



NATIONAL SECURITY AUTHORITY

Version 1.0

Specifying the content and formal specifications of document formats for QES

24 July 2007

This English version of the Slovak document No. 3198/2007/IBEP-004 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

Department of Information Security and Electronic Signature

Budatínska č. 30, 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	Basic set of MIME types for documents being signed	7
	Table 1 Basic MIME types of documents for QES.....	7
	Table 2 Basic MIME types of document coding for QES	7
	Annex A (informative) Document type limitations for QES document visualization needs.....	8
	A.1 ASCII textual document in UTF-8.....	8
	A.2 RTF document.....	8
	A.3 PDF document.....	8
	A.4 HTML and XHTML document.....	8
	A.5 XML document.....	8
	A.6 TIF picture.....	8
	A.7 PNG picture.....	9
	A.8 Combination of document type.....	9
	Annex B (informative) Examples of documents in MIME coding	10
	B.1 An example of a textual document in UTF-8.....	10
	B.2 An example of PDF document	10
	B.3 An example of several documents in one multipart MIME coding	11
	Annex C (informative) Bibliography.....	13
	Annex D History.....	14

1 Introduction

During signing and verifying the Qualified Electronic Signature (hereinafter referred to as “QES”) [2, 4, 5, 9, 10, 12, 13, 19] it is also required, in addition to AdES signing and verifying itself [1, 6, 11, 14, 16, 21, 22], to ensure unambiguous visualization of signed documents.

2 Scope

The NSA issues the present standard in accordance with the Act on Electronic Signature, Article 10 paragraph 2 (j). The standard is issued for purposes of providing an unambiguous electronic document processing in QES signing and verification. The present document technically specifies properties of document basic set that are defined in Annex 3 of the NSA regulation No. 233/2007 Coll. on manner and procedure of electronic signature use in commercial and administrative communication. The present document defines a transport format for documents being signed which task is to ensure an unambiguous type identification of the document being signed for visualization needs.

3 References

References to documents defining used types and methods.

- [1] ETSI TS 101 733 Electronic Signature Formats (CAdES)
- [2] ETSI TR 102 272 ASN.1 format for signature policies
- [3] RFC 3280 X.509 PKI Certificate and Certificate Revocation List 4-2002
- [4] RFC 3739 Qualified Certificates Profile 3-2004
- [5] ETSI TS 101 862 Qualified Certificate Profile
- [6] RFC 3852 Cryptographic Message Syntax 7-2004
- [7] RFC 3161 Time-Stamp Protocol (TSP) 8-2001
- [8] RFC 2560 X.509 PKI Online Certificate Status Protocol 8-1999
- [9] NSA Qualified Electronic Signature Formats
- [10] Regulation of the NSA, No. 537/2002 Coll. on format and manner of QES creation
- [11] ETSI TS 102 280 X.509 V.3 Cert. Profile for Cert. Issued to Natural Persons
- [12] ETSI TR 102 437 Guidance on TS 101 456
- [13] ETSI TS 101 456 Policy Requirements for cert. authorities issuing qualified cert.
- [14] ETSI TS 102 042 Policy Requirements for cert. authorities issuing public key cert.
- [15] ETSI TS 102 231 Provision of harmonized Trust-service status information 3-2006
- [16] ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)
- [17] RFC 2560 X.509 PKI Online Certificate Status Protocol 6-1999
- [18] RFC 3548 The Base16, Base32, and Base64 Data Encodings 7-2003
- [19] Regulation of the NSA, No. 233/2007 Coll. on manner and procedure of electronic signature use in commercial and administrative communication
- [20] ISO/IEC 3166 Codes for the representation of countries
- [21] RFC 2822 Internet Message Format 4-2001
- [22] RFC 2046 MIME Part Two-Media Types 11-1996
- [23] RFC 3629 UTF-8, a transformation format of ISO 10646 11-2003

4 Abbreviations

AdES	Advanced Electronic Signature
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
CRLF	the carriage return (CR) character (ASCII value 13) followed immediately by the line feed (LF) character (ASCII value 10)
DER	Distinguished Encoding Rules (for ASN.1)
ESS	Enhanced Security Services (enhances CMS)
HTML	Hypertext Markup Language
HTTP	Hyper Text Transfer Protocol
ISO	International Organization for Standardization
MIME	Multipurpose Internet Mail Extensions
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKIX	internet X.509 Public Key Infrastructure
QC	Qualified Certificate
SHA-1	Secure Hash Algorithm 1
TSA	Time-Stamping Authorities
TSP	Time Stamp Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF-8	Transformation format of ISO 10646
XAdES	XML Advanced Electronic Signature
XHTML	Extensible Hypertext Markup Language
XML	eXtensible Markup Language
QES	Qualified Electronic Signature

5 Basic set of MIME types for documents being signed

Documents being signed by QES [9] shall be stored in a format that enables unambiguous document type identification for a visualized component of the application for QES. To ensure this basic QES property, there was selected a coding of documents being signed into MIME [21] with the exact restricted minimal set of MIME types [22] and codings [18] that shall be recognized and processed by applications for QES. Thus, it will ensure an unambiguous identification of document types and interoperability between individual applications as they will be able to identify if they can visualize the given document type unambiguously and hence to verify created QES.

In internal CADES [1] (Enveloping Signature in XAdES [16]) signature, the MIME textual file containing electronic document (s) with registered MIME types is signed directly. In external CADES [1] (Detached Signature in XAdES [16]) signature, the external MIME textual file that has “EML” extension and contains electronic document (s) with registered MIME types is signed.

Table 1 Basic MIME types of documents for QES

	Registered MIME Content-Type	Short description
1.	message/rfc822	General marking of MIME message envelope containing MIME types as specified below.
2.	multipart/mixed; boundary=”a divider –of documents”	Defines a sequence of signed documents which MIME codings are divided by a divider given in <i>boundary</i> attribute.
3.	text/plain; charset=UTF-8	ASCII textual document in UTF-8 coding.
4.	text/rtf	Microsoft/Apple Rich Text Format (RTF)
5.	application/pdf	Adobe Portable Document Format (PDF)
6.	text/html; charset=UTF-8	HTML format
7.	text/xml; charset=UTF-8	XML format
8.	application/xhtml+xml; charset=UTF-8	XHTML format
9.	image/tiff	Tag Image File Format
10.	image/png	Portable Network Graphics format

Table 2 Basic MIME types of document coding for QES

	MIME Content-Transfer-Encoding	Short description
1.	8bit	Coding of a character up to 8 bits.
2.	base64	Coding of a document by means of Base64.

Annex A (informative) Document type limitations for QES document visualization needs

A.1 ASCII textual document in UTF-8

According to the present document the Content-Transfer-Encoding 8bit coding of a textual document in UTF-8 requires a limited line length on recommended 76 characters in MIME. According to [21] each line of characters MUST be no more than 998 characters, and SHOULD be no more than 78 characters, excluding the CRLF.

The Content-Transfer-Encoding base64 coding of a textual document in UTF-8 does not require any restrictions on the line length in the number of characters.

A.2 RTF document

A document in RTF shall contain only static objects and all necessary document components shall be directly in RTF document, i.e. it shall not contain references on external resources that might change visualization. RTF shall not contain other document types than defined in [19] and pictures which visualization is not unambiguous, i.e. animations and pictures with used lossy (irreversible) compression.

A.3 PDF document

A document in PDF shall contain only static objects and all necessary document components shall be directly in PDF document, i.e. it shall not contain references on external resources that might change visualization. PDF shall not contain other document types than defined in [19] and pictures which visualization is not unambiguous, i.e. animations and pictures with used lossy (irreversible) compression.

A.4 HTML and XHTML document

A document in HTML and XHTML shall contain only static objects and all necessary document components shall be directly in HTML and XHTML document, i.e. it shall not contain references on external resources that might change visualization. HTML and XHTML shall not contain other document types than defined in [19] and pictures which visualization is not unambiguous, i.e. animations and pictures with used lossy (irreversible) compression.

A.5 XML document

A document in XML shall contain only static objects and all necessary document components shall be directly in XML document, i.e. it shall not contain references on external resources that might change visualization. XML shall not contain other document types than defined in [19] and pictures which visualization is not unambiguous, i.e. animations and pictures with used lossy (irreversible) compression.

A.6 TIFF picture

TIFF picture shall contain only static representation and shall not contain references on external resources that might change visualization. TIFF picture shall not contain pictures which

visualization is not unambiguous, i.e. animations and pictures with used lossy (irreversible) compression.

A.7 PNG picture

PNG picture shall contain only static representation and shall not contain references on external resources that might change visualization. PNG picture shall not contain pictures which visualization is not unambiguous, i.e. animations and pictures with used lossy (irreversible) compression.

A.8 Combinations of document types

If an electronic document being signed contains a sequence of documents or encapsulated documents, then types of such documents shall be only of the type defined in [19].

B.3 An example of several documents in one multipart MIME coding

```

Content-Type: multipart/mixed; boundary="-----_NextPart_000_"

This is a multi-part message in MIME format.

-----_NextPart_000_
Content-type: text/plain; charset=UTF-8
Content-Transfer-Encoding: 8bit

Dear Colleagues,

Thank you for putting the details of the possible security attack into
CIRCA.

Best regards,
Peter

-----_NextPart_000_
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: base64

77u/DQoyMTM0MjUxL7FocSNxL7FocWlxI3FocW+xaHEvsW+xaHEjcw+xaUNCg0KxL7FocSNxL7F
ocSNDQogxL7FocSNxaHEvsSNDQoNCmEgdGFrIGRhbGVqDQo=

-----_NextPart_000_
Content-Type: text/rtf
Content-Transfer-Encoding: base64

e1xydGYxXGFuc2lcYW5zaWNwZzEyNTBcZGVmZjBcZGVmbGFuZzEwNTF7XGZvbnR0Ymx7XGYwXGZz
d2lzc1xmY2hhcnNldDIzOHtcKlxmbmFtZSBBcm1hbDdt9QXJpYWwgQ0U7fXtczjFczm5pbFxmY2hh
cnNldDAgO3l9DQp7XCpcZ2VuZXJhdG9yIE1zZnRlZG10IDUuNDEuMTUuMTUwNzt9XHZpZXdraW5k
NFx1YzFccGFyZFxmfXmczIwXCdjOGlzdG8gdGVzdCBcJ2U4byBcJzlhXCdlOGlqIFwnOWRhIFwn
YmVcJ2ZhXCdlOGEgXCc5ZVwnZWRCJzllbGlzJ2U4a3UgbVwnZTRzYSBuXCdmYVwnOWQgYSBtXCdm
ZGxkJ2U4aVwnZThrYSBrXCdmNFwnZjIyIGxGxbmcxMDMzXGYxXHBhcg0KfQ0KAA==

-----_NextPart_000_
Content-Type: application/pdf
Content-Transfer-Encoding: base64

JVBERi0xLjQKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0ZURlY29k
ZT4+CnN0cmVhbQp4nIVSPU8DMQwVLZRyoEJL+doyJsOFON9ekRASG9Vt1KmITkVq+f8STu+uOemQ
NDg4IDAwMDAwIG4gCjAwMDAwMTMzMDCgMDAwMDAgbiAKdHJhaWxlco8PCAvU2l6ZSAxNiAvUm9v
dCAxIDAgUiAvSW5mbyAyIDAgUgovSUQgWzwlQzIyNUi0RkIxQzU2RTVFMEUxOTAYQzgyNTdDOUI4
Nj48NUMyMjVCNEZCMUM1NkU1RTBFMTkwMkM4MjU3QzlcODY+XQo+PgpdGFydhhyZWYKMTQ5MjIK
JSVFT0YK

-----_NextPart_000_
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: base64

77u/PgH0bWw+DQoNCjxoZWfKpg0KPHRpdGx1PlRoZSB0aXRzZSBpcyBub3QgZGlzcGxheWVvPC90
aXRzZT4NCjwvaGVhZD4NCg0KPGJvZHK+DQo8cD5UaGlzIHRleHQgaXMgZGlzcGxheWVvPC9wPg0K
PC9ib2R5Pg0KDQo8L2h0bWw+DQo=

-----_NextPart_000_
Content-type: text/xml; charset=UTF-8
Content-Transfer-Encoding: base64

77u/PD94bWwgdmVyc2lvbj3igJwxLjhigJ0gZW5jb2Rpbmc94oCcVVRGLTjigJ0/Pg0KPCFET0NU
WVBFIHJlcXVlc3QgUFVCTE1DID4NCjxkb2M+DQo8cG9zdG9vZGU+MjEzNDI1K8S+xaHEjcs+xaHF
pcSNxaHFvsWhxL7FvsWhxI3FvsWlPC9wb3N0Y29kZT4NCg0KPHBvc3RuYW11PpsS+xaHEjcs+xaHE

```


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>

Annex D History

Version	Date of issuing	Note	Editor
Version 1.0 Č.: 3198/2007/IBEP-013	24 July 2007	First edition	Ing. Peter Rybár, NSA