ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor 2004**

	Informační technologie - Bezpečnostní techniky - Specifikace služeb TTP na podporu aplikace digitálních podpisů	ČSN ISO/IEC 15945 36 9793

Information technology - Security techniques - Specification of TTP services to support the application of digital signatures

Technologies de l’information - Techniques de sécurité - Spécifications des services TTP pour supporter l’application des
signatures numériques

Informationstechnik - IT-Sicherheitsverfahren - Specifikation der Dienste eines Trust-Zenters zur Unterstützung der
Anwendung von Digitalen Signaturen

Tato norma je českou verzí mezinárodní normy ISO/IEC 15945:2002. Mezinárodní norma ISO/IEC 15945:2002
má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 15945:2002. The International
Standard ISO/IEC 15945:2002 has the status of a Czech Standard.

69321

Národní předmluva

Citované normy

Doporučení ITU-T X.501 (1997) | ISO/IEC 9594-2:1998 dosud nezavedena

Doporučení ITU-T X.509 (2000) | ISO/IEC 9594-8:2001 zavedena v ČSN ISO/IEC 9594-8:2003 (36 9671) Informační technologie - Propojení otevřených systémů - Adresář: Základní struktury certifikátu veřejného klíče a certifikátu atributu

Doporučení ITU-T X.520 (1997) | ISO/IEC 9594-6:1998 dosud nezavedena

Doporučení ITU-T X.680 (1997) | ISO/IEC 8824-1:1998 dosud nezavedena

Doporučení ITU-T X.681 (1997) | ISO/IEC 8824-2:1998 dosud nezavedena

Doporučení ITU-T X.682 (1997) | ISO/IEC 8824-3:1998 dosud nezavedena

Doporučení ITU-T X.683 (1997) | ISO/IEC 8824-4:1998 dosud nezavedena

Doporučení ITU-T X.690 (1997) | ISO/IEC 8825-1:1998 dosud nezavedena

Doporučení ITU-T X.810 (1995) | ISO/IEC 10181-1:1996 zavedena v ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury pro otevřené systémy: Přehled

Doporučení ITU-T X.813 (1996) | ISO/IEC 10181-4:1997 zavedena v ČSN ISO/IEC 10181-4:1999 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury pro otevřené systémy: Struktura nepopiratelnosti

ISO/IEC 9796-2:1997 zavedena v ČSN ISO/IEC 9796-2:1999 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy používající hašovací funkci, nahrazena ISO/IEC 9796-2:2000

ISO/IEC 9796-3:2000 zavedena v ČSN ISO/IEC 9796:3:2002 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech

ISO/IEC 10118-1:1994, nahrazena ISO/IEC 10118-1:2000, zavedena v ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně

ISO/IEC 10118-2:1994, nahrazena ISO/IEC 10118-2:2000 zavedena v ČSN ISO/IEC 10118-2:2002 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce využívající algoritmus n-bitové blokové šifry

ISO/IEC 10118-3:1998 zavedena v ČSN ISO/IEC 10118-3:2000 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Dedikované hašovací funkce, nahrazena ISO/IEC 10118-3:2003

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1:1998 (36 9785) Informační technologie -

Bezpečnostní techniky - Správa klíčů - Část 1: Všeobecně

ISO/IEC 11770-2:1996 zavedena v ČSN ISO/IEC 11770-2:1999 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 2: Mechanismy používající symetrické techniky

ISO/IEC 11770-3:1999 zavedena v ČSN ISO/IEC 11770-3:2002 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 13888-1:1997 zavedena v ČSN ISO/IEC 13888-1:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně

ISO/IEC 13888-2:1998 zavedena v ČSN ISO/IEC 13888-2:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost -Část 2: Mechanismy používající symetrické techniky

ISO/IEC 13888-3:1997 zavedena v ČSN ISO/IEC 13888-3:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost -Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 14888-1:1998 zavedena v ČSN ISO/IEC 14888-1:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně

ISO/IEC 14888-2:1999 zavedena v ČSN ISO/IEC 14888-2:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě

ISO/IEC 14888-3:1998 zavedena v ČSN ISO/IEC 14888-3:2001 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu

ISO/IEC 15946-2:2002 dosud nezavedena

Vysvětlivky k textu převzaté normy

Pro účely této normy je

1) anglický termín „out of band“ překládán jako „jiný než dohodnutý způsob komunikace“

2) anglický termín „nonce“ není překládán;

3) anglický termín „selfsigned“ je překládán jako „seboupodepsaný“

4) anglický termín „revocation“ je překládán jako „revokace“, možný překlad je rovněž „odvolání“

5) anglický termín „security“ je překládán jako „bezpečnost“.

Upozornění na národní poznámky

Do normy byla k článku 8.3.5.2 doplněna informativní národní poznámka.

Národní poznámka

Při implementaci tohoto Doporučení | Mezinárodní normy je třeba zohlednit, že případné rozpory budou

řešeny v novele zákona o elektronickém podpisu (např. čl. 5.1.1).

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Prázdná strana

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Specifikace služeb TTP na podporu aplikace digitálních podpisů

ISO/IEC 15945
První vydání
2002-02

ICS 35.040

Obsah

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (mezinárodní elektrotechnická komise) tvoří specializovaný systém světové normalizace. Národní orgány, které jsou členy ISO a IEC, se podílejí na vývoji mezinárodních norem prostřednictvím technických komisí, zřízených příslušnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 3 směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních

norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Je třeba upozornit, že některé prvky této mezinárodní normy mohou být předmětem patentových práv. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

ISO/IEC 15645 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT*, ve spolupráci s ITU-T. Identický text byl vydán jako Dop. ITU-T X.843.

Přílohy A až C této mezinárodní normy mají pouze informativní charakter.

Úvod

Vývoj informačních technologií stejně jako infrastruktury celosvětové komunikace dnes otevírá možnost implementovat elektronický obchod v ekonomicky významném rozsahu. Digitální podpisy jsou důležitou technikou, která dodává těmto komerčním aplikacím a dalším aplikačním oblastem, které vyžadují právně účinné elektronické transakce, bezpečnost.

Digitální podpisy jsou vhodné k zajištění integrity dat a k autentizaci účastníků transakcí. Mohou představovat analogii ručního podpisu u digitálních objednávek, nabídek a kontraktů. Nejdůležitější vlastností digitálních podpisů v tomto kontextu je, že osoba, která podepsala dokument, nemůže tuto skutečnost úspěšně popřít. Tato vlastnost se nazývá „nepopiratelnost vytvoření“ dokumentu.

V některých zemích a v mezinárodních souvislostech je prosazována legislativa týkající se digitálních podpisů s cílem podpořit rozvoj elektronického obchodu a dalších aplikačních oblastí, které vyžadují právně účinné elektronické transakce.

Existuje mnoho norem, které specifikují digitální podpisy a jejich využití k různému účelu, například. pro nepopiratelnost autentizace. Je implementováno nebo plánováno mnoho komerčních aplikací i služeb, nabízených důvěryhodnými třetími stranami ve spojení s digitálním podpisem. Pro ekonomicky a právně účinné celosvětové používání digitálních podpisů je nutná interoperabilita těchto TTP, mezi sebou navzájem a s komerčními aplikacemi.

Cílem tohoto Doporučení | Mezinárodní normy je definovat služby, požadované k podpoře aplikace digitálních podpisů pro nepopiratelnost vytvoření dokumentu. Protože použití mechanismů digitálního podpisu k zajištění nepopiratelnosti vytvoření dokumentu implikuje integritu dokumentu a autenticitu jeho tvůrce, mohou být služby popsané v tomto Doporučení | Mezinárodní normě také spojovány k implementaci služeb integrity a autenticity. Způsob, kterým je to provedeno, podporuje interoperabilitu mezi TTP i mezi TTP a komerčními aplikacemi.

POZNÁMKA Neexistuje žádný podstatný důvod, proč by mělo být požadováno, aby každá TTP plánující podporu digitálního podpisu nabízela všechny tyto služby. Je možné, aby mnoho TTP, nabízejících různé služby, spolupracovalo při podpoře použití digitálních podpisů. Ale z pohledu potenciálních komerčních aplikací může být požadován celý rozsah těchto služeb a v tomto scénáři se stává dokonce interoperabilita důležitější. Je to další důvod, proč shromáždit všechny tyto služby v jednom dokumentu.

1 Předmět normy

Toto Doporučení | Mezinárodní norma definuje ty služby TTP, které jsou potřebné k podpoře aplikace digitálních podpisů pro účely nepopiratelnosti vytvoření dokumentů.

Toto doporučení | Mezinárodní norma také definuje rozhraní a protokoly, aby umožnila interoperabilitu mezi entitami přidruženými k těmto službám TTP.

Definice technických služeb a protokolů jsou požadovány proto, aby vzaly v úvahu implementaci služeb TTP a souvisících komerčních aplikací.

Toto Doporučení | Mezinárodní norma se zaměřuje na:

– implementaci a interoperabilitu;

– specifikaci služeb a

– technické požadavky.

Toto Doporučení | Mezinárodní norma nepopisuje management TTP nebo jiné organizační, provozní nebo personální problémy. O těchto tématech je převážně pojednáváno v Dop. ITU-T X.842 | ISO /IEC TR 14516, *Informační technologie - Bezpečnostní techniky - Směrnice k používání a managementu služeb důvěryhodných třetích stran.*

POZNÁMKY

1 Protože hlavním tématem tohoto Doporučení | Mezinárodní normy je interoperabilita, platí následující omezení:

i) V tomto Doporučení | Mezinárodní normě jsou uvedeny pouze ty služby, které mohou TTP nabídnout koncovým entitám nebo jiné TTP.

ii) Jsou uvedeny pouze služby, které mohou být vyžadovány a/nebo dodány prostřednictvím digitálních zpráv, které mohou být předmětem normalizace.

iii) Podrobně jsou specifikovány pouze ty služby, pro které mohou být dohodnuty v době vydání tohoto Doporučení | Mezinárodní normy široce akceptovatelné normalizované zprávy.

Další služby budou specifikovány v samostatných dokumentech, až budou mít k dispozici široce akceptovatelné normalizované zprávy. Zejména budou definovány v samostatném dokumentu služby pro vyznačení času.

2 Datové struktury a zprávy v tomto Doporučení | Mezinárodní normě budou specifikovány v souladu s dokumenty RFC, RFC 2510 a RFC 2511 (pro služby managementu certifikátu) a RFV 2560 (pro služby OCSP). Formát žádosti o certifikát také umožňuje interoperabilitu s PKCS#10. Odkazy na dokumenty zmíněné v této poznámce jsou uvedeny v příloze C.

3 Další normalizační snahy o služby TTP existují ve specifických prostředích a aplikacích, jako je SET nebo EDIFACT. Ty jsou mimo rozsah tohoto Doporučení | Mezinárodní normy.

4 Toto Doporučení | Mezinárodní norma definuje pro tyto služby technické specifikace. Tyto specifikace

jsou nezávislé na politikách, specifických právních předpisech a organizačních modelech (které mohou například definovat, jak jsou sdíleny povinnosti a odpovědnosti mezi Certifikačními autoritami a Registračními autoritami). Politika TTP, nabízející služby popsané v tomto Doporučení | Mezinárodní normě, bude muset samozřejmě specifikovat, jak bude TTP splňovat právní předpisy a další aspekty, zmíněné dříve. Zejména musí politika specifikovat, jak je určena validita digitálních podpisů a certifikátu.

-- Vynechaný text --