ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Září 2013**

Informační technologie – Bezpečnostní techniky – Schémata digitálního podpisu umožňující obnovu zprávy – Část 2: Mechanismy založené na faktorizaci celých čísel

ČSN ISO/IEC 9796-2
36 9780

Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms

Technologies de l,information – Techniques de sécurité – Schémas de signature numérique rétablissant le message –
Partie 2: Mécanismes basés sur une factorisation entiere

Tato norma je českou verzí mezinárodní normy ISO/IEC 9796-2:2010. 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 9796-2:2010. 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 dokumentech

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

Souvisící ČSN

ČSN ISO/IEC 9797-2:2013 (36 9782) Informační technologie – Bezpečnostní techniky – Kódy pro autentizaci zprávy (MACs) – Část 1: Mechanismy používající blokovou šifru

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

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 9796-2
Schémata digitálního podpisu umožňující obnovu zprávy – Třetí vydání
Část 2: Mechanismy založené na faktorizaci celých čísel 2010-12

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 mezi-
národních 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 i 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.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. ISO a IEC nelze činit odpovědnou za identifikaci jakýchkoliv nebo všech patentových práv.

ISO/IEC 9796-2 vypracovala společná technická komise ISO/IEC JTC 1 *Informační technologie*, subkomise 27 *IT Bezpečnostní techniky*.

Toto třetí vydání zrušuje a nahrazuje druhé vydání (ISO/IEC 9796-2:2002), jehož je technickou revizí. Zahrnuje také změnu ISO/IEC 9796-2:2002/Amd.1:2008.

Implementace, které vyhovují ISO/IEC 9796-2 (první vydání) a které používají hašovací kód o délce nejméně 160 bitů, budou vyhovovat ISO/IEC 9796-2 (třetí vydání). Všimněme si však, že implementace, vyhovující ISO/IEC 9796-2 (první vydání), které používají hašovací kód o délce menší než 160 bitů, nebudou vyhovovat ISO/IEC 9796-2 (třetí vydání). Implementace, které vyhovují ISO/IEC 9796-2 (druhé vydání), budou vyhovovat ISO/IEC 9796-2 (třetí vydání).

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*

Další části mohou následovat.

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 ověřovací klíč, ale není dán podpisový klíč, musí být výpočetně neproveditelné vytvořit platný podpis pro jakoukoliv zprávu.
- Jsou-li dány podpisy vytvořené autorem podpisu, musí být výpočetně neproveditelné vytvořit platný podpis k nové zprávě nebo obnovit podpisový klíč.
- Musí být výpočetně neproveditelné, a to i pro autora podpisu, nalézt dvě odlišné zprávy s totožným podpisem.

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

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 podpisový klíč, nazývající se proces podpisu.
- Proces, který používá ověřovací klíč, nazývající se proces ověření.

Existují dva druhy mechanismů digitálních podpisů:

- Jestliže pro daný podpisový klíč jsou dva podpisy vytvořené pro tutéž zprávu identické, mechanismus se nazývá „bez prvků náhodného výběru“ (nebo deterministický); viz ISO/IEC 14888-1.
- Jestliže pro danou zprávu a podpisový klíč vytvoří každá aplikace procesu podpisu odlišný podpis, mechanismus se nazývá „s prvky náhodného výběru“.

První a třetí ze tří mechanismů specifikovaných v této části ISO/IEC 9796 jsou deterministické (bez prvků náhodného výběru), zatímco druhý mechanismus zahrnuje prvky náhodného výběru.

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

- Když musí být celá zpráva uložena a/nebo přenesena společně s podpisem, mechanismus se nazývá „mechanismus podpisu s dodatkem“ (viz ISO/IEC 14888).
- Když může být z podpisu obnovena celá zpráva nebo její část, mechanismus se nazývá „mechanismus podpisu umožňující obnovu zprávy“ [viz ISO/IEC 9796 (všechny části)].

POZNÁMKA 2 Jakýkoliv mechanismus podpisu umožňující obnovu zprávy, např. mechanismy specifikované v ISO/IEC 9796 (všechny části), může být přeměněn tak, aby poskytnul digitální podpis s dodatkem. Toho je možné dosáhnout aplikací mechanismu podpisu na hašovací kód odvozený jako funkce zprávy. Při použití tohoto přístupu se na něm musí dohodnout všechny strany generující a ověřující podpisy, a musí také mít prostředky k jednoznačné identifikaci hašovací funkce, která má být použita k vygenerování hašovacího kódu ze zprávy.

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

Mechanismy specifikované v této části ISO/IEC 9796 používají hašovací funkci pro hašování celé zprávy (eventuálně ve více než jedné části). Hašovací funkce pro digitální podpisy jsou specifikovány v ISO/IEC 10118.

1 Předmět normy

Tato část ISO/IEC 9796 specifikuje tři schémata digitálního podpisu umožňující obnovu zprávy, z nichž dvě jsou deterministická (bez prvků náhodného výběru) a jedno z nich zahrnuje prvky náhodného výběru. Bezpečnost všech tří schémat je založena na obtížnosti faktorizace velkých čísel. Všechna tři schémata mohou poskytovat buďto úplnou nebo částečnou obnovu zprávy.

Tato část ISO/IEC 9796 specifikuje metodu tvorby klíče pro tři schémata podpisu. Techniky pro správu klíčů a pro generování náhodných čísel (požadovaná u schématu podpisu s prvky náhodného výběru) jsou mimo rozsah této části ISO/IEC 9796.

První mechanismus specifikovaný v této části ISO/IEC 9796 je použitelný pouze v existujících implementacích, a je uchován z důvodu zpětné kompatibility.