ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Prosinec 2011**

Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 5: Mechanismy používající techniku nulových znalostí

ČSN ISO/IEC 9798-5
36 9743

Information technology – Security techniques – Entity authentication – Part 5: Mechanisms using zero-knowledge techniques

Technologies de l,information – Techniques de sécurité – Authentification d,entité – Partie 5: Mécanismes utilisant des techniques a divulgation nulle

Informationstechnik – Sicherheitsverfahren – Mechanismen zur Authentifikation von Instanzen – Teil 5: Mechanismen auf Basis von Zero-Knowledge-Techniken

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-5:2009. 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 9798-5:2009. It was translated by Czech Office for Standards, Metrology a Testing. It has the same status as the official version.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 9798-5 (36 9743) z července 2001.

Národní předmluva

Změny proti předchozím normám

Toto třetí vydání je technickou revizí druhého vydání z roku 2004. Přidává nové mechanismy založené na diskrétním logaritmu eliptických křivek.

Souvisící ČSN

ČSN ISO/IEC 9798-1:2011 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit – 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 11770-3:2002 (36 9785) Informační technologie – Bezpečnostní techniky – Správa klíčů – Část 3: Mechanismy používající asymetrické techniky

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 9798-5
Autentizace entit – Třetí vydání
Část 5: Mechanismy používající techniku nulových znalostí 2009-12

ICS 35.040

Obsah

Strana

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 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.

Mezinárodní norma ISO/IEC 9798-5 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

Třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 9798-5:2004), jehož je technickou revizí. Toto vydání přidává nové mechanismy založené na diskrétním logaritmu eliptických křivek.

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 techniku digitálního podpisu*
- *Část 4: Mechanismy používající kryptografickou kontrolní funkci*
- *Část 5: Mechanismy používající techniku nulových znalostí*
- *Část 6: Mechanismy používající manuální přenos dat*

Úvod

Tato část ISO/IEC 9798 specifikuje autentizační mechanismy, které zahrnují výměny informací mezi nárokující stranou a ověřovatelem.

Podle typů výpočtů, které bude provádět nárokující strana a ověřovatel, mohou být mechanismy rozděleny do následujících čtyř hlavních skupin (viz Přílohu C).

- První skupina (viz kapitoly 4 a 5) je charakterizována provedením krátkých modulárních umocňování. Velikost výzvy je třeba optimalizovat, protože má proporcionální dopad na pracovní zatížení.
- Druhá skupina (viz kapitoly 6, 7 a 8) je charakterizována možností „kupónové strategie“ pro nárokující stranu. Ověřovatel může autentizovat nárokující stranu s velmi omezenou výpočetní kapacitou. Velikost výzvy nemá na pracovní zatížení praktický dopad.
- Třetí skupina (viz 9.2) je charakterizována možností kupónové strategie pro ověřovatele. Ověřovatel s velmi omezenou výpočetní kapacitou může autentizovat nárokující stranu. Velikost výzvy nemá na pracovní zatížení žádný dopad.

- Čtvrtá skupina (viz 9.3) nemá možnost kupónové strategie.

ISO a IEC upozorňují na skutečnost, že existují prohlášení, že na shodu s touto částí ISO/IEC 9798 může mít vliv použití následujících patentů a jejich protějšků v ostatních zemích:

US 4 995 082 vydaný 1991-02-19, Autor: C.P. Schnorr,

US 5 140 634 vydaný 1992-08-18, Autor: L.C. Guillou a J-J. Quisquater,

EP 0 311 470 vydaný 1992-12-16, Autor: L.C. Guillou a J-J. Quisquater,

EP 0 666 664 vydaný 1995-02-02, Autor: M. Girault.

ISO a IEC nezaujímají žádné stanovisko k důkazům, platnosti a rozsahu těchto patentových práv.

Držitelé těchto patentových práv ujistili ISO a IEC, že jsou ochotni vyjednávat o licencích s uživateli po celém světě při zachování rozumných a nediskriminačních termínů a podmínek. V tomto smyslu jsou výroky držitelů těchto patentových práv organizacemi ISO a IEC zaprotokolovány. Informace je možné získat na adresách dále uvedených.

RSA Security Inc. Attention General Counsel 174 Middlesex Turnpike Bedford, MA 01730, USA	US 4 995 082
France Telecom R&D Service PIV 38-40 Rue du Général Leclerc F 92794 Issy les Moulineaux Cedex 9, France	US 5 140 634, EP 0 311 470, EP 0 666 664
Philips International B.V. Corporate Patents a Trademarks P.O. Box 220 5600 AE Eindhoven, The Netherlands	US 5 140 634, EP 0 311 470

France Telecom prohlašuje, že aplikace patentů ve vztahu ke kapitolám 6 (GQ2) a 8 (GPS2) čekají na projednání. Čísla patentů budou poskytnuta, jakmile budou k dispozici. ISO/IEC pak požádá o příslušné vyjádření.

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje mechanismy autentizace entit používající techniku nulových znalostí:

- mechanismy založené na identitách a poskytující jednostrannou autentizaci;
- mechanismy založené na faktorizaci celých čísel a poskytující jednostrannou autentizaci;
- mechanismy založené na diskrétních logaritmech vzhledem k číslům, která jsou buď prvočísla, nebo složená čísla, a poskytující jednostrannou autentizaci;
- mechanismy založené na asymetrických šifrovacích systémech a poskytující buď jednostrannou autentizaci, nebo vzájemnou autentizaci;
- mechanismy založené na diskrétních logaritmech eliptických křivek a poskytující jednostrannou autentizaci.

Tyto mechanismy jsou sestrojeny s použitím principů technik nulových znalostí, ale nejsou to nutně pro každou volbu parametrů nulové znalosti odpovídající přísné definici.