ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen

2001

	Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 4: Mechanismy používající kryptografickou kontrolní funkci	ČSN ISO/IEC 9798-4 36 9743

Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function

Technologies de l'information - Techniques de sécurité - Authentification d'entité - Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Informationstechnik - IT-Sicherheitsverfahren - Authentifikation von Instanzen - Teil 4: Mechanismen auf Basis einer kryptographischen Prüffunktion

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-4:1999. Mezinárodní norma ISO/IEC 9798-4:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9798-4:1999. The International Standard ISO/IEC 9798-4:1999 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 9798-4 (36 9743) z června 1998.

61072

Národní předmluva

Citované normy

ISO/IEC 9797:1994 zavedena v ČSN ISO/IEC 9797 (36 9782) Informační technologie - Bezpečnostní techniky - Mechanismus integrity dat používající kryptografickou kontrolní funkci s využitím algoritmu blokové šifry, nahrazena ISO/IEC 9797-1:1999

ISO/IEC 9798-1:1997 zavedena v ČSN ISO/IEC 9798-1 (36 9743) Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - 1. část: Obecný model

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 - Autentizace entit - Část 2: Mechanismy používající kryptografickou kontrolní funkci

ISO/IEC 9798-4

Druhé vydání

1999-12-15

ICS 35.040.00

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 komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 3 direktiv ISO/IEC.

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 ke schvalování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících členů.

Pozornost je nutno věnovat možnosti, že některé prvky této části ISO/IEC 9798 mohou být předmětem patentových práv. ISO a IEC nelze považovat za odpovědné za identifikování některých nebo všech

takových patentových práv.

Mezinárodní norma ISO/IEC 9798-4 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 9798-4:1995), jehož je technickou revizí. Implementace, které odpovídají ISO/IEC 9798-4 (první vydání), budou také odpovídat ISO/IEC 9798-4 (druhé vydání).

ISO/IEC 9798 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Autentizace entit:*

- *Část 1: Všeobecně*
- *Část 2: Mechanismy používající symetrické šifrovací algoritmy*
- *Část 3: Mechanismy používající techniky digitálního podpisu*
- *Část 4: Mechanismy používající kryptografickou kontrolní funkci*
- *Část 5: Mechanismy používající techniky s nulovými znalostmi*

Mohou následovat další části.

Příloha A této části ISO/IEC 9798 je pouze informativní.

---

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje mechanismy autentizace entit používající kryptografickou kontrolní funkci. Dva z nich se zabývají autentizací jednotlivé entity (unilaterální autentizace), zatímco zbývající mechanismy jsou určeny pro vzájemnou autentizaci dvou entit.

Mechanismy specifikované v této části ISO/IEC 9798 používají časově proměnné parametry jako jsou vyznačení času, pořadová čísla nebo náhodná čísla k tomu, aby se zabránilo akceptování platných autentizačních informací v pozdější době nebo více než jedenkrát.

Je-li použito vyznačení času nebo pořadové číslo, je pro unilaterální autentizaci nutný jeden průchod, zatímco k dosažení vzájemné autentizace jsou nutné dva průchody. Je-li použita metoda výzvy a odpovědi, využívající náhodná čísla, jsou pro unilaterální autentizaci nutné dva průchody, zatímco k dosažení vzájemné autentizace jsou nutné tři průchody

Příklady kryptografických kontrolních funkcí jsou uvedeny v ISO/IEC 9797.

-- Vynechaný text --