ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Únor**
2002

	Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů 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 - Schéma de signature numérique rétablissant le message - Partie 3: Mécanismes basés sur les logarithmes discrets

Informationstechnik - IT Sicherheitsverfahren - Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht - Teil 3: Mechanismen auf Basis des diskreten Logarithmus

Tato norma je českou verzí mezinárodní normy ISO/IEC 9796-3:2000. Mezinárodní norma ISO/IEC 9796-3:2000 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9796-3:2000. The International Standard ISO/IEC 9796-3:2000 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 9796 (36 9780) ze srpna 1996.

63473

Národní předmluva

Citované normy

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

ISO/IEC 11770-3:1999 dosud nezavedena

ISO/IEC 14888-1:1998 zavedena v ČSN ISO/IEC 14888-1 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 1: Všeobecně

ISO/IEC 15946 (části 1 a 2, budou publikovány) dosud nezavedeny.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Schémata digitálních podpisů umožňující obnovu zprávy - Část 3: Mechanismy založené na diskrétních logaritmech

ISO/IEC 9796-3
První vydání
2000-04-15

Obsah

Strana

Úvod 6

1 Předmět normy 7

2 Normativní odkazy 7

3 Termíny a definice

..... 7

4 Označení, konvence a legenda k obrázkům..... 9

4.1 Označení a notace 9

4.2 Kódovací konvence, délka a velikost pole..... 10

4.3 Legenda k obrázkům 10

5 Požadavky 10

5.1 Volby pro svázání mechanismu podpisu a hašovací funkce..... 10

6 Proces podpisu 11

6.1 Vytvoření předběžného podpisu 11

6.2 Vytvoření hašovacího tokenu 11

6.3 Formátování datového vstupu 12

6.4 Výpočet podpisu 12

6.5 Formátování podepsané zprávy

..... 13

7 Proces ověření 13

7.1 Otevření podepsané zprávy 13

7.2 Obnovení předběžného podpisu a datového vstupu..... 14

7.3 Obnovení zprávy a (zkráceného) hašovacího tokenu..... 15

7.4 Opakovaný výpočet hašovacího tokenu..... 15

7.5 Porovnání obnovených a opakovaně vypočtených (zkrácených) hašovacích tokenů..... 15

8 Schémata podpisu umožňující obnovu zprávy..... 15

9 Schéma podpisu v poli prvočísel 15

9.1 Parametry domény 15

9.2 Podpis a ověřovací klíč 16

9.3 Randomizér a předběžný podpis..... 16

9.4 První část podpisu 16

9.5 Funkce podpisu .....

..... 16

9.6 Funkce ověření 16

9.7 Obnova datového vstupu 16

10 Schéma podpisu na eliptické křivce..... 16

10.1 Parametry domény 16

10.1.1 Rovnice a pravidla grupy pro pole nad prvočíslem..... 17

10.1.2 Rovnice a pravidla grupy pro pole nad mocninou dvou..... 17

10.2 Podpisový a ověřovací klíč 17

10.3 Randomizér a předběžný podpis..... 17

10.4 Výpočet první části podpisu 17

10.5 Funkce podpisu 17

10.6 Funkce ověření

..... 17

10.7 Obnova datového vstupu 17

Příloha A (normativní) Validace parametrů domény a veřejných klíčů..... 18

A.1 Schéma podpisu v poli prvočísel 18

A.1.1 Validace parametrů domény 18

A.1.2 Validace ověřovacího klíče 18

A.2 Schéma podpisu na eliptické křivce..... 18

A.2.1 Validace parametrů domény 18

A.2.2 Validace ověřovacího klíče 19

Příloha B (informativní) Numerické příklady I - Mechanismy podpisu v konečných polích..... 20

B.1 Příklady s částečnou obnovou..... 20

B.1.1 Příklad s hašovací funkcí SHA-1 (Dedikovaná hašovací funkce 3 z ISO/IEC 10118-3)..... 21

B.1.2 Příklad s hašovací funkcí RIPEMD-160 (Dedikovaná hašovací funkce 1 z ISO/IEC 10118-3)..... 21

B.1.3 Příklad s hašovací funkcí RIPEMD-128 (Dedikovaná hašovací funkce 2 z ISO/IEC 10118-3)..... 22

B.2 Příklady s úplnou obnovou..... 22

B.2.1 Příklad s hašovací funkcí RIPEMD -128 (Dedikovaná hašovací funkce 2 z ISO/IEC 10118-3)..... 23

Příloha C (informativní) Numerické příklady II - Mechanismy eliptických křivek..... 24

C.1 Eliptické křivky nad polem prvočísel..... 24

C.1.1 Příklad s hašovací funkcí RIPEMD-160 (Dedikovaná hašovací funkce 1 z ISO/IEC 10118-3)..... 24

C.1.2 Příklad s hašovací funkcí RIPEMD -128 (Dedikovaná hašovací funkce 2 z ISO/IEC 10118-3)..... 24

C.2 Eliptické křivky nad rozšířeným polem $GF(2^n)$..... 25

C.2.1 Příklad s hašovací funkcí RIPEMD 160 (Dedikovaná hašovací funkce 1 z ISO/IEC 10118-3)..... 25

C.2.2 Příklad s hašovací funkcí RIPEMD-128 (Dedikovaná hašovací funkce 2 z ISO/IEC 10118-3)..... 25

Příloha D (informativní) Informace o patentech..... 26

Bibliografie 27

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 mezinárodní komise, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrženy v souladu s pravidly uvedenými v Direktivách ISO/IEC, Část 3.

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC 1. Návrhy mezinárodních norem, přijaté společnou technickou komisí, se rozesílají národním orgánům k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Pozornost je věnována možnosti, že některé prvky této části ISO/IEC 9796 mohou být předmětem patentových práv. ISO a IEC nemohou být odpovědné za identifikaci některých nebo všech takovýchto práv.

Mezinárodní norma ISO/IEC 9796-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

Toto první vydání ruší a nahrazuje ISO/IEC 9796:1991, které bylo technicky revidováno.

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

– *Část 2: Mechanismy používající hash funkci*

– *Část 3: Mechanismy založené na diskrétních logaritmech*

Příloha A je nedílnou součástí této části ISO/IEC 9796. Přílohy B až D jsou pouze informativní.

Úvod

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

Mechanismus digitálního podpisu splňuje následující požadavky:

– za předpokladu, že je dán pouze ověřovací klíč a není dán podpisový klíč, je výpočetně neproveditelné vytvořit jakoukoliv zprávu a platný podpis pro tuto zprávu;

– podpisy vytvořené autorem podpisu nemohou být použity pro vytvoření jakékoliv nové zprávy a pro platný podpis pro tuto zprávu ani pro obnovu podpisového klíče;

– je výpočetně neproveditelné dokonce i pro autora podpisu nalézt dvě odlišné zprávy s tímtéž podpisem.

POZNÁMKA 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 sestává ze soukromého podpisového klíče a odpovídajícího veřejného ověřovacího klíče;

– proces použití podpisového klíče; tento proces se nazývá proces podpisu;

– proces použití ověřovacího klíče; tento proces se nazývá proces ověření.

Existují dva typy mechanismů digitálního podpisu:

– jestliže podpisy vytvořené pro stejnou zprávu jsou pro každý daný podpisový klíč totožné, mechanismus se nazývá nerandomizovaný (nebo deterministický, viz ISO/IEC 14888-1);

– jestliže každá aplikace procesu podpisu vytváří pro danou zprávu a daný podpisový klíč odlišný podpis, mechanismus se nazývá randomizovaný.

Schémata digitálního podpisu mohou být také rozdělena do těchto dvou kategorií:

– jestliže má být celá zpráva uložena a/nebo přenášena spolu s podpisem, mechanismus se nazývá „mechanismus podpisu s dodatkem“ (viz ISO/IEC 14888-1);

– jestliže je celá zpráva nebo její část obnovena z podpisu, mechanismus se nazývá „mechanismus podpisu umožňující obnovu zprávy“ (viz ISO/IEC 9796).

POZNÁMKA Jakýkoliv mechanismus podpisu umožňující obnovu zprávy, například mechanismus specifikovaný v ISO/IEC 9796, může být převeden na digitální podpis s dodatkem. V tomto případě je podpis vytvářen aplikací mechanismu podpisu na hašovací token zprávy.

Mechanismy specifikované v ISO/IEC 9796 poskytují úplnou nebo částečnou obnovu zprávy s cílem snížit použitou pamě» a přetížení přenosu.

Mechanismy použité v této části ISO/IEC 9796 používají hašovací funkci pro hašování celé zprávy. Hašovací funkce pro digitální podpisy jsou specifikovány v ISO/IEC 10118. Jestliže je zpráva dostatečně krátká, může být celá obsažena v podpisu a může být obnovena z podpisu v procesu ověření. V ostatních případech může být část zprávy obsažena v podpisu a její zbývající část je uložena a/nebo přenášena spolu s podpisem.

1 Předmět normy

Tato část ISO/IEC 9796 specifikuje dvě schémata randomizovaného digitálního podpisu umožňující obnovu zprávy. Bezpečnost obou schémat je založena na obtížnosti problému diskrétních logaritmů. První schéma je definováno v poli prvočísel a druhé na eliptické křivce.

Tato část normy také definuje schéma redundance s použitím hašovacích kódů a specifikuje, jakým způsobem se mají kombinovat základní podpisová schémata se schématy redundancí.

Tato část normy také popisuje volitelné kontrolní pole v hašovacím tokenu, které může poskytnout podpisu dodatečnou bezpečnost.

-- Vynechaný text --