

**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 entière

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

Související 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

Strana

Předmluva 6

Úvod 7

1 Předmět normy 8

2 Citované dokumenty 8

3 Termíny a definice 8

4 Symboly a zkrácené termíny 10

5 Konverze mezi řetězci bitů a celými čísly 11

6 Požadavky 11

7 Model procesu podpisu a procesu ověření 12

7.1 Obecně 12

7.2 Podpisování zprávy 13

7.2.1 Přehled 13

7.2.2 Alokace zprávy 13

7.2.3 Tvorba reprezentanta zprávy 13

7.2.4 Tvorba podpisu 13

7.3 Ověřování podpisu 13

7.3.1	Přehled	13
7.3.2	Otevírání podpisu	14
7.3.3	Obnova zprávy	14
7.3.4	Sestavení zprávy	14
7.4	Specifikování podpisového schématu	14
8	Schéma digitálního podpisu č. 1	14
8.1	Obecně	14
8.2	Parametry	14
8.2.1	Délka modulu	14
8.2.2	Volby pole koncového návěští	14
8.2.3	Kapacita	15
8.3	Tvorba reprezentanta zprávy	15
8.3.1	Hašování zprávy	15
8.3.2	Formátování	15
8.4	Obnova zprávy	16
9	Schéma digitálního podpisu č. 2	16
9.1	Obecně	16
9.2	Parametry	16
9.2.1	Délka modulu	16
9.2.2	Délka hodnoty salt	16
9.2.3	Volby pole koncového návěští	17
9.2.4	Kapacita	17
9.3	Tvorba reprezentanta zprávy	17
9.3.1	Hašování zprávy	17
9.3.2	Formátování	17
9.4	Obnova zprávy	17
10	Schéma digitálního podpisu č. 3	18

Příloha A (normativní) Modul ASN.1 19

A.1 Obecně 19

A.2 Použití následných identifikátorů objektů 21

Příloha B (normativní) Systém s veřejným klíčem pro digitální podpis 22

B.1 Termíny a definice 22

B.2 Symboly a zkratky 22

B.3 Tvorba klíčů 23

B.3.1 Veřejný ověřovací exponent 23

B.3.2 Tajné prvočíselné faktory a veřejné modulo 23

B.3.3 Soukromý podpisový exponent 23

B.4 Funkce tvorby podpisu 23

B.5 Funkce otevírání podpisu 24

B.6 Alternativní funkce tvorby podpisu 24

B.7 Alternativní funkce otevírání podpisu 24

Příloha C (normativní) Funkce generování masky 25

C.1 Symboly a zkratky 25

C.2 Požadavky 25

C.3 Specifikace 25

C.3.1 Parametry 25

C.3.2 Generování masky 25

Příloha D (informativní) O identifikátorech hašovacích funkcí a volbě obnovitelné délky zprávy 26

Příloha E (informativní) Příklady 27

E.1 Příklady s veřejným exponentem v hodnotě 3 27

E.1.1 Příklad procesu tvorby klíče 27

E.1.2 Příklady s úplnou obnovou 27

E.1.3 Příklady s částečnou obnovou 33

E.2 Příklady s veřejným exponentem v hodnotě 2 39

E.2.1 Příklad procesu tvorby klíče 39

E.2.2 Příklady s úplnou obnovou 39

E.2.3 Příklady s částečnou obnovou 44

Bibliografie 52

Odmítnutí odpovědnosti za manipulaci s PDF souborem

Tento soubor PDF může obsahovat vložené typy písma. V souladu s licenční politikou Adobe lze tento soubor tisknout nebo prohlížet, ale nesmí být editován, pokud nejsou typy písma, které jsou vloženy, používány na základě licence a instalovány v počítači, na němž se editace provádí. Při stažení tohoto souboru přejímají jeho uživatelé odpovědnost za to, že nebude porušena licenční politika Adobe. Ústřední sekretariát ISO nepřijímá za její porušení žádnou odpovědnost.

Adobe je obchodní značka „Adobe Systems Incorporated“.

Podrobnosti o softwarových produktech použitých k vytvoření tohoto souboru PDF lze najít ve Všeobecných informacích, které se vztahují k souboru; parametry, na jejichž základě byl PDF soubor vytvořen, byly optimalizovány pro tisk. Soubor byl zpracován s maximální péčí tak, aby ho členské organizace ISO mohly používat. V málo pravděpodobném případě, že vznikne problém, který se týká souboru, informujte o tom Ústřední sekretariát ISO na níže uvedené adrese.



DOKUMENT CHRÁNĚNÝ COPYRIGHTEM

© ISO/IEC 2010

Veškerá práva vyhrazena. Pokud není specifikováno jinak, nesmí být žádná část této publikace reprodukována nebo používána v jakékoliv formě nebo jakýmkoliv způsobem, elektronickým nebo mechanickým, včetně fotokopí a mikrofilmů, bez písemného svolení buď od organizace ISO na níže uvedené adrese, nebo od členské organizace ISO v zemi žadatele.

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, nepopíratelnost 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, nazývaný se proces podpisu.
- Proces, který používá ověřovací klíč, nazývaný 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 poskytl 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.

Konec náhledu - text dále pokračuje v placené verzi ČSN.