


Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 4: Digitální podpisy umožňující obnovu zprávy	ČSN ISO/IEC 15946-4  36 9794
---	---------------------------------------

Information technology - Security techniques - Cryptographic techniques based on elliptic curves -  
Part 4: Digital signatures giving message recovery

Technologies de l'information - Techniques de sécurité - Techniques cryptographiques basées sur les  
courbes  
elliptiques - Partie 4: Signatures digitales offrant un message de recouvrement

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-4:2004. Překlad byl zajištěn Českým  
normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15946-4:2004. It was  
translated by Czech Standards Institute. It has the same status as the official version.

	© Český normalizační institut, 2006 <b>76733</b> Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.
---	---

techniky - Schémata digitálního podpisu umožňující obnovu zprávy - Část 3: Mechanismy založené na diskretních logaritmech

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

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

ISO/IEC 15946-1:2002 zavedena v ČSN ISO/IEC 15946-1:2005 (36 9794) Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 1: Všeobecně

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Strana 3

---

#### MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky -  
Kryptografické techniky založené na eliptických křivkách -  
Část 4: Digitální podpisy umožňující obnovu zprávy

ISO/IEC 15946-4  
První vydání  
2004-10

#### 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 nepřejímá 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 Vše-obecných 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.

© ISO/IEC 2004

Všechna práva vyhrazena. ©ádná část této normy nesmí být reprodukována nebo zpracována jakoukoliv jinou formou, jako například elektronickou, mechanickou, 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 22 734 10 79

e-mail [copyright@iso.ch](mailto:copyright@iso.ch)

Web [www.iso.ch](http://www.iso.ch)

Strana 4

---

Obsah

Strana

Úvod

.....	8
<b>1</b> Předmět normy	..... ..... 9
<b>2</b> Citované normativní dokumenty	..... 9
<b>3</b> Termíny a definice	..... ..... 10
<b>4</b> Symboly a zkrácené termíny	..... 12
<b>4.1</b> Symboly a notace	..... ..... 12
<b>4.2</b> Kódovací konvence, délka a velikost pole.....	..... 12
<b>4.3</b> Legenda k obrázkům	

.....	13
<b>5</b>	Procesy
.....	13
<b>5.1</b>	Proces generování parametrů
.....	13
<b>5.1.1</b>	Parametry domény
.....	13
<b>5.1.2</b>	Parametry uživatele
.....	13
<b>5.1.3</b>	Validita parametrů
.....	14
<b>5.2</b>	Proces generování podpisu
.....	14
<b>5.3</b>	Proces ověřování podpisu
.....	14
<b>6</b>	Všeobecný model digitálních podpisů umožňujících obnovu zprávy.....
	15
<b>6.1</b>	Požadavky
.....	15
<b>6.1.1</b>	Parametry domény
.....	15
<b>6.1.2</b>	Typ redundance
.....	

.....	15
<b>6.2</b> Přehled funkcí a postupů	
.....	
... 16	
<b>6.2.1</b> Podpisový a ověřovací klíč	
.....	
. 16	
<b>6.2.2</b> Randomizér a předběžný podpis.....	
16	
<b>6.2.3</b> Výpočet první části podpisu	
.....	
17	
<b>6.2.4</b> Výpočet druhé části podpisu	
.....	
17	
<b>6.2.5</b> Obnovení předběžného podpisu	
.....	17
<b>6.2.6</b> Obnovení vstupních dat	
.....	
..... 17	
<b>6.3</b> Proces generování podpisu	
.....	
17	
<b>6.3.1</b> Vytvoření randomizéru a předběžného podpisu.....	18
<b>6.3.2</b> Rozdělení zprávy	
.....	
..... 18	
<b>6.3.3</b> Vytvoření vstupních dat	
.....	
..... 18	

<b>6.3.4</b>	Výpočet podpisu	.....	.....
		.....	18
<b>6.3.5</b>	Formátování podepsané zprávy	.....	18
<b>6.4</b>	Proces ověřování podpisu	.....	.....
		.....	19
<b>6.4.1</b>	Otevření podepsané zprávy	.....	20
<b>6.4.2</b>	Ověření velikosti podpisu	.....	20
<b>6.4.3</b>	Obnovení předběžného podpisu a vstupních dat.....	.....	21
<b>6.4.4</b>	Obnovení vstupních dat nebo zprávy.....	.....	21
<b>6.4.5</b>	Opakovaný výpočet hašovacího tokenu.....	.....	21
<b>6.4.6</b>	Kontrola podpisu	.....	.....
		.....	21
<b>7</b>	ECNR (Podpis založený na eliptických křivkách dle Nyberg-Rueppela s obnovou zprávy).....	.....	21
<b>7.1</b>	Parametry domény a uživatele	.....	21

.....	21
<b>7.2.1</b> Vytvoření randomizéru a předběžného podpisu (Výpočty eliptické křivky).....	22
<b>7.2.2</b> Výpočty modulo grupy řádu $G$ (Aritmetické operace v $F(n)$ ).....	22
<b>7.2.3</b> Formátování podepsané zprávy .....	22
<b>7.3</b> Proces ověření podpisu .....	22
<b>7.3.1</b> Ověření velikosti podpisu .....	22
<b>7.3.2</b> Obnovení předběžného podpisu a vstupních dat (Výpočty eliptické křivky).....	22
<b>7.3.3</b> Obnovení vstupních dat nebo zprávy.....	22
<b>7.3.4</b> Kontrola podpisu .....	22
<b>8</b> ECMR (Podpis založený na eliptických křivkách dle Miyajihho s obnovou zprávy).....	22
<b>8.1</b> Parametry domény a uživatele .....	22
<b>8.2</b> Proces generování podpisu .....	23
<b>8.2.1</b> Vytvoření randomizéru a předběžného podpisu (Výpočty eliptické křivky).....	23
<b>8.2.2</b> Výpočty podpisu (Výpočty modulo grupy řádu $G$ ).....	23
<b>8.2.3</b> Formátování podepsané	

zprávy	23
.....	
<b>8.3</b> Proces ověření podpisu	.....
.....	23
<b>8.3.1</b> Ověření velikosti podpisu	.....
.....	23
<b>8.3.2</b> Obnovení předběžného podpisu a vstupních dat (Výpočty eliptické křivky).....	23
<b>8.3.3</b> Obnovení vstupních dat nebo zprávy.....	24
<b>8.3.4</b> Kontrola podpisu	.....
.....	24
<b>9</b> ECAO (Podpis založený na eliptických křivkách dle Abe-Okamoto s obnovou zprávy).....	24
<b>9.1</b> Parametry domény a uživatele	.....
.....	24
<b>9.1.1</b> Vytváření vstupních dat	.....
.....	24
<b>9.2</b> Proces generování podpisu	.....
.....	24
<b>9.2.1</b> Vytvoření randomizéru a předběžného podpisu (Výpočty eliptické křivky).....	24
<b>9.2.2</b> Výpočty podpisu (Výpočty modulo grupy řádu $G$ ).....	25
<b>9.2.3</b> Formátování podepsané zprávy	.....
.....	25
<b>9.3</b> Proces ověření podpisu	



.....	25
<b>9.3.1</b> Ověření velikosti podpisu	.....
.....	25
<b>9.3.2</b> Obnovení předběžného podpisu a vstupních dat (Výpočty eliptické křivky).....	25
<b>9.3.3</b> Obnovení vstupních dat nebo zprávy.....	25
<b>9.3.4</b> Kontrola podpisu	.....
.....	25
<b>10</b> ECPV (Podpis založený na eliptických křivkách dle Pintsov-Vanstona s obnovou zprávy).....	25
<b>10.1</b> Parametry domény a uživatele	.....
.....	25
<b>10.2</b> Proces generování podpisu	.....
.....	26
<b>10.2.1</b> Vytvoření randomizéru a předběžného podpisu (Výpočty eliptické křivky).....	26
<b>10.2.2</b> Vytváření vstupních dat	.....
.....	26
<b>10.2.3</b> Výpočty podpisu (Výpočty modulo grupy řádu $G$ ).....	26
<b>10.2.4</b> Formátování podepsané zprávy	.....
.....	26
<b>10.3</b> Proces ověření podpisu	.....
.....	26
<b>10.3.1</b> Ověření velikosti podpisu	.....

.....  
... 27

**10.3.2** Obnovení předběžného podpisu a vstupních dat (Výpočty eliptické křivky)..... 27

Strana 6

Strana

**10.3.3** Obnovení vstupních dat nebo zprávy..... 27

**10.3.4** Kontrola podpisu  
.....  
..... 27

**11** ECKNR (Podpis založený na eliptických křivkách KCDSA/Nyberg-Rueppel s obnovou zprávy)..... 27

**11.1** Parametry domény a uživatele  
..... 27

**11.2** Proces generování podpisu  
.....  
28

**11.2.1** Vytvoření randomizéru a předběžného podpisu (Výpočty eliptické křivky)..... 28

**11.2.2** Výpočty modulo grupy řádu  $G$  (Aritmetické operace v  $F(n)$ )..... 28

**11.2.3** Formátování podepsané zprávy  
..... 28

**11.3** Proces ověření podpisu  
.....  
..... 28

**11.3.1** Ověření velikosti podpisu  
.....  
... 28

**11.3.2** Obnovení předběžného podpisu a vstupních dat (Výpočty eliptické křivky)..... 28

<b>11.3.3</b> Obnovení vstupních dat nebo zprávy.....	29
<b>11.3.4</b> Kontrola podpisu ..... .....	29
<b>Příloha A</b> (informativní) Číselné příklady.....	30
<b>Příloha B</b> (informativní) Souhrn vlastností mechanismů.....	43
<b>Příloha C</b> (informativní) Informace o patentech.....	45
Bibliografie ..... .....	46

Strana 7

---

## 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 2 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.

Mezinárodní norma ISO/IEC 15946-4 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie*, subkomise SC 27, *Bezpečnostní techniky IT*.

ISO/IEC 15946 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách*:

- Část 1: Všeobecně
- Část 2: Digitální podpisy
- Část 3: Ustavení klíčů

## Úvod

Potenciálně užitečná třída kryptografických systémů s veřejným klíčem sestává ze schémat založených na eliptických křivkách definovaných nad konečnými poli. Kryptografické systémy s veřejným klíčem založené na eliptických křivkách využívají následující dva poznatky:

- Každá eliptická křivka má binární operaci „+“, pomocí které vytváří konečnou abelovskou grupu.
- Zákon grupy se u eliptických křivek rozšiřuje přirozeným způsobem k „diskrétní exponenciaci“ bodové grupy eliptické křivky.

Na základě diskrétního umocňování eliptické křivky je možné snadno odvodit obdoby eliptické křivky ze známých schémat s veřejným klíčem Diffie-Hellmana a ElGamala.

Bezpečnost takového systému s veřejným klíčem závisí na obtížnosti určení diskrétních logaritmu v grupě bodů eliptické křivky. Pro podobné velikosti parametrů je tento problém - při současné úrovni znalostí - mnohem obtížnější než faktorizace celých čísel nebo výpočet diskrétních logaritmu v konečném poli. Ve skutečnosti od té doby, co Miller a Koblitz v r.1985 nezávisle navrhli použití eliptických křivek u kryptografických systémů s veřejným klíčem, nebyl zaznamenán žádný významný pokrok ve vypořádání se s problémem diskrétního logaritmu eliptických křivek. Obecně platí, že určit diskrétní logaritmy eliptických křivek jsou schopné pouze algoritmy, které vyžadují exponenciální čas. Proto je možné u systémů s veřejným klíčem založených na eliptických křivkách použít daleko kratší parametry než je tomu u systému RSA nebo klasických systémů založených na diskrétních logaritmech, které využívají multiplikativní grupu některého konečného pole. To přináší významně kratší digitální podpisy a systémové parametry a umožňuje použít při výpočtech menší celá čísla.

Aby uspokojila rostoucí zájem o technologie s veřejným klíčem založené na eliptických křivkách, definuje tato část ISO/IEC 15946 metody pro implementaci technik digitálního podpisu založených na eliptických křivkách umožňujících obnovu zprávy.

Mezinárodní organizace pro normalizaci (ISO) a Mezinárodní elektrotechnická komise (IEC) upozorňuje na to, že je třeba věnovat pozornost skutečnosti, že vyhovění této mezinárodní normě může zahrnovat použití patentů.

ISO a IEC nezaujímají stanovisko k evidenci, platnosti a rozsahu těchto patentových práv.

Držitelé těchto patentových práv ujistili ISO a IEC, že jsou ochotni dohodnout s uživateli na celém světě licence za rozumných a nediskriminačních okolností a podmínek. V tomto ohledu jsou prohlášení držitelů těchto patentovaných práv registrována u ISO a IEC. Informace lze získat u:

ISO/IEC JTC 1/SC 27 Standing Document 8 (SD 8) „*Patent Information*“

SD 8 je veřejně dostupný na: <http://www.din.de/ni/sc27>

Je třeba upozornit na to, že některé prvky této mezinárodní normy mohou být předmětem jiných patentových práv než těch, které jsou uvedeny výše. ISO a IEC nepřejímají odpovědnost za identifikaci

některých nebo všech patentových práv.

## 1 Předmět normy

ISO/IEC 15946 specifikuje kryptografické techniky s veřejným klíčem založené na eliptických křivkách. Tyto techniky zahrnují metody ustavení klíčů pro symetrické kryptografické techniky a mechanismy digitálního podpisu.

Předmět této části ISO/IEC 15946 je omezen na kryptografické techniky založené na eliptických křivkách definovaných nad konečnými poli (včetně speciálních případů řádu prvočísel s charakteristikou dvě). Repräsentace prvků vlastních konečných polí (tj. jejichž báze je použita) je mimo rozsah této části ISO/IEC 15946.

Tato část ISO/IEC 15946 specifikuje pět odlišných mechanismů pro digitální podpisy umožňující obnovu zprávy. Matematický základ a všeobecné techniky nutné pro implementaci mechanismů jsou popsány v ISO/IEC 15946-1.

Mechanismy digitálního podpisu mohou být rozděleny do následujících dvou kategorií.

- Když má být celá zpráva uložena a/nebo přenesena s podpisem, mechanismus se nazývá „mechanismus podpisu s dodatkem“.
- Když může být celá zpráva nebo její část obnovena z podpisu, mechanismus se nazývá „mechanismus podpisu umožňující obnovu zprávy“. Mechanismy specifikované v této části ISO/IEC 15946 spadají do druhé kategorie, tj. umožňují buďto úplnou nebo částečnou obnovu zprávy. [Pro schémata digitálního podpisu s dodatkem založená na eliptických křivkách viz ISO/IEC 15946-2.]

POZNÁMKA V aplikacích, kde je použita k poskytnutí bezpečnostních služeb kombinace algoritmů nebo kde je algoritmus parametrizován volbou kombinace jiných algoritmů, taková kombinace může být specifikována jako posloupnost identifikátorů objektů přiřazených k těmto algoritmům nebo vložení identifikátorů objektů algoritmů nižší úrovně pole parametrů struktury identifikátoru algoritmu specifikujících vyšší úroveň algoritmů (například specifikací identifikátoru objektu hašovací funkce jako parametru ve struktuře identifikátoru algoritmu schématu podpisu). Struktura identifikátoru algoritmu je definována v ISO/IEC 9594-8.

POZNÁMKA Kódování identifikátorů objektů je závislé na aplikaci.

---

-- Vynechaný text --