



**Informační technologie -
Bezpečnostní techniky -
Mechanismy autentizace entit -
1. část: Obecný model**

Květen 1997

**ČSN
ISO/IEC 9798-1**

36 9743

Information technology - Security techniques - Entity authentication mechanisms - Part 1: General model

Technologies de l'information - Techniques de sécurité - Mécanismes d'authentification d'entités
Partie 1: Modèle général

Informationstechnik - Sicherheitsverfahren Mechanismen zur Authentifikation von Instanzen - Teil 1:
Allgemein Modell

Tato norma je identická s ISO/IEC 9798-1:1991.

This standard is identical with ISO/IEC 9798-1:1991.

Vypracování normy

Zpracovatel normy: Ing. Hana Pačesová, CSc.

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Ó Český normalizační institut, 1997

21610

MEZINÁRODNÍ NORMA
Informační technologie -
Bezpečnostní techniky -
Mechanismy autentizace entit -

ISO/IEC 9798-1
První vydání
1991-09-01

1. Část: Obecný model

MDT: 681.32:621.39:003.26

Deskriptory: data processing, data transmission, information interchange, protection of information, authentication,

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 9798-1 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*. ISO/IEC 9798 sestává z následujících částí pod obecným názvem *Informační technologie - Bezpečnostní techniky - Mechanismus autentizace entit*:

- 1. část: *Obecný model*
- 2. část: *Autentizace entit s využitím symetrických technik*
- 3. část: *Autentizace entit s využitím algoritmu s veřejným klíčem*

Příloha A této části ISO/IEC 9798 má pouze informativní charakter.

ÚVOD

Mechanismus autentizace entit umožňuje ověření identity, prohlašované jednou entitou, jinou entitou.

Autenticita entit může být zjištěna pouze v okamžiku autentizační výměny. Aby mohla být zaručena autenticita následných vyměněných dat, musí být autentizační výměna použita společně s bezpečnými prostředky komunikace (např. se službou zajištění integrity).

Ten, kdo se vydává za jinou entitu, může uskutečnit k pozdějšímu datu opakovaný přenos platné autentizační výměny (je to forma „maskování se“). Jako ochrana před takovýmto opakovaným přenosem může být použit časově proměnný parametr, jako je označení času, pořadové číslo nebo výzva.

Entity obecně pro autentizační účely generují a uskutečňují výměnu normalizovaných zpráv, nazývaných token. Pro autentizaci jedné z entit jinou entitou je potřebná při nejmenším výměna jednoho tokenu a pro vzájemnou autentizaci při nejmenším výměna dvou tokenů. Další token může být potřebný tehdy, jestliže pro započítí autentizační výměny musí být odeslána výzva. Jednostranná autentizace poskytuje jedné entitě záruku o identitě jiné entity, ale ne naopak. Vzájemná autentizace poskytuje záruku o vzájemné identitě oběma entitám.

Strana 4

1 Předmět normy

Tato část ČSN ISO/IEC 9798 specifikuje mechanismy autentizace entit, používající bezpečnostní techniky. Tyto mechanismy jsou používány pro potvrzení, že entita je opravdu tou entitou, za kterou se prohlašuje. Entita, která má být autentizována, prokazuje svoji identitu znalostí určitého tajemství. Mechanismy jsou definovány jako výměny informací mezi entitami a, kde je to vyžadováno, výměnami s důvěryhodnou třetí stranou.

Podrobnosti mechanismů a obsahy autentizačních výměn nejsou v této části ISO/IEC 9798 specifikovány, ale jsou obsaženy v dalších částech této mezinárodní normy.

-- Vynechaný text --