ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Duben 2012**

Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 6: Mechanismy využívající manuální přenos dat

ČSN ISO/IEC 9798- 6
36 9743

Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer

Technologies de l,information – Techniques de sécurité – Authentification d,entité – Partie 6: Mécanismes utilisant un transfert manuel de données

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-6:2010. 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 9798-6:2010. It was translated by the Czech Office for Standards, Metrology and Testing. It has the same status as the official version.

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 9798-1:2010 zavedena v ČSN ISO/IEC 9798-1:2011 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 1: Všeobecně

Souvisící ČSN

ČSN ISO/IEC 10118-1:2002 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 1: Všeobecně

ČSN ISO/IEC 10118-3:2004 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 3: Dedikované hašovací funkce

ČSN ISO/IEC 10118-4:2001 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce – Část 4: Hašovací funkce používající modulární aritmetiku

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

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 9798-6
Autentizace entit – Druhé vydání
Část 6: Mechanismy využívající manuální přenos dat 2010-12

ICS 35.040

Obsah

Strana

Předmluva 5

Úvod 6

1 Předmět normy 7

2 Citované dokumenty 7

3 Termíny a definice 7

4 Symboly a zkrácené termíny 8

5 Celkové požadavky 9

6 Mechanismy používající krátkou kontrolní hodnotu 10

6.1 Obecně 10

6.2 Mechanismus 1 – Jedno zařízení s jednoduchým vstupem, jedno zařízení s jednoduchým výstupem 10

6.3 Mechanismus 2 – Zařízení s jednoduchými vstupními schopnostmi 11

7 Mechanismy používající manuální přenos krátké digest hodnoty nebo krátkého klíče 12

7.1 Obecně 12

7.2 Mechanismus 3 – Jedno zařízení s jednoduchým vstupem, jedno zařízení s jednoduchým výstupem 13

7.3 Mechanismus 4 – Jedno zařízení s jednoduchým vstupem, jedno zařízení s jednoduchým výstupem 14

7.4 Mechanismus 5 – Zařízení s jednoduchými vstupními schopnostmi 15

7.5 Mechanismus 6 – Zařízení s jednoduchými vstupními schopnostmi 16

8 Mechanismy používající MAC 17

8.1 Obecně 17

8.2 Mechanismus 7 – Zařízení s jednoduchými výstupními schopnostmi 18

8.3 Mechanismus 8 – Jedno zařízení s jednoduchým vstupem, jedno zařízení s jednoduchým výstupem 20

Příloha A (normativní) Moduly ASN.1 22

Příloha B (informativní) Použití protokolů manuální autentizace pro výměnu tajných klíčů 24

Příloha C (informativní) Použití protokolů manuální autentizace pro výměnu veřejných klíčů 26

Příloha D (informativní) O bezpečnosti mechanismu a volbách délky parametrů 28

Příloha E (informativní) Metoda pro generování krátkých kontrolních hodnot 30

Příloha F (informativní) Komparativní analýza bezpečnosti a efektivnosti mechanismu 1–8 32

Příloha G (informativní) Metody pro generování krátkých digest hodnot 34

Bibliografie 35

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 odpovědné za identifikaci jakéhokoliv nebo všech patentových práv.

Mezinárodní norma ISO/IEC 9798-6 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 9798-6:2005), ke kterému byla přidána nová kapitola 7, obsahující čtyři nové mechanismy. Zahrnuje také Technickou opravu ISO/IEC 9798-6:2005/Cor.1:2009. Implementace, které vyhovují prvnímu vydání, budou vyhovovat také druhému vydání.

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

- *Část 1: Všeobecně*
- *Část 2: Mechanismy využívající symetrické šifrovací algoritmy*
- *Část 3: Mechanismy využívající techniky digitálního podpisu*
- *Část 4: Mechanismy využívající kryptografickou kontrolní funkci*
- *Část 5: Mechanismy využívající techniky nulových znalostí*
- *Část 6: Mechanismy využívající manuální přenos dat*

Úvod

V sítích komunikačních zařízení je často pro dvě zařízení nutné provést proceduru autentizace entit s použitím kanálu, který může být předmětem jak pasivních, tak aktivních útoků, kde aktivní útok může zahrnovat zlovolnou třetí stranu, vkládající data do kanálu a/nebo modifikující, vymazávající nebo opakující data, která byla legitimně tímto kanálem poslána. Další části ISO/IEC 9798 specifikují mechanismy autentizace entit, použitelné v případech, kdy dvě zařízení sdílejí tajný klíč, nebo kde jedno zařízení má autentizovanou kopii veřejného klíče pro druhé zařízení.

V této části ISO/IEC 9798 jsou specifikovány mechanismy autentizace entit, nazývané manuální mechanismy autentizace, kde neexistuje takový předpoklad předem ustavených vztahů mezi klíči. Místo toho je autentizace entit dosaženo manuálním přenášením krátkých datových řetězců z jednoho zařízení na druhé, nebo manuálním porovná-váním krátkých datových řetězců, které jsou výstupem ze dvou zařízení.

Pro účely této části ISO/IEC 9798 je význam termínu autentizace entit odlišný od významu použitého v jiných částech ISO/IEC 9798. Místo ověřování jedním zařízením, že druhé zařízení má prohlašovanou identitu (a naopak), obě zařízení, které jsou ve vlastnictví uživatele, ověřují, že odpovídajícím způsobem sdílejí datový řetězec s druhým zařízením v době provedení mechanismu. Tento datový řetězec by měl samozřejmě obsahovat identifikátory pro jedno nebo obě zařízení.

Jak je popsáno v informativních přílohách B a C, mechanismus manuální autentizace může být použit jako základ pro ustavení tajného klíče nebo pro spolehlivou výměnu veřejných klíčů. Mechanismus manuální autentizace by mohl být také použit pro spolehlivou výměnu dalších tajných nebo veřejných bezpečnostních parametrů, včetně prohlášení bezpečnostní politiky nebo vyznačení času (časových razítek).

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje osm mechanismů autentizace entit založených na manuálním přenosu dat mezi autentizačními zařízeními. Označuje, jak mohou být tyto mechanismy použity k podpoře funkcí správy klíčů, a poskytuje návod na bezpečné volby parametrů pro mechanismy. Porovnává úrovně bezpečnosti a efektivnosti těchto osmi mechanismů.

Takové mechanismy mohou být vhodné v různých situacích. Jedna taková aplikace je v soukromých sítích, kde majitel dvou soukromých zařízení pro bezdrátovou komunikaci si přeje, aby uskutečnily postup autentizace entit jako část procesu jejich přípravy pro použití v síti.