ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Duben 2012**

Informační technologie – Bezpečnostní techniky – Autentizace entit – Část 3: Mechanismy využívající techniky digitálního podpisu

ČSN
ISO/IEC 9798-3+Amd. 1
36 9743

Information technology – Security techniques – Entity authentication –
Part 3: Mechanisms using digital signature techniques

Technologies de l,information – Techniques de sécurité – Authentification d,entité –
Partie 3: Mécanismes utilisant des techniques de signature numériques

Tato norma je českou verzí mezinárodní normy ISO/IEC 9798-3:1998 včetně změny ISO/IEC 9798-3:1998/Amd.1:2010 a včetně opravy ISO/IEC 9798-3:1998/Cor.1:2009-09. 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 9798-3:1998, including its Amendment ISO/IEC 9798-3:1998/Amd.1:2010 and including its Corrigendum ISO/IEC 9798-3:1998/Cor.1:2009-09. It was translated by the 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 9798-3 (36 9743) z června 1997.

Národní předmluva

Změny proti předchozí normě

Toto druhé vydání zrušuje a nahrazuje první vydání této normy, které bylo technicky revidováno. Implementace založené na prvním vydání budou vyhovovat také druhému vydání této normy.

Informace o citovaných dokumentech

ISO/IEC 9798-1:1997 nezavedena

Vysvětlivky k textu převzaté normy

Do normy jsou zapracovány změna ISO/IEC 9798-3:1998/Amd.1:2010 a oprava ISO/IEC 9798-3:1998/Cor.1:2009-09. Změny jsou v textu označeny svislou čárou. Na zapracované opravy upozorňuje národní poznámka.

Upozornění na národní poznámky

V kapitole 3 a v bibliografii je uvedena národní poznámka, která upozorňuje na zapracování opravy ISO/IEC 9798:1998/Cor.1:2009-09.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 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 9798-3
Autentizace entit – Druhé vydání
Část 2: Mechanismy využívající techniky digitálního podpisu 1998-10-15
+ ZMĚNA 1
2010-06-01

ICS 35.040

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 jakéhokoli nebo všech patentových práv.

Mezinárodní norma ISO/IEC 9798-3 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 9798-3:1993), které bylo technicky revidováno. Implementace, které vyhovují ISO/IEC 9798-3 (první vydání), budou vyhovovat také ISO/IEC 9798-3 (druhé vydání).

Změna 1 k ISO/IEC 9798-3:1998 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

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*

Další části mohou následovat.

Příloha A této části ISO/IEC 9798-3 je informativní a příloha B normativní.

1 Předmět normy

Tato část ISO/IEC 9798 specifikuje mechanismy autentizace entit používající digitální podpisy založené na asymetrických technikách. Dva mechanismy zajišťují autentizaci jednotlivé entity (jednostranná autentizace), zatímco zbývající mechanismy jsou určeny pro vzájemnou autentizaci dvou entit. K ověření identity entity je používán digitální podpis. Může být zapojena důvěryhodná třetí strana.

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.

Je-li použito vyznačení času (časové razítko) nebo pořadové číslo, je pro jednostrannou autentizaci potřebný jeden průchod, zatímco pro vzájemnou autentizaci jsou potřebné dva průchody. Je-li použita metoda výzvy a odezvy využívající náhodná čísla, jsou pro jednostrannou autentizaci potřebné dva průchody, zatímco pro vzájemnou autentizaci jsou potřebné tři nebo čtyři průchody (v závislosti na

použitém mechanismu).

Konec náhledu - text dále pokračuje v placené verzi ČSN.