

	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 -
Část 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

Informationstechnik - Sicherheitsverfahren - Digitaler Unterschriftsmechanismus mit Rückgewinnung
der Nachricht -
Teil 2: Mechanismen auf der Basis der Faktorisierung ganzer Zahlen

Tato norma je českou verzí mezinárodní normy ISO/IEC 9796-2:2002. Mezinárodní norma ISO/IEC 9796-2:2002 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9796-2:2002. The International Standard ISO/IEC 9796-2:2002 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 9796-2 (36 9780) z července 1999.

Národní předmluva

Citované normy

ISO/IEC 9796-3:2000 zavedena v ČSN ISO/IEC 9796-3:2002 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 3: Mechanismy založené na diskretních logaritmech

ISO/IEC 9797-2:2001 dosud nezavedena

ISO/IEC 9798-1:1997 zavedena v ČSN ISO/IEC 9798-1:1999 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 1: Všeobecně

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

ISO/IEC 14888 (všechny části) zavedena v ČSN ISO/IEC 14888 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem

Národní poznámka

Pro účely této normy je anglický termín "salt" překládán jako „hodnota salt“. Anglický termín "randomized" je překládán jako „s prvky náhodného výběru“.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA

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

ISO/IEC 9796-2
Druhé vydání
2002-10-01

Odmítavé stanovisko k 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, ledaže by typy písma, které jsou vloženy, byly 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 vytváření tohoto souboru PDF, lze najít ve Všeobecných informacích, které jsou k souboru připojeny; parametry, pomocí kterých 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, tj. když vznikne problém, který se týká souboru, informujte o tom na níže uvedené adrese Ústřední sekretariát ISO.

Všechna práva vyhrazena. Není-li uvedeno jinak, nesmí být žádná část této publikace reprodukována nebo zpracována jakoukoli jinou formou, jako jsou například elektronické nebo mechanické prostředky, včetně fotokopíí a mikrofilmu, bez písemného povolení ISO; povolení lze vyžádat na níže uvedené adrese nebo u členské národní organizace 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.ch

Web www.iso.ch

Strana 4

Obsah

Strana

Úvod

..... 6

1 Předmět normy

.. 9

2 Normativní odkazy

9

3	Termíny a definice	9
4	Symboly a zkrácené termíny	11
5	Konverze mezi řetězcí bitů a celými čísly	12
6	Požadavky	13
7	Model procesu podpisu a procesu ověření	14
7.1	Podpisování zprávy	14
7.1.1	Přehled	14
7.1.2	Alokace zprávy	14
7.1.3	Tvorba reprezentanta zprávy	15
7.1.4	Tvorba podpisu	15
7.2	Ověřování podpisu	15
7.2.1	Přehled	15
7.2.2	Otevírání podpisu	15

7.2.3	Obnova zprávy	
..	15	
7.2.4	Kompletování zprávy	 16
7.3	Specifikace podpisového schématu.....	16
8	Schéma digitálního podpisu č. 1.....	16
8.1	Parametry	 16
8.1.1	Délka modulu	 16
8.1.2	Volby pole koncového návěští.....	16
8.1.3	Kapacita	 16
8.2	Tvorba reprezentanta zprávy.....	17
8.2.1	Hašování zprávy	 17
8.2.2	Formátování	 17
8.3	Obnova zprávy	 17
9	Schéma digitálního podpisu č.2.....	18

9.1	Parametry	
		
		18
9.1.1	Délka modulu	
		
	...	18
9.1.2	Délka hodnoty salt	
		18
9.1.3	Volby pole koncového návěští	
		18
9.1.4	Kapacita	
		
		19
9.2	Tvorba reprezentanta zprávy	
		19
9.2.1	Hašování zprávy	
		
		19
9.2.2	Formátování	
		
		19
9.3	Obnova zprávy	
		
	..	19
10	Schéma digitálního podpisu č. 3	
		20
Příloha A	(normativní) Systém s veřejným klíčem pro digitální podpis	
		21
Příloha B	(normativní) Funkce generování masky	
		25

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

Příloha D (informativní)

Příklady.....
27

Bibliografie

..... 54

Strana 6

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 příslušnou 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 JTC1.

Mezinárodní normy jsou navrhovány v souladu s pravidly obsaženými v části 3 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75 % z hlasujících členů.

ISO/IEC 9796-2 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

Toto druhé vydání ruší a nahrazuje první vydání (ISO/IEC 9796-2:1997), které bylo technicky revidováno. Implementace, které vyhovují ISO/IEC 9796-2 (první vydání) a které používají hašovací kód o délce nejméně 160 bitů, budou vyhovovat ISO/IEC 9796 (druhé vydání). Implementace vyhovující ISO/IEC 9796-2 (první vydání), které používají hašovací kód o délce menší než 160 bitů nebudou vyhovovat ISO/IEC 9796 (druhé vydání).

ISO/IEC 9796 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy*:

Část 1: Mechanismy používající redundanci

Část 2: Mechanismy založené na faktorizaci celých čísel

Část 3: Mechanismy založené na diskrétních logaritmech

Mohou následovat další části.

Úvod

Mechanismy digitálního podpisu mohou být použity k poskytování služeb, jako je např. 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 Výpočetní neproveditelnost 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 Jakýkoliv mechanismus 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 je 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.

Strana 8

Informace o patentech

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že vyhovění této části ISO/IEC 9796 může zahrnovat použití patentu týkajícího se „Schématu pravděpodobnostního podpisu“ (Patent U.S. 6 266 771 uveřejněný 2001-07-24).

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu tohoto patentového práva.

Držitel tohoto patentového práva ujistil ISO a IEC, že je ochoten dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu je prohlášení držitele tohoto patentovaného práva registrováno u ISO a IEC. Informace lze získat u:

University of California

Senior Licensing Officer

Office of Technology Transfer

1111 Franklin Street, 5th Floor

Oakland, California 94607-5200

USA

Je třeba upozornit na to, že některé prvky této části ISO/IEC 9796 mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

Strana 9

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.

Uživatelům této normy doporučujeme tam, kde je to možné, zvolit druhý mechanismus (schéma digitálního podpisu č. 2). V prostředích, kde je generování náhodných proměnných autorem podpisu považováno za neproveditelné, je však doporučeno schéma digitálního podpisu č. 3. Schéma digitálního podpisu č. 1 se použije pouze v prostředích, kde je vyžadována kompatibilita se systémy, které implementovaly první vydání této normy. Schéma digitálního podpisu č. 1 je však kompatibilní pouze se systémy, implementujícími první vydání této normy, které používají hašovací kódy dlouhé nejméně 160 bitů.

-- Vynechaný text --