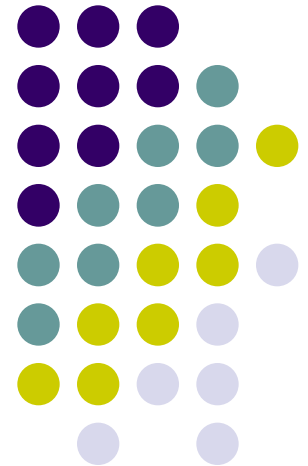
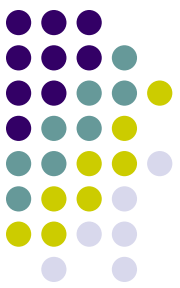


ASN.1:

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
```



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
```

PKCS#7 Sample

France.p7s



ASN.1 Editor - Opening File: France.p7s

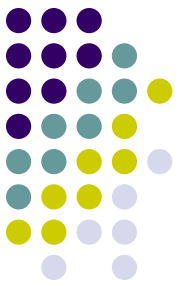
File View Tools Help

(39,139) SEQUENCE

- (181,967) CONTEXT SPECIFIC (0)
 - (1152,453) SET
 - (1156,449) SEQUENCE
 - (1160,1) INTEGER : '1'
 - (1163,63) SEQUENCE
 - (1165,58) SEQUENCE
 - (1167,43) SET
 - (1169,41) SEQUENCE
 - (1171,3) OBJECT IDENTIFIER : commonName : '2.5.4.3'
 - (1176,34) PRINTABLE STRING : 'Country Signing CA FRA RSA3072SHA1'
 - (1212,11) SET
 - (1214,9) SEQUENCE
 - (1216,3) OBJECT IDENTIFIER : countryName : '2.5.4.6'
 - (1221,2) PRINTABLE STRING : 'fr'
 - (1225,1) INTEGER : '2'
 - (1228,9) SEQUENCE
 - (1230,5) OBJECT IDENTIFIER : sha1 : '1.3.14.3.2.26'
 - (1237,0) NULL
 - (1239,93) CONTEXT SPECIFIC (0)
 - (1241,24) SEQUENCE
 - (1243,9) OBJECT IDENTIFIER : contentType : '1.2.840.113549.1.9.3'
 - (1254,11) SET
 - (1256,9) OBJECT IDENTIFIER : data : '1.2.840.113549.1.7.1'
 - (1267,28) SEQUENCE
 - (1269,9) OBJECT IDENTIFIER : signingTime : '1.2.840.113549.1.9.5'
 - (1280,15) SET
 - (1282,13) UTC TIME : '061204101915Z'
 - (1297,35) SEQUENCE
 - (1299,9) OBJECT IDENTIFIER : messageDigest : '1.2.840.113549.1.9.4'
 - (1310,22) SET
 - (1312,20) OCTET STRING : 'F65EC9C78EA67FDD4DF868DC4BA5FFE4F025DA18'
 - (1334,13) SEQUENCE
 - (1336,9) OBJECT IDENTIFIER : : '1.2.840.113549.1.1.10'
 - (1347,0) SEQUENCE
 - (1349,256) OCTET STRING : '3AA6264B6731CCC3CFOD1CCB424830A03F403D7E3D842F51F9034EBF7FA9E63379029A8F36E0AE5829391F6343E0D84C858'

File Name: C:\Documents and Settings\Administrator\Plocha\pki_files\France.p7s

Size: 1609 (bytes)



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
```

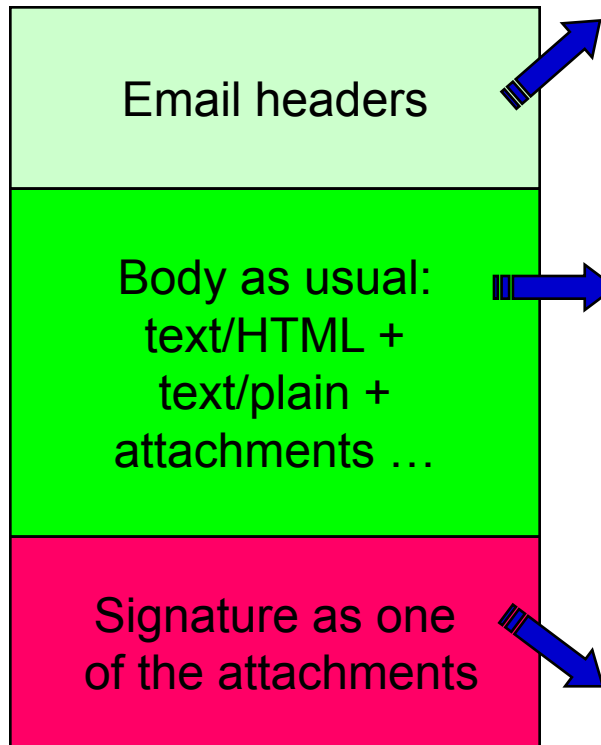
S/MIME



- 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"
```

```
MIAGCSqGSIB3DQEHAQCAMIACAQExCzAJBgUrDgMCGGUAMIAGCSqGSIB3DQEHAQAQAAoIIFojCCAlcw
ggHAAgEBMA0GCSqGSIB3DQEBBAAMHUXCzAJBgNVBAYTAkNaMQ8wDQYDQQIEwZNB3JhdmdExDTAL
BgNVBACtBEJybm8xDjAMBGNVBAoTBUXhYmFrMRAwDgYDQQEwdUZXRND0IENBMSQwIgwYJKoZIhvcN
AQkBFhUppm2uQGxhYmFrLmZpLm11bmkuY3owHhcNMDgxMjAxMTAwMjMwMjMwMjMwMjMwMjMwMjMw
WjBzMQswCQYDQQQEGwJdWJEPMA0GA1UECBGTW9yYXZzMmQ0wCwYDQQHEwRCcm5uMQ4wDAYDQQK
EwVMYyWJhazETMBEGA1UEAxMKW1JJSEEGdGUzdDEFMBA0GCSqGSIB3DQEJARYQenJpaGFAZmkubXUu
aS5jejCBnzANBghkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAyYiN1pcju5wWA1GNjjIjHMyqvsNPXpEG
```

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
```

```
ghyHhHUujhJhjH77n8HHGTrFvbnj756tbB9HG4UQpfyF467GhIGFHFYT6  
4UQpfyF467GhIGFHFYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrFvbnj  
n8HHGTrFvhJhjH776tbB9HG4UQbnj7567GhIGFHFYT6ghyHhHUujpfyF4  
7GhIGFHFYT64UQbnj756
```

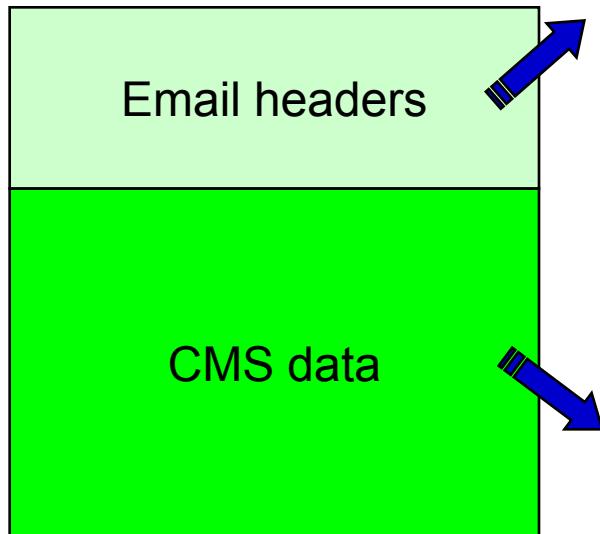
Base64 encoded
DER encoded
CMS SignedData

```
--boundary42--
```

Source:
RFC 5751

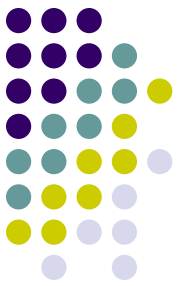


S/MIME: Opaque signature



```
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
dGVudC1UeXB10iBtdWx0aXBhcnQvYVwx0ZXJuYXRpdmU7DQoJYm91bmRhcnc9Ii0tLS09X051eHRQ
YXJ0XzAwMF8wMDFGxzAxQzk1M0E1LjM40Tc30EQwIgd0KQpUaGlzIGl2IGEGbXUzdGktcGFydCBt
ZXNzYWdlIGluIE1JTUUGZm9ybWFF0G0KQotLS0tLS09X051eHRQYXJ0XzAwMF8wMDFGxzAxQzk1
M0E1LjM40Tc30EQwDQpDb250ZW50LUR5cGU6IHR1eHQvcGxhaW47DQoJY2hhcnN1dD0idXhtYXNj
aWkiDQpDb250ZW50LURyYW5zZmUyLUUuY29kaW5n0ia3Ym10DQoNC1R1c3RudmFjaSB6cHJhdmen
Cg0KQotLS0tLS09X051eHRQYXJ0XzAwMF8wMDFGxzAxQzk1M0E1LjM40Tc30EQwDQpDb250ZW50
LUR5cGU6IHR1eHQvaHRtbDsNCgljaGFyc2U0PSJ1cy1hc2NpaSINCkNvbnR1bnQtUHJhbnNmZXIt
RW5jb2Rpbmc6IHF1b3R1ZC1wcm1udGFibGUNCg0KPGh0bWwgeG1sbnM6dj0zRCJ1cm46c2NoZW1h
cy1taWNyb3NuZnQtY29t0nZtbCIgPQ0KeG1sbnM6bz0zRCJ1cm46c2NoZW1hcy1taWNyb3NuZnQt
Y29t0m9mZmljZTpvZmZpY2UiID0NCnhtbG5z0nc9M0QidXJuOnNjaGVtYXhtbWljcm9zb2Z0LWVu
bTpvZmZpY2U6d29yZCIgPQ0KeG1sbnM9M0QiaHR0cDovL3d3dy53My5vcmcvUFIvUkVULWh0bWw0
MCI+DQoNCjxoZWFKPg0KPE1FUEEgSFRUUC1FUUVUJUj0zRCJDb250ZW50LUR5cGU6IENPT1RFT1Q9
M0QidGV4dC9odG1s0yA9DQpjaGFyc2U0PTNEdXhtYXNjaWkiPg0KPG11dGEgYmFtZT0zREd1bmVv
YXRvcibjB250ZW50PTNEIk1pY3Jvc29mdCBXb3JkIDExIChmaWx0ZXJlZCBtZWRpdW0pIj4NCjxz
dH1sZT4NCjwhLS0NCiAvKiBTdH1sZSBEZwZpbm10aW9ucyAqLW0KIHAuTXNuTm9ybWFFsLCBsaS5N
c290b3JtYVwsIGRpd15Nc290b3JtYVwNCg17bWfyZ21u0jBjbT5NCg1tYXJnaW4tYm90dG9t0i4w
MDAxcHQ7DQoJZm9udC1zaXp10jEYLjBwdDsNCg1mb250LWZhbW1seToiUGltZXMgTmU3IFJvbWFWU
```



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
```

```
567GhIGFHFYT6ghyHhHUujpFyF4f8HHGTrfvhJhjH776tbB9HG4UQbnj7  
77n8HHGT9HG4UQpFyF467GhIGFHFYT6rfvbnj756tbBghyHhHUujhJhjH  
HUujhJh4UQpFyF467GhIGFHFYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh  
6YT64U0GhIGFHFQbnj75
```

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



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 |

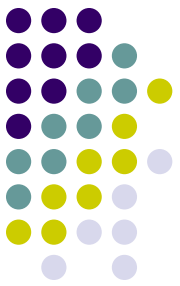
- Source: ETSI TS 102 176-1 V2.0.0 (2007-11)
- Recommended signature schemes
- Starting date: 2006

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 podatelním
 - 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

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



Akreditované CA

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



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.xml | 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 |