ČESKÁ NORMA

ICS 03.060

Únor 1996

Bankovnictví - Autentizace přihlášením

ČSN
ISO 11131

97 9002

Banking and related financial services - Sign-on authentication

Banque et services financiers liés aux opérations bancaires - Authentification par signature

Bankwesen und zusammenhängende Finanzdienstleistungen - Unterschriftsbeglaubigung

Tato norma je identická s ISO 11131:1992, první vydání.

Národní předmluva

Citované normy

ISO 8372:1987 dosud nezavedena

ISO 8730 zavedena v ČSN ISO 8730 Bankovnictví - Požadavky na autentizaci zprávy (bankovní služby pro velkou klientelu) (97 9008)

ISO 8732:1988 zavedena v ČSN ISO 8732 Bankovnictví - Správa klíčů (bankovní služby pro velkou klientelu)

ISO 10126-1:1991 zavedena v ČSN 10126-1 Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - 1. část: Obecné principy

ISO 10126-2:1991 zavedena v ČSN 10126-2 Bankovnictví - Postupy pro šifrování zpráv (bankovní služby pro velkou klientelu) - 2. část: Algoritmus DEA

Vypracování normy

Zpracovatel: Ing. Dagmar Jírová, IČO l865l399

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

Bankovnictví a související finanční služby
Autentizace podpisem

ISO 11131
První vydání
1992-09-15

Obsah strana

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 organizace, vládní i nevládní, s nimiž ISO navázala pracovní styk. ISO úzce spolupracuje s Mezinárodní elektrotechnickou komisí (IEC) ve všech záležitostech normalizace v elektrotechnice.

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 11131 byla připravena technickou komisí ISO/TC 68 *Bankovnictví a související finanční služby*,

subkomisí SC2, *Operace a postupy*.

Technické normativní prvky této mezinárodní normy jsou založeny na ANSI X9.26.

Příloha A této mezinárodní normy má pouze informativní charakter.

Úvod

Finanční instituce používají ve stále větší míře elektronickou komunikační technologii, aby svým zákazníkům poskytly služby, které jsou přesnější, bez chyb a odpovídají potřebám individuelního klienta. Taková technika umožňuje zákazníkovi zvýšenou měrou přímý přístup k aplikacím finanční instituce, uloženým na jejích počítačích (nebo jejich podepsání). Jako specifické příklady lze uvést převody fondů a služby spojené s řízením hotovostí.

Historicky standardní metodou, přijatou finančním sektorem k zajištění přímého přístupu k systému provozovatele služby, je použití individuálního identifikátoru pro každého uživatele (userid) v kombinaci s tajným heslem.

Účinnost takovýchto systémů hesel má však svá omezení. Prezentace hesla k autentizaci uživatele v čitelném tvaru může být kompromitována mnoha způsoby. Heslo může být např. uhádnuto, odposlechnuto nebo srozumitelně zobrazeno na displeji. Existují dvě možná ohrožení - vydávání se za někoho jiného a opakovaný přenos:

- Vydávání se za někoho jiného je napodobení entity předložením ukradeného hesla; obvykle je doprovázeno dalšími útoky jako je modifikace dat.

- Opakovaný přenos je opakovaná prezentace zaznamenané platné datové výměny s novějším datem s cílem dosáhnout neautorizovaného účinku.

Procedura zajišťující bezpečný podpis, kdy obě strany sdílejí společný tajný klíč, vyžaduje splnění řady podmínek, zahrnující dále uvedené požadavky:

a) zachovat integritu hardwarového a softwarového řešení uzlů v systému autentizace;

b) zachovat integritu autentizační informace (např. přiřazení identifikátorů uživatele (userid),

výběr hesla, změny hesla, prostředky pro zrušení přístupu, audit neúspěšných podpisových pokusů) mezi žadatelem a grantorem;

c) zachovat kontinuitu autentizace během relace po úspěšném podpisu;

d) zajistit možnost provádění auditu neúspěšných pokusů o podpis;

e) zajistit integritu systému správy klíčů proti kompromitování a zneužití;

f) zajistit důvěrnost přenášené autentizační informace;

g) zajistit prostředky pro detekci opakovaného přenosu ověřením autentizační informace;

1 Předmět normy

Tato mezinárodní norma realizuje podmínky (f) a (g) uvedené v úvodu. Specifikuje tři druhy autentizace podpisem mezi entitami vyžadujícími přístup a entitami schopnými udělit přístup:

a) Autentizace uživatele prostřednictvím Personální autentizační informace (PAI) jako je např. heslo;

b) Autentizace uživatele pomocí klíče jedinečného pro každého uživatele;

c) Autentizace uzlu pomocí klíče jedinečného pro každý uzel;

Tato mezinárodní norma je určena pro použití spolu se symetrickým algoritmem (s tajným klíčem), kde žadatel i grantor používají stejný klíč.

V odstavci 6 je uveden příklad protokolu, který splňuje požadavky této mezinárodní normy; k dosažení interoperability je nutná shoda s touto normou. V příloze A jsou uvedena omezení vztahující se k této normě.

-- Vynechaný text --