ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Září 2013**

Informační technologie – Bezpečnostní techniky – Schémata digitálního podpisu umožňující obnovu zprávy – Část 3: Mechanismy založené na diskrétních logaritmech

ČSN ISO/IEC 9796-3
36 9780

Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms

Technologies de l,information – Techniques de sécurité – Schémas de signature numérique rétablissant le message –
Partie 3: Mécanismes basés sur les logarithmes discrets

Tato norma je českou verzí mezinárodní normy ISO/IEC 9796-3:2006. 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 9796-3:2006. 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 dokumentech

ISO/IEC 10118 (všechny části) zavedena v ČSN ISO/IEC 10118 (36 9930) Informační technologie – Bezpečnostní techniky – Hašovací funkce

ISO/IEC 15946-1:2002 nezavedena

Vysvětlivky k textu převzatého dokumentu

Anglický termín symbol se překládá českým slovem symbol, protože se zde používá ve významu nadřazeného termínu vůči podřazeným termínům: značky, znaky, označení atd., aby se všechny tyto termíny nemusely vypisovat.

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. Miroslav Škop

MEZINÁRODNÍ NORMA

Informační technologie – Bezpečnostní techniky – ISO/IEC 9796-3
Schémata digitálního podpisu umožňující obnovu zprávy – Druhé vydání
Část 3: Mechanismy založené na diskrétních logaritmech 2006-09

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 celosvětové normalizace. Národní orgány, které jsou členy ISO nebo IEC, se podílejí na vypracování mezinárodních norem prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. Technické komise ISO a IEC spolupracují v oborech společného zájmu. Práce se zúčastňují také další vládní a nevládní mezinárodní organizace, s nimiž ISO a IEC navázaly pracovní styk. V oblasti informační technologie zřídily ISO a IEC společnou technickou komisi ISO/IEC JTC 1.

Návrhy mezinárodních norem jsou vypracovávány v souladu s pravidly danými směrnicemi ISO/IEC, část 2.

Hlavním úkolem společné technické komise je vypracování mezinárodních norem. Návrhy mezinárodních norem přijaté společnou technickou komisí jsou rozesílány národním členům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % hlasujících národních orgánů.

ISO/IEC 9796-3 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise 27 *IT Bezpečnostní techniky*.

Toto druhé vydání zrušuje a nahrazuje první vydání (ISO/IEC 9796-3:2000), jehož je technickou revizí. Jsou specifikovány nové mechanismy a identifikátory objektů.

ISO/IEC 9796 se skládá z následujících částí se společným názvem *Informační technologie – Bezpečnostní*

techniky – Schémata digitálního podpisu umožňující obnovu zprávy:

- *Část 2: Mechanismy založené na faktorizaci celých čísel*
- *Část 3: Mechanismy založené na diskrétních logaritmech*

Úvod

Mechanismy digitálního podpisu mohou být použity k poskytování služeb, jako je například autentizace entit, autentizace původu dat, nepopiratelnost a integrita dat.

Mechanismus digitálního podpisu splňuje následující požadavky:

- je-li dán pouze veřejný ověřovací klíč, ale není dán soukromý podpisový klíč, je výpočetně neproveditelné vytvořit platný podpis pro jakoukoliv danou zprávu;
- podpisy vytvořené autorem podpisu nemohou být použity k vytvoření platného podpisu pro jakoukoliv novou zprávu ani pro obnovu podpisového klíče;
- je výpočetně neproveditelné, a to i pro autora podpisu, nalézt dvě odlišné zprávy s totožným podpisem.

Většina mechanismů digitálního podpisu je založena na asymetrických kryptografických technikách a zahrnuje tři základní operace:

- proces generování dvojic klíčů, kde každá dvojice obsahuje soukromý podpisový klíč a odpovídající veřejný ověřovací klíč;
- proces, který používá soukromý podpisový klíč, nazývající se ***proces generování podpisu***;
- proces, který používá veřejný ověřovací klíč, nazývající se ***proces ověření podpisu***.

Existují dva druhy mechanismů digitálních podpisů:

- jestliže pro každý daný soukromý podpisový klíč jsou podpisy vytvořené pro tutéž zprávu identické, mechanismus je označován ***bez prvků náhodného výběru*** (nebo ***deterministický***) [viz ISO/IEC 14888-1];
- jestliže pro danou zprávu a daný soukromý podpisový klíč vytvoří každá aplikace procesu podpisu odlišný podpis, mechanismus je označován ***s prvky náhodného výběru***.

Tato část ISO/IEC 9796 specifikuje mechanismy s prvky náhodného výběru.

Mechanismy digitálního podpisu je také možné rozdělit do dvou následujících kategorií:

- jestliže musí být celá zpráva uložena a/nebo přenesena společně s podpisem, mechanismus se nazývá ***mecha-***
  nismus podpisu s dodatkem [viz ISO/IEC 14888];
- jestliže může být z podpisu obnovena celá zpráva nebo její část, mechanismus se nazývá ***mechanismus podpisu umožňující obnovu zprávy***.

Jestliže je zpráva dostatečně krátká, pak může být celá zpráva obsažena v podpisu a obnovena z podpisu v procesu ověření podpisu. Jinak může být část zprávy obsažena v podpisu a zbytek uložen a/nebo přenesen společně s podpisem. Mechanismy specifikované v ISO/IEC 9796 umožňují buďto úplnou nebo částečnou obnovu s cílem snížit náklady na uložení a přenos.

Tato část ISO/IEC 9796 zahrnuje šest mechanismů, z nichž jeden byl obsažen v ISO/IEC 9796-3:2000 a pět z nich je obsaženo v ISO/IEC 15946-4:2004. Mechanismy specifikované v této části ISO/IEC 9796 používají hašovací funkci pro hašování celé zprávy. Hašovací funkce jsou specifikovány v ISO/IEC 10118. Některé z mechanismů specifikovaných v této části ISO/IEC 9796 používají grupu v eliptické křivce nad konečným polem. ISO/IEC 15946-1:2002 popisuje matematický základ a obecné techniky nutné pro implementování kryptosystémů založených na eliptických křivkách nad konečnými poli.

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňují na to, že je třeba věnovat pozornost skutečnosti, že vyhovění tomuto dokumentu může zahrnovat použití patentů týkajících se mechanismů NR, ECMR a ECAO uvedených v kapitole 8, 10 a 11, v tomto pořadí.

Oblast	**Patent číslo**	**Datum vydání**	**Autoři**
NR [viz kapitolu 8]	US 5 600 725, EP 0 639 907	1997-02-04	K. Nyberg a R. A. Rueppel
ECMR [viz kapitolu 10]	JP H09-160492 (aplikace patentu)		A. Miyaji
ECAO [viz kapitolu 11]	JP 3 434 251	2003-08-04	M. Abe a T. Okamoto

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

Držitelé těchto patentových práv ujistili ISO a IEC, že jsou ochotni dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu jsou prohlášení držitele těchto patentovaných práv registrována u ISO a IEC. Informace lze získat u následujících společností:

Patent číslo	**Název držitele patentových práv**	**Kontaktní adresa**
US 5 600 725, EP 0 639 907	Certicom Corp.	5520 Explorer Drive, 4th Floor, Mississauga, Ontario, Canada L4W 5L1
JP H09-160492	Matsushita Electric Industrial Co., Ltd.	Matsushita IMP Building 19th Floor, 1-3-7, Siromi, Chuo-ku, Osaka 540-6319, Japan
JP 3 434 251	NTT Intellectual Property Center	9-11 Midori-Cho 3-chome, Musashino-shi, Tokyo 180-8585, Japan

Je třeba upozornit na to, že některé prvky tohoto dokumentu mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech takovýchto patentových práv.

POZNÁMKA 1 Výpočetní proveditelnost závisí na konkrétních bezpečnostních požadavcích a na prostředí.

POZNÁMKA 2 Jakýkoliv mechanismus podpisu umožňující obnovu zprávy – například mechanismus specifikovaný v této části ISO/IEC 9796 – může být konvertován na poskytnutí digitálních podpisů s dodatkem. V tomto případě je podpis vytvořen aplikací mechanismu podpisu na hašovací token zprávy.

1 Předmět normy

Tato část ISO/IEC 9796 specifikuje šest schémat digitálních podpisů umožňujících obnovu zprávy. Bezpečnost těchto schémat je založena na obtížnosti problému diskrétních logaritmů, který je definován na konečném poli nebo na eliptické křivce nad konečným polem.

Tato část ISO/IEC 9796 také definuje volitelné řídící (kontrolní) pole v hašovacím tokenu, které může poskytnout podpisu další bezpečnost.

Tato část ISO/IEC 9796 specifikuje mechanismy s prvky náhodného výběru.

Mechanismy specifikované v této části ISO/IEC 9796 umožňují buďto úplnou nebo částečnou obnovu zprávy.

POZNÁMKA Schémata digitálního podpisu s dodatkem, založená na diskrétních logaritmech, jsou uvedena v ISO/IEC 14888-3.