ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Říjen

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.

76661

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

MEZINÁRODNÍ NORMA

Informační technologie - Bezpečnostní techniky - Kryptografické techniky založené na eliptických křivkách - Část 3: Ustavení klíčů

ISO/IEC 15946-3

První vydání

2002-12

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

Obsah

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.

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 nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

---

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 --