ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Listopad**
2002

	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně	ČSN ISO/IEC 10118-1 36 9930

Information technology - Security techniques - Hash-functions - Part 1: General

Technologies de l’information - Techniques de sécurité - Fonctions de brouillage - Partie 1: Généralités

Informationstechnik - Sicherheitsverfahren - Hash-funktionnen - Teil 1: Allgemeines Modell

Tato norma je českou verzí mezinárodní normy ISO/IEC 10118-1:2000. Mezinárodní norma ISO/IEC 10118-1:2000 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10118-1:2000. The International Standard ISO/IEC 10118-1:2000 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 10118-1 (36 9930) z června 1996.

65541

Národní předmluva

Citované normy

ISO/IEC 9797-1 zavedena v ČSN ISO/IEC 9797-1 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC) - Část 1: Mechanismy používající blokovou šifru

ISO/IEC 9797-2 dosud nezavedena

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 1: Všeobecně

ISO/IEC 10118-1
2. vydání
2000-06

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 dotyčnou organizací a zabývajících se určitou oblastí technické činnosti. Technické komise ISO a IEC spolupracují v oblastech společných zájmů. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly uvedenými v části 3 směrnice ISO/IEC.

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

Pozornost je věnována možnosti, že některé prvky této části ISO/IEC 10118 mohou být předmětem patentových práv. ISO a IEC nesmí být považovány za zodpovědné za identifikaci jakýchkoliv nebo všech patentových práv.

Mezinárodní norma ISO/IEC 10118-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

Toto druhé vydání ruší a nahrazuje první vydání (ISO/IEC 10118-1: 1994), které bylo technicky revidováno, aby byl přidán všeobecný model hašovacích funkcí. Implementace, které vyhovují ISO/IEC 10118-1:1994 budou vyhovovat také tomuto vydání ISO/IEC 10118-1.

ISO/IEC 10118 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Hašovací funkce:*

– *Část 1: Všeobecně*

– *Část 2: Hašovací funkce používající algoritmus n-bitové blokové šifry*

– *Část 3: Dedikované hašovací funkce*

– *Část 4: Hašovací funkce používající modulární aritmetiku*

Příloha A je normativní součástí této části ISO/IEC 10118.

1 Předmět normy

ISO/IEC 10118 specifikuje hašovací funkce a je proto použitelná pro poskytnutí služeb autentizace, integrity a nepopiratelnosti. Hašovací funkce mapují pomocí specifikovaného algoritmu libovolné řetězce bitů na řetězce bitů pevné délky. Mohou být použity pro

– zredukování zprávy na krátký otisk, určený jako vstup pro mechanismus digitálního podpisu a

– předání daného bitového řetězce uživateli, aniž by došlo k vyzrazení tohoto řetězce.

POZNÁMKA Hašovací funkce specifikované v této části ISO/IEC 10118 nezahrnují použití tajných klíčů. Tyto hašovací funkce však mohou být použity společně s tajnými klíči k vytvoření autentizačních kódů zprávy . Kódy pro autentizaci zprávy (Message Authentication Codes - MAC) poskytují autentizaci původu dat i integritu zprávy. Výpočet MACu nalezne uživatel v ISO/IEC 9797.

Tato část ISO/IEC 10118 obsahuje definice, symboly, zkratky a požadavky, které jsou společné všem dalším částem ISO/IEC 10118.

-- Vynechaný text --