



NATIONAL SECURITY AUTHORITY

Version 1.1

Signature Policies for QES

16 December 2007

NATIONAL SECURITY AUTHORITY

Department of Information Security and Electronic Signature

Budatínska č. 30, P.O. BOX 16, 850 07 Bratislava 57

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

E-mail: sep@nbusr.sk

Content

1	Abbreviations	4
2	Scope.....	5
3	Policy processing for QES	6
3.1	Recommendation of the process for the signature policy selection in application for QES	7
3.2	Signature verification process in application for QES.....	7
4	Signature policies formats	8
4.1	Transfer of ASN.1 signature policies into policies for signatures in XAdES ETSI TS 101 903 format.....	8
	Table 1 Basic ASN.1 algorithms and attributes and their OIDs	8
4.2	Textual description of the signature policy attributes minimally required	9
5	Specific signature policies.....	11
5.1	Signature policy for Qualified Electronic Signature with a time stamp, for textual documents in ASCII and UTF8 coding, for internal or external signature types	11
	The signature policy can be used for internal as well for external types of signatures where in internal signatures it is unambiguous due to policy type that it deals with the signed textual document in UTF8 coding. In internal CMS signatures the textual document can begin with a MIME heading whose type and coding range, due to unambiguity in the QES creation and verification, is specified by the document “Qualified Electronic Signatures Formats”.	11
	Annex A (informative) Bibliography.....	12
	Annex B History	13

1 Abbreviations

ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation 1
CA	Certification Authority
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules (for ASN.1)
ES	Electronic Signature
ESS	Enhanced Security Services (enhances CMS)
GMT	Greenwich Mean Time
HTTP	HyperText Transfer Protocol
ISO	International Organization for Standardization
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Provider
OID	Object Identifier
PKCS	Public Key Cryptographic Standards, Standards published by RSA, Labs.
RIPMD-160	Race Integrity Primitives Evaluation Message Digest 160
PKIX	internet X.509 Public Key Infrastructure
QC	Qualified Certificate
RSA	Rivest, Shamir and Adleman Algorithm
SHA-1	Secure Hash Algorithm 1
SP	Signature Policy
SSCD	Secure-Signature-Creation Device
TSA	Time-Stamping Authorities
TSP	Time Stamp Protocol
TST	Time-Stamp Token
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
XAdES	XML Advanced Electronic Signature
XER	XML Encoding Rules (for ASN.1)
XML	Extensible Markup Language
QES	Qualified Electronic Signature

2 Scope

The present document is issued in accordance with §4 of the NSA Regulation No. 537/2002 Coll. on the format and method of the Qualified Electronic Signature creation, on the method of the NSA public key publication, on the procedure and conditions of the Qualified Electronic Signature verification, on the time stamp format and method of its creation, on requirements for the time data source and requirements for maintaining the time stamp documentation (on the electronic signature and time stamp creation and verification). The document specifies the use of signature policies for the Qualified Electronic Signature creation and verification according to the Act No. 215/2002 Coll. on electronic signature. The aim of the present document is to make the process of the Qualified Electronic Signature creation and verification (hereinafter referred to as “QES”) more transparent, unified and in particular simplified for subjects which create and verify QES. The document describes the framework of the signature policies use and the basic set of signature policies that can be extended, if required, to other signature policies for Qualified Electronic Signature.

Correct verification of Qualified Electronic Signatures and certification path on the basis of the signature policy is the key precondition to provide the compatibility and unified environment of the electronic signature in the area of signature policies in the Slovak Republic with respect to the electronic signature environment especially in EU member states.

The aim of the present document is not only to create an independent standard for given area but to create an unambiguous, minimal and mandatory profile of signature policies for certification service providers, applications creators and certainly for electronic signature users.

Signature policies are available on the web site

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

Used definitions are based primarily on standards in Annex A, regulations and acts. Their definitions are summarized and their use is specified by the document.

Basic documents of the Slovak legislation for the electronic signature

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

Qualified Electronic Signatures Formats

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

Attention to the translation of the present document

The Qualified Electronic Signature presented in the present document, according to the legislation being valid in the issuing time of the document, had to meet more requirements than Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Since 2007 the rules became simplified in order to provide the interoperability within EU member states.

The term electronic signature used in the present document means simple, advanced or qualified electronic signatures being not in compliance with requirements for QES in the Slovak legislation.

3 Policy processing for QES

The NSA approves signature policies for QES (hereinafter referred to as “approved SPs”). Approved SPs are published on web site of the NSA. Each of signature policy for CMS (ASN.1) signatures is published in two formats:

- in mandatory DER coding and
- in informative XER coding, as a transformation from DER coding, with the textual description in Slovak language.

Approved SPs are issued in accordance with the document “Signature Policies Administration”. This document contains detailed description of the content of Qualified Electronic Signature of approved SPs in the “integrity archival signature” format that consists especially of the sequence of hash values of DER documents of approved SPs and times of the end of individual approved SPs validity (in *notice* field, in *GeneralizedTime* format). The “integrity archival signature” format is defined in the document “Approved Qualified Electronic Signatures Formats”.

In CMS signatures the application shall be able to verify and display for the user a hash (digital fingerprint) from the part of the DER coded signature policy. Displayed hash is computed from the DER coded signature policy *SignaturePolicy* without heading, it means from fields *signPolicyHashAlg* and *signPolicyInfo*. Computed hash is also a part of the reference on a signature policy that is stored directly in attributes being signed of CMS signature.

Control process:

- the application for QES, for example at start-up, reads and verifies the integrity archival signature “ApprovedSignaturePolicies.p7m”, from which after verification it obtains a list of approved SPs file names, their hashes and times of approved SPs validity termination,
- the signature of the approved SPs list is verified by a qualified certificate (with a certificate policy 1.3.158.36061701.0.0.1.10.5.0.1) which is checked by the root certificate of the NSA (the signature verification method and detailed rules of approved SPs are described in the document “Signature Policies Administration”),
- the obtained list of approved SPs hash values and times of approved SPs validity termination is used later on by the application to determine if the signature being verified is a Qualified Electronic Signature (according to the Slovak legislation) or only an electronic signature and if the electronic signature being verified is valid,
- in the QES verification, only the signature, which in signed attributes contains the reference on the signature policy (hash) compliant with one of the approved SPs from the approved SPs list, where the list was obtained in the first step and the signature itself being verified was created before the time of approved SP validity termination, shall be declared as QES.

3.1 Recommendation of the process for the signature policy selection in application for QES

The application for the QES creation should have *DropDown* menu containing the signature policies list (with the text from the field *fieldOfApplication* from every signature policy). The signature policy for the signature being created is set on the basis of the policy selection from the list.

A signer through the signature policy selection determines the signature attributes *signerRules* that shall be inserted in the signature by the application. The signer, along with the policy selection, defines attributes required from a verifier *verifierRules* which shall be added to the signature by the verifier if he agrees with the signature verification according to the policy selected by the signer. For example while signing with a time stamp the signer is not required to insert the time stamp but if the verifier finds out that the time stamp is not inserted, he shall do it because it is required by *verifierRules*.

3.2 Signature verification process in application for QES

The application shall check the signature on the basis of the signature policy according to which the signature was created. The signature policy identifier is directly inserted in the signature by the signer, in attributes being signed and thus an unambiguous and non-repudiated identification of the selected signature policy is provided by the signature. Verification by other policy than is the policy selected by the signer is inadmissible.

In verification the application displays information about the policy according to which a given signature is verified. This information shall contain OID, hash and *fieldOfApplication* of the signature policy.

All requirements of the signature policy shall be met while verifying the signature according to the signature policy. For example the verification of an internal signature (a signed document is directly a part of DER signature *.p7m) according to the policy used only for an external signature `<externalSignedData> true </externalSignedData>` is marked as invalid.

In case there are not met all conditions for the Qualified Electronic Signature verification (e.g. a signed document format, a signature format, a qualified certificate and other requirements from the signature policy as for example: if the signature policy contains the ROOT certificate, then the ROOT certificate of the certification path shall correspond with one of the ROOT certificates indicated in the signature policy, etc.), the Qualified Electronic Signature created in such way shall be declared as invalid. In no case it is allowed to change the classification of the signature from QES to a “common” electronic signature in spite of meeting requirements that are required by the “common” electronic signature.

The signature shall be also declared as invalid in case the application is not able to interpret the whole used signature policy during the verification.

While verifying QES, the signature is not possible to be verified if the application is not able to display the signed data to a verifier (for example it cannot display “RTF” type of the document).

In the QES verification the signature of signature policies shall be valid to the time when the Qualified Electronic Signature of the document is verified.

4 Signature policies formats

Given rules of signature policies are mainly used for signatures of CMS type (in ASN.1) where the policy is coded in DER coding. DER coding is transformed into XER coding due to transparency and simple presentation of the policy in DER coding.

The NSA approves signature policies for QES (hereinafter referred to as “approved SPs”).

4.1 Transfer of ASN.1 signature policies into policies for signatures in XAdES ETSI TS 101 903 format

Policies being valid for CMS signatures can be equally valid for XML signatures according to XAdES ETSI TS 101 903 when the ASN.1 attributes are superseded by XML elements according to Table 19 from the document “Approved Qualified Electronic Signatures Formats” in the processing of DER policy.

If a specific policy is required for XML signatures according to XAdES ETSI TS 101 903, then the document with XML policy is processed binary and its hash is indicated in the signed list in the archival signature “ApprovedSignaturePolicies.p7m”

Table 1 Basic ASN.1 algorithms and attributes and their OIDs

	ASN.1 attribute or algorithm	OID
1.	id-contentType	1 2 840 113549 1 9 3
2.	id-messageDigest	1 2 840 113549 1 9 4
3.	id-signingTime	1 2 840 113549 1 9 5
4.	Id-aa-ets-otherSigCert	1 2 840 113549 1 9 16 2 19
5.	id-aa-signingCertificate	1 2 840 113549 1 9 16 2 12
6.	id-aa-ets-sigPolicyId	1 2 840 113549 1 9 16 2 15
7.	id-aa-signatureTimeStampToken	1 2 840 113549 1 9 16 2 14
8.	id-aa-ets-certificateRefs	1 2 840 113549 1 9 16 2 21
9.	id-aa-ets-revocationRefs	1 2 840 113549 1 9 16 2 22
10.	id-aa-ets-escTimeStamp	1 2 840 113549 1 9 16 2 25
11.	id-aa-ets-certCRLTimestam	1 2 840 113549 1 9 16 2 26
12.	id-aa-ets-certValues	1 2 840 113549 1 9 16 2 23
13.	id-aa-ets-revocationValues	1 2 840 113549 1 9 16 2 24
14.	id-aa-ets-archiveTimestamp	1 2 840 113549 1 9 16 2 27
15.	id-aa-ets-contentTimestamp	1 2 840 113549 1 9 16 2 20
16.	id-aa-ets-signerLocation	1 2 840 113549 1 9 16 2 17
17.	sha1	1 3 14 3 2 26
18.	ripemd160	1 3 36 3 2 1
19.	shalwithRSAEncryption	1 2 840 113549 1 1 5
20.	rsaSignatureWithripemd160	1 3 36 3 3 1 2
21.	rsaEncryption	1 2 840 113549 1 1 1

4.2 Textual description of the signature policy attributes minimally required

```

<SignaturePolicy>
  <signPolicyHashAlg>
    <algorithm>
      OID of the algorithm to compute the hash value from the signature policy fields
      signPolicyHashAlg and signPolicyInfo.
    </algorithm>
  </signPolicyHashAlg>
  <signPolicyInfo>
    <signPolicyIdentifier>
      OID of the signature policy.
    </signPolicyIdentifier>
    <dateOfIssue>
      The date of the policy issuance.
    </dateOfIssue>
    <policyIssuerName>
      <GeneralName>
        <directoryName>
          The name of the policy issuer.
        </directoryName>
      </GeneralName>
      <GeneralName>
        <uniformResourceIdentifier>
          Policy http address in DER coding.
        </uniformResourceIdentifier>
      </GeneralName>
    </policyIssuerName>
    <fieldOfApplication>
      Textual description of the policy type and purpose and according to what legal
      system it is applicable.
    </fieldOfApplication>
    <signatureValidationPolicy>
      <signingPeriod>
        <notBefore>
          The time since when is the policy applicable for signing.
        </notBefore>
        <notAfter>
          The time till when is the policy applicable for signing.
        </notAfter>
      </signingPeriod>
      <commonRules>
        <signerAndVerifierRules>
          <signerRules>
            Requirements for the signer.
            <externalSignedData>
              true   - external signature
              false  - internal signature
              - if the externalSignedData attribute is not present, then the
              policy is intended for both signature types
            </externalSignedData>
            <mandatedSignedAttr>
              A list of mandatory signed CMS attributes.
            </mandatedSignedAttr>
            <mandatedUnsignedAttr>
              A list of mandatory unsigned CMS attributes.
            </mandatedUnsignedAttr>
            <mandatedCertificateRef>

```

```

    <signerOnly/>
        A reference on a signer's certificate is inserted into signature
        attributes Id-aa-ets-otherSigCert, id-aa-signingCertificate or
        XML element SigningCertificate.
    </mandatedCertificateRef>
    <mandatedCertificateInfo>
        < fullPath/>
            Certificates of the whole path from the signer's certificate up
            to the trustworthy root certificate are inserted into the CMS
            signature field certificates in the block SignedData.
    </mandatedCertificateInfo>
</signerRules>
<verifierRules>
    <mandatedUnsignedAttr>
        A list of mandatory unsigned CMS attributes.
    </mandatedUnsignedAttr>
</verifierRules>
</signerAndVerifierRules>
<signingCertTrustCondition>
    <signerTrustTrees>
        <CertificateTrustPoint>
            Conditions for a set of trustworthy root certificates where the certification
            path, built from the signer's certificate or the certificate of a time stamp, shall
            terminate.
            <trustpoint>
                A set of trustworthy root certificates where the certification path, built
                from the signer's certificate or the certificate of a time stamp, shall
                terminate.
            </trustpoint>
            <acceptablePolicySet>
                <CertPolicyId>
                    A list of OID identifiers that shall be in every certificate of the
                    certification path from the value determined below in
                    requireExplicitPolicy. A control intersection is made from the union
                    of OIDs from the certificate extensions CertificatePolicies and
                    QcStatements.
                </CertPolicyId>
            </acceptablePolicySet>
            <policyConstraints>
                <requireExplicitPolicy>
                    It determines from what certification path level towards the signer's
                    certificate the checking of the explicit signature policy starts (for
                    example from acceptablePolicySet).
                </requireExplicitPolicy>
            </policyConstraints>
        </CertificateTrustPoint>
    </signerTrustTrees>
    <signerRevReq>
        <endCertRevReq>
            It contains a method of validity control of the signer's certificate or
            the certificate of a time stamp. For example by means of CRL, OCSP,
            ...
        </endCertRevReq>
    <caCerts>
        It contains a method of validity control of certification authorities'
        certificates in created path from the signer's certificate or the
        certificate of a time stamp. For example by means of CRL, OCSP, ...
    </caCerts>

```

```

    </signerRevReq>
  </signingCertTrustCondition>
  <timeStampTrustCondition>
    <cautionPeriod>
      The field is described in detail by the document “Certification Path Control”;
      the following section is just a partial summary of the mentioned document.
      Minimal period from the oldest valid time stamp of the signature during
      which a verifier shall wait in order to obtain mandatory data about validity of
      certificates in the signer’s certification path and in certification path of the
      oldest valid time stamp of the signature. While verifying signatures with
      qualified certificates issued according to Slovak legislation, it is necessary to
      wait for the first CRL only, after the oldest valid time stamp of the signature.
    </cautionPeriod>
  </timeStampTrustCondition>
  <algorithmConstraintSet>
    <signerAlgorithmConstraints>
      A set of algorithms and possibly a minimal size of their keys used for the
      creation and verification of signatures, certificates, time stamps...
    </signerAlgorithmConstraints>
  </algorithmConstraintSet>
</commonRules>
<commitmentRules>
  <CommitmentRule>
    <selCommitmentTypes>
      <CHOICE>
        <empty></empty>
      </CHOICE>
    </selCommitmentTypes>
  </CommitmentRule>
</commitmentRules>
</signatureValidationPolicy>
</signPolicyInfo>
<signPolicyHash>
  A control hash of the signature policy integrity computed from merged values of
  signPolicyHashAlg and signPolicyInfo.
</signPolicyHash>
</SignaturePolicy>

```

5 Specific signature policies

5.1 Signature policy for Qualified Electronic Signature with a time stamp, for textual documents in ASCII and UTF8 coding, for internal or external signature types

The signature policy can be used for internal as well for external types of signatures where in internal signatures it is unambiguous due to policy type that it deals with the signed textual document in UTF8 coding. In internal CMS signatures the textual document can begin with a MIME heading whose type and coding range, due to unambiguity in the QES creation and verification, is specified by the document “Qualified Electronic Signatures Formats”.

Annex A (informative) Bibliography

- [1] RFC 3280 X.509 PKI Certificate and Certificate Revocation List April 2002
[2] RFC 2560 X.509 PKI Online Certificate Status Protocol June 1999
[3] NSA Qualified Certificates Formats November 2005

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>

ETSI TS 102 176-1: "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms."

Electronic Signatures

<http://www.cen.eu/CENORM/BusinessDomains/businessdomains/iss/cwa/electronic+signatures.asp>

CWA 14890-1 Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

CWA 14890-2 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

CEN/TC+224- Standards under development

<http://www.cen.eu/CENORM/BusinessDomains/TechnicalCommitteesWorkshops/CENTechnicalCommittees/WP.asp?param=6205&title=CEN/TC%2B224>

prEN 14890-1 Application Interface for smart cards used as secure signature creation devices - Part 1: Basic services

prEN 14890-2 Application Interface for smart cards used as secure signature creation devices - Part 2: Additional services

Annex B History

Version	Date of issuing	Note	Editor
V 1.0	24 August 2005	First issuing	Ing. Peter Rybár, NSA RNDr. Július Šiška, PhD., KPMG
Version 1.1	6 November 2005	Unified format of the NSA documents	Ing. Peter Rybár, NSA