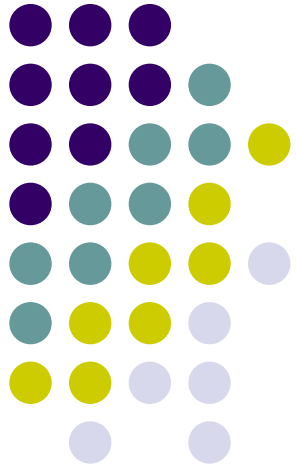
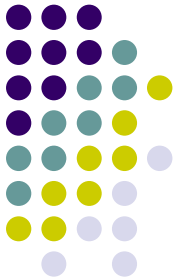
ASN.1:
Cryptographic files
CMS + S/MIME

Zdeněk Říha



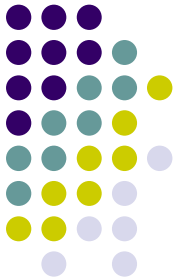
ASN.1 – PKCS#7 / CMS



```
ContentInfo ::= SEQUENCE {
  contentType ContentType,
  content [0] EXPLICIT ANY DEFINED BY contentType }

ContentType ::= OBJECT IDENTIFIER

SignedData ::= SEQUENCE {
  version CMSVersion,
  digestAlgorithms DigestAlgorithmIdentifiers,
  encapContentInfo EncapsulatedContentInfo,
  certificates [0] IMPLICIT CertificateSet OPTIONAL,
  crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
  signerInfos SignerInfos }

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

EncapsulatedContentInfo ::= SEQUENCE {
  eContentType ContentType,
  eContent [0] EXPLICIT OCTET STRING OPTIONAL }

SignerInfos ::= SET OF SignerInfo
```

Source:
RFC 5652

ASN.1 - PKCS#7 / CMS

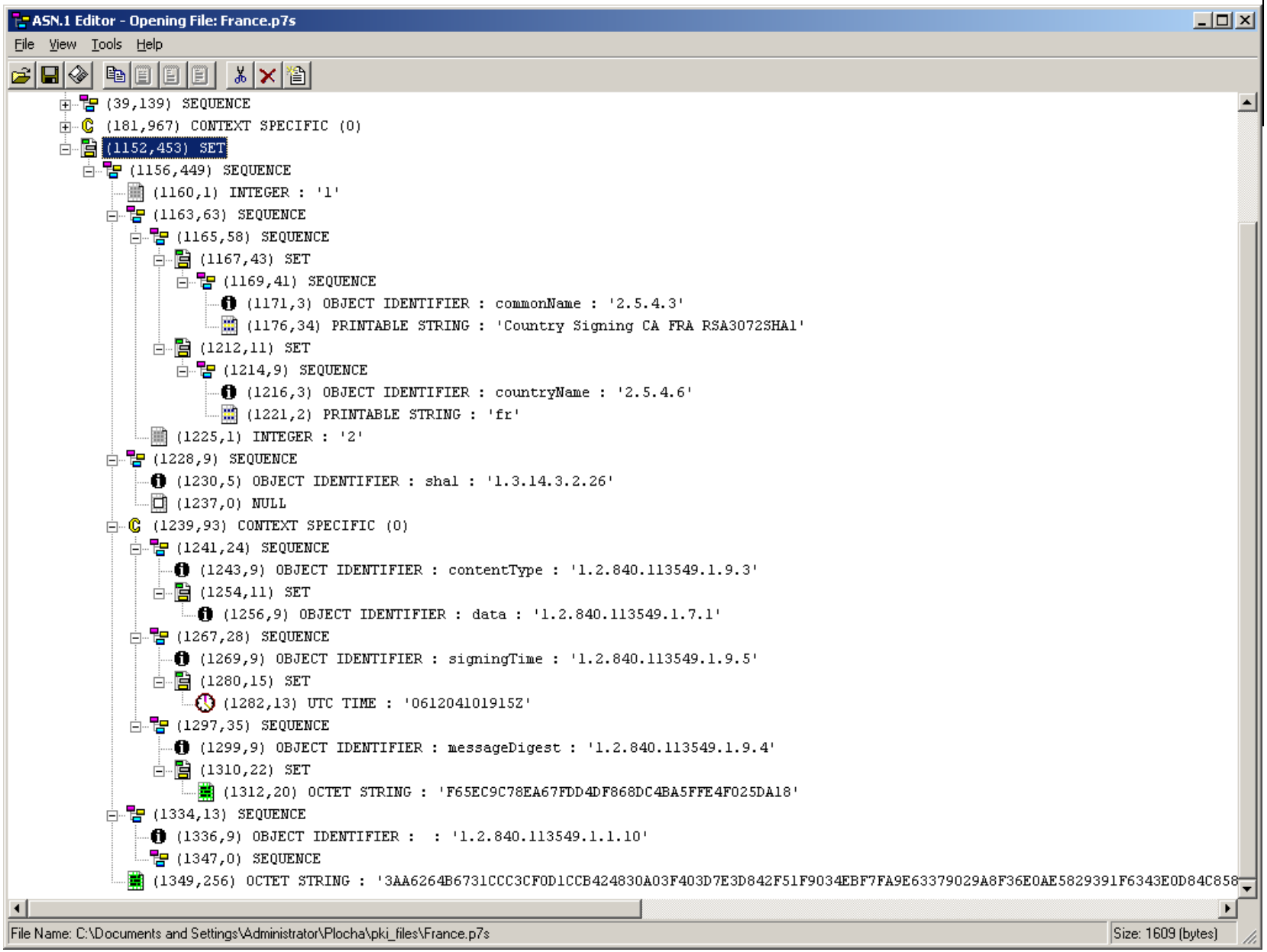


```
SignerInfo ::= SEQUENCE {
  version CMSVersion,
  sid SignerIdentifier,
  digestAlgorithm DigestAlgorithmIdentifier,
  signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
  signatureAlgorithm SignatureAlgorithmIdentifier,
  signature SignatureValue,
  unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL }

SignerIdentifier ::= CHOICE {
  issuerAndSerialNumber IssuerAndSerialNumber,
  subjectKeyIdentifier [0] SubjectKeyIdentifier }

SignedAttributes ::= SET SIZE (1..MAX) OF Attribute

UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute

Attribute ::= SEQUENCE {
  attrType OBJECT IDENTIFIER,
  attrValues SET OF AttributeValue }

AttributeValue ::= ANY

SignatureValue ::= OCTET STRING
```

Source:
RFC 5652

PKCS#7 Sample

France.p7s

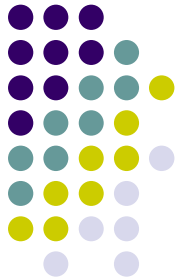


ASN.1 – PKCS#8

```
-- Private-key information syntax

 PrivateKeyInfo ::= SEQUENCE {
   version Version,
   privateKeyAlgorithm AlgorithmIdentifier,
   privateKey PrivateKey,
   attributes [0] Attributes OPTIONAL }

 Version ::= INTEGER {v1(0)} (v1,...)

 PrivateKey ::= OCTET STRING

 Attributes ::= SET OF Attribute

-- Encrypted private-key information syntax

 EncryptedPrivateKeyInfo ::= SEQUENCE {
     encryptionAlgorithm AlgorithmIdentifier,
     encryptedData EncryptedData
 }

 EncryptedData ::= OCTET STRING
```

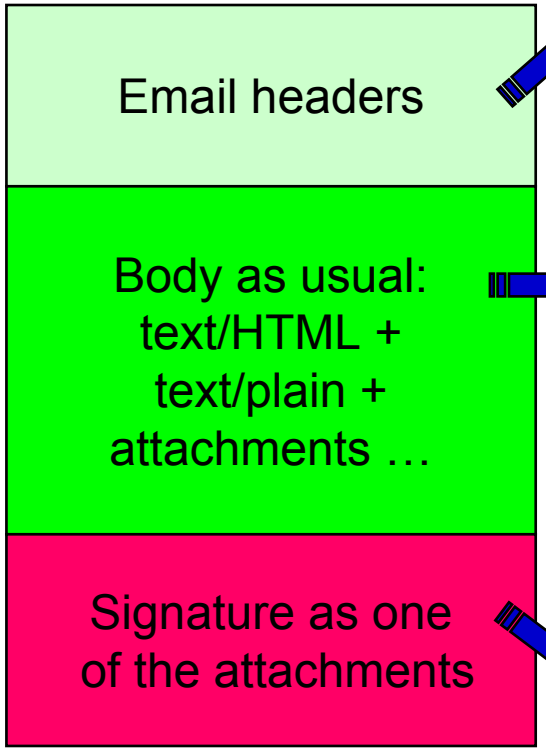
Source:
PKCS#8

S/MIME



- Secure email
  - Digitally signed and/or encrypted
  - Allows hierarchical signatures/encryptions
  - Combines MIME (structure of email) and CMS/PKCS#7 (for data protection)
  - For digital signatures 2 possible ways to code the signature
    - Normal email + signature (detached) as “attachment”
      - Transparent signature
      - Email readable also in email clients not supporting S/MIME
    - Everything in a single CMS/PKCS#7
      - Opaque signatures
      - Email not readable in email clients not supporting S/MIME

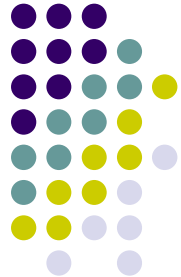
S/MIME: Transparent signature




```
From: "Zdenek Riha" <zriha@fi.muni.cz>
To: <zriha@math.muni.cz>
Subject: Test
Date: Mon, 1 Dec 2008 11:06:03 +0100
MIME-Version: 1.0
Message-ID: <000801c9539c$6dfc61b0$3b30fb93@zriha>
Content-Type: multipart/signed;
        protocol="application/x-pkcs7-signature";
        micalg=SHA1;
        boundary="----=_NextPart_000_0000_01C953A4.CC8CA0C0"
X-Mailer: Microsoft Office Outlook 11


This is a multi-part message in MIME format.

------=_NextPart_000_0000_01C953A4.CC8CA0C0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_001_0001_01C953A4.CC8CA0C0"


------=_NextPart_001_0001_01C953A4.CC8CA0C0
Content-Type: text/plain;
        charset="us-ascii"
Content-Transfer-Encoding: 7bit

Test message


------=_NextPart_000_0000_01C953A4.CC8CA0C0
Content-Type: application/x-pkcs7-signature;
        name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="smime.p7s"

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIFojCCA1cw
ggHAAgEBMA0GCSqGSIb3DQEBBAUAMHUxCzAJBgNVBAYTAkNaMQ8wDQYDVQQIEwZNb3JhdmExDTAL
BgNVBAcTBEJybm8xDjAMBgNVBAoTBUxhYmFrMRAwDgYDVQQDEwdUZXN0IENBMSQwIgYJKoZIhvcN
AQkBFhVpbmZvQGxhYmFrLmZpLm11bmkuY3owHhcNMDgxMjAxMTAwMjMwWhcNMDkxMjAxMTAwMjMw
WjBzMQswCQYDVQQGEwJDWjEPMA0GA1UECBMGTW9yYXZhMQ0wCwYDVQQHEwRCcm5vMQ4wDAYDVQQK
EwVMYWJhazETMBEGA1UEAxMKW1JJSEEgdGVzdDEfMB0GCSqGSIb3DQEJARYQenJpaGFAZmkubXVu
aS5jejCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyYiN1pcjU5wWAlGNjjIJhWyqvsNPXpEG
```

test_smime_transparent.eml

S/MIME: Transparent signature

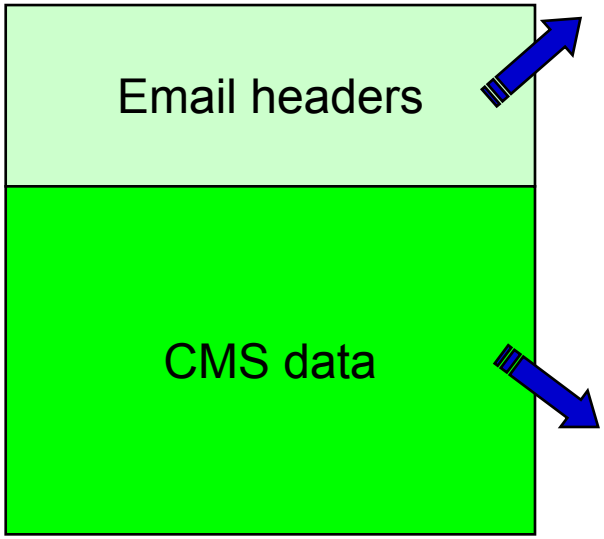


```
Content-Type: multipart/signed;
   protocol="application/pkcs7-signature";
   micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

Base64 encoded
DER encoded
CMS SignedData

Source:
RFC 5751

S/MIME: Opaque signature

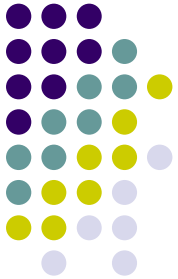



```
From: "Zdenek Riha" <zriha@fi.muni.cz>
To: <zriha@math.muni.cz>
Subject: Test
Date: Mon, 1 Dec 2008 11:09:04 +0100
Message-ID: <002301c9539c$d6efc090$3b30fb93@zriha>
MIME-Version: 1.0
Content-Type: application/x-pkcs7-mime;
        smime-type=signed-data;
        name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
        filename="smime.p7m"
```

```
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAaCAJIAEggePQ29u
dGVudC1UeXB1OiBtdWx0aXBhcnQvYWx0ZXJuYXRpdmU7DQoJYm91bmRhcnk9Ii0tLS09X051eHRQ
YXJ0XzAwMF8wMDFGXzAxQzk1M0E1LjM4OTc3OEQwIg0KDQpUaGlzIGlzIGEgbXVsdGktcGFydCBt
ZXNzYWdlIGluIE1JTUUgZm9ybWF0Lg0KDQotLS0tLS09X051eHRQYXJ0XzAwMF8wMDFGXzAxQzk1
M0E1LjM4OTc3OEQwDQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47DQoJY2hhcnNldD0idXMtYXNj
aWkiDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRlc3RvdmFjaSB6cHJhdmEN
Cg0KDQotLS0tLS09X051eHRQYXJ0XzAwMF8wMDFGXzAxQzk1M0E1LjM4OTc3OEQwDQpDb250ZW50
LVR5cGU6IHRleHQvaHRtbDsNCgljaGFyc2V0PSJ1cy1hc2NpaSINCkNvbnRlbnQtVHJhbnNmZXIt
RW5jb2Rpbmc6IHF1b3RlZC1wcmludGFibGUNCg0KPGh0bWwgeG1sbnM6dj0iZCJ1cm46c2NoZW1h
cy1taWNyb3NvZnQtY29tOnZtbCIgPQ0KeG1sbnM6bz0iZCJ1cm46c2NoZW1hcy1taWNyb3NvZnQt
Y29tOm9mZmljZTpvZmZpY2UiID0NCnhtbG5zOnc9M0QidXJuOnNjaGVtYXMtbWljcm9zb2Z0LWNv
bTpvZmZpY2U6d29yZCIgPQ0KeG1sbnM9M0QiaHR0cDovL3d3dy53My5vcmcvVFIvUkVDLWh0bWw0
MCI+DQoNCjxoZWFkPg0KPE1FVEEgSFRUUC1FUVVJVj0zRCJDb250ZW50LVR5cGUiIENPT1RFT1Q9
M0QidGV4dC9odG1sOyA9DQpjaGFyc2V0PTNEdXMtYXNjaWkiPg0KPG1ldGEgbmFtZT0zREdlbmVy
YXRvciBjb250ZW50PTNEIk1pY3Jvc29mdCBXb3JkIDExICAhaWx0ZXJlZCBtZWRpdW0pIj4NCjxz
dHlsZT4NCjwhLS0NCiAvKiBEZWZpbml0aW9ucyAqLw0KIHAuTXNvTm9ybWFsLCBsaS5N
c290b3JtYWwsIGRpdi5Nc290b3JtYWwNCgl7bWFyZ2luOjBjbTsNCgltYXJnaW4tYm90dG9tOi4w
MDAxcHQ7DQoJZm9udC1zaXplOjEyLjBwdDsNCglmb250LWZhbWlseToiVGltZXMgTmV3IFJvbWFu
```

test_smime_opaque.eml

S/MIME: Opaque signature

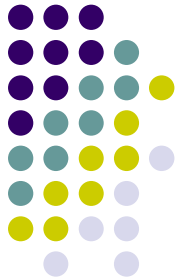


```
Content-Type: application/pkcs7-mime; smime-type=signed-data;
     name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7
77n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHUujhJhjH
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh
6YT64V0GhIGfHfQbnj75
```

Base64 encoded
DER encoded
CMS SignedData (includes data AND signature)

Source:
RFC 5751

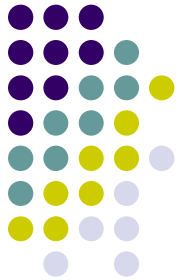
ETSI recommendation



Entry name of the signature suite	1 years	3 years	6 years	10 years
sha1-with-rsa	1 024	unknown	not recommended	
sha256-with-rsa	1 024	1 536	2 048	2 048
RSASSA-PSS with mgf1SHA-1Identifier	1 024	1 536	2 048	2 048
RSASSA-PSS with mgf1SHA-224Identifier	1 024	1 536	2 048	2 048
RSASSA-PSS with mgf1SHA-256Identifier	1 024	1 536	2 048	2 048
sha1-with-dsa	1 024	unknown	not recommended	
sha1-with-ecdsa	163	unknown	not recommended	
sha224-with-ecdsa	224	224	224	224
sha256-with-ecdsa	256	256	256	256

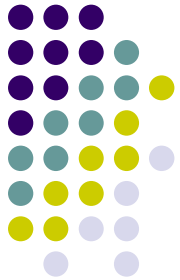
- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended signature schemes
- Starting date: 2006

Česká republika & EU & ETSI



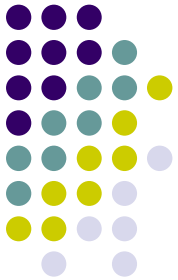
- EU
  - SMĚRNICE 1999/93/EC EVROPSKÉHO PARLAMENTU A RADY ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
- ČR
  - Zákon č. 227/2000 Sb. o elektronickém podpisu
  - Několikrát novelizován
  - Podzákonné předpisy
    - Nařízení vlády č. 495/2004 Sb, kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů
    - Vyhláška č. 496/2004 Sb. k elektronickým podatelnám
    - Vyhláška č. 378/2006 Sb., o postupech kvalifikovaných poskytovatelů certifikačních služeb

Česká republika & EU & ETSI



- Vyhláška č. 378/2006 Sb.
  - „používá důvěryhodné systémy a postupy, které splňují požadavky standardu pro tyto systémy, který je uveden v bodu 1 přílohy č. 1 této vyhlášky“
  - 1. CWA 14167-1 – Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements.
    - „Security requirements for TWSs also include a minimum set of requirements to be fulfilled by the signature algorithms and their parameters allowed for use by CSPs. These requirements are provided in [ALGO].“
    - [ALGO] ETSI SR 002 176 - Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures.

Stanovisko MV ČR

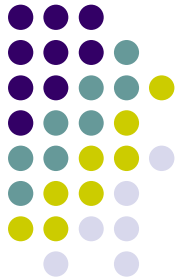


- „V návaznosti na směrnici ES č. 1999/93/EC o zásadách Společenství pro elektronické podpisy a v ní obsažený princip vzájemného uznávání kvalifikovaných certifikátů vydaných v kterémkoliv členském státu EU je nezbytné vycházet z dokumentu ALGO paper, který stanoví, že od 1. 1. 2010 je algoritmus SHA-1 „unusable“ a je tedy nezbytné ukončit jeho používání pro oblast elektronického podpisu a zahájit přechod na bezpečnější algoritmy třídy SHA-2. Česká republika patří k těm členským státům, ve kterých je tento přechod rozložen do delšího časového období. Je však nezbytné jej realizovat, a tak zachovat důvěru uživatelů v bezpečnost elektronického podpisu.“

  - poskytovatelé certifikačních služeb přestanou vydávat kvalifikované certifikáty s algoritmem SHA-1 nejpozději do 31. 12. 2009,
  - poskytovatelé certifikačních služeb zahájí vydávání kvalifikovaných certifikátů s hashovací funkcí třídy SHA-2 nejpozději 1. 1. 2010 (mohou tak však učinit kdykoliv dříve); tato změna se samozřejmě týká i vydávání kořenových certifikátů, kterými poskytovatel certifikačních služeb označuje jím vydané certifikáty,
  - aplikace, ve kterých je elektronický podpis používán, musí podporovat nejpozději od 1. 1. 2010 všechny algoritmy třídy SHA-2,
  - podpora algoritmu SHA-1 musí být v aplikacích zachována minimálně do 31.12.2010

Zdroj: MV ČR

Dohoda českých akreditovaných CA



- „Kvalifikované certifikáty s hashovací funkcí třídy SHA-2, které začnou vydávat nejpozději od 1. ledna 2010, budou všichni tři poskytovatelé přednostně nabízet s hashovací funkcí SHA-256 v kombinaci s algoritmem RSA s délkou klíče 2048 bitů. Poskytovatel certifikačních služeb může na základě vlastního rozhodnutí a základě požadavků svých zákazníků vydávat kvalifikované certifikáty i s některou z dalších funkcí z rodiny SHA-2, tj. SHA-224, SHA-384 nebo SHA-512.“

  - Ministerstvo vnitra nemá námitek proti této dohodě. Tvůrce aplikací pracujících se zaručeným elektronickým podpisem založeném na kvalifikovaném certifikátu je však nutné upozornit, že je nezbytné vytvořit prostředí pro akceptování všech čtyř hashovacích funkcí rodiny SHA-2, a to i s ohledem na akceptaci kvalifikovaných certifikátů vydaných v jiných členských státech EU

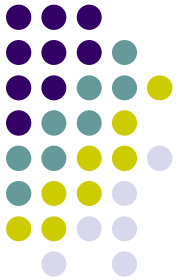
Zdroj: MV ČR

Akreditované CA

- První certifikační autorita, a. s.
- Česká pošta, s. p.,
- eIdentity a. s.,

Zdroj: MV ČR

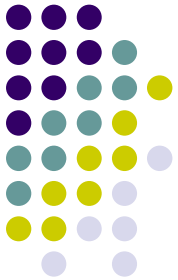
Poslední změny zákona



- „Za elektronický podpis splňující požadavky odstavce 1 se považuje rovněž zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném poskytovatelem certifikačních služeb usazeném v některém z členských států Evropské unie, byl-li kvalifikovaný certifikát vydán v rámci služby vedené v seznamu důvěryhodných certifikačních služeb, jako služba, pro jejíž poskytování je poskytovatel certifikačních služeb akreditován, nebo jako služba, nad jejímž poskytováním je vykonáván dohled.“

Zdroj:
§ 11 zákona 227/2000 Sb.

Jak na to v praxi



- Každá země EU vydává seznam důvěryhodných certifikačních služeb
  - TSL: Trusted Services List
- Ne každá země však takový seznam digitálně podepisuje …
- Seznam je k dispozici mimo jiné na http://tsl.gov.cz/
  - Řada odkazů na lidsky čitelné a strojově zpracovatelně (XML) TSL seznamy zemí EU

Seznam TSL

Seznam TSL

Seznam TSL členských států EU byl načten z internetové adresy **https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml** 20.09.2010 v 08.16 (CET). Jedná se o čas serveru, na kterém je provozována tato aplikace. Čas serveru je synchronizován s NTP serverem time.ufe.cz (stratum 1). Příští aktualizace seznamu proběhne 20.09.2010 v 09.16 (CET)

Seznam TSL

Stát	URL strojově zpracovatelného TSL	URL lidsky čitelného TSL
Belgie (BE)	http://tsl.belgium.be/tsl-be.xml Podpis TSL je platný, není však možné ověřit podpisový certifikát. Jeho obsah má jen informační hodnotu, nelze na něj spoléhat.	http://tsl.belgium.be/tsl-be.pdf
Bulharsko (BG)	Není k dispozici	http://www.crc.bg/section.php?lang=en&id=31
Česká republika (CZ)	http://tsl.gov.cz/publ/TSL_CZ.xtsl	http://tsl.gov.cz/publ/TSL_CZ.pdf
Dánsko (DK)	http://www.itst.dk/digitale-losninger/digital-signatur/in... TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://www.itst.dk/digitale-losninger/digital-signatur/in...
Estonsko (EE)	http://sr.riik.ee/tsl/estonian-tsl.xml TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://sr.riik.ee/tsl/estonian-tsl.pdf
Finsko (FI)	http://www.ficora.fi/attachments/suomiry/5m5T1qldW/truste... Formát XML souboru není dle specifikace XML.	http://www.ficora.fi/attachments/suomiry/5m5SI2GEj/truste...
Francie (FR)	http://references.modernisation.gouv.fr/sites/default/fil... TSL není elektronicky podepsaný, jeho obsah má proto jen informační hodnotu, nelze na něj spoléhat.	http://references.modernisation.gouv.fr/sites/default/fil...

Služba MV ČR: CertIQ

- Určí, zda certifikát byl vydán jako kvalifikovaný v nějaké zemi EU

Certifikát

Soubor: cert10569926.cer
Vystaveno pro: SERIALNUMBER=ICA - 10134279, EMAILADDRESS=tupa.irena@tiscali.cz, OU=PORTALZP-ZZ, O=MUD. Irena Tupá, L="Žatec, Javorová 2692, 43801", CN=MUD. Irena Tupá, C=CZ
Sériové číslo certifikátu: 10569926
Vystavitel: OU=I.CA - Accredited Provider of Certification Services,O=První certifikační autorita\, a.s.,CN=I.CA - Qualified Certification Authority\, 09/2009,C=CZ
Platnost od: 20.09.2010 10:37 CEST
Platnost do: 20.09.2011 10:37 CEST

Výsledek ověření, zda se jedná o kvalifikovaný certifikát*

* kvalifikovaný certifikát ve smyslu směrnice Evropského parlamentu a Rady 1999/93/ES o zásadách Společenství pro elektronické podpisy, resp. zákona č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů

Na základě informací dostupných v TSL zveřejněných členskými státy lze tento certifikát považovat za kvalifikovaný.

Porovnání proběhlo oproti TSL dostupným 20.09.2010 v 21.17 (CET). Jedná se o čas serveru, na kterém je provozována tato aplikace. Čas serveru je synchronizován s NTP serverem time.ufe.cz (stratum 1).

Tato aplikace ověřuje pouze, zda je certifikát kvalifikovaný, neověřuje však jeho platnost.

Služby, kterým odpovídá zadaný certifikát

	Stát	Vydavatel
1.	CZ	Ministerstvo vnitra České republiky