ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Listopad

2002

	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 2: Hašovací funkce používající *n*-bitovou blokovou šifru	ČSN ISO/IEC 10118-2 36 9930

Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an *n*-bit block cipher

Technologies de l'information - Techniques de sécurité - Fonctions de brouillage - Partie 2: Fonctions de brouillage
utilisant un chiffrement par blocs de *n* bits

Informationstechnik - Sicherheitsverfahren - Hash-Funktionnen - Teil 2: Hash-Funktionnen auf Basis eines
n-bit-Blockschlüssel-Algorithmus

Tato norma je českou verzí mezinárodní normy ISO/IEC 10118-2:2000. Mezinárodní norma ISO/IEC 10118-2:2000 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10118-2:2000. The International Standard ISO/IEC 10118-2:2000 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 10118-2 (36 9930) z června 1996.

65569

Národní předmluva

Citované normy

ISO/IEC 10116:1997 zavedena v ČSN ISO/IEC 10116 (36 9742) Informační technologie - Bezpečnostní techniky - Módy činnosti pro n-bitovou blokovou šifru

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

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 2: Hašovací funkce používající *n*-bitovou blokovou šifru

ISO/IEC 10118-2
2. vydání
2000-12

ICS 35.040

Deskriptory: informační technologie, bezpečnostní techniky, hašovací funkce, n-bitová bloková šifra, metoda doplnění, inicializační hodnota, kruhová funkce, výstupní transformace, DEA.

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 směrnic 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.

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 10118-2: 1994), které bylo technicky revidováno, aby vyhovovalo všeobecnému modelu popsanému v ISO/IEC 10118-1 a aby byly přidány dvě další hašovací funkce. Implementace, které vyhovují ISO/IEC 10118-2:1994, budou vyhovovat také tomuto vydání ISO/IEC 10118-2.

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 n-bitovou blokovou šifru*

– *Část 3: Dedikované hašovací funkce*

– *Část 4: Hašovací funkce používající modulární aritmetiku*

Přílohy A a B této části ISO/IEC 10118 jsou pouze informativní.

Úvod

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) věnují pozornost skutečnosti, že se prohlašuje, aby bylo možné vyhovět této části ISO/IEC 10118, že může dojít k použití patentu týkajícího se „Autentizace dat pomocí kódů detekce modifikace na základě veřejné jednosměrné šifrovací funkce“, (U.S. Patent 4,908,861, vydaný 1990-03-13).

ISO a IEC nezastávají žádné stanovisko pokud jde o důkaz, platnost a rozsah patentových práv.

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout licence s případnými zájemci z celého světa za rozumných a nediskriminačních podmínek. V tomto ohledu je prohlášení držitele patentového práva registrováno u ISO a IEC. Informace jsou dostupné na adrese:

Director of Licencing
International Business Machine Corporation
500 Columbus Avenue
Thornwood, NY 10594
U.S.A.

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.

1 Předmět normy

Tato část ISO/IEC 10118 specifikuje hašovací funkce, které využívají algoritmus *n*-bitové blokové šifry. Jsou proto vhodné pro prostředí, ve kterém je takový algoritmus již implementován.

Jsou specifikovány čtyři hašovací funkce. První poskytuje hašovací kódy o délce, která je menší nebo rovna *n*, kde *n* je délka bloku použitého algoritmu. Druhá poskytuje hašovací kódy o délce, která je menší nebo rovna 2*n*; třetí poskytuje hašovací kódy o délce, která je rovna 2*n* a čtvrtá poskytuje hašovací kódy o délce 3*n*. Všechny čtyři hašovací funkce specifikované v této části ISO/IEC 10118 vyhovují všeobecnému modelu specifikovanému v části 1 této mezinárodní normy.

-- Vynechaný text --