ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Květen**
2001

	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně	ČSN ISO/IEC 14888-1 36 9788

Information technology - Security techniques - Digital signatures with appendix - Part 1: General

Technologies de l’information - Techniques de sécurité - Signatures digitales avec appendice - Partie 1: Généralités

Informationstechnik - IT Sicherheitsverfahren - Digitale Signaturen mit Anhang - Teil 1: Allgemeines Modell

Tato norma je českou verzí mezinárodní normy ISO/IEC 14888-1:1998. Mezinárodní norma ISO/IEC 14888-1:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 14888-1:1998. The International Standard ISO/IEC 14888-1:1999 has the status of a Czech Standard.

60509

Národní předmluva

Citované normy

ISO/IEC 9796:1991 zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy, nahrazena ISO/IEC 9796-3:2000

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

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

ISO/IEC 11770-3:1999 dosud nezavedena

Vypracování normy

Zpracování normy: 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 umožňující obnovu zprávy - Část 1: Všeobecně

ISO/IEC 14888-1
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 navázalo pracovní styk.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Mezinárodní norma ISO/IEC 14888-1 byla připravena společnou technickou komisí ISO/IEC JTC1, *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 certifikátech*

Úvod

Mechanismy digitálního podpisu jsou asymetrické kryptografické techniky, které mohou být použity k zajištění služeb autentizace entit, autentizace původu dat, integrity dat a nepopiratelnosti. Existují dva druhy mechanismů digitálních podpisů:

– pokud proces ověření vyžaduje zprávu jako součást vstupu, mechanismus se nazývá „mechanismus podpisu s dodatkem“. Ve výpočtu dodatku je zapojena hašovací funkce. V ISO/IEC 10118 jsou specifikovány hašovací funkce určené pro použití v digitálních podpisech s dodatkem.

– pokud proces ověření zpřístupňuje zprávu společně s její specifickou redundancí (označovanou někdy jako stín zprávy), mechanismus se nazývá „mechanismus podpisu umožňující obnovu zprávy“. Schémata redundance navržená pro použití jako část schématu podpisu jsou specifikována v normě o více částech ISO/IEC 9796.

Tyto dva typy se vzájemně nevylučují. Konkrétně jakýkoliv mechanismus digitálního podpisu umožňující obnovu zprávy, např. mechanismus specifikovaný v ISO/IEC 9796, může být použit pro zajištění digitálního podpisu s dodatkem. V tomto případě je podpis vytvořen aplikací procesu podpisu na hašovací token zprávy.

---

1 Předmět normy

ISO/IEC 14888 specifikuje několik mechanismů digitálního podpisu s dodatkem pro zprávy libovolné délky. Tato část ISO/IEC 14888 obsahuje obecné principy a požadavky na digitální podpis s dodatkem. Obsahuje rovněž definice a označení společná pro všechny části ISO/IEC 14888.

-- Vynechaný text --