Digital signatures in the Czech Republic

The digital signature law in the Czech Republic is based on the act number 227/2000 as changed by acts 226/2002, 517/2002 and 440/2004. The law itself uses quite general terms and tries to be technology independent. The technological details are hidden in other regulations.

Let's first look at some terms as defined by the law on digital signatures.

§ 2
Vymezení některých pojmů

Pro účely tohoto zákona se rozumí:

a) *elektronickým podpisem* údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě,
b) *zaručeným elektronickým podpisem* elektronický podpis, který splňuje následující požadavky:
    1. je jednoznačně spojen s podepisující osobou,
    2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
    3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
    4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,
c) *elektronickou značkou* údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které splňují následující požadavky:
    1. jsou jednoznačně spojené s označující osobou a umožňují její identifikaci prostřednictvím kvalifikovaného systémového certifikátu,
    2. byly vytvořeny a připojeny k datové zprávě pomocí prostředku pro vytváření elektronických značek, které označující osoba může udržet pod svou výhradní kontrolou,
    3. jsou k datové zprávě, ke které se vztahují, připojeny takovým způsobem, že je možné zjistit jakoukoli následnou změnu dat.

…

i) *kvalifikovaným poskytovatelem certifikačních služeb* poskytovatel certifikačních služeb, který vydává kvalifikované certifikáty nebo kvalifikované systémové certifikáty nebo kvalifikovaná časová razítka nebo prostředky pro bezpečné vytváření elektronických podpisů (dále jen „kvalifikované certifikační služby") a splnil ohlašovací povinnost podle § 6,
j) *akreditovaným poskytovatelem certifikačních služeb* poskytovatel certifikačních služeb, jemuž byla udělena akreditace podle tohoto zákona,
k) *certifikátem* datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování elektronických podpisů s podepisující osobou a umožňuje ověřit její identitu, nebo spojuje data pro ověřování elektronických značek s označující osobou a umožňuje ověřit její identitu,
l) *kvalifikovaným certifikátem* certifikát, který má náležitosti podle §12 a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

m) *kvalifikovaným systémovým certifikátem* certifikát, který má náležitosti podle §12a a byl vydán kvalifikovaným poskytovatelem certifikačních služeb,

…

Certifikát (certificate) – binding public key to a subject, this is what we generally know as a certificate.
Kvalifikovaný certifikát (qualified certificate) – certificate having some mandatory fields (see §12) issued by qualified certificate provider.
Poskytovatel certifikačních služeb (certificate provider) – anyone who issues certificates (e.g. you or me).
Kvalifikovaný poskytovatel certifikačních služeb (qualified certificate provider) – certificate provider that fulfills some rules and informs the ministry about its activities.
Akreditovaný poskytovatel certifikačních služeb (accredited certificate provider) – a certificate provider that fulfills some rules and obtains an accreditation from the ministry.
Elektronický podpis (electronic signature) is basically anything which identifies the signer (e.g. nick name). It does not have much value.
Zaručený elektronický podpis (secured electronic signature) is basically a digital signature.
Elektronická značka (electronic sign/mark) – technologically the same as digital signature, but every signature does not have to be manually read and approved by the signing subject (qualified electronic sign/mark is based on system certificate (see §12a) instead of certificate (see §12))
Zaručený elektronický podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb (secured electronic signature based on a qualified certificate issued by an accredited certificate provider) – the only signature accepted by governmental offices (veřejná moc), see §11.

§ 12
Náležitosti kvalifikovaného certifikátu

(1) Kvalifikovaný certifikát musí obsahovat:

a) označení, že je vydán jako kvalifikovaný certifikát podle tohoto zákona,
b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,
c) jméno, popřípadě jména, a příjmení podepisující osoby nebo pseudonym s příslušným označením, že se jedná o pseudonym,
d) zvláštní znaky podepisující osoby, vyžaduje-li to účel kvalifikovaného certifikátu,
e) data pro ověřování podpisu, která odpovídají datům pro vytváření podpisu, jež jsou pod kontrolou podepisující osoby,
f) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný certifikát vydává,

g) číslo kvalifikovaného certifikátu unikátní u daného poskytovatele certifikačních služeb,
h) počátek a konec platnosti kvalifikovaného certifikátu,
i) případně údaje o tom, zda se používání kvalifikovaného certifikátu omezuje podle povahy a rozsahu jen pro určité použití,
j) případně omezení hodnot transakcí, pro něž lze kvalifikovaný certifikát použít.

(2) Omezení pro použití kvalifikovaného certifikátu podle odstavce 1 písm. i) a j) musí být zjevná třetím stranám.

(3) Další osobní údaje smí kvalifikovaný certifikát obsahovat jen se svolením podepisující osoby.

§ 12a

Náležitosti kvalifikovaného systémového certifikátu

Kvalifikovaný systémový certifikát musí obsahovat

a) označení, že je vydán jako kvalifikovaný systémový certifikát podle tohoto zákona,
b) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,
c) jednoznačnou identifikaci označující osoby, případně prostředku pro vytváření elektronických značek,
d) data pro ověřování elektronických značek, která odpovídají datům pro vytváření elektronických značek, jež jsou pod kontrolou označující osoby,
e) elektronickou značku poskytovatele certifikačních služeb založenou na kvalifikovaném systémovém certifikátu poskytovatele, který kvalifikovaný systémový certifikát vydává,
f) číslo kvalifikovaného systémového certifikátu unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,
g) počátek a konec platnosti kvalifikovaného systémového certifikátu,
h) omezení pro použití kvalifikovaného systémového certifikátu, přičemž tato omezení musí být zjevná třetím stranám.

§12b

Náležitosti kvalifikovaného časového razítka

Kvalifikované časové razítko musí obsahovat

a) číslo kvalifikovaného časového razítka unikátní u daného kvalifikovaného poskytovatele certifikačních služeb,
b) označení pravidel, podle kterých kvalifikovaný poskytovatel certifikačních služeb kvalifikované časové razítko vydal,
c) v případě právnické osoby obchodní firmu nebo název a stát, ve kterém je kvalifikovaný poskytovatel usazen; v případě fyzické osoby jméno, popřípadě jména, příjmení, případně dodatek, a stát, ve kterém je kvalifikovaný poskytovatel usazen,
d) hodnotu času, která odpovídá koordinovanému světovému času při vytváření kvalifikovaného časového razítka,

e) data v elektronické podobě, pro která bylo kvalifikované časové razítko vydáno,
f) elektronickou značku kvalifikovaného poskytovatele certifikačních služeb, který kvalifikované časové razítko vydal.

Other interesting parts include:

§ 16
Uznávání zahraničních kvalifikovaných certifikátů

(1) Certifikát, který je vydán poskytovatelem certifikačních služeb usazeným v některém z členských států Evropské unie jako kvalifikovaný, je kvalifikovaným certifikátem ve smyslu tohoto zákona.
(2) Certifikát, který je vydán jako kvalifikovaný ve smyslu tohoto zákona v jiném než členském státu Evropské unie, je kvalifikovaným certifikátem ve smyslu tohoto zákona pokud:

a) poskytovatel certifikačních služeb splňuje podmínky práva Evropských společenství[1)] a byl akreditován k působení jako akreditovaný poskytovatel certifikačních služeb v některém z členských států Evropské unie, nebo
b) poskytovatel certifikačních služeb usazený v některém z členských států Evropské unie, který splňuje podmínky práva Evropských společenství,[1)] převezme odpovědnost za platnost a správnost certifikátu ve stejném rozsahu jako u svých kvalifikovaných certifikátů, nebo
c) to vyplývá z mezinárodní smlouvy.

§ 17
Prostředky pro bezpečné vytváření a ověřování elektronických podpisů

(1) Prostředek pro bezpečné vytváření podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že:

a) data pro vytváření podpisu se mohou vyskytnout pouze jednou a že jejich utajení je náležitě zajištěno,
b) data pro vytváření podpisu nelze při náležitém zajištění odvodit ze znalosti způsobu jejich vytváření a že podpis je chráněn proti padělání s využitím existující dostupné technologie,
c) data pro vytváření podpisu mohou být podepisující osobou spolehlivě chráněna proti zneužití třetí osobou.

(2) Prostředky pro bezpečné vytváření podpisu nesmí měnit data, která se podepisují, ani zabraňovat tomu, aby tato data byla předložena podepisující osobě před vlastním procesem podepisování.
(3) Prostředky pro bezpečné vytváření elektronických podpisů musí být před svým použitím bezpečným způsobem vydány a data pro vytváření elektronických podpisů musí být důvěryhodným způsobem v těchto prostředcích vytvořena nebo do nich přidána.
(4) Prostředek pro bezpečné ověřování podpisu musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, aby

a) data používaná pro ověření podpisu odpovídala datům zobrazeným osobě provádějící ověření,
b) podpis byl spolehlivě ověřen a výsledek tohoto ověření byl řádně zobrazen,

c) ověřující osoba mohla spolehlivě zjistit obsah podepsaných dat,
d) pravost a platnost certifikátu při ověřování podpisu byly spolehlivě zjištěny,
e) výsledek ověření a totožnost podepisující osoby byly řádně zobrazeny,
f) bylo jasně uvedeno použití pseudonymu,
g) bylo možné zjistit veškeré změny ovlivňující bezpečnost.

§17a
Prostředky pro vytváření elektronických značek

(1) Prostředek pro vytváření elektronických značek musí za pomoci odpovídajících technických a programových prostředků a postupů minimálně zajistit, že
a) data pro vytváření elektronických značek jsou dostatečným způsobem utajena a jsou označující osobou spolehlivě chráněna proti zneužití třetí osobou,
b) označující osoba je informována, že zahajuje používání tohoto prostředku.

(2) Prostředek pro vytváření elektronických značek musí být nastaven tak, aby i bez další kontroly označující osoby označil právě a pouze ty datové zprávy, které označující osoba k označení zvolí.

(3) Prostředek pro vytváření elektronických značek musí být chráněn proti neoprávněné změně a musí zaručovat, že jakákoli jeho změna bude patrná označující osobě.

These paragraphs just confirm that no technical details or instructions are provided by this law.

More technical details were specified in “Vyhláška ÚOOÚ č. 366/2001”. The annexes 1 and 2 quote which asymmetric algorithms can be used and their parameters:

Podpisové schéma	Asymetrický algoritmus	Minimální parametry asymetrického algoritmu	Metoda určená pro padding	Hašovací funkce
001	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	SHA1
002	RSA	MinModLen=1020	emsa-pss	SHA1
003	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	RIPEMD160
004	RSA	MinModLen=1020	emsa-pss	RIPEMD160
005	DSA	pMinLen=1024 qMinLen=160	-	SHA1
006	ECDSA-F_p	qMinLen=160 r0Min=10^4 MinClass=200	-	SHA1
007	ECDSA-$F2^m$	qMinLen=160 r0Min=10^4 MinClass=200	-	SHA1
008	RSA	MinModLen=1020	emsa-pkcs #1-v1.5	MD5
009	RSA	MinModLen=1020	emsa-pss	MD5

The last 2 algorithms cannot be used for CA keys (for a clear reason☺). For the annex number 2 special explanation was published by the ministry.

This specification changed in 2006 and now only a reference to ETSI documents (standards) is made.

Basically for the signed message PKCS#7 format is used, for email delivery S/MIME encapsulation is used (PGP and other formats are not supported).

For “elektronické podatelny” additional regulation is available: “Vyhláška o elektronických podatelnách 496/2001”. In an annex of this regulation the process of signature verification is described:

a) verification that the certificate is valid in the terms of time (start of validity < now() < end of validity)
b) verification whether the certificate has been correctly signed by the issuing CA
c) verification whether the certificate has not been revoked (check against the CRL – the valid CRL is the **first one issued after** the delivery of the message)
d) verify whether the CRL has been correctly signed by the issuing CA
e) if the certificate path is longer verify every item of the chain according to a) to d)

A timestamp can be attached to a digitally signed message, but does not have much value. The only reasonable use can be in the situation when the certificate was revoked just after the signature and before the message has reached the recipient. In such cases the digital signature without a timestamp cannot be considered valid, but if a timestamp proving the message has been created before the certificate revocation is attached, the digital signature can be verified as valid.

Technicalities

Technically the digital signature has a form of the CMS (cryptographic message syntax) SignedData structure. The CMS as a successor of PKCS#7 is defined in RFC 2630. The ASN.1 syntax of SignedDate is:

```
id-signedData OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }

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

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

SignerInfos ::= SET OF SignerInfo

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
```

Assignments:

1. Create a program that will verify a signature. The input is an email message (including all the headers) and a directory with trusted CA certificates (download from MICR). The output is yes/no. Use any programming language (you are not allowed to run other external programs, shell scripts are therefore out of question) and any crypto library (recommended is C and OpenSSL, use the PKCS7_verify function). The program should:
    a. Output the signed data {3} (you have to support both types of signatures (multipart/signed, application/pkcs7-mime))
    b. Verify the signature {3} (you do not have to handle more than one signature (i.e. several SignerInfos in one SignedData structure); only RSA-PKCS#1 version 1.5 must be supported)
    c. Verify the certificate {3} (expect that the certificate is stored in SignedData and CA certs are in a directory)
    d. Verify the CRL {3} (download the CRL from the web site of the CA) (you can choose whether you want to support the Czech legislation approach (first after) or the normal approach (between Issued and Next))