ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Prosinec 2011**

Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 1: Všeobecně

ČSN ISO/IEC 9798-1
36 9743

Information technology – Security techniques – Entity authentication – Part 1: General

Technologies de l,information – Techniques de sécurité – Authentification d,entité – Partie 1: Généralités

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-1:2010. Překlad byl zajištěn Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 9798-1:2010. It was translated by Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 9798-1 (36 9743) z května 1997.

Národní předmluva

Změny proti předchozím normám

Toto třetí vydání je technickou revizí druhého vydání ISO/IEC 9798-1:1997.

Souvisící ČSN

ČSN EN ISO/IEC 7498-1:1997 (36 9614) Informační technologie – Propojení otevřených systémů – Základní referenční model – Základní model (ISO/IEC 7498-1:1994)

ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií. Prepojenie otvorených systémov (OSI). Základný referenčný model. Část 2: Bezpečnostná architektúra

ČSN ISO/IEC 9796-2:2004 (36 9780) Informační technologie – Bezpečnostní techniky – Schémata digitálního podpisu umožňující obnovu zprávy – Část 2: Mechanismy založené na faktorizaci celých čísel

ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů: Přehled

ČSN ISO/IEC 10181-2:1998 (36 9694) Informační technologie – Propojení otevřených systémů – Bezpečnostní struktury otevřených systémů: Struktura autentizace

ČSN ISO/IEC 13888-1 (36 9787) Informační technologie – Bezpečnostní techniky IT – Nepopiratelnost – Část 1: Všeobecně

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 20 Informační technologie

Pracovník Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 9798-1
Autentizace entit – Třetí vydání
Část 1: Všeobecně 2010-07

ICS 35.040

Obsah

ISO copyright office

Case postale 56 · CH-1211 Geneva 20

Tel. + 41 22 749 01 11

Fax + 41 22 749 09 47

E-mail copyright@iso.org

Web www.iso.org

Published in Switzerland

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 dotyčnou 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 JTC 1.

Návrhy mezinárodních norem jsou zpracovány v souladu s pravidly uvedenými v části 2 směrnic ISO/IEC.

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

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědným za identifikaci libovolného patentového práva nebo všech takových patentových práv.

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

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 9798-1:1997), jehož je technickou revizí.

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 nulových znalostí*
- *Část 6: Mechanismy používající manuální přenos dat*

Úvod

V systémech obsahujících komunikaci v reálném čase je autentizace entit bezpečnostní službou zásadního významu. V závislosti na konkrétní aplikaci a bezpečnostních cílech může autentizace entit zahrnovat použití jednoduchého protokolu s jedním průchodem poskytujícího jednostrannou autentizaci, nebo protokolu s více průchody poskytujícího jednostrannou nebo vzájemnou autentizaci mezi komunikujícími stranami.

Cílem autentizace entit je prokázat, zda nárokující strana prohlašující určitou identitu je opravdu tím, za koho se vydává. Aby se dosáhlo tohoto cíle, měla by zde být předem existující infrastruktura, která spojuje entitu s kryptografickým tajemstvím (například Infrastruktura veřejného klíče). Ustavení takové infrastruktury je mimo rozsah ISO/IEC 9798.

V ISO/IEC 9798 jsou specifikovány různé druhy protokolů autentizace entit, aby zajišťovaly různé bezpečnostní systémy a bezpečnostní cíle. Když například útoky opakovaného přenosu nejsou praktické nebo nejsou pro specifický systém problémem, postačí jednoduché protokoly s menším počtem průchodů mezi nárokující stranou a ověřovatelem. Avšak ve složitějších komunikačních systémech jsou skutečnou hrozbou útoky typu „man-in-the-middle“ a útoky opakovaného přenosu. V takových případech bude k dosažení bezpečnostních cílů systému nezbytný jeden ze složitějších protokolů z ISO/IEC 9798.

Existují dva hlavní modely autentizačních protokolů. V jednom modelu komunikují nárokující strana a ověřovatel přímo, aby potvrdily autenticitu identity nárokující strany. Ve druhém modelu prokazují entity autenticitu identit pomocí společné důvěryhodné třetí strany.

Bezpečnostní vlastnosti schématu, které musí být zváženy před výběrem autentizačního protokolu, zahrnují následující:

- prevenci útoku opakovaného přenosu;
- prevenci útoku zrcadlení (odrazem);
- prevenci vynuceného zpoždění;
- vzájemnou/jednostrannou autentizaci;
- zda může být použito předem ustavené tajemství, nebo je nutné zapojit důvěryhodnou třetí stranu, aby pomohla ustavit takové sdílené tajemství.

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje model autentizace a všeobecné požadavky a omezení pro mechanismy autentizace entit, které používají 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 jsou obsaženy v dalších částech ISO/IEC 9798.