ČESKÁ TECHNICKÁ NORMA

ICS 35.240.40

Prosinec 1997

Bankovnictví - Správa klíčů (bankovní služby pro drobnou klintelu) Část 1: Úvod do správy klíčů

ČSN EN IS O 11568-1

97 9114

Banking - Key management (retail) - Part 1: Introduction to key management

Banque - Gestion de clés (services aux particuliers) - Partie 1: Introduction à la gestion de clés

Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 1: Einführung in die Schlüsselverwaltung

Tato norma přejímá anglickou verzi evropské normy EN ISO 11568-1:1994. Evropská norma EN ISO 11568-1:1994 má status české technické normy.

This standard implements the English version of the European Standard EN ISO 11568-1:1994. The European Standard EN ISO 11568-1:1994 has the status of a Czech Standard.

Anotace obsahu

Tato část normy ČSN EN ISO 11568 specifikuje zásady pro správu klíčů v šifrovacích systémech implementovaných v prostředí bankovních služeb pro drobnou klientelu. Prostředí bankovních služeb pro drobnou klientelu zahrnuje rozhraní mezi zařízením akceptujícím kartu a držitelem karty a mezi držitelem karty a jejím vydavatelem. Příklad tohoto prostředí je popsán v příloze B a nebezpečí spojená s implementací této normy do prostředí bankovních služeb pro drobnou klientelu jsou uvedena v příloze C. Tato část normy ČSN EN ISO 11568 se týká jak klíčů systémů symetrických šifer, kde jak odesílatel tak příjemce používají tentýž tajný(é) klíč(e), tak tajných a veřejných klíčů v systémech asymetrických šifer, pokud není stanoveno jinak. Postup pro schválení kryptografických algoritmů používaných pro správu klíčů je specifikován v příloze A.

Používání šifer často zahrnuje řídící (kontrolní) informace jiné než klíče, např. inicializační vektory (původce) a identifikátory klíčů. Tyto další informace se souhrnně nazývají „materiál klíče". Ačkoliv tato část normy ČSN EN ISO 11568 se výslovně věnuje správě klíčů, zásady, služby a techniky použitelné pro klíče se mohou týkat také materiálu klíče.

Tato část normy ČSN EN ISO 11568 je vhodná pro využití ve finančních institucích a dalších organizacích, které pracují v oblasti bankovních služeb pro drobnou klientelu, kde výměna informací vyžaduje důvěrnost, integritu a autenticitu. Bankovní služby pro drobnou klientelu zahrnují, ale nejsou limitovány takovými postupy jako je autorizace vkladů a úvěrů v místě prodeje, transakce výdajových automatů a ATM, atd.

Nahrazení předchozích norem

Tato norma nahrazuje ČSN EN ISO 11568-1 (97 9114) Bankovnictví- Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů z prosince 1996.

Národní předmluva

Struktura normy

ČSN EN ISO 11568 po hlavním názvem Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) se skládá z následujících částí:

- Část 1: Úvod do správy klíčů
- Část 2: Techniky správy klíčů pro symetrickou šifru
- Část 3: Životní cyklus klíče pro symetrickou šifru
- Část 4: Techniky správy klíčů pro asymetrickou šifru
- Část 5: Životní cyklus klíče pro asymetrickou šifru
- Část 6: Schémata pro správu klíčů

Změny proti předchozí normě

Proti předchozí normě dochází ke změně způsobu převzetí EN ISO 11568-1:1996 do soustavy norem ČSN. Zatímco ČSN EN ISO 11568-1 z prosince 1997 převzala EN ISO 11568-1:1996 schválením k přímému používání jako ČSN, tato norma ji přejímá převzetím originálu s překladem úvodní části normy.

Citované normy

ISO 8908:1993 zavedena v ČSN ISO 8908 Bankovnictví a související bankovní služby - Slovník a datové prvky (97 9118)

Vypracování normy

Zpracovatel: INFO 7, Praha, IČO: 44266154 Ing. Jiří Roleček,

Technická normalizační komise: TNK 42 Výměna dat

Pracovník Českého normalizačního institutu: Ing. Petr Wallenfels

EVROPSKÁ NORMA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO 11568-1
Červen 1996

ICS 35 100

Deskriptory: viz ISO norma

Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů (ISO 11568-1:1994)

Banking - Key management (retail) - Part 1: Introduction to key management(ISO 11568-1:1994)

Banque - Gestion de clés (services aux particuliers) - Partie 1: Introduction ŕ la gestion de clés(ISO 11568-1:1994)

Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 1: Einführung in die Schlüsselverwaltung (ISO 11568-1:1994)

Tato evropská norma byla schválena CEN

Členové CEN jsou povinni splnit požadavky Vnitřních předpisů CEN/CENELEC, v nichž jsou stanoveny podmínky, za kterých se této evropské normě bez jakýchkoliv modifikací uděluje statut národní normy.

Aktualizované seznamy a bibliografické citace týkající se těchto národních norem lze vyžádat v Ústředím sekretariátu CEN nebo u každého člena CEN.

Tato evropská norma existuje ve třech oficiálních verzích (anglické, francouzské, německé). Verze v každém jiném jazyce přeložená členem CEN do jeho vlastního jazyka, a kterou notifikuje Ústřednímu sekretariátu CEN, má stejný status jako oficiální verze.

Členy CEN jsou národní normalizační orgány Belgie, České republiky, Dánska, Finska, Francie, Irska, Islandu, Itálie, Lucemburska, Německa, Nizozemska, Norska, Portugalska, Rakouska, Řecka, Spojeného království, Španělska, Švédska a Švýcarska.

CEN

Evropská komise pro normalizaci

European Committee for Standardization

Comité Européen de Normalisation

Europäisches Komitee für Normung

Ústřední sekretariát: rue de Strassart 36, B-1050 Brussels

Předmluva

Text mezinárodní normy vypracovaný v technické komisi ISO/TC 68 „Bankovnictví a související finanční služby" Mezinárodní organizace pro normalizaci (ISO) byl převzat jako evropská norma technickou komisí CEN/TC 224 „Strojem čitelné karty, související rozhraní a postupy", sekretariátem při AFNOR.

Této evropské normě musí být udělen status národní normy buď vydáním identického textu, nebo schválením k přímému používání nejpozději do prosince 1996 a konfliktní národní normy musí být zrušeny nejpozději do prosince 1996.

V souladu s Vnitřními předpisy CEN/CENELEC se následující země zavazují, že zavedou tuto evropskou

normu: Belgie, Česká republika, Dánsko, Finsko, Francie, Irsko, Island, Itálie, Lucembursko, Německo, Nizozemsko, Norsko, Portugalsko, Rakousko, Řecko, Spojené království, Španělsko, Švédsko a Švýcarsko.

Oznámení o schválení

Text mezinárodní normy ISO 11568-1:1994 byl schválen CEN jako evropská norma bez jakýchkoliv modifikací.

INTERNATIONAL STANDARD

ISO 11568-1 First edition 1994-12-01

Banking - Key management (retail) -

Part 1:

Introduction to key management

Banque - Gestion de clés (services aux particuliers) -

Partie 1: Introduction ŕ la gestion de clés

Reference number

ISO 11568-1:1994(E)

Obsah strana

Contents Page

International Organization for Standardization

Case Postale 56 · CH-1211 Genčve 20 · Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 11568-1 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services,* Subcommittee SC 6, *Financial transaction cards, related media and operations.*

ISO 11568 consists of the following parts, under the general title *Banking - Key management (retail):*

- *Part 1: Introduction to key management*
- *Part 2: Key management techniques for symmetric ciphers*
- *Part 3: Key life cycle for symmetric ciphers*
- *Part 4: Key management techniques for asymmetric ciphers*

- Part 5: Key life cycle for asymmetric ciphers

- Part 6: Key management schemes

Annex A forms an integral part of this part of ISO 12568. Annexes B, C and D are for information only.

Introduction

ISO 11568 describes procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Key management of keys used in an Integrated Circuit Card (ICC) environment is nor covered by ISO 11568 but will be addressed in another ISO standard.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this standard addresses the key management requirements that are applicable in the accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machine (ATM) transactions.

Key management is the process whereby cryptographic keys are provided for use between authorized communicating parties and those keys continue to be subject to secure procedures until they have been destroyed. The security of the eciphered data is dependent upon the prevention of disclosure and unauthorized modification, substitution, insertion, or termination of keys. Thus, key management is concerned with the generation, storage, distribution, use, and destruction procedures for keys. Also, by the formalization of such procedures, provision is made for audit trails to be established.

This part of ISO 11568 does not provide a means to distinguish between parties who share common keys. The final details of the key management procedures need to be agreed upon between the communicating parties concerned and will thus remain the responsibility of the communication parties. One aspect of the details to be agreed upon will be the identity and duties of particular individuals. ISO 11568 does nor concern itself with allocation of individual responsibilities; this needs to be considered for each key management implementation.

ISO 9564 and ISO 9807 specify the use of cryptographic operations within retail financial transactions for personal identification number (PIN) encipherment and message authentication, respectively. ISO 11568 is applicable to the management of the keys introduced by those standards. Additionally, the key management procedures may themselves require the introduction of further keys, e. g. key encipherment keys. The key management procedures are equally applicable to those keys.

Prázdná strana!

Banking - Key management (retail) -

Part 1:

Introduction to key management

1 Scope

This part of ISO 11568 specifies the principles for the management of keys used in cipher systems implemented within the retail banking environment. The retail banking environment involves the interface between a card accepting device and n acquirer and between an acquirer and a card issuer. An example of this environment is described in annex B, and threats associated with the implementation of this standard in the retail banking environment are elaborated in annex C.

This part of ISO 11568 applies both to the keys of symmetric cipher systems, where both originator and recipient use the same secret key(s), and to the secret and public keys of asymmetric cipher systems, unless otherwise stated. The procedure for the approval of cryptographic algorithms used for key management is specified in annex A.

The use of ciphers often involves control information other than keys, e. g., initialization vectors and key identifiers. This other information is collectively called „keying material". Although this part of ISO 11568 specifically addresses the management of keys, the principles, services, and techniques applicable to keys may also be applied to keying material.

This part of ISO 11568 is appropriate for use by financial institutions and other organizations engaged in the area of retail financial services, where the interchange of information requires confidentiality, integrity, or authentication. Retail financial services include but are not limited to such processes as POS debit and credit authorizations, automated dispensing machine and ATM transactions, etc.

-- Vynechaný text --