ČESKÁ TECHNICKÁ NORMA

ICS 35.040 **Červen**
2001

	Informační technologie - Bezpečnostní techniky - Postupy pro registraci kryptografických algoritmů	ČSN ISO/IEC 9979 36 9781

Information technology - Security techniques - Procedures for the registration of cryptographic algorithms

Technologies de l’information - Techniques de sécurité - Procédures d’enregistrement des algorithmes cryptographiques

Informationstechnik - Sicherheitsverfahren - Verfahren für die Registrierung von kryptografischen Algorithmen

Tato norma je českou verzí mezinárodní normy ISO/IEC 9979:1999. Mezinárodní norma ISO/IEC 9979:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 9979:1999. The International Standard ISO/IEC 9979:1999 has the status of a Czech Standard.

Nahrazení předchozích norem

Touto normou se nahrazuje ČSN ISO/IEC 9979 (36 9781) z listopadu 1996.

61282

Národní předmluva

Citované normy

ISO/IEC 8825:1990 zavedena v ČSN ISO/IEC 8825:1994 (36 9635) Informační technika - Propojení otevřených systémů - Specifikace základních kódovacích pravidel pro abstraktní syntaktickou notaci jedna (ASN.1)

ISO/IEC 8825:1990 *Information technology - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*

ISO/IEC 9834-1:1993 zavedena v ČSN ISO/IEC 9834-1:1997 (36 9674) Informační technologie - Propojení otevřených systémů - Procedury pro činnost registračních orgánů OSI: Všeobecné procedury

ISO/IEC 9834-1:1993 *Information technology - Open Systems Interconnection - Procedures for the operation of OSI Registration Authorities: General procedures*

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČO 61470716

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA
Informační technologie - Bezpečnostní techniky - Postupy pro registraci kryptografických algoritmů

ISO/IEC 9979
Druhé vydání
1999-04-01

ICS 35.040

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.

ISO a IEC ustavily v oblasti informační technologie 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 9979 byla připravena společnou technickou komisí ISO/IEC JTC1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

Toto druhé vydání ruší a nahrazuje první vydání (ISO/IEC 9979:1991), jehož je technickou revizí.

Příloha A je integrální součástí této mezinárodní normy. Příloha B je pouze informativní.

---

1 Předmět normy

Tato mezinárodní norma specifikuje postupy pro registraci kryptografických algoritmů a formu položek registru.

Tato mezinárodní norma je určena pro použití těmi, kdo si přejí vytvořit položky registru, a Registrační autoritou.

ISO/IEC registr kryptografických algoritmů má funkci obecného odkazu pro identifikaci kryptografických algoritmů jedinečným názvem. Registr je také místem, kde se ukládají základní parametry identifikované položkou registru. Hlavním cílem registru je umožnit entitám identifikovat a projednat dohodnutý kryptografický algoritmus.

-- Vynechaný text --