ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Červen

2001

	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu	ČSN ISO/IEC 14888-3 36 9788

Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms

Technologies de l'information - Techniques de sécurité - Signatures digitales avec appendice - Partie 3: Mécanismes fondés sur certificat

Informationstechnik - IT Sicherheitsverfahren - Digitale Signaturen mit Anhang - Teil 3: Zertifikatsbasierte Mechanismen

Tato norma je českou verzí mezinárodní normy ISO/IEC 14888-3:1998. Mezinárodní norma ISO/IEC 14888-3:1998 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 14888-3:1998. The International Standard ISO/IEC 14888-3:1998 has the status of a Czech Standard.

61281

Národní předmluva

Citované normy

ISO/IEC 14888-1:1998 zavedena v ČSN ISO/IEC 14888-1 (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 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě

ISO/IEC 9796:1991 zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schéma digitálního podpisu umožňující obnovu zprávy

ISO/IEC 9796-2:1997 zavedena v ČSN ISO/IEC 9796-2 (36 9780) Informační technologie - Bezpečnostní techniky - Schéma digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy používající hash funkci

ISO/IEC 10118-3:1998 zavedena v ČSN ISO/IEC 10118-3 (36 9930) Informační technologie - Bezpečnostní techniky - Hash funkce - Část 3: Dedikované hash funkce

ISO/IEC 10118-4:1998 zavedena v ČSN ISO/IEC 10118-4 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu	**ISO/IEC 14888-3** První vydání 1998-12-15 Opraveno a přetisknuto 1999-12-15

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 mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

ISO a IEC ustavily v oblasti informačních technologií společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Mezinárodní norma ISO/IEC 14888-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

ISO/IEC 14888 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem:*

- *Část 1: Všeobecně*
- *Část 2: Mechanismy založené na identitě*
- *Část 3: Mechanismy založené na certifikátu*

Mohou následovat další části.

Přílohy A a B jsou nedílnou součástí této části ISO/IEC 14888. Přílohy C až G jsou pouze informativní.

1 Předmět normy

ISO/IEC 14888 specifikuje mechanismy digitálního podpisu s dodatkem pro zprávy libovolné délky a lze ji použít k zajištění služeb autentizace původu dat, nepopiratelnosti a integrity dat.

Tato část ISO/IEC 14888 specifikuje mechanismy digitálního podpisu s dodatkem založené na certifikátu. Tato část ISO/IEC 14888 poskytuje zejména 1) obecný popis mechanismů digitálního podpisu založených na certifikátu, jejichž bezpečnost je založena na obtížnosti problému diskrétních logaritmů tvořících základ komutativních grup (viz kapitolu 6), 2) obecný popis mechanismů digitálního podpisu založených na certifikátu, jejichž bezpečnost je založena na obtížnosti faktorizace (viz kapitolu 7), a 3) řadu normativních mechanismů digitálního podpisu s dodatkem používajících mechanismy založené na certifikátu pro zprávy libovolné délky (viz přílohy A a B).

-- Vynechaný text --