ČESKÁ TECHNICKÁ NORMA

ICS 35.240.40

Prosinec 1997

Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) Část 2: Techniky správy klíčů pro symetrickou šifru

ČSN EN IS O 11568-2

97 9114

Banking - Key management (retail) - Part 2: Key management techniques for symmetric ciphers

Banque - Gestion de clés (services aux particuliers) - Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques

Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 2: Schlüsselverwaltungstechniken für symmetrisch Verschlüsselungen

Tato norma přejímá anglickou verzi evropské normy EN ISO 11568-2:1994. Evropská norma EN ISO 11568-2:1994 má status české technické normy.

This standard implements the English version of the European Standard EN ISO 11568-2:1994. The European Standard EN ISO 11568-2:1994 has the status of a Czech Standard.

Anotace obsahu

Tato část normy ČSN EN ISO 11568 specifikuje techniky ochrany kryptografických klíčů pro symetrické šifry užívané v prostředí bankovních služeb pro drobnou klientelu. Je aplikovatelná v libovolné organizaci, která je zodpovědná za implementované procedury k ochraně klíčů během jejich životního cyklu. Techniky popsané v této části umožňují dodržení zásad popsaných v normě ČSN EN ISO 11568-1. Popsané techniky jsou aplikovatelné v libovolném algoritmu pro symetrickou n-bitovou blokovou šifru. Notace použitá v této části normy ČSN EN ISO 11568 jsou uvedena v příloze A. Algoritmus schválený pro použití v technikách popsaných v této části normy je uveden v příloze B.

Nahrazení předchozích norem

Tato norma nahrazuje ČSN EN ISO 11568-2 (97 9114) Bankovnictví- Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru 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 11568-2:1996 do soustavy norem ČSN. Zatímco ČSN EN ISO 11568-2 z března 1997 převzala EN ISO 11568-2:1996 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) ISO/IEC 10116:1991 zavedena v ČSN ISO/IEC 10116 Informační technologie - Mody činnosti pro algoritmus n-bitové blokové šifry (36 9742)

ISO 11568-1:1994 zavedena v ČSN EN ISO 11568-1 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 1: Úvod do správy klíčů (97 9194)

ISO 11568-3:1994 zavedena v ČSN EN ISO 11568-3 Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 3: Životní cyklus pro symetrickou šifru (97 9194)

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

EN ISO 11568-2
Červen 1996
NORME EUROPÉENNE
EUROPÄISCHE NORM

ICS 35 100

Deskriptory: viz ISO norma

Bankovnictví - Správa klíčů (bankovní služby pro drobnou klientelu) - Část 2: Techniky správy klíčů pro symetrickou šifru (ISO 11568-2:1994)

Banking - Key management (retail) - Part 2: Key management techniques for symmetric ciphers(ISO 11568-2:1994)

Banque - Gestion de clés (services aux particuliers) - Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques(ISO 11568-2:1994)

Bankwesen - Schlüsselverwaltung (Einzelhandel) - Teil 2: Schlüsselverwaltungstechniken für symmetrisch Verschlüsselungen (ISO 11568-2:1994)

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 11568-2:1994 byl schválen CEN jako evropská norma bez jakýchkoliv modifikací.

INTERNATIONAL STANDARD

ISO 11568-2 First edition 1994-12-01

Banking - Key management (retail) -

Part 2:

Key management techniques for symmetric ciphers

Banque - Gestion de clés (services aux particuliers) - Partie 2: Techniques de gestion de clés pour les algorithmes cryptographiques symétriques

Reference number

ISO 11568-2:1994(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 approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 11568-2 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

Annexes A, B and C form an integral part of this part of ISO 11568. Annexes D, E and F are for information only.

Introduction

ISO 11568 is one of a series of standards describing procedures for the secure management of 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 not 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 machines (ATM) transactions.

ISO 11568-2 describes key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

- key separation

- key substitution prevention

- key identification

- key synchronization

- key integrity

- key confidentiality

- key compromise detection

The key management services and the corresponding key management techniques are cross referenced in clause 6.

INTERNATIONAL STANDARD Ó **ISO ISO 11568-2:1994(E)**

Banking - Key management (retail) -

Part 2:

Key management techniques for symmetric ciphers

1Scope

This part of ISO 11568 specifies techniques for the protection of the cryptographic keys for symmetric ciphers used in a retail banking environment.

It is applicable to any organization which is responsible for implementing procedures for the protection of keys during the life cycle. The techniques described in this part enable compliance with the principles described in ISO 11568-1.

The techniques described are applicable to any symmetric *n*-bit block cipher algorithm.

The notation used in this part of ISO 11568 is given in annex A.

Algorithms approved for use with the techniques described in this part of ISO 11568 are given in annex B.

-- Vynechaný text --