

2006

Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 3: Ustavení klíčů	ČSN ISO/IEC 15946-3 36 9794
---	-----------------------------------

Information technology - Security techniques - Cryptographic techniques based on elliptic curves -
Part 3: Key
establishment

Technologies de l'information - Techniques de sécurité - Techniques cryptographiques basées sur les
courbes
elliptiques - Partie 3: Établissement de clé

Informationstechnik - IT-Sicherheitsverfahren - Kryptographische Techniken auf Basis von eliptischen
Kurven -
Teil 3: Schlüsselbereitstellung

Tato norma je českou verzí mezinárodní normy ISO/IEC 15946-3:2002. Překlad byl zajištěn Českým
normalizačním institutem. Má stejný status jako oficiální verze.

This standard is the Czech version of the International Standard ISO/IEC 15946-3:2002. It was translated
by Czech Standards Institute. It has the same status as the official version.



© Český normalizační institut, 2006

76661

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

Národní předmluva

Informace o citovaných normativních dokumentech

ISO/IEC 9796 (2. a 3. část) zavedena v ČSN ISO/IEC 9796 (36 9780) Informační technologie - Bezpečnostní techniky - Schémata digitálního podpisu umožňující obnovu zprávy

ISO/IEC 9797 (všechny části) zavedena v ČSN ISO/IEC 9797 (36 9782) Informační technologie - Bezpečnostní techniky - Kódy pro autentizaci zprávy (MAC)

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

ISO/IEC 11770-3:1999 zavedena v ČSN ISO/IEC 11770-3 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

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

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

ISO/IEC 15946-2:2002 zavedena v ČSN ISO/IEC 15946-2 (36 9794) Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 2: Digitální podpisy

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

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 vytvoření 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.

© ISO 1999

Všechna práva vyhrazena. Žádná část této normy nesmí být reprodukována nebo zpracována jakoukoliv jinou formou, jako například elektronickou, mechanickou, včetně fotokopí 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

Web www.iso.ch

Strana 4

Obsah

Strana

Předmluva

.....
..... 6

Úvod

.....
..... 7

1 Předmět

	normy	8
2	Normativní odkazy	8
3	Termíny a definice	8
4	Symboly a zkrácené termíny	12
5	Funkce odvození klíče	12
6	Násobení kofaktorů	13
7	Závazek klíče	13
8	Mechanismy dohody o klíči	14
8.1	Společná informace	14
8.2	Neinteraktivní dohoda o klíči typu Diffie-Hellmann (KANIDH)	14
8.2.1	Uspořádání	14
8.2.2		

Mechanismus	14
8.2.3	
Vlastnosti	14
8.3	Dohoda o klíči typu ElGamal (KAEG)..... 15
8.3.1	Uspořádání
 15
8.3.2	Mechanismus
 15
8.3.3	Vlastnosti
 15
8.4	Dohoda o klíči typu Diffie-Hellmann
 15
8.4.1	Uspořádání
 15
8.4.2	Mechanismus
 15
8.4.3	Vlastnosti
 16
8.5	Dohoda o klíči typu Diffie-Hellmann s dvěma dvojicemi klíčů (KADH2KP)..... 16
8.5.1	Uspořádání
 16

8.5.2	Mechanismus
	16
8.5.3	Vlastnosti
	16
8.6	Dohoda o klíči typu Diffie-Hellmann s dvěma podpisy a potvrzením klíčů (KADH2SKC).....	17
8.6.1	Uspořádání
	17
8.6.2	Mechanismus
	17
8.6.3	Vlastnosti
	18
9	Mechanismy dohody nezahrnuté v ISO/IEC 11770-3.....	18
9.1	Společné informace
	18
9.2	Úplný sjednocený model
	...	19
9.2.1	Uspořádání
	19
9.2.2	Mechanismus
	19
9.2.3	Vlastnosti

.....	19
9.3 Dohoda o klíčích typu MQV s 1 průchodem (KAMQV1P).....	19
9.3.1 Uspořádání	19
9.3.2 Mechanismus	19
9.3.3 Vlastnosti	20

9.4 Dohoda o klíčích typu MQV s 2 průchody (KAMQV2P).....	20
9.4.1 Uspořádání	20
9.4.2 Mechanismus	20
9.4.3 Vlastnosti	20
10 Mechanismy transportu klíčů	20
10.1 Společné informace	21

10.2	Transport klíčů typu ElGamal (KTEG).....	21
10.2.1	Uspořádání	21
10.2.2	Mechanismus	21
10.2.3	Vlastnosti	22
10.3	Transport klíčů typu ElGamal s podpisem původce (KTEGOS).....	22
10.3.1	Uspořádání	22
10.3.2	Mechanismus	22
10.3.3	Vlastnosti	23
11	Potvrzení klíče	23
Příloha A	(informativní) Příklady funkcí odvození klíče.....	25
A.1	Funkce odvození klíče podle IEEE P1363.....	25
A.1.1	Předběžné podmínky	25
A.1.2		

Vstup	25
A.1.3	
Akce	25
A.1.4	
Výstup	25
A.2	Funkce odvození klíče podle ANSI
X9.42	25
A.2.1	Nezbytné předpoklady
	25
A.2.2	Vstup
	25
A.2.3	Akce
	26
A.2.4	Výstup
	26
A.2.5	Syntaxe
ASN.1	26
A.3	Funkce odvození klíče podle ANSI
X9.63	27
A.3.1	Nezbytné předpoklady
	27
A.3.2	Vstup

.....	27
A.3.3	
Akce	
.....	
.....	27
A.3.4	
Výstup	
.....	
.....	28
Příloha B (informativní) Porovnání vlastností mechanismů uplatňovaných v této normě.....	29
B.1	
Bezpečnostní vlastnosti	
.....	
.....	29
B.2	
Úvahy o výkonnosti	
.....	
.....	30
Bibliografie	
.....	
.....	32

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.

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

ISO a IEC ustavily v oblasti informační technologie společnou technickou komisi, ISO/IEC JTC1. 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 15946-3 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
- Část 4: Digitální podpisy umožňující obnovu zprávy

Přílohy A a B této části mezinárodní normy ISO/IEC 15946 mají pouze informativní charakter.

Strana 7

Úvod

Některé z nejzajímavějších a potenciálně užitečných kryptografických systémů s veřejným klíčem, které jsou v současné době dostupné, jsou kryptografické systémy založené na eliptických křivkách definovaných nad konečnými poli. Koncept kryptografického systému s veřejným klíčem založeného na eliptické křivce je poměrně jednoduchý:

- Každá eliptická křivka je vybavena binární operací „+“, pomocí které vytváří konečnou abelovskou grupu.
- Zákon grupy se u eliptických křivek rozšiřuje přirozeným způsobem k „diskrétní exponenciaci“ bodové grupy eliptické křivky.
- Na základě diskrétní exponenciace eliptické křivky je možné snadno odvodit obdoby eliptické křivky z velmi známých schémat s veřejným klíčem Diffie-Hellmana a ElGamala.

Bezpečnost takového systému s veřejným klíčem závisí na obtížnosti určení diskrétních logaritmů v grupě bodů eliptické křivky. Tento problém je - při současné úrovni znalostí - mnohem obtížnější než faktorizace celých čísel nebo výpočet diskrétních logaritmů 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. Je proto 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 nějakého konečného pole. To přináší významně kratší digitální podpisy a systémové parametry a umožňuje použít při výpočtech menší celá čísla.

Tato část ISO/IEC 15946 popisuje schémata, která mohou být použita pro dohodu o klíčích a schémata, která mohou být použita pro transport klíčů. Kde je to možné, jsou schémata analogická k metodám obsaženým v ISO/IEC 11770-3. Schémata, která nejsou obsažena v ISO/IEC 11770-3 jsou zohledněna jako taková.

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)

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 nepřijímají odpovědnost za identifikaci některých nebo všech patentových práv.

Strana 8

1 Předmět normy

Mezinárodní norma ISO/IEC 15946 specifikuje kryptografické techniky s veřejným klíčem založené na eliptických křivkách. Norma je rozdělena do čtyř částí a zahrnuje ustavení klíčů pro systémy s tajným klíčem a mechanismy digitálního podpisu.

Tato část ISO/IEC 15946 specifikuje techniky pro ustavení klíčů, což zahrnuje dohodu o klíčích a transport klíčů, používané eliptickými křivkami.

Předmět této normy je omezen na kryptografické techniky založené na eliptických křivkách definovaných nad konečnými poli mocnin řádu prvočísel (včetně speciálních případů řádu prvočísel s charakteristikou dvě). Reprezentace prvků vlastních konečných polí (tj. jejichž báze je použita) je mimo rozsah této normy. Tato norma nespecifikuje zcela implementaci technik, které definuje. Mohou existovat odlišné produkty, které vyhovují této mezinárodní normě a dosud nejsou kompatibilní.

-- Vynechaný text --