# ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Květen 2001**

| | | |
|---|---|---|
| | Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě | ČSN ISO/IEC 14888-2<br><br>36 9788 |

Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms

Technologies de l'information - Techniques de sécurité - Signatures digitales avec appendice - Partie 2: Mécanismes basés sur des identités

Informationstechnik -- IT Sicherheitsverfahren - Digitale Signaturen mit Anhang - Teil 2: Identitätsbasierte Mechanismen

Tato norma je českou verzí mezinárodní normy ISO/IEC 14888-2:1999. Mezinárodní norma ISO/IEC 14888-2:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 14888-2:1999. The International Standard ISO/IEC 14888-2:1999 has the status of a Czech Standard.



**61073**



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 14888-1 dosud nezavedena

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky k textu.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

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 2: Mechanismy založené na identitě** | **ISO/IEC 14888-2** První vydání 1999-12-15 |
| ICS 35.040 | |

Obsah

Strana

---

---

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 14888-2 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 certifikátech*

Mohou následovat další části.

Přílohy A a B této části ISO/IEC 14888 jsou pouze informativní.



# 1 Předmět normy

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

Tato část ISO/IEC 14888 specifikuje obecnou strukturu a základní procedury, které vytvářejí proces podpisu a ověření na identitě založeném mechanismu digitálního podpisu s dodatkem pro zprávy libovolné délky.

**-- Vynechaný text --**