ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Prosinec 2011**

Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 2: Mechanismy využívající symetrické šifrovací algoritmy

ČSN ISO/IEC 9798-2
36 9743

Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms

Technologies de l,information – Techniques de sécurité – Authentification d,entité – Partie 2: Mécanismes utilisant des algorithmes de chiffrement symétriques

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-2:2008 včetně opravy ISO/IEC 9798-2:2008/Cor.1:2010-02. 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 9798-2:2008 including its Corrigendum ISO/IEC 9798-2:2008/Cor.1:2010-02. 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 9798-2 (36 9743) z prosince 2000.

Národní předmluva

Změny proti předchozím normám

Toto třetí vydání je technickou revizí druhého vydání ISO/IEC 9798-2:1999. Zahrnuje také technické korigendum ISO/IEC 9798-2/Cor.1:2004. Norma byla doplněna o kapitolu 7 „Mechanismy, které zahrnují třetí stranu“, normativní přílohu „OIDs a syntaxe ASN.1“ a informativní přílohu „Vlastnosti mechanismů autentizace entit“.

Informace o citovaných normativních dokumentech

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

Souvisící ČSN

ČSN ISO/IEC 9797-1:2001 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro

autentizaci zprávy (MAC) – Část 1: Mechanismy používající blokovou šifru

ČSN ISO/IEC 9798-5:2011 (36 9743) Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 5: Mechanismy používající techniku nulových znalostí

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 9798-2
Autentizace entit – Třetí vydání
Část 2: Mechanismy využívající symetrické šifrovací algoritmy 2008-12

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 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.

Mezinárodní norma ISO/IEC 9798-2 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 9798-2:1999), jehož je technickou revizí. Zahrnuje také Technickou opravu ISO/IEC 9798-2:1999/Cor.1:2004. Implementace, které vyhovují druhému vydání, budou vyhovovat také třetímu vydání.

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*

Další části mohou následovat.

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje mechanismy autentizace entit používající symetrické šifrovací algoritmy. Čtyři mechanismy zajišťují autentizaci entit mezi dvěma entitami, není-li zapojena žádná důvěryhodná třetí strana; dva z nich jsou mechanismy jednostranně autentizující jednu entitu druhé entitě, zatímco další dva jsou mechanismy pro vzájemnou autentizaci dvou entit. Zbývající mechanismy vyžadují důvěryhodnou třetí stranu k ustavení společného tajného klíče, a uskutečňují vzájemnou nebo jednostrannou autentizaci entit.

Mechanismy specifikované v této části ISO/IEC 9798 používají časově proměnné parametry, například vyznačení času (časové razítko), pořadová čísla nebo náhodná čísla, aby se zabránilo tomu, že bude platná autentizační informace akceptována později nebo více než jednou.

Není-li zapojena žádná důvěryhodná třetí strana a je použito vyznačení času (časové razítko) nebo pořadové číslo, je pro jednostrannou autentizaci potřebný jeden průchod, zatímco pro vzájemnou autentizaci jsou potřebné dva průchody. Není-li zapojena žádná důvěryhodná třetí strana a je použita metoda výzvy a odpovědi využívající náhodná čísla, jsou pro jednostrannou autentizaci potřebné dva průchody, zatímco pro vzájemnou autentizaci jsou potřebné tři průchody. Je-li důvěryhodná třetí strana zapojena, jakákoliv doplňková komunikace mezi entitou a důvěryhodnou třetí stranou vyžaduje v komunikační výměně dva další průchody.