES, are described in the document "Signature policies for QES" on the web page <http://www.nbusr.sk/en/electronic-signature/signature-politics/index.html>. Pursuant to requirements of EU Commission, TL will be also issued according to TS 102 231 from the version 3.1.1 from 2010.

7 The Qualified Electronic Signature validity of the document

The qualified electronic signature validity of the document is always determined to the time of the signature of the document, which is defined by the time stamp of the signature (if used). The validity of time stamps is determined to the time when these time stamps are issued and thus SP being valid in that time must be also found.

Certification paths which are used to control the signer's certificate and certificates of the certification path must terminate on the trusted certificate defined in TL which was valid in a given time and date.

Certification paths of time stamps must terminate on the trusted certificate defined in TL which was valid in the time of creating the controlled time stamp.

The control time of the electronic signature of the document is:

- 1) The time from the electronic signature time stamp of the document.
- 2) In the time stamp it is the time following the time defined in the time stamp which is close to actual verification time and which is preceding the time thisUpdate from the latest issued CRL (OCSP) for verification of the time stamp certificate.

And if the signature does not contain the signature time stamp:

- 3) The time from the secure audit log containing the hash of the electronic signature.
- 4) The time close to actual verification time which is preceding the time thisUpdate from the latest issued CRL (OCSP) for the certificate verification of the signer of the document. All certificates of the whole certification path must be valid to the time defined in thisUpdate for verification of the certificate validity of the signer and it is also required to obtain CRL (OCSP) for verification of the whole certification path up to the trusted certificate where each CRL (OCSP) beginning from CRL (OCSP) for the certificate verification of the signer of the document is issued in the same time or later time than the previous CRL (OCSP).

If the used approved SP is also valid to the control time and other legislative requirements for the qualified electronic signature validity are met, then the qualified electronic signature of the document can be declared as valid. The situation is similar with the time stamp verification when the approved SP being valid that time must be used to the time from the controlled time stamp.

Annex A (informative) Examples of approved SPs and trusted certificates in TL

A.1 The example of signed TXT file in TL

FILE=http://ep.nbusr.sk/kca/certs/kca/20040114163833ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= A6D7D70982CB73BE7FA69470029E7EF9360EEA68
NOTICE= 20060114155622Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://ep.nbusr.sk/kca/certs/kca/20 050222161337ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= 4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A
NOTICE= 20150222154357Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://www.nbusr.sk/ipublisher/20050221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=751B1B1B03A503727E34FC2A6F9779F5EB9B2595
NOTICE= 20150221165146Z NotAfter, OID=1.1.2, FieldOfApplication=(ES-C) Podpisová p.
FILE= http://www.nbusr.sk/ipublisher/20150221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=C50A7053039A4BB5D5329C3F47263E7D5F07DDED
NOTICE=20150221165146Z NotAfter, OID=1.1.3, FieldOfApplication=(ES-T) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/20050102172151ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=31CC3582F4423DB1D2023D5379B38F28E1B8753B
NOTICE=20050102172151Z NotAfter, OID=1.1.4, FieldOfApplication=(ES-UTF8) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/**20050221165146Z**signaturePolicy1.der
HASH(SHA1:1 3 14 3 2 26)=6528E51733D55648F43B4472227498C13995EB8F
NOTICE=**20150221165146Z** NotAfter, OID=1.1.5, FieldOfApplication=(ES) Podpisová politika

A.2 Examples of revocation of approved SPs with OID 1.1.5 in TL

FILE=http://ep.nbusr.sk/kca/certs/kca/20040114163833ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= A6D7D70982CB73BE7FA69470029E7EF9360EEA68
NOTICE= 20060114155622Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://ep.nbusr.sk/kca/certs/kca/20050222161337ZtrustedCertificate.cer
HASH(SHA1:1 3 14 3 2 26)= 4EA3F1135F43A4D521973DAA1FBEB3CDF2DCF75A
NOTICE= 20150222154357Z NotAfter, ExplicitPolicy=1.3.158.36061701.0.0.0.1.2.2
FILE=http://www.nbusr.sk/ipublisher/20050221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=751B1B1B03A503727E34FC2A6F9779F5EB9B2595
NOTICE= 20150221165146Z NotAfter, OID=1.1.2, FieldOfApplication=(ES-C) Podpisová p.
FILE= http://www.nbusr.sk/ipublisher/20050221165146ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=C50A7053039A4BB5D5329C3F47263E7D5F07DDED
NOTICE=20150221165146Z NotAfter, OID=1.1.3, FieldOfApplication=(ES-T) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/20040102172151ZsignaturePolicy.der
HASH(SHA1:1 3 14 3 2 26)=31CC3582F4423DB1D2023D5379B38F28E1B8753B
NOTICE=20050102172151Z NotAfter, OID=1.1.4, FieldOfApplication=(ES-UTF8) Podpisová p.
FILE=http://www.nbusr.sk/ipublisher/**20050221165146Z**signaturePolicy1.der
HASH(SHA1:1 3 14 3 2 26)=6528E51733D55648F43B4472227498C13995EB8F
NOTICE=**20080221165146Z** NotAfter, OID=1.1.5, FieldOfApplication=(ES) Podpisová politika

Annex B (informative) Revisions made since previous version

B.1 Additional requirements

The following items have been added which significantly affect the requirements:

None.

B.2 Updated requirements

The following items have been updated to extend choices or otherwise modify requirements:

None.

B.3 Clarifications

The following items have been updated to clarify existing requirements:

None.

B.4 Editorial

A number of other editorial changes were made which do not affect the technical content of the present document:

None.

Annex C (informative) Bibliography

Basic documents of the Slovak Republic legislation for electronic signature

<http://www.nbusr.sk/en/electronic-signature/legislation/index.html>

Qualified electronic signature formats

<http://www.nbusr.sk/en/electronic-signature/approved-formats/index.html>

Certification path creation and certificate validity verification

<http://www.nbusr.sk/en/electronic-signature/verification/index.html>

- IETF RFC 4158 "Internet X.509 Public Key Infrastructure: Certification Path Building"

Notice: Available at <http://www.rfc-archive.org/getrfc.php?rfc=4158>

- IETF RFC 5217 "Multi-Domain PKI Interoperability" July 2008

Notice: Available at <http://www.rfc-archive.org/getrfc.php?rfc=5217>

- IETF RFC 4853 (2007): "Cryptographic Message Syntax (CMS) Multiple Signer Clarification"
- IETF RFC 3447 (2003): "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"
- ISO/IEC 8825-1:1998, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
- ISO/IEC 19794-2:2005, Biometrics — Biometric Data Interchange Formats — Part 2: Finger Minutiae
- IETF RFC 3279 (2002): "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
- IETF RFC 4055 (2005): "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile"
- IETF RFC 3281 (2002): "An Internet Attribute Certificate profile for Authorization"
- IETF RFC 3370 (2002): "Cryptographic Message Syntax (CMS) Algorithms"
- ETSI TR 102 038: "TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies"
- ETSI TS 101 861: "Time stamping profile"
- EN 14890-2:2008: "Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services"
- ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates"
- ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"
- CWA 14167-1: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements"
- CWA 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic module for CSP Signing Operations with Backup - Protection Profile"
- CWA 14167-3: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)"
- CWA 14167-4: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP"
- W3C Recommendation (10 June 2008): "XML Signature Syntax and Processing (Second Edition)"

Notice: Available at <http://www.w3.org/TR/xmlsig-core/>

- W3C Recommendation (10 December 2002): "XML Encryption Syntax and Processing"

Notice: Available at <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/>

- CWA 14169: "Secure Signature-Creation Devices "EAL 4+""
- IETF RFC 4949 "Internet Security Glossary, Version 2" August 2007

Notice: Available at <http://www.rfc-archive.org/getrfc.php?rfc=4949>

- NIST X.509 path validation test suite

Notice: Available at <http://csrc.nist.gov/pki/testing/x509paths.html>
<http://csrc.nist.gov/pki/testing/pathdiscovery.html>

- Object Identifier (OID) Repository: ITU-T X.660 & X.670 Recommendation series (or ISO/IEC 9834 series of International Standards)

Notice: Available at <http://www.oid-info.com/>

- FESA – Forum of European Supervisory Authorities,

Notice: Available at <http://www.fesa.rtr.at>

- OID tree structure,

Notice: Available at <http://www.darmstadt.gmd.de/secude/Doc/htm/oidgraph.htm>

- Common ISIS-MTT Specification for interoperable PKI applications. Version 1.1. 16 March 2004
- Internet Draft "X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA"

Notice: Available at <http://tools.ietf.org/html/draft-ietf-pkix-sha2-dsa-ecdsa-05>

- Internet Draft "X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) "

Notice: Available at <http://tools.ietf.org/html/draft-ietf-pkix-rfc3161bis-01>

- TeleTrusT Deutschland e. V., "OID-Liste",

Notice: Available at <http://www.teletrust.de/index.php?id=171>

European Commission <http://ec.europa.eu/>

- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

Notice: Available at

http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31999L0093&model=guichett

- IDABC stands for Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens. - eSignature Agenda & Presentations

Notice: Available at <http://ec.europa.eu/idabc/en/document/7312>

- European Network and Information Security Agency (ENISA)

Notice: Available at <http://www.enisa.europa.eu/>

- PKIX Status Pages <http://tools.ietf.org/wg/pkix/>

Annex D History

Version	Date of issuing	Note	Editor
Version 1.0. No. 1859/2010/IBEP/OEP-001	7 July 2009	First edition	Peter Rybár, NSA