ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen

2002

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

Information technologies - Security techniques - Key Management - Part 3: Mechanisms using asymmetric techniques

Technologies de l´information - Techniques de sécurité - Gestion de clés - Partie 3: Mechanismes utilisant des techniques asymétriques

Informationstechnik - Sicherheittechniken - Schlüsselmanagement - Teil 3: Mechanismen unter Benutzung von asymmetrischen Techniken

Tato norma je českou verzí mezinárodní normy ISO/IEC 11770-3:1999. Mezinárodní norma ISO/IEC 11770-3:1999 má status české technické normy.

This standard is the Czech version of the International Standard ISO/IEC 11770-3:1999. The International Standard ISO/IEC 11770-3:1999 has the status of a Czech Standard.

64114

Národní předmluva

Citované normy

ISO 7498-2: 1989 zavedena v ČSN ISO/IEC 7498-2 (36 9615) Systémy na spracovanie informácií - Prepojenie otvorených systémov - Základný referenčný model - Čas» 2: Bezpečnostná architektura

ISO/IEC 9594-8 1995 dosud nezavedena, nahrazena ISO/IEC 9594-8:2001

ISO/IEC 9798-3:1998 zavedena v ČSN ISO/IEC 9798-3 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 3: Mechanismy používající techniky digitálního podpisu, nahrazena ISO/IEC 9798-3:2000

ISO/IEC 10118-1:1994 zavedena v ČSN ISO/IEC 10118-1 (36 9830) Informační technologie - Bezpečnostní techniky - Hash funkce - Část 1: Všeobecně, nahrazena ISO/IEC 10118-1:2000

ISO/IEC 10181-1:1996 zavedena v ČSN ISO/IEC 10181-1(36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktura otevřených systémů - Část 1: Přehled

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura správy klíčů

Národní poznámka

Pro účely této normy se anglické slovo „security“ překládá českým slovem „bezpečnost“.

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 - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 11770-3
První vydání
1999-11-01

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 mezinárodní organizace, vládní i nevládní, s nimiž ISO a IEC navázalo pracovní styk.

Mezinárodní normy jsou navrhovány podle pravidel, uvedených ve Směrnicích ISO/IEC, Část 3.

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.

Pozornost je věnována možnosti, že některé prvky této části ISO/IEC 11770 mohou být předmětem patentových práv. ISO a IEC nesmí být považovány za zodpovědné za identifikaci jakýchkoliv nebo všech patentových práv.

Mezinárodní norma ISO/IEC 11770-3 byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT.*

ISO/IEC 11770 se skládá z následujících částí se společným názvem *Informační technologie - Bezpečnostní techniky - Správa klíčů:*

– *Část 1: Struktura*

– *Část 2: Mechanismy používající symetrické techniky*

– *Část 3: Mechanismy používající asymetrické techniky*

Mohou následovat další části.

Přílohy A až E této části ISO/IEC 11770 jsou pouze informativní

1 Předmět normy

Tato část ISO/IEC 11770 určuje mechanismy správy klíčů založené na asymetrických kryptografických technikách. Zabývá se specificky použitím asymetrických technik, aby se dosáhlo těchto cílů:

1 Ustavit sdílený tajný klíč pro symetrickou kryptografickou techniku mezi dvěma entitami *A* a *B* dohodou na klíči. V mechanismu dohody na tajném klíči je tajný klíč výsledkem datové výměny mezi dvěma entitami *A* a *B*. Ani jedna z nich nemůže předem určit hodnotu sdíleného tajného klíče.

2 Ustavit sdílený tajný klíč pro symetrickou kryptografickou techniku mezi dvěma entitami *A* a *B*

transportem klíče. V mechanismu transportu tajného klíče je tajný klíč vybrán jednou entitou *A* a je přenesen k jiné entitě *B*, vhodně chráněn asymetrickými technikami.

3 Zpřístupnit veřejný klíč jedné entity jiným entitám transportem klíče. V mechanismu transportu veřejného klíče musí být veřejný klíč entity *A* přenesen k dalším entitám autentizovaným způsobem, není však vyžadováno utajení.

Některé mechanismy této části ISO/IEC 11770 jsou založeny na příslušných autentizačních mechanismech uvedených v ISO/IEC 9798-3.

Tato část ISO/IEC 11770 se nezabývá aspekty správy klíčů jako je např.

– správa životního cyklu klíče,

– mechanismy ke generování nebo validaci dvojic asymetrických klíčů,

– mechanismy pro ukládání, archivování, vymazání, zničení atd. klíčů.

Zatímco tato část ISO/IEC 11770 se explicitně nezabývá distribucí soukromého klíče entity (z dvojice asymetrických klíčů) od důvěryhodné třetí strany k entitě, která klíč požaduje, mohou být k dosažení tohoto cíle použity popsané mechanismy transportu klíčů.

Tato část ISO/IEC 11770 neřeší implementace transformací, použitých v mechanismech správy klíčů.

POZNÁMKA K dosažení autenticity zpráv správy klíčů je možné přijmout opatření pro zajištění autenticity v protokolu o ustavení klíče nebo použít systém podpisu s veřejným klíčem k podpisu zpráv výměny klíčů.

-- Vynechaný text --