ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Říjen**
2004

	Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 3: Dedikované hašovací funkce	ČSN ISO/IEC 10118-3 36 9930

Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions

Technologies de l’information - Techniques de sécurité - Fonctions de brouillage - Partie 3: Fonctions de brouillage dédiées

Informationstechnik - Sicherheitsverfahren - Hash-Funktionen - Teil 3: Dedizierte Hash-Funktionen

Tato norma je českou verzí mezinárodní normy ISO/IEC 10118-3:2004. Mezinárodní norma ISO/IEC 10118-3:2004 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 10118-3:2004. The International Standard ISO/IEC 10118-3:2004 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 10118-3 (36 9930) z června 2000.

Národní předmluva

Změny proti předchozí normě

Ve třetím vydání ISO/IEC 10118-3 je uveden popis celkem sedmi odlišných dedikovaných hašovacích funkcí oproti původním třem.

Citované normy

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

Vysvětlivky k textu převzaté normy

Pro účely této normy se anglický termín round function překládá jako cyklická funkce.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 3: Dedikované hašovací funkce

ISO/IEC 10118-3
Třetí vydání
2004-03

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 další mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk. ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 2 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

ISO/IEC 10118-3 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT*.

Toto třetí vydání ruší a nahrazuje druhé vydání (ISO/IEC 10118-3:2003), které bylo technicky revidováno.

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*

Úvod

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že některé prvky této mezinárodní normy mohou být předmětem patentových práv.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu tohoto patentového práva.

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu je prohlášení držitele tohoto patentovaného práva registrováno u ISO a IEC. Informace lze získat u:

ISO/IEC JTC1/SC27 Standing Document 8 (SD8) "*Patent Information*"

Standing Document 8 (SD8) je veřejně přístupný na: http://www.ni.din.de/sc27.

Je třeba upozornit, že některé prvky této části mezinárodní normy mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

---

1 Předmět normy

Tato část ISO/IEC 10118 specifikuje dedikované hašovací funkce, tj. specificky navržené dedikované funkce. Hašovací funkce v této části ISO/IEC 10118 jsou založeny na iterativním použití cyklické funkce. Je specifikováno sedm odlišných cyklických funkcí, z nichž vzniknou odlišné dedikované hašovací funkce.

První a třetí dedikované hašovací funkce popsané v kapitole 7 a 9 poskytují hašovací kódy dlouhé až 160 bitů; druhá funkce uvedená v kapitole 8 poskytuje hašovací kódy dlouhé až 128 bitů; čtvrtá funkce uvedená v kapitole 10 poskytuje hašovací kódy dlouhé až 256 bitů; šestá funkce uvedená v kapitole 12 poskytuje hašovací kódy pevné délky 384 bitů; a pátá a sedmá funkce uvedené v kapitolách 11 a 13 poskytují hašovací kódy dlouhé až 512 bitů.

-- Vynechaný text --