



**Informační technologie - Bezpečnostní techniky -
Mechanismy autentizace entit -
Část 3: Autentizace entit používající algoritmus
s veřejným klíčem**

**ČSN
ISO/IEC 9798-3**

36 9743

Information technology - Security techniques - Entity authentication mechanisms Part 3: Entity authentication using a public key algorithm

Technologies de l'information - Techniques de sécurité - Mécanismes d'authentification d'entités
Partie 3: Authentification d'entité utilisant un algorithme à clé publique

Informationstechnik - Sicherheitsverfahren - Mechanismen zur Authentifikation von Instanzen Teil 3:
Authentifikation von Instanzen unter Benutzung eines Algorithmus mit öffentlichen Schlüssel

Tato norma je identická s ISO/IEC 9798-3:1993.

This standard is identical with ISO/IEC 9798-3:1993.

Národní předmluva

Vypracování normy

Zpracovatel: Ing. Hana Pačesová, CSc., IČO 7919

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Ó Český normalizační institut, 1997

Prázdná strana!

MEZINÁRODNÍ NORMA
Informační technologie -
Bezpečnostní techniky -
Mechanismy autentizace entit -
Část 3: Autentizace entit
používající algoritmus s veřejným klíčem.

ČSN ISO/IEC 9798-3
První vydání
1993-11-15

MDT 681.3:621.39:003.26

Deskriptory: data processing, data transfer, information interchange, protection of information, authentication, algorithms.

Předmluva

ISO (Mezinárodní organizace pro normalizaci) a IEC (Mezinárodní elektrotechnická komise) vytvářejí specializovaný systém celosvětové normalizace. Národní organizace, které jsou členy ISO nebo IEC, se účastní prací na vývoji mezinárodních norem prostřednictvím technických komisí, ustavených příslušnými organizacemi pro práci na jednotlivých úsecích 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 navázalo pracovní styk.

V oblasti informačních technologií ustavilo ISO a IEC 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 9798-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie, podvýbor SC 27, Bezpečnostní techniky IT.*

ISO/IEC 9798 sestává z následujících částí pod obecným názvem *Informační technologie - Bezpečnostní techniky - Mechanismy autentizace entit*:

- 1. část: *Obecný model*
- 2. část: *Autentizace entit používající symetrické techniky*
- 3. část: *Autentizace entit používající algoritmus s veřejným klíčem*

Mohou následovat další části.

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

1 Předmět normy

Tato část ČSN ISO/IEC 9798 specifikuje mechanismy autentizace entit používající algoritmus s veřejným klíčem. Dva mechanismy jsou určeny pro autentizaci jedné entity (unilaterální autentizace), zbývající pro vzájemnou autentizaci dvou entit. Digitální podpis je používán k ověření identity určité entity. Procesu se může účastnit třetí strana.

Mechanismy specifikované v této části ISO/IEC 9798 používají parametry proměnné s časem jako 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

Strana 4

výzvy a odpovědi používající náhodná čísla, jsou pro unilaterální autentizaci nutné dva průchody, zatímco k dosažení vzájemné autentizace jsou nutné tři nebo čtyři průchody (v závislosti na použitém mechanismu).

-- Vynechaný text --