ČESKÁ TECHNICKÁ NORMA

ICS 35.240.40

Květen

1998

	Bankovnictví - Správa klíčů prostřednictvím asymetrických algoritmů - Část 1: Zásady, postupy a formáty	ČSN ISO 11166-1 97 9118

Banking **-** Key management by means of asymmetric algorithms - Part 1: Principles, procedures and formats

Banque - Gestion de clés au moyen d,algorithmes asymétriques - Partie 1: Principes, procédures et formats

Bankwesen - Schlüsselverwaltung durch asymmetrische Algorithmen - Teil 1: Grundsätze, Prozeduren und Formate

Tato norma je českou verzí mezinárodní normy ISO 11166-1:1994. Mezinárodní norma ISO 11166-1 má status české technické normy.

This standard is the Czech version of the International Standard ISO 11166-1:1994. The International Standard ISO 11166-1:1994 has the status of a Czech standard.

52058

Národní předmluva

Citované normy

ISO/IEC 646:1991 zavedena v ČSN ISO/IEC 646 Informační technika - 7-bitový kódovaný soubor znaků ISO pro výměnu informací (36 9104)

ISO 8730:1990 zavedena v ČSN ISO 873O:1995 Bankovnictví - Požadavky na autentizaci zpráv (bankovní služby pro velkou klientelu) (97 9008)

ISO 8731-1:1987 zavedena v ČSN ISO 8731-1:1995 Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 1: DEA (97 9003)

ISO 8731-2:1992 zavedena v ČSN ISO 8731-2:1995 Bankovnictví - Schválené algoritmy pro autentizaci zprávy - Část 2: Algoritmus autentikátora zprávy (97 9003)

Vypracování normy

Zpracovatel normy: Ing. Hana Pačesová, IČO 7919

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

MEZINÁRODNÍ NORMA	
Bankovnictví - Správa klíčů prostřednictvím	ISO 11166-1
asymetrických algoritmů -	První vydání
Část 1: Zásady, postupy a formáty	1994-11-15

MDT

Deskriptory: banking, banking documents, financial processing, data processing, messages, inter-bank payment messages, protection of information, key management, security techniques, authentication, message authentication codes, algorithms, procedure, formats, generalities.

Předmluva

ISO (Mezinárodní organizace pro normalizaci) je celosvětovou federací národních normalizačních organizací (členů ISO). Na mezinárodních normách obvykle pracují technické komise ISO. Každý člen ISO, který se zajímá o předmět, pro který byla vytvořena technická komise, má právo být zastoupen v této technické komisi. Práce se zúčastňují i mezinárodní komise, vládní i nevládní, s nimiž ISO navázalo pracovní styk. ISO úzce spolupracuje ve všech záležitostech technické normalizace s Elektrotechnickou komisí (IEC).

Návrhy mezinárodních norem přijaté technickými komisemi se rozesílají členům ISO k hlasování. Vydání mezinárodní normy vyžaduje souhlas alespoň 75% z hlasujících členů.

Mezinárodní norma ISO 11166-1 byla připravena technickou komisí ISO/TC 68, *Bankovnictví a souvisící finanční služby*, subkomise 2, *Činnosti a postupy.*

Tato část ISO 11166 souvisí s ISO 8732 *Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu), na základě které byla vyvinuta.*

ISO 11166-1 sestává z následujících částí se společným názvem *Bankovnictví - Správa klíčů prostřednictvím asymetrických algoritmů:*

- *Časť 1: Zásady, postupy a formáty*
- *Část 2: Schválené algoritmy používající kryptosystém RSA.*

Přílohy A až F této části ISO 11166 jsou pouze pro informaci.

Obsah

Tato mezinárodní norma popisuje postupy pro bezpečnou správu materiálu klíče, používané k ochraně zpráv v prostředí bankovních služeb pro velkou klientelu.

Správa klíčů je proces, při kterém jsou kryptografické klíče a inicializační vektory (materiál klíče) poskytnuty k použití dvěma stranám a jsou předmětem postupů bezpečného zacházení až do doby, kdy jsou zničeny. Bezpečnost dat zašifrovaných nebo autentizovaných prostřednictvím materiálu klíče je závislá na prevenci neautorizovaného odhalení, modifikace, nahrazení, vložení nebo vymazání klíčů nebo inicializačních vektorů (IV). Jestliže jsou tyto kompromitovány, nemůže již být zajištěna bezpečnost souvisících dat. Správa klíčů se proto zabývá postupy pro generování, distribuci, uložení, správu, monitorování, zničení a zálohování materiálů klíče. Formalizace těchto postupů vede k návrhu na zřízení auditních záznamů.

Automatizovaná distribuce klíčů je prostředek, který poskytuje dvěma komunikujícím stranám identický symetrický materiál klíče (kryptografické klíče, a kde je to potřebné, i IV) použitím definovaného postupu prostřednictvím komunikačního kanálu. Automatizovaná distribuce klíčů v této normě používá dva typy klíčů:

(1) Klíče pro asymetrické algoritmy: tyto klíče jsou používané k zašifrování a dešifrování datových klíčů a také k vytváření a ověřování digitálních podpisů pro autentizaci datových klíčů nebo zpráv obsahujících tyto klíče.

(2) Klíče pro symetrické algoritmy: tyto klíče jsou datové klíče, které jsou předmětem správy klíčů. Jsou také používány k poskytnutí hodnot pro kontrolu integrity (MAC) pro některé zprávy vyměňované pro správu klíčů.

Úroveň bezpečnosti, které má být dosaženo, se musí vztahovat k určitému počtu faktorů, včetně citlivosti dotyčných dat a pravděpodobnosti, že budou narušena, praktičnosti jakéhokoliv předpokládaného šifrovacího procesu a ceny za pořízení a narušení speciálních prostředků na zajištění bezpečnosti. Je proto nutné dohodnout pro každou komunikující dvojici rozsah a podrobnosti postupů týkajících se bezpečnosti a správy klíčů. Absolutní bezpečnost není prakticky dosažitelná, takže cílem postupů pro správu klíčů nemusí být jen snížení příležitosti k narušení bezpečnosti, ale i ”vysoká” pravděpodobnost detekce každého nezákonného přístupu nebo změny materiálu klíče, které mohou nastat přes jakákoliv bezpečnostní opatření. To je aplikovatelné na všechny stupně generování a použití materiálu klíče, včetně těch procesů, které se vyskytnou v kryptografickém zařízení a těch, které se vztahují ke komunikaci kryptografických klíčů a inicializačních vektorů mezi komunikujícími dvojicemi nebo centry pro klíče. Proto i když všude, kde je to možné, specifikovala tato norma požadavky v absolutních podmínkách, nelze se v některých případech vyhnout určitému stupni subjektivity. Např. definování četnosti změn klíčů je mimo rozsah této normy a bude záviset na stupni rizika, spojeného s výše uvedenými faktory.

1. část této mezinárodní normy je rozdělena do dále uvedených částí:

1. Všeobecně

2. Certifikace klíčů

3. Automatická distribuce materiálu klíče

4. Zprávy kryptografické služby

Konečné podrobnosti postupů pro správu klíčů musí být dohodnuty mezi dotyčnou komunikující dvojicí a tato dvojice také za ně zůstává zodpovědná. Jedním aspektem podrobností, které budou muset být dohodnuty, je identita a povinnosti vybraných jednotlivců. Tato mezinárodní norma se nezabývá

přidělením individuálních odpovědností, protože ty musí být posouzeny jedinečně při každé implementaci správy klíčů.

Příloha A podává přehled používaných zásad.

Oddíl 1: Všeobecně

1.1 Předmět normy

Tato část ISO 11166 specifikuje metody pro správu materiálu klíč**e** používaného pro zašifrování, dešifrování a autentizaci zpráv vyměňovaných v průběhu finančních transakcí pouze v oblasti bankovních služeb pro velkou klientelu. Specifikuje požadavky na

i) řízení materiálu klíče v průběhu jeho životního cyklu k prevenci neautorizovaného odhalení, modifikace, nahrazení a opakovaného přenosu;

ii) ruční nebo automatickou distribuci materiálu klíče, aby byla možná interoperabilita mezi kryptografickým zařízením nebo vybavením, používajícím stejný algoritmus;

iii) zajištění integrity materiálu klíče v průběhu všech fází jeho životního cyklu, včetně jeho generování, distribuce, ukládání, zápisu, používání, archivování a zničení;

iv) obnovu v případě selhání procesu distribuce klíčů.

Tato část ISO 11166 poskytuje prostředek, který může identifikovat auditní záznam pro celý materiál klíče.

Tato mezinárodní norma je navržena pro správu materiálu klíče, používaného u symetrických algoritmů. Distribuce klíčů je prováděna s použitím asymetrického algoritmu nebo algoritmů. Je navržena pro zprávy formátované a přenášené v kódovaných sadách znaků.

Tato mezinárodní norma definuje dvě alternativní metody, pomocí kterých získají dvě komunikující strany totožný materiál symetrického klíče, který potom mohou použít k ochraně komunikací.

Jedna metoda je *přeprava klíče*, při které jedna strana generuje materiál klíče a posílá ho druhé straně, přičemž ho přiměřeně chrání použitím asymetrických algoritmů.

Druhá metoda je *výměna klíče*, při které každá strana komunikující dvojice posílá té druhé blok dat, a s použitím přijatého bloku dat odvozuje materiál klíče takovým způsobem, aby sady materiálu klíče, takto odvozené těmito dvěma stranami, byly identické.

POZNÁMKA - Dobře známý příklad výměny klíčů je metoda výměny klíčů podle Diffie-Hellmana.

V této mezinárodní normě zahrnuje termín *distribuce klíčů* jak přepravu klíčů tak jejich výměnu. Tato část ISO 11166 zahrnuje přepravu klíčů, ale nevylučuje výměnu klíčů. Specifické postupy výměny klíčů mohou být předmětem dalších částí této mezinárodní normy.

Specifikované postupy jsou vhodné k využití finančními ústavy a jejich korporativními a vládními zákazníky, a v dalších vztazích, kde výměna informací vyžaduje důvěrnost, ochranu a autentizaci.

-- Vynechaný text --