

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

Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms

Technologies de l'information - Techniques de sécurité - Signatures digitales avec appendice - Partie 2: Mécanismes basés sur des identités

Informationstechnik -- IT Sicherheitsverfahren - Digitale Signaturen mit Anhang - Teil 2: Identitätsbasierte Mechanismen

Tato norma je českou verzí mezinárodní normy ISO/IEC 14888-2:1999. Mezinárodní norma ISO/IEC 14888-2:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 14888-2:1999. The International Standard ISO/IEC 14888-2:1999 has the status of a Czech Standard.

© Český normalizační institut,
2001

61073

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

Citované normy

ISO/IEC 9796:1991 zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy; nahrazena ISO/IEC 9796-3:2000

ISO/IEC 14888-1 dosud nezavedena

Upozornění na národní přílohu

Do této normy byla doplněna národní příloha NA, která obsahuje vysvětlivky k textu.

Vypracování normy

Zpracovatel: Ing. Vladimír Pračke, IČO 40654419

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 2: Mechanismy založené na identitě	ISO/IEC 14888-2 První vydání 1999-12-15
ICS 35.040	

Obsah

Strana

1	Předmět normy	
..	6	
2	Normativní odkazy	
.....	6	
3	Všeobecně	
.....	6	
4		

Definice

..... 6

5

Notace

..... 7

5.1

Symboly

..... 7

6 Proces vytvoření

klíče..... 7

6.1 Generování parametrů

domény..... 7

6.2 Vytvoření ověřovacího klíče a generování podpisového

klíče..... 8

7 Proces

podpisu

..... 8

7.1 Vytvoření předběžného

podpisu..... 8

7.2 Příprava

zprávy

..... 9

7.3 Výpočet

svědka

..... 9

7.4 Výpočet

podpisu

..... 10

8 Proces

ověření

..... 11

8.1 Příprava

zprávy

.....
. 11

8.2 Získání
svědka

.....
. 11

8.3 Výpočet ověřovací
funkce.....

11

8.4 Ověření
svědka

.....
13

9 Mechanismus podpisu dle Guillou -
Quisquatera.....

13

9.1 Funkce pro odvození veřejného
klíče.....

13

9.2 Příprava
zprávy

.....
. 13

9.3 Výpočet
svědka

.....
13

9.4 Výpočet první části
podpisu.....

13

9.5 Výpočet
přiřazení

.....
13

10 Podpisy založené na identitě s krátkým
přiřazením.....

14

10.1 Příprava
zprávy

.....
. 14

10.2 Výpočet
svědka

.....
14

10.3 Výpočet přiřazení

.....
14

11 Podpisy založené na identitě umožňující obnovu hašovacího kódu zprávy..... 14

11.1 Výpočet svědka

.....
14

11.2 Výpočet první části podpisu..... 14

Příloha A (informativní) Numerické příklady..... 15

A.1 Numerický příklad procesu vytvoření klíče..... 15

Strana 4

Strana

A.1.1 Generování parametrů domény..... 15

A.1.2 Vytvoření ověřovacího a podpisového klíče..... 16

A.2 Numerický příklad Guillou-Quisquaterova mechanismu podpisu, popsaného v kapitole 9..... 16

A.2.1 Proces podpisu 16

A.2.2 Proces ověření 17

A.3 Numerický příklad mechanismu podpisu založeného na identitě s krátkým přiřazením, popsaného v kapitole 10 18

A.3.1 Proces

podpisu

.....
18

A.3.2 Proces

ověření

.....
. 19

A.4 Numerický příklad podpisů založených na identitě umožňujících obnovu hašovacího kódu zprávy,

popsaných v kapitole

11..... 20

A.4.1 Proces

podpisu

.....
20

A.4.2 Proces

ověření

.....
. 20

Příloha B

(informativní)

.....
22

Národní příloha NA

(informativní)

..... 23

Bibliografie

.....
..... 24

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 14888-2 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 certifikátech

Mohou následovat další části.

Přílohy A a B této části ISO/IEC 14888 jsou pouze informativní.

1 Předmět normy

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

Tato část ISO/IEC 14888 specifikuje obecnou strukturu a základní procedury, které vytvářejí proces podpisu a ověření na identitě založeném mechanismu digitálního podpisu s dodatkem pro zprávy libovolné délky.

-- Vynechaný text --