

	Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu	ČSN ISO/IEC 14888-3 36 9788
---	---	---------------------------------------

Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms

Technologies de l'information - Techniques de sécurité - Signatures digitales avec appendice - Partie 3: Mécanismes fondés sur certificat

Informationstechnik - IT Sicherheitsverfahren - Digitale Signaturen mit Anhang - Teil 3: Zertifikatsbasierte Mechanismen

Tato norma je českou verzí mezinárodní normy ISO/IEC 14888-3:1998. Mezinárodní norma ISO/IEC 14888-3:1998 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 14888-3:1998. The International Standard ISO/IEC 14888-3:1998 has the status of a Czech Standard.

© Český normalizační institut,
2001

61281

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány
a rozšiřovány jen se souhlasem Českého normalizačního institutu.

Citované normy

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 14888-2:1999 zavedena v ČSN ISO/IEC 14888-2 (36 9788) Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 2: Mechanismy založené na identitě

ISO/IEC 9796:1991 zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schéma digitálního podpisu umožňující obnovu zprávy

ISO/IEC 9796-2:1997 zavedena v ČSN ISO/IEC 9796-2 (36 9780) Informační technologie - Bezpečnostní techniky - Schéma digitálního podpisu umožňující obnovu zprávy - Část 2: Mechanismy používající hash funkce

ISO/IEC 10118-3:1998 zavedena v ČSN ISO/IEC 10118-3 (36 9930) Informační technologie - Bezpečnostní techniky - Hash funkce - Část 3: Dedikované hash funkce

ISO/IEC 10118-4:1998 zavedena v ČSN ISO/IEC 10118-4 (36 9930) Informační technologie - Bezpečnostní techniky - Hašovací funkce - Část 4: Hašovací funkce používající modulární aritmetiku

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem - Část 3: Mechanismy založené na certifikátu	ISO/IEC 14888-3 První vydání 1998-12-15 Opraveno a přetisknuto 1999-12-15
---	--

ICS 35.040

Obsah

Strana

1 Předmět
normy

.....
.. 6

2	Normativní odkazy	6
3	Všeobecně	6
4	Definice	7
5	Symboly a notace	7
6	Mechanismy digitálního podpisu založené na diskretních logaritmech	8
6.1	Proces generování klíče	8
6.2	Proces podpisu	8
6.3	Proces ověření	11
7	Mechanismy digitálního podpisu založené na faktorizaci	13
7.1	Proces generování klíče	13
7.2	Proces podpisu	13
7.3	Proces ověření	14

Příloha A (normativní) Příklady digitálních podpisů s dodatkem, založených na certifikátu, využívajících diskretní

logaritmy.....	15
----------------	----

A.1 Příklady založené na neeliptických křivkách.....	15
--	----

A.1.0 Symboly a notace	
----------------------------------	--

.....	15
-------	----

A.1.1 U.S. Digital Signature Algorithm (DSA).....	15
---	----

A.1.2 Podpisy Pointchevala/Vaudenaye	
.....	17

A.2 Příklad založený na eliptických křivkách.....	19
---	----

A.2.1 DSA na bázi eliptických křivek.....	19
---	----

Příloha B (normativní) Příklad digitálních podpisů s dodatkem, založených na certifikátu, využívajících faktorizaci	
.....	22

B.1 Digitální podpisy s hašováním založené na ISO/IEC 9796.....	22
---	----

B.1.1 Generování parametrů domény.....	22
--	----

B.1.2 Generování podpisového klíče a ověřovacího klíče.....	22
---	----

B.1.3 Proces podpisu	
.....	22

B.1.4 Proces ověření	
.....	23

B.2 ESIGN	
.....	23

B.2.1 Generování parametrů	
-----------------------------------	--

domény..... 23

B.2.2 Generování podpisového klíče a ověřovacího
klíče..... 23

B.2.3 Proces
podpisu

.....
23

Strana 4

Strana

B.2.4 Proces
ověření

.....
. 24

Příloha C (informativní) FIPS PUB 186 Generování prvočísel P a
Q..... 25

Příloha D (informativní) Matematický základ eliptických
křivek..... 26

D.1 Eliptické křivky a

body.....
26

D.1.1 Pravidla pro sčítání eliptických křivek nad
 F_p 26

D.1.2 Pravidla pro sčítání eliptických křivek nad
 F_{2^m} 27

Příloha E (informativní) Numerické příklady digitálních podpisů s dodatkem, založených na
certifikátu..... 28

E.1 Algoritmus digitálního podpisu U.S. (U.S. Digital Signature Algorithm
(DSA))..... 28

E.1.1 Parametry
DSA

.....
. 28

E.1.2 Podpisový klíč DSA a ověřovací klíč
DSA..... 28

E.1.3 DSA na data
zprávy

..... 28

E.1.4	Podpis DSA.....	28
E.1.5	Ověřovací hodnoty DSA.....	28
E.2	Algoritmus podpisu Pointchevala/Vaudenaye.....	28
E.2.1	Parametry Pointchevala/Vaudenaye.....	28
E.2.2	Podpisový klíč a ověřovací klíč Pointchevala/Vaudenaye.....	29
E.2.3	Pointcheval/Vaudenay na data zprávy.....	29
E.2.4	Podpis Pointchevala/Vaudenaye.....	29
E.2.5	Hodnoty ověření Pointchevala/Vaudenaye.....	29
E.3	DSA na bázi eliptických křivek.....	29
E.3.1	Příklad 1: Pole F_2^m , m=191.....	29
E.3.2	Příklad 2: Pole F_p , 192-bitové prvočíslo p.....	30
E.4	Digitální podpis s hašováním založený na ISO/IEC 9796.....	31
E.4.1	Příklad s lichým v (v = 3).....	31
E.4.2	Příklad se sudým v (v = 2).....	32
E.5	Algoritmus podpisu ESIGN.....	34
E.5.1	Parametry domény ESIGN.....	34
E.5.2	Podpisový klíč a ověřovací	

klíč.....	34
-----------	----

E.5.3 Proces podpisu

ESIGN.....	35
------------	----

E.5.4 Ověření

ESIGN.....	37
------------	----

Příloha F (informativní) Požadované charakteristiky pro volbu podpisového schématu.....

38

Příloha G (informativní) Informace o

patentech.....	39
----------------	----

Bibliografie

.....	40
-------	----

Strana 5

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

ISO a IEC ustavily v oblasti informačních technologií 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 % hlasujících členů.

Mezinárodní norma ISO/IEC 14888-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

ISO/IEC 14888 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Digitální podpisy s dodatkem*:

- Část 1: Všeobecně
- Část 2: Mechanismy založené na identitě
- Část 3: Mechanismy založené na certifikátu

Mohou následovat další části.

Přílohy A a B jsou nedílnou součástí této části ISO/IEC 14888. Přílohy C až G jsou pouze informativní.

1 Předmět normy

ISO/IEC 14888 specifikuje mechanismy digitálního podpisu s dodatkem pro zprávy libovolné délky a lze ji použít k zajištění služeb autentizace původu dat, nepopiratelnosti a integrity dat.

Tato část ISO/IEC 14888 specifikuje mechanismy digitálního podpisu s dodatkem založené na certifikátu. Tato část ISO/IEC 14888 poskytuje zejména 1) obecný popis mechanismů digitálního podpisu založených na certifikátu, jejichž bezpečnost je založena na obtížnosti problému diskretních logaritmů tvořících základ komutativních grup (viz kapitolu 6), 2) obecný popis mechanismů digitálního podpisu založených na certifikátu, jejichž bezpečnost je založena na obtížnosti faktorizace (viz kapitolu 7), a 3) řadu normativních mechanismů digitálního podpisu s dodatkem používajících mechanismy založené na certifikátu pro zprávy libovolné délky (viz přílohy A a B).

-- Vynechaný text --