ČESKÁ TECHNICKÁ NORMA

ICS 35.040

Květen 2004

	Informační technologie - Bezpečnostní techniky - Směrnice pro používání a řízení služeb důvěryhodných třetích stran	ČSN ISO/IEC TR 14516 36 9791

Information technology - Security techniques - Guidelines for the use and management of Trusted Third Party services

Technologies de l’information - Techniques de sécurité - Lignes directrices pour l’emploi et la gestion des services TTP

Informationstechnik - Sicherheitsverfahren - Richtlinien für die Netzung und das Management von Trust-Zentern

Tato norma je českou verzí technické zprávy ISO/IEC TR 14516:2002. Technická zpráva ISO/IEC TR 14516:2002 má status české technické normy.

This standard is the Czech version of the Technical Report ISO/IEC TR 14516:2002. The Technical Report ISO/IEC TR 14516:2002 has the status of a Czech Standard.

69564

Národní předmluva

Citované normy

ISO 7498-2:1989 zavedena v ČSN ISO 7498-2:1993 (36 9615) Systémy na spracovanie informácií - Propojenie otvorených systémov (OSI) - Základný referenčný model - Čas» 2: Bezpečnostná architektura

ISO/IEC 9798-1:1997 zavedena v ČSN ISO/IEC 1997 (36 9743) Informační technologie - Bezpečnostní techniky - Autentizace entit - Část 1: Všeobecně

ISO/IEC 11770-1:1996 zavedena v ČSN ISO/IEC 11770-1:1998 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 1: Struktura

ISO/IEC 11770-2:1996 zavedena v ČSN ISO/IEC 1999 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 2: Mechanismy používající symetrické techniky

ISO/IEC 11770-3:1999 zavedena v ČSN ISO/IEC 2002 (36 9785) Informační technologie - Bezpečnostní techniky - Správa klíčů - Část 3: Mechanismy používající asymetrické techniky

ISO/IEC TR 13335-1:1996 zavedena v ČSN ISO/IEC TR 13335-1:1999 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT

ISO/IEC TR 13335-2:1997 zavedena v ČSN ISO/IEC TR 13335-2:2000 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT

ISO/IEC TR 13335-3:1998 zavedena v ČSN ISO/IEC TR 13335-3:2000 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT

ISO/IEC TR 13335-4:2000 zavedena v ČSN ISO/IEC TR 13335-4:2002 (36 9786) Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr bezpečnostních opatření

ISO/IEC 13888-1:1997 zavedena v ČSN ISO/IEC 13888-1:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost - Část 1: Všeobecně

ISO/IEC 13888-2:1998 zavedena v ČSN ISO/IEC 13888-2:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost -Část 2: Mechanismy používající symetrické techniky

ISO/IEC 13888-3:1997 zavedena v ČSN ISO/IEC 13888-3:2001 (36 9787) Informační technologie - Bezpečnostní techniky - Nepopiratelnost -Část 3: Mechanismy používající asymetrické techniky

ISO/IEC 15443 dosud nezavedena

Doporučení ITU-T X.509:2001 | ISO/IEC 9594-8:2001 zavedena v ČSN ISO/IEC 9594-8:2003 (36 9671) Informační technologie - Propojení otevřených systémů - Adresář: Veřejný klíč a struktury atributových certifikátů

Doporučení CCITT X.800:1991 nezavedeno

Doporučení ITU-T X.810:1995 | ISO/IEC 10181-1:1996 zavedena v ČSN ISO/IEC 10181-1:1998 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury pro otevřené systémy: Přehled

Doporučení ITU-T X.813:1996 | ISO/IEC 10181-4:1997 zavedena v ČSN ISO/IEC 10181-4:1999 (36 9694) Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury pro otevřené systémy: Struktura nepopiratelnosti

Vysvětlivky k textu převzaté normy

V této normě je použit z důvodu návaznosti na již zavedené normy výraz revokace (anglicky revocation). Ve stejném významu je možné použít i výraz odvolání.

Národní poznámka

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

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

Technická normalizační komise: TNK 42, Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

---

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 3 Směrnic ISO/IEC.

Hlavním úkolem společné technické komise je příprava mezinárodních norem. Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Za výjimečných okolností může společná technická komise navrhnout zveřejnění technické zprávy jednoho z následujících typů:

– typ 1, když navzdory opakovaným snahám není možné získat pro zveřejnění mezinárodní normy požadovanou podporu;

– typ 2, když je subjekt dosud ve stádiu technického vývoje nebo kde z jakýkoliv jiných důvodů existuje budoucí nikoliv však okamžitá možnost dohody ohledně mezinárodní normy;

– typ 3, když technická komise shromáždila data různého druhu z materiálu, který je obvykle zveřejněn jako mezinárodní norma (např. současný stav vědeckého vývoje).

Technické zprávy typu 1 a 2 jsou předmětem revize do tří let od zveřejnění, aby se rozhodlo, zda-li mohou být přeměněny na mezinárodní normy. Technické zprávy typu 3 nemusejí být nutně revidovány do doby, než jsou data, která poskytují, považována za neplatná nebo neužitečná.

Je třeba upozornit, že některé prvky této mezinárodní normy mohou být předmětem patentových práv. ISO a IEC nepřejímají odpovědnost za identifikaci některých nebo všech patentových práv.

ISO/IEC TR 14516, což je technická zpráva typu 3, byla připravena společnou technickou komisí ISO/IEC JTC 1, *Informační technologie,* subkomise SC 27, *Bezpečnostní techniky IT*, ve spolupráci s ITU-T. Identický text byl vydán jako Dop. ITU-T X.842.

Prázdná strana

TECHNICKÁ ZPRÁVA

Informační technologie - Bezpečnostní techniky - Směrnice pro používání a řízení služeb důvěryhodných třetích stran

ISO/IEC TR 14516

První vydání

2002-06

Obsah

Úvod

K dosažení odpovídající úrovně obchodní důvěry při provozování systémů IT přispívá značnou měrou zajištění praktických a náležitých právních a technických kontrol. Organizace musí mít důvěru v to, že systémy IT nabízejí jednoznačné výhody a že je možné se na takové systémy spolehnout v tom, že zachovají podnikatelské závazky a vytvoří podnikatelské příležitosti.

Výměna informací mezi dvěma entitami v sobě zahrnuje prvek důvěry, tj. že např. příjemce předpokládá, že identita odesilatele je ve skutečnosti odesilatel, a naopak odesilatel předpokládá, že identita příjemce je ve skutečnosti příjemce, kterému je informace určena. Tento „implikovaný prvek důvěry“ nemusí být postačující a může k tomu, aby se usnadnila důvěryhodná výměna informací, vyžadovat použití důvěryhodné třetí strany (TTP).

Role TTP zahrnuje poskytnutí záruky, že podnikatelská činnost a jiné důvěryhodné (např. vládní aktivity) zprávy a transakce jsou přenášeny k zamýšlenému příjemci, na správné místo, že zprávy jsou přijaty včas a bezchybně, a že v případě jakýchkoliv obchodních sporů, které se mohou objevit, existují vhodné metody pro vytvoření a dodání požadovaných svědectví k prokázání toho, co se stalo. Služby poskytnuté TTP mohou obsahovat služby, které jsou nezbytné pro správu klíčů, management certifikátů, podporu identifikace a autentizace, službu atributu privilegií, nepopiratelnost, služby vyznačení času, služby elektronického veřejného notáře a adresářové služby. TTP mohou poskytovat některé nebo všechny tyto služby.

TTP musí být navržena, implementována a provozována tak, aby poskytla záruku za bezpečnostní služby, které poskytuje, a aby splnila aplikovatelné právní a regulační požadavky. Druhy a úrovně zavedené nebo požadované ochrany se mění v závislosti na typu poskytnuté služby a kontextu, ve kterém je obchodní aplikace provozována.

Cílem tohoto Doporučení | Technické zprávy je poskytnout:

a) směrnice pro managery TTP, vývojové pracovníky a provozní zaměstnance a pomoci jim při používání a managementu TTP;

b) poučení pro entity ohledně služeb vykonávaných TTP a příslušných rolí a odpovědností TTP a entit při používání jejich služeb.

Další aspekty obsažené v tomto Doporučení | Technické zprávě mají poskytnout:

a) přehled popisu poskytnutých služeb;

b) pochopení role TTP a jejich funkčních prvků;

c) základ pro vzájemné uznání služeb, poskytnutých různými TTP;

d) poučení o vzájemném působení entit a TTP.

1 Předmět normy

Se zajiš»ováním a provozem důvěryhodných třetích stran (TTP) je spojen určitý počet s bezpečností souvisících problémů, pro který je nutný obecný návod sloužící jako pomoc podnikatelským entitám, vývojovým pracovníkům a poskytovatelům systémů a služeb, atd. Zahrnuje to návod k řešení problémů týkajících se rolí, postavení a vztahů TTP a entit používajících služby TTP, generických bezpečnostních požadavků, kdo by mohl poskytovat jaký typ bezpečnosti, jaká jsou možná bezpečnostní řešení a provozní používání a management bezpečnosti služeb TTP.

Toto Doporučení | Technická zpráva poskytuje návod pro používání a management TTP, jasnou definici poskytovaných základních povinností a služeb, jejich popis a jejich účel a role a odpovědnosti TTP a entit používajících služby těchto TTP. Je určeno v prvé řadě pro managery systémů, vývojové pracovníky, operátory TTP a uživatele v podnicích, pro výběr služeb těchto TTP, vyžadovaných pro konkrétní požadavky, jejich další management, použití a provozní rozmístění a ustavení bezpečnostní politiky v TTP. Nemělo by být použito jako základ pro formální hodnocení TTP nebo pro porovnání různých TTP.

Toto Doporučení | Technická zpráva určuje rozdílné hlavní kategorie služeb TTP zahrnující: vyznačení času, nepopiratelnost, správu klíčů, management certifikátů a elektronického veřejného notáře. Každá z těchto hlavních kategorií sestává z několika služeb, které logicky patří dohromady.

-- Vynechaný text --