

Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards —

Part 3: Cryptographic key relationships

The European Standard EN ISO 10202-3:1998 has the status of a British Standard

ICS 35.240.15

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

National foreword

This British Standard is the English language version of EN ISO 10202-3:1998. It is identical with ISO 10202-3:1998.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Banking, Securities and other financial services, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

Attention is drawn to the fact that CEN and CENELEC standards normally include an annex which lists normative references to international publications with their corresponding European publications. The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the EN ISO title page, page 2, the ISO title page, page ii, pages 1 to 15 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 November 1998

© BSI 06-1999

ISBN 0 580 30580 5

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
National foreword	Inside front cover
Foreword	2
Foreword	ii
Text of ISO 10202-3	1

English version

Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards — Part 3: Cryptographic key relationships

(ISO 10202-3:1998)

Cartes de transactions financières —
Architecture de sécurité des systèmes de
transactions financières utilisant des cartes à
circuit intégré — Partie 3: Relations entre les
clés cryptographiques
(ISO 10202-3:1998)

Bankkarten — Sicherheitsarchitektur in
Zahlungsverkehrssystemen für Karten mit
integrierten Schaltkreisen —
Teil 3: Beziehungen zwischen
kryptographischen Schlüsseln
(ISO 10202-3:1998)

This European Standard was approved by CEN on 29 May 1998.

CEN members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CEN member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN member into its own language and notified to the Central Secretariat has the same status as the official versions.

CEN members are the national standards bodies of Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and United Kingdom.

CEN

European Committee for Standardization
Comité Européen de Normalisation
Europäisches Komitee für Normung

Central Secretariat: rue de Stassart 36, B-1050 Brussels

Foreword

The text of the International Standard ISO 10202-3:1998 has been prepared by Technical Committee ISO/TC 68 “Banking, securities and other financial services” in collaboration with Technical Committee CEN/TC 224 “Machine-readable cards, related device interfaces and operations”, the secretariat of which is held by AFNOR.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by January 1999, and conflicting national standards shall be withdrawn at the latest by January 1999.

According to the CEN/CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Czech Republic, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom.

Endorsement notice

The text of the International Standard ISO 10202-3:1998 was approved by CEN as a European Standard without any modification.

Contents

	Page
Foreword	2
1 Scope	1
2 Normative references	1
3 Definitions and abbreviations	2
4 General security principles	2
5 Notation for key relationships and associated keys	2
6 Key relationships	3
7 Key relationships for ICCs	5
8 Key relationships for sams	8
Annex A (normative) Key relationships (ICC) table	10
Annex B (normative) Key relationships (SAM) table	11
Annex C (informative) Example for cryptographic key hierarchy in an IC	12
Annex D (informative) How to use the cryptographic keys	13
Figure 1 — Stages of the ICC or SAM preparation and keys used during that process.	4
Figure 2 — Transaction relationships	5
Figure 3 — Cryptographic key layered structure for ICCs	6
Figure 4 — Cryptographic key layered structure for SAMs	8
Table 1 — Key nomenclature	3
Table 2 — Possible production keys before card personalisation	6
Table 3 — Key relationships during card personalisation	7
Table 4 — Key relationships during or after card personalisation	8
Table 5 — Possible production keys before SAM initialisation	8
Table 6 — Key relationships during SAM initialisation	9

INTERNATIONAL STANDARD

**ISO
10202-3**

First edition
1998-07-01

Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards —

Part 3: Cryptographic key relationships

*Cartes de transactions financières — Architecture de sécurité des systèmes
de transactions financières utilisant des cartes à circuit intégré —*

Partie 3: Relations avec les clés de chiffrement



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 voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 10202-3 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

ISO 10202 consists of the following parts, under the general title *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*:

- *Part 1: Card life cycle;*
- *Part 2: Transaction process;*
- *Part 3: Cryptographic key relationships;*
- *Part 4: Secure application modules;*
- *Part 5: Use of algorithms;*
- *Part 6: Cardholder verification;*
- *Part 7: Key management;*
- *Part 8: General principles and overview.*

Annex A and Annex B form an integral part of this part of ISO 10202. Annex C and Annex D are for information only.

Descriptors: Banking, financial transactions, security techniques, identification cards, credit cards, IC cards, coded representation, cryptography.