6 Přílohy

6.1 Standardy

6.1.1 ISO

ISO byla založena v r. 1947. Je celosvětovou federací členských národních normalizačních organizací – ISO Member Bodies (AFNOR, ANSI, BSI, DIN, SCC …). Jako členské národní normalizační organizace jsou vybírány vždy nejreprezentativnější normalizační organizace v dané zemi.

ISO (a IEC) přiděluje odpovědnost za vývoj norem v konkrétních oblastech *technickým výborům*, *Technical Committees* (TC). Technický výbor si určuje svůj program v rámci vymezeném svojí rodičovskou organizací (ISO nebo IEC) sám, a to tak, aby zadaný úkol vyřešil. TC dělí svoji působnost na *podvýbory*, *SubCommittees* (SC). Podvýbory se dělí na *pracovní skupiny*, *Working Groups* (WG). V pracovních skupinách se skutečně pracuje, výše se jen schvaluje. Evoluce struktur TC/SC/WG je pomalá, tyto struktury pracují a existují obvykle několik let. Mezi technické výbory zabývající se normami bezpečnosti IT patří především:

- *ISO TC68* (bankovnictví)
- *ISO/IEC JTC1* (informační technologie).

6.1.1.1 Relevantní normy ISO

Jedná se prakticky o všechny nejvýznamnější ISO TC, které se věnují normám bezpečnosti IT, ISO TC68 (bankovnictví) a ISO/IEC JTC1 (informační technologie).

ISO TC68 se sice zabývá hlavně bankovními normami, ale TC68 vydal také celou řadu obecných norem bezpečnosti – ISO 8730 a ISO 8731-1/2 definující integritní mechanismy, ISO 8732 a ISO 11166-1/2 specifikující správu kryptografických klíčů. Činnost TC68 z hlediska bezpečnosti byla dělena mezi podvýbory a pracovní skupiny následovně:

- TC68/SC2: bezpečnost mezibankovních styků
- TC68/SC6/WG6: bezpečnost styku se zákazníky
- TC68/SC6/WG7: bezpečnostní architektura bankovních systémů na bázi čipových karet (činnost WG7 byla v současnosti pravděpodobně již ukončena).

Mezi nejvýznamnější podvýbory působící v rámci *ISO/IEC JTC1* relevantní k bezpečnosti IT patří:

- SC6: telekomunikace a výměna informací mezi systémy

  SC6 má odpovědnost za správu dolních úrovní (1-4) ISO RM OSI modelu, tj. za komunikační podsystémy sítí otevřených systémů. SC6 definoval normy

ISO/IEC 11577 – Network Layer Security Protocol (NLSP) a ISO/IEC 10736 – Transport Layer Security Protocol (TLSP).

- SC17: normalizace čipových karet a s nimi souvisejících zařízení
  Z výsledků činnosti SC17 lze upozornit zejména na normu ISO/IEC 7816.
- SC27: techniky bezpečnosti IT
  SC27 je podvýbor odpovědný za normalizaci generických metod a technik bezpečnosti IT, za normy kryptografických technik a za mezinárodní normy pro hodnocení bezpečnosti. Zabývá se identifikací generických požadavků na bezpečnostní funkce, vývojem bezpečnostních technik a mechanismů, vývojem bezpečnostních návodů a vývojem dokumentace a norem pro podporu správy bezpečnosti IT. Svoji činnost dělí do tří pracovních skupin:
  - WG1: Požadavky na bezpečnost, bezpečnostní služby a návody – správa bezpečnosti a problémy kompatibility z hlediska bezpečnosti s ostatními normalizačními výbory.
  - WG2: Bezpečnostní techniky a mechanismy – kryptografické techniky, normy bezpečnostních mechanismů.
  - WG3: Kritéria hodnocení bezpečnosti – počítačová bezpečnost, kritéria hodnocení apod.

Následující podvýbory v současnosti již ukončily svoji činnost. V minulé dekádě ovšem patřily obory jejich působnosti mezi technologicky vysoce progresivní:

- SC18: zpracování dokumentů a s tím související komunikace
  SC18 se věnuje normám elektronické pošty (WG4) a architekturám otevřených (normalizovaných) dokumentů, *ODA* (Open Document Architecture).
- SC21: propojování otevřených systémů, správa dat, otevřené distribuované zpracování
  SC21 je podvýbor odpovědný za Referenční model OSI – model sítí (WG1), za adresářové služby a správu propojených otevřených systémů – Directory and OSI Management (WG4) a za protokoly horních (5–7) vrstev modelu OSI – správu procesů, prezentaci dat a aplikační služby (WG8). SC21 rovněž vypracoval v r. 1988 základní ISO normu bezpečnost sítí, OSI Security Architecture, ISO 7498-2, která je v současné době v SC21 doplňována o novou normu bezpečnostních funkcí otevřených systémů – jedná se o sedmidílný "Security Frameworks Standard", ISO/IEC 10181, Bezpečnostní soustavy.

Některé normy těchto podvýborů přešly do správy podvýboru JTC1/SC6, kterému se tímto rozšířila oblast působnosti. Většinu norem z oblasti působnosti bývalých podvýborů SC18 a SC21, které se dále nevyvíjí, spravuje přímo sekretariát JTC1.
V oblasti působnosti *SC27/WG1* je především správa bezpečnosti. SC27/WG1 je odpovědná za udržování norem:

- ISO/IEC 9979 z r. 1999 – procedury pro registraci kryptografických algoritmů
- ISO/IEC 11770-1 – Správa klíčů, Část 1: Prostředí (připraveno k publikaci).

SC27/WG1 rovněž pracuje na:

- technické zprávě TR 13335, části 1-5, směrnice pro správu bezpečnosti IT, dosud jsou publikovány části 1–3

- technické zprávě TR 14516, směrnice pro použití a správu třetích důvěryhodných stran, TTP (Trusted Third Parties)
- normě ISO/IEC 15816, informace (objekty) požadované pro plnění bezpečnostních služeb (Security Information Objects), v současnosti ve stavu CD
- normě ISO/IEC 15945, specifikace služeb TTP (služeb třetích důvěryhodných stran) pro podporu používání digitálních podpisů, v současnosti na úrovni WD.

V oblasti působnosti *SC27/WG2* jsou normy kryptografických technik, tj. bezpečnostních mechanismů, SC27/WG2 je odpovědná za udržování norem:

- ISO/IEC 10116, režimy činnosti blokových šifer
  jedná se o inovaci normy ISO 8372 z r. 1987 a normu ISO/IEC 10116 z r. 1997 (2. vydání).
- ISO/IEC 9797, integritní mechanismy
  jedná se o normu ISO/IEC 9797 z r. 1994 (2. vydání) v současné době přepracovávanou do normy ISO/IEC 9797-1, ke které se vyvíjí rovněž část 2.
- ISO/IEC 9798, autentizační mechanismy (protokoly)
  jedná se o normy ISO/IEC 9798-1 z r. 1997 (2. vydání), ISO/IEC 9798-2 z r. 1994, ISO/IEC 9798-3 z r. 1998 (2. vydání), ISO/IEC 9798-4 z r. 1995 a o normu ISO/IEC 9798-5 z r. 1999.
- ISO/IEC 11770, správa kryptografických klíčů
  jedná se o normy ISO/IEC 11770-2 z r. 1996 a ISO/IEC 11770-3 z r. 1998.
- ISO/IEC 9796, digitální podpisy s obnovou zprávy
  ISO/IEC 9796 z r. 1991, ISO/IEC 9796-2 z r. 1997 a CD 9796-4.
- DIS 14888, digitální podpisy v dodatku zprávy
  v současné době jsou vypracovány DIS 14888-1, DIS 14888-2 a DIS 14888-3.
- ISO/IEC 10118, hašovací funkce
  jedná se o normy ISO/IEC 10118-1 a -2 z r. 1994, ISO/IEC 10118-3 z r. 1998 a o DIS 10118-4.
- ISO/IEC 13888, mechanismy nepopiratelnosti
  jedná se o normy ISO/IEC 13888-1 z r. 1997, ISO/IEC 13888-2 z r. 1998 a o normu ISO/IEC 13888-3 z r. 1997.
- ISO/IEC 15946, kryptografie na bázi eliptických křivek
  norma připravovaná ve třech částech, v současnosti jsou všechny na úrovni WD.
- ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements byla oficiálně publikována 15. října 2005. Vydání této normy nahrazuje její předchozí verzi známou pod označením BS7799-2:2002. Norma ISO/IEC 27001 si klade za cíl poskytnout doporučení, jak aplikovat ISO/IEC 17799 (do budoucna ISO/IEC 27002) v rámci procesu ustavení, provozu, údržby a zlepšování systému řízení bezpečnosti informací (ISMS) v organizaci v souladu se systémy řízení kvality nebo bezpečnosti prostředí. Norma popisuje vhodný systém řízení, strukturu a procesy pro řízení bezpečnosti informací podle opatření definovaných v ISO/IEC 17799.

V oblasti působnosti *SC27/WG3* jsou především **kritéria hodnocení bezpečnosti IT.** Výsledkem jeho činnosti je norma ISO/IEC 15408, Evaluation Criteria for IT Security, která byla vydána v červnu 1999.

6.1.1.2 ISO 15489

Nejvýznamnější normou ISO, která se problematikou správou elektronických dokumentů zabývá je standard ISO 15489, který byl přijat v říjnu 2001. Představuje (podle http://naa.gov.au/) dosud nejlepší management dokumentů na mezinárodní scéně. Své základy nalezl v australském národním standardu *AS 4390-1996: Record management*.
ISO 15489 se skládá ze dvou částí:
- AS ISO 15489.1 Records Management . Part 1: General
- AS ISO 15489.2 Records Management . Part 1: Guidelines

První část je věnována aktuálnímu standardu, který tvoří schéma pro uchovávání dat prostřednictvím definic vysokoúrovňových principů a metod. Hovoří se zde o výhodách správy záznamů, potřebách identifikovat hranice prostředí, ve kterých organizace působí a o důležitosti přiřazení zodpovědnosti za uchovávání dat. Mimo jiné popisuje i návrh takovýchto systémů (*Design of recordkeeping systems* . *DIRS* nebo hůře *DIRKS*) a výčet procesů a řízení správy dokumentů. Svým rozsahem pokrývá i monitoring a audit nebo za.kolování zaměstnanců.
Druhá část představuje doplňující technické zprávy, které popisují detaily a návody sloužící organizacím k lepšímu pochopení a nasazení standardu do svých struktur a organizačních zásad.

Standard představuje pro organizace řídící schéma, podle kterého mohou vytvořit své vlastní postupy a metody sloužící k uchovávání záznamů. Obě části standardu jsou vytvořeny tak, aby pomáhaly institucím vytvářet, získávat a spravovat kompletně a přesně data a aby zároveň vyhověly právním náležitostem i podnikovým potřebám na straně jedné a splnily očekávání jejich investorů na straně druhé. Standard je možné aplikovat pro data v jakémkoliv formátu na různých datových médiích, vytvořených nebo přijatých libovolnou veřejnou nebo soukromou institucí. Stejně jako předchozí standard AS 4390 představuje současný ISO standard základní soubor konceptů pro Národní archiv pokud jde o způsoby uchovávání dat, použité metody a návody pro realizaci.

V textu standardu je velká část věnována i problematice metadat. Jako základ byl vzat *Dublin Core* a přes několik dalších mezistupňů došlo k vytvoření souboru atributů, který je možné najít v příloze. Zajímavostí také je, že v příloze standardu najdeme i formulář pro zaslání požadavku autorům například z důvodu chybějícího nebo naopak přebytečného atributu

6.1.1.3 ČSN ISO

6.1.1.3.1 Nové relevantní ČSN ISO normy (určené pro certifikační autority a autority časových razítek)

Na návrh Ministerstva informatiky byly ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví č.2/2006 vyhlášeny dvě nové české technické normy:

ČSN ETSI TS 101 456 V1.3.1 Elektronické podpisy a infrastruktury - Požadavky na postupy certifikační autority vydávající kvalifikované certifikáty
Třídící znak: 874004. Katalog: 74529 Vydána: únor 2006. Účinnost: 01.03.2006 Norma je v anglickém jazyce, zapracovaným dokumentem je ETSI TS 101 456
V1.3.1:2005, je vyhlášena věstníkem, nevyšla tiskem.

ČSN ETSI TS 102 023 V1.2.1 Elektronické podpisy a infrastruktury - Požadavky na postupy autorit časových razítek
Třídící znak: 874005 Katalog: 74528 Vydána: únor 2006. Účinnost: 01.03.2006 Norma je v anglickém jazyce, zapracovaným dokumentem je ETSI TS 102 023
V 1.2.1:2003, je vyhlášena věstníkem, nevyšla tiskem.

Obě uvedené normy se jsou závazné pro kvalifikované poskytovatele certifikačních služeb na základě připravované vyhlášky k zákonu č. 227/2000 Sb., o elektronickém podpisu.

6.1.1.3.2 Přehled ČSN ISO z oblasti bezpečnosti informačních technologií

ČSN ISO/IEC 2382-1 Informační technologie - Slovník - Část 1: Základní termíny
ČSN ISO/IEC 2382-8 Informační technologie - Slovník - Část 8: Bezpečnost
ČSN ISO/IEC 2382-14 Informační technologie - Slovník - Část 14: Spolehlivost
ČSN ISO/IEC 10116 Informační technologie - Bezpečnostní techniky - Módy činnosti pro n-bitovou blokovou šifru
ČSN ISO/IEC 10118-1 Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně
ČSN ISO/IEC 10118-2 Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce používající n-bitovou blokovou šifru
ČSN ISO/IEC 10118-3 Informační technologie - Bezpečnostní techniky - Hash funkce - Část 3: Dedikované haš funkce
ČSN ISO/IEC 10118-4 Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku
ČSN ISO 10126-1 Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - Část 1: Obecné zásady
ČSN ISO 10126-2 Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu). Část 2: Algoritmus DEA
ČSN ISO 10202-1 Identifikační karty. Karty pro finanční transakce. Bezpečnostní architektura systémů finančních transakcí využívajících karty s integrovanými obvody. Část 1: Životní cyklus karty

ČSN ISO 11131 Bankovnictví - Autentizace přihlášením
ČSN ISO 11166-1 Bankovnictví - Správa klíčů prostřednictvím asymetrických algoritmů - Část 1: Zásady, postupy a formáty
ČSN ISO 11166-2 Bankovnictví - Správa klíčů pomocí asymetrických algoritmů - Část 2: Schválené algoritmy používající kryptosystém RSA
ČSN EN ISO 11568-1 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů
ČSN EN ISO 11568-2 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru
ČSN EN ISO 11568-3 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 3: Životní cyklus klíče pro symetrickou šifru
ČSN ISO/IEC 11770-1 Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura
ČSN ISO/IEC 11770-2 Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC 11770-3 Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC TR 13335-1 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT
ČSN ISO/IEC TR 13335-2 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT
ČSN ISO/IEC TR 13335-3 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT
ČSN ISO/IEC TR 13335-4 Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření
ČSN ISO/IEC 13888-1 Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně
ČSN ISO/IEC 13888-2 Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 2: Mechanismy používající symetrické techniky
ČSN ISO/IEC 13888-3 Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 3: Mechanismy používající asymetrické techniky
ČSN ISO/IEC 14888-1 Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně
ČSN ISO/IEC 14888-2 Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě
ČSN ISO/IEC 14888-3 Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu
ČSN ISO/IEC 15408-1 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 1: Úvod a všeobecný model
ČSN ISO/IEC 15408-2 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky
ČSN ISO/IEC 15408-3 Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 3: Požadavky na záruky bezpečnosti
ČSN ISO/IEC 17799 Informační technologie - Soubor postupů pro řízení informační bezpečnosti

ČSN ISO 6166 Cenné papíry a příbuzné finanční nástroje - Mezinárodní systém identifikačního číslování cenných papírů (ISIN)
ČSN ISO 7775 Bankovnictví - Cenné papíry - Schéma pro typy zpráv
ČSN ISO 8372 Zpracování informací - Módy činnosti pro algoritmus 64-bitové blokové šifry
ČSN ISO 8730 Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu)
ČSN ISO 8731-1 Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 1: DEA
ČSN ISO 8731-2 Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 2: Algoritmus autentikátora zprávy
ČSN ISO 8732 Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu)
ČSN ISO 8908 Bankovnictví a související finanční služby - Slovník a datové prvky
ČSN ISO 9564-1 Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 1: Principy a techniky ochrany PIN
ČSN ISO 9564-2 Bankovnictví - Řízení a bezpečnost osobních identifikačních čísel. Část 2: Schválené algoritmy pro šifrování PIN
ČSN ISO 9735-5 Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 5: Pravidla bezpečnosti pro dávkovou EDI (autentičnost, integrita a nepopření původu)
ČSN ISO 9735-6 Elektronická výměna dat pro správu, obchod a dopravu (EDIFACT) - Pravidla syntaxe aplikační úrovně (Číslo verze syntaxe: 4) - Část 6: Bezpečnostní autentizace a potvrzení (Zpráva AUTACK)
ČSN ISO/IEC 9796-2 Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy využívající hašovací funkci
ČSN ISO/IEC 9796-3 Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech
ČSN ISO/IEC 9797 Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry
ČSN ISO/IEC 9797-1 Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 1: Mechanismy používající blokovou šifru
ČSN ISO/IEC 9798-1 Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - 1. část: Obecný model
ČSN ISO/IEC 9798-2 Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 2: Mechanismy používající symetrické šifrovací algoritmy
ČSN ISO/IEC 9798-3 Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 3: Autentizace entit používající algoritmus s veřejným klíčem
ČSN ISO/IEC 9798-4 Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci

ČSN ISO/IEC 9798-5 Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 5: Mechanismy používající techniku nulových znalostí
ČSN ISO 9807 Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro drobnou klientelu)
ČSN ISO/IEC 9979 Informační technologie - Bezpečnostní techniky - Postupy pro registraci kryptografických algoritmů

6.1.2 ETSI

Přehled relevantních dokumentů ETSI v oblasti elektronického podpisu, časových razítek a kvalifikovaných certifikátů

ETSI - Evropský institut pro normalizaci v telekomunikacích (European Telecommunications Standards Institute) se sídlem v Sophia Antipolis (Francie) byl založen v roce 1988). Jedná se o neziskovou organizací, jejímž hlavním posláním je vypracovávat normy ETSI EN (telekomunikační řady), normy ETSI ES (normy nižší úrovně), technické specifikace (ETSI TS), technické zprávy (ETSI TR), zvláštní zprávy (ETSI SR), technické základy pro předpisy (ETSI TBR), dřívější telekomunikační normy (ETSI-ETS) a předběžné telekomunikační normy (ETSI I-ETS), technické zprávy ETSI (ETSI-ETR) a pokyny ETSI (ETSI EG) v oblasti telekomunikací a elektronických komunikací. Telekomunikační normy ETSI EN jsou na základě dohod přejímány jako národní normy jednotlivých členských státu EU.

V roce 2006 a začátkem letošního roku byly zveřejněny nové verze technických specifikací a technických zpráv. V závorce u jednotlivých dokumentů jsou data, kdy byl daný dokument publikován, případně v jaké fázi se momentálně nachází.

6.1.2.1 Technické specifikace (TS)

ETSI TS 102 904 V1.1.1 (2007-01-12) Electronic Signatures and Infrastructures; Profiling for Electronic Signatures based on ETSI TS 101 903

ETSI TS 101 734 V1.1.1 (2007-01-12) Electronic Signatures and Infrastructures; Profiling for Electronic Signatures based on ETSI TS 101 733

ETSI TS 102 231 V2.1.1 (2006-03-10) Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information

ETSI TS 102 176-1 V1.3.1 (Drafting stage, TB adoption of WI 2006-09-01)

Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms

ETSI TS 102 176-2 V1.3.1 (Drafting stage, TB adoption of WI 2006-09-01)

Electronic Signatures and Infrastructures (ESI) Algorithms and Parameters for Secure Electronic Signatures; Part 2: Secure channel protocols and algorithms for signature creation devices

ETSI TS 102 042 V1.2.3 (2006-12-08) Electronic Signatures and Infrastructures (ESI) Policy requirements for certification authorities issuing public key certificates

ETSI TS 101 903 V1.3.2 (2006-03-07) XML Advanced Electronic Signatures (XAdES)

ETSI TS 101 862 V1.3.3 (2006-01-06) Qualified Certificate profile

ETSI TS 101 861 V1.3.1 (2006-01-27) Time stamping profile

ETSI TS 101 733 V1.7.3 (2007-01-11) Electronic Signatures and Infrastructures (ESI) CMS Advanced Electronic Signatures (CAdES)

ETSI TS 101 456 V1.4.2 (2006-12-14) Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates

ETSI TS 101 456 V1.4.1 (2006-02-02) Electronic Signatures and Infrastructures (ESI) Policy requirements for certification authorities issuing qualified certificates

6.1.2.2 Technické zprávy (TR)

ETSI TR 102 458 V1.1.1 (2006-04-20) Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certifcate

Policy and the European Qualified Certificate Policy (TS 101 456)

ETSI TR 102 438 V1.1.1 (2006-03-06) Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe

ETSI TR 102 437 V1.1.1 (2006-10-03) Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy requirements for certification authorities issuing qualified certificates)

Pro vyhledávání dokumentů a zjišťování stavu rozpracovanosti jednotlivých dokumentů je možné používat adresu

http://webapp.etsi.org/WorkProgram/SimpleSearch/QueryForm.asp

6.1.3 CEN/CENLEC

Evropský výbor pro normalizaci (CEN)
http://www.cenorm.be/
Posláním CEN je podporovat dobrovolnou technickou harmonizaci v Evropě ve shodě s celosvětovými orgány a jejich partnery v Evropě.

Harmonizace ztenčuje obchodní bariéry, zvyšuje bezpečnost, umožňuje výměnu zboží, systémů a služeb a zvyšuje základní technické porozumění. V Evropě CEN spolupracuje s CENELEC (Evropský výbor pro elektrotechnickou normalizaci) a ETSI (Evropský telekomunikační normalizační institut).

Evropský výbor pro elektrotechnickou normalizaci (CENELEC)
http://www.cenelec.be/
CENELEC byl ustanoven roku 1973 jako nevýdělečně činná organizace v rámci belgického práva. Oficiálně byl uznán jako evropská normalizační organizace Evropskou komisí nařízením 83/189 EEC.

6.1.3.1 Standardy CEN/ISSS 2006 - elektronická fakturace (včetně požadavků na archivaci daňových dokladů)

eInvoice_Task_1_1_EDI_n82.pdf
eInvoice_Task_1_2_Mandatory_data_in_the_invoice.xls
eInvoice_Task_1_2_Storage_n86.pdf
eInvoice_Task_1_3_Recommendation_Identifier_n83.pdf
eInvoice_Task_1_4_Code_set_for_text_Clauses_n84.pdf
eInvoice_Task_1_5_Suvey_on_VATDataElement_n85.pdf
eInvoice_Task_1_5_Table_exemptions_tables.xls
eInvoice_Task_1_5_Table_VAT_data_elements.xls
eInvoice_Task_2_1_2_3_Digital_Signature_n81.pdf
eInvoice_Task_3_1_2_DRAFT_n86.pdf
eInvoice_Task_3_1_2_Storage_Annex_n87.pdf
eInvoice_Task_3_3_Service_provider_n88.pdf
eInvoice_Task_3.4_ref_model_march2006.pdf
n23.doc

Všechny výše uvedené dokumenty byly v podobě návrhu dány k veřejné diskuzi v dubnu 2006.
http://www.cenorm.be/CENORM/BusinessDomains/businessdomains/isss/activity/draft_doc_11apr.asp

6.1.3.2 Standardy CEN věnované elektronickému podpisu (procesy, bezpečnost)

CWA 14167 (Multipart)

CWA 14167-1
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-01-2003-Jun.pdf)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements

CWA 14167-2
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-02-2004-May.pdf)

Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP signing operations with backup - Protection profile (CMCSOB-PP)

CWA 14167-3
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-03-2004-May.pdf)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic module for CSP key generation services - Protection profile (CMCKG-PP)

CWA 14167-4
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14167-04-2004-May.pdf)
Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic module for CSP signing operations - Protection profile - CMCSO PP

CWA 14169
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14169-00-2004-Mar.pdf)
Secure Signature-creation devices "EAL 4+"

CWA 14170
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14170-00-2004-May.pdf)
Security requirements for signature creation applications

CWA 14171
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14171-00-2004-May.pdf)
General guidelines for electronic signature verification

CWA 14172 (Multipart)

CWA 14172-1
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-01-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 1: General introduction

CWA 14172-2
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-02-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes

CWA 14172-3
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-03-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures

CWA 14172-4
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-04-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification

CWA 14172-5
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-05-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices

CWA 14172-6
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-06-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified

CWA 14172-7
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-07-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 7:
Cryptographic modules used by Certification Service Providers for signing operations and key generation services

CWA 14172-8
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14172-08-2004-Mar.pdf)
EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes
CWA 14355
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14355-00-2004-Mar.pdf)
Guidelines for the implementation of Secure Signature-Creation Devices

CWA 14365 (Multipart)
CWA 14365-1
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14365-01-2004-Mar.pdf)
Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects

CWA 14365-2
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14365-02-2004-Mar.pdf)
Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software Signature Creation Devices

CWA 14890 (Multipart)
CWA 14890-1
(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf)
Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

CWA 14890-2

(ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-02-2004-May.pdf)
Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services

6.1.4 RFC (Request For Comment)

Historickým vývojem vznikla tradice publikování dokumentů RFC. Její vznik se datuje do roku 1969 a souvisí se zprovozněním ARPANETu, ze kterého se později vyvinul dnešní Internet. Postgraduální studenti a další řešitelé ARPANEtu, jejichž postavení jim neumožňovalo, aby své četné nápady a podněty, mnohdy velmi užitečné a podnětné, nějak vnucovaly svým profesorům a intenzivněji se domáhali jejich pozornosti, své návrhy proto začali sepisovat ve formě dokumentů, kterým dali výstižné pojmenování Request For Comment (doslova: žádost o komentář). Tyto dokumenty předkládali těm, kterých se týkaly, resp. kteří byli kompetentní je posuzovat, přijímat požadovaná rozhodnutí apod. Tradice publikování dokumentů RFC vydržela až do dnešních dnů. Změnil se ale věcný obsah a celkový smysl dokumentů RFC - s postupem času to stále méně byly náměty a nápady, usilující o vznik nějakého řešení, a čím dál tím více to byla tato řešení jako taková.

Dnes jsou dokumenty RFC používány jako specifická forma dokumentace, vydávána pro potřeby Internetu (ale nepřímo i pro potřeby mnohem širšího okruhu sítí a služeb). „Vydavatelem“ RFC je IETF (*Internet Engineering Task Force).*

> Pro správné pochopení významu dokumentů RFC je potřebné si ještě uvědomit a náležitě zdůraznit, že jejich obsahem nejsou zdaleka jen standardy - tedy popisy řešení, která mají povahu závazných standardů (byť standardů "de facto", a nikoli "de jure", ale přesto velmi důsledně uznávaných a dodržovaných). Ve formě dokumentů RFC jsou vydávány i jiné dokumenty, například návody, doporučení, či vysvětlení, a v poslední době i stanoviska a názory.

RFC jsou veřejně dostupná (http://www.ietf.org/rfc.html), ale zdaleka ne všechna jsou standardy v rámci internetové komunity.

V listopadu 2001 bylo pouze 61 RFC schválenými, plnoprávnými *de facto* normami (*RFC 3000 Internet Official Protocol Standards*) a jsou vyjma čísla RFC také označeny číslem normy (STD #). K 1.1.2007 bylo celkem 67 takovýchto specifických norem.

Dokumenty RFC v celkovém počtu více jak **5000** (k 1.10.2007) již obsahují statisíce stránek textu. Pro vyhledávání se dá využít tzv. index, který je dostupný na : http://www.ietf.org/iesg/1rfc_index.txt , součástí citace v indexu je i aktuální status dokumentu.

- **PKIX:** Public Key Infrastructure (X.509)
  - RFC 2459: "Certificate and CRL Profile"
  - RFC 2510: "Certificate Management Protocols"
  - RFC 2511: "Certificate Request Message Format"
  - RFC 2527: "Certificate Policy and Certification Practices Framework"
  - RFC 2528: "Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates"
  - RFC 2559: "Operational Protocols - LDAPv2"
  - RFC 2560: "Online Certificate Status Protocol - OCSP"
  - RFC 2585: "Operational Protocols - FTP and HTTP"
  - RFC 2587: "LDAPv2 Schema"
  - RFC 2797: "Certificate Management Messages over CMS"
  - RFC 2875: "Diffie-Hellman Proof-of-Possession Algorithms"
  - RFC 3029: "Data Validation and Certification Server Protocols"
  - RFC 3039: "Qualified Certificates Profile"
  - RFC 3161: "Time-Stamp Protocol (TSP)"
  - RFC 3279: "Algorithms and Identifiers for the PKIX Certificate and Certificate Revocation List (CRL) Profile"
  - RFC 3280: "Certificate and CRL Profile"
  - RFC 3281: "An Internet Attribute Certificate Profile for Authorization"
  - RFC 3379: "Delegated Path Validation and Delegated Path Discovery Protocol Requirements"
  - RFC 3628: "Policy Requirements for Time-Stamping Authorities (TSAs)"
  - RFC 3647: "Certificate Policy and Certification Practices Framework"
  - RFC 3709: "Logotypes in X.509 Certificates"
  - RFC 3739: "Qualified Certificates Profile"
  - RFC 3770: "Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)"
  - RFC 3779: "X.509 Extensions for IP Addresses and AS Identifiers"
  - RFC 3820: "Proxy Certificate Profile"
  - RFC 3874: "A 224-bit One-way Hash Function: SHA-224"
  - RFC 4043: "Permanent Identifier"
  - RFC 4055: "Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"
  - RFC 4158: "Certification Path Building"
  - RFC 4210: "Certificate Management Protocol (CMP)"
  - RFC 4211: "Certificate Request Message Format (CRMF)"
  - RFC 4212: "Alternative Certificate Formats for the Public-Key Infrastructure Using X.509 (PKIX) Certificate Management Protocols"
  - RFC 4325: "Authority Information Access Certificate Revocation List (CRL) Extension"
  - RFC 4386: "Repository Locator Service"
  - RFC 4387: "Operational Protocols: Certificate Store Access via HTTP"
  - RFC 4476: "Attribute Certificate (AC) Policies Extension"

- RFC 4491: "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with PKIX"

- **S/MIME:** S/MIME Mail Security
  - RFC 2311: "S/MIME Version 2 Message Specification"
  - RFC 2312: "S/MIME Version 2 Certificate Handling"
  - RFC 2630: "Cryptographic Message Syntax"
  - RFC 2631: "Diffie-Hellman Key Agreement Method"
  - RFC 2632: "S/MIME Version 3 Certificate Handling"
  - RFC 2633: "S/MIME Version 3 Message Specification"
  - RFC 2634: "Enhanced Security Services for S/MIME"
  - RFC 2785: "Methods for Avoiding the 'Small-Subgroup' Attacks on the Diffie-Hellman Key Agreement Method for S/MIME"
  - RFC 2876: "Use of the KEA and SKIPJACK Algorithms in CMS"
  - RFC 2984: "Use of the CAST-128 Encryption Algorithm in CMS"
  - RFC 3058: "Use of the IDEA Encryption Algorithm in CMS"
  - RFC 3125: "Electronic Signature Policies"
  - RFC 3126: "Electronic Signature Formats for long term electronic signatures"
  - RFC 3183: "Domain Security Services using S/MIME"
  - RFC 3185: "Reuse of CMS Content Encryption Keys"
  - RFC 3211: "Password-based Encryption for CMS"
  - RFC 3217: "Triple-DES and RC2 Key Wrapping "
  - RFC 3218: "Preventing the Million Message Attack on Cryptographic Message Syntax"
  - RFC 3274: "Compressed Data Content Type for CMS"
  - RFC 3278: "Use of Elliptic Curve Cryptography (ECC) Algorithms in CMS"
  - RFC 3369: "Cryptographic Message (CMS)Syntax"
  - RFC 3370: "Cryptographic Message Syntax (CMS) Algorithms"
  - RFC 3394: "Advanced Encryption Standard (AES) Key Wrap Algorithm"
  - RFC 3537: "Wrapping a Hashed Message Authentication Code (HMAC) key ..."
  - RFC 3560: "Use of the RSAES-OAEP Key Transport Algorithm in CMS"
  - RFC 3565: "Use of the Advanced Encryption Standard (AES) Encryption Algorithm in CMS"
  - RFC 3657: "Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)"
  - RFC 3850: "S/MIME Version 3.1 Certificate Handling"
  - RFC 3851: "S/MIME Version 3.1 Certificate Message Specification"
  - RFC 3852: "Cryptographic Message Syntax (CMS)"
  - RFC 3854: "Securing X.400 Content with S/MIME"
  - RFC 3855: "Transporting S/MIME Objects in X.400"
  - RFC 4010: "Use of the SEED Encryption Algorithm in Cryptographic Message Syntax (CMS)"
  - RFC 4056: "Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)"

        - RFC 4134: "Examples of S/MIME Messages"
        - RFC 4262: "X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities"
        - RFC 4490: "Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)"
- **TLS:** Transport Layer Security
    - RFC 2246: "The TLS Protocol Version 1.0"
    - RFC 2712: "Addition of Kerberos Cipher Suites to TLS"
    - RFC 2817: "Upgrading to TLS Within HTTP/1.1"
    - RFC 2818: "HTTP Over TLS"
    - RFC 2830: "LDAP v3: Extension for Transport Layer Security"
    - RFC 3268: "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)"
    - RFC 3546: "Transport Layer Security (TLS) Extensions"
    - RFC 3749: "Transport Layer Security Protocol Compression Methods"
    - RFC 4132: "Addition of Camellia Cipher Suites to Transport Layer Security (TLS)"
    - RFC 4261: "Common Open Policy Service (COPS) Over Transport Layer Security (TLS)"
    - RFC 4279: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)"
    - RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1"
    - RFC 4366: "Transport Layer Security (TLS) Extensions"
    - RFC 4492: "Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)"
    - RFC 4507: "Transport Layer Security (TLS) Session Resumption without Server-Side State"
- SPKI: Simple Public Key Infrastructure
- OpenPGP: An Open Specification for Pretty Good Privacy
- IETF/W3C XML Signature WG
- IPSEC: IP Security Protocol
- IPSRA: IP Security Remote Access
- The venerable PEM specification:
    - RFC 1421 --- ASCII --- PostScript
    - RFC 1422 --- ASCII --- PostScript
    - RFC 1423 --- ASCII --- PostScript
    - RFC 1424 --- ASCII --- PostScript
- RFC 1847: "Security Multiparts for MIME"
- RFC 1848: "MIME Object Security Services (MOSS)"
- RFC 2015: "MIME Security with Pretty Good Privacy (PGP)"
- RFC 2480: "Gateways and MIME Security Multiparts"
- RFC 3156: "MIME Security with OpenPGP"
- RFC 3174: "US Secure Hash Algorithm 1 (SHA1)"

6.1.5 Standardy PKCS (Public-Key Cryptographic Standards)

Tyto standardy jsou dnes všeobecně známé a použité v celé řadě dnešních kryptografických produktů. Jedná se o de facto normy, které jsou v současné době vytvářeny v laboratořích firmy RSA Security (dříve RSA) ve spolupráci s řadou vývojářů z celého světa. Poprvé tyto standardy byly publikovány v roce 1991 jako výsledek jednání určité skupiny pracovníků, kteří implementovali technologii kryptografie s veřejným klíčem (publikováno na : NIST/OSI Implementors' Workshop, dokument SEC-SIG-91-16.) V roce 1993 bylo zveřejněno prvních deset standardů ve formální podobě, která je dodnes zachovávána.
Od té doby byly několikráte upravovány a doplňovány. Původní standardy PKCS #2 a PKCS#4 byly včleněny do PKCS #1 a tato čísla již nebyla obsazena.

Dnes existují následující PKCS:

- **PKCS #1:RSA Cryptography Standard**
- **PKCS #3:Diffie-Hellman Key Agreement Standard**
- **PKCS #5:Password-Based Cryptography Standard**
- **PKCS #6:Extended-Certificate Syntax Standard**
- **PKCS #7:Cryptographic Message Syntax Standard**
- **PKCS #8:Private-Key Information Syntax Standard**
- **PKCS #9:Selected Attribute Types**
- **PKCS #10:Certification Request Syntax Standard**
- **PKCS #11:Cryptographic Token Interface Standard**
- **PKCS #12:Personal Information Exchange Syntax Standard**
- **PKCS #13: Elliptic Curve Cryptography Standard**
- **PKCS #15: Cryptographic Token Information Format Standard**

Všechny tyto normy jsou relevantní při řešení úschovy elektronických dokumentů, pokud se využívá digitální podpis, či zabezpečení dat šifrováním.

6.1.6 Standardy projektu LTANS

LTANS (Long-term Archive and Notary Services)

webovská stránka ltans: http://ltans.edelweb.fr/

Přehled relevantních návrhů standardů (zatím draft):

ERS (Evidence Record Syntax) http://tools.ietf.org/wg/ltans/draft-ietf-ltans-ers/draft-ietf-ltans-ers-09.txt , January 04, 2007

LTAP (Long-term Archive Protocol) http://www.ietf.org/internet-drafts/draft-ietf-ltans-ltap-03.txt , 23.10.2006

Long-term Archive Service Requirements – http://ltans.edelweb.fr/draft-ietf-ltans-reqs-05.txt, říjen 2005