ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Červen 1998

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 - Mécanismes d'authentification d'entité - Partie 4: Mécanismes utilisant une fonction cryptographique de vérification

Informationstechnik - Sicherheitsverfahren - Mechanismen zur Authentifikation von Instanzen - Teil 4: Mechanismen unter Benutzung einer kryptographischen Prüffunktion

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-4:1995. Mezinárodní norma ISO/IEC 97984:1995 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9798-4:1995. The International Standard ISO/IEC 9798-4:1995 has the status of a Czech Standard.

52002

Národní předmluva

Citované normy

ISO/IEC 9798-1:1991 zavedena v ČSN ISO/IEC 9798-1 Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit - Část 1: Obecný model (36 9743), nahrazena ISO/IEC 9798-1:1997

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie -
Bezpečnostní techniky - Autentizace entit -
Část 4: Mechanismy používající kryptografickou kontrolní funkci

ISO/IEC 9798-4
První vydání
1995-03-15

MDT 35.040.00

Deskriptory: data processing, information interchange, data transmission, protection of information, security techniques, authentication, message authentication codes, algorithms.

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 navázalo pracovní styk.

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

Mezinárodní norma ISO/IEC 9798-4 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* podkomise SC 27, *Bezpečnostní techniky IT.*

ISO/IEC 9798 se skládá z následujících částí se společným názvem *Informační technologie -*

Bezpečnostní techniky - Mechanismy autentizace entit:

- *Část 1: Všeobecný model*

- *Část 3: Autentizace entit používající algoritmus s veřejným klíčem*

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

- *Část 2: Mechanismy používající symetrické šifrovací algoritmy*

- *Část 4: Mechanismy používající kryptografickou kontrolní funkci*

- *Část 5: Mechanismy používající techniky s nulovým rozšířením znalostí*

POZNÁMKA - Úvodní prvek názvů částí 1 a 3 bude sjednocen s úvodním prvkem názvů částí 2, 4 a 5 při příští revizi částí 1 a 3 ISO/IEC 9798.

Mohou následovat další části.

Přílohy A, B, C a D této části ISO/IEC 9798 jsou pouze pro informaci.

1 Předmět normy

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

Mechanismy specifikované v této části ISO/IEC 9798 používají časově proměnné parametry jako je označení času, pořadová čísla nebo náhodná čísla k tomu, aby se zabránilo použití platných autentizačních informací v pozdější době.

Jestliže je použito označení času nebo pořadové číslo, je pro unilaterální autentizaci nutný jeden průchod, zatímco k dosažení vzájemné autentizace jsou nutné dva průchody. Jestliže je použita metoda

výzvy a odpovědi, používající 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 příloze C.

-- Vynechaný text --