

This is a preview of "ISO 11568:2023". [Click here to purchase the full version from the ANSI store.](#)

First edition
2023-02

Financial services — Key management (retail)

Services financiers — Gestion de clés (services aux particuliers)



Reference number
ISO 11568:2023(E)

© ISO 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

This is a preview of "ISO 11568:2023". [Click here to purchase the full version from the ANSI store.](#)

Contents

	Page
Foreword	v
Introduction	vi
1 Scope	1
1.1 General.....	1
1.2 Scope exclusions.....	1
2 Normative references	1
3 Terms and definitions	2
4 Key management requirements	12
4.1 General.....	12
4.1.1 Key management strategy.....	12
4.1.2 Dual control and split knowledge of secret or private keys.....	12
4.1.3 Permissible key forms.....	13
4.1.4 Logging.....	14
4.1.5 Cryptographic strength.....	15
4.1.6 Key locations.....	15
4.1.7 Single-purpose key usage.....	15
4.2 Secure cryptographic device.....	17
4.2.1 General requirements.....	17
4.2.2 Additional SCD requirements for devices used in SKDAT.....	18
4.3 Additional CA requirements.....	19
4.4 Additional RA requirements.....	19
4.5 Key blocks.....	20
4.5.1 Overview of key blocks.....	20
4.5.2 Key attributes.....	21
4.5.3 Integrity of the key block.....	21
4.5.4 Key and sensitive attributes field.....	21
4.6 Key creation.....	22
4.6.1 Symmetric key creation.....	22
4.6.2 Asymmetric key creation.....	23
4.7 Key component and key share creation.....	24
4.8 Check values.....	24
4.8.1 Introduction.....	24
4.8.2 Symmetric key check value calculation.....	25
4.8.3 Asymmetric key check value calculation.....	25
4.9 Key distribution.....	25
4.9.1 Symmetric key distribution.....	25
4.9.2 SKDAT asymmetric key distribution.....	29
4.10 Key loading.....	30
4.10.1 General.....	30
4.10.2 Loading key components or shares.....	31
4.11 Key utilization.....	32
4.11.1 General key utilization requirements.....	32
4.11.2 Additional key utilization requirements for SKDAT.....	33
4.12 Key storage.....	33
4.12.1 Cleartext key component and share storage.....	33
4.12.2 Public key storage.....	34
4.13 Key replacement.....	34
4.14 Key destruction.....	35
4.14.1 General.....	35
4.14.2 Key destruction from an SCD.....	36
4.14.3 Destruction of a key in cryptogram form.....	36
4.14.4 Component and share destruction.....	36
4.15 Key backup.....	36

This is a preview of "ISO 11568:2023". [Click here to purchase the full version from the ANSI store.](#)

4.16	Key archiving.....	36
4.17	Key compromise.....	37
5	Transaction key management techniques.....	38
5.1	General.....	38
5.2	Method: master keys or transaction keys.....	38
5.3	Derived unique key per transaction.....	39
5.3.1	General.....	39
5.3.2	DUKPT key management.....	39
5.3.3	Unique initial keys.....	42
5.3.4	AES DUKPT.....	43
5.3.5	KSN compatibility mode.....	46
5.3.6	Derived key OIDs.....	47
5.3.7	Keys and key sizes.....	47
5.3.8	Helper functions and definitions.....	48
5.3.9	Key derivation function algorithm.....	49
5.3.10	Derivation data.....	50
5.3.11	"Create Derivation Data" (local subroutine).....	51
5.3.12	Security considerations.....	52
5.3.13	Host security module algorithm.....	54
5.3.14	General.....	54
5.3.15	"Derive Initial Key".....	54
5.3.16	"Host Derive Working Key".....	55
5.3.17	Intermediate derivation key derivation data examples.....	55
5.3.18	Working key derivation data examples.....	56
5.3.19	Transaction-originating device algorithm.....	57
5.4	Host-to-host UKPT.....	62
Annex A (informative) Key and component check values.....		64
Annex B (normative) Split knowledge during transport.....		68
Annex C (informative) Trust models and key establishment.....		70
Annex D (informative) Symmetric key life cycle.....		78
Annex E (informative) Asymmetric key life cycle phases.....		80
Annex F (normative) Approved algorithms.....		83
Annex G (informative) AES DUKPT pseudocode notation.....		84
Annex H (informative) AES DUKPT test vectors.....		87
Annex I (informative) TDEA-derived unique key per transaction.....		88
Annex J (informative) Roles in payment environment.....		109
Annex K (informative) Roles in symmetric key distribution using asymmetric techniques.....		112
Bibliography.....		115

This is a preview of "ISO 11568:2023". [Click here to purchase the full version from the ANSI store.](#)

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Financial services, security*.

This document cancels and replaces the former ISO 11568 series, which has been technically revised.

The main changes are as follows:

- all parts of the series combined into a single document;
- fixed key no longer included in the permissible methods of transaction key management;
- required key replacement policy (see [4.13](#)) added;
- cleartext key injection removed;
- AES DUKPT introduced as a key management method.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Retail financial transactions are often transmitted over potentially non-secure channels, which, if exploited, can result in fraud. The vast range in value and volume of such transactions exposes participants to severe risks, which can be uninsurable. To protect against these risks, many institutions are employing encryption. The encryption algorithms used are in the public domain. The security and reliability of any process based on these algorithms is directly dependent on the protection afforded to secrets called cryptographic keys.

This document describes requirements and provides guidance for the secure management of cryptographic keys used to protect sensitive information in a retail financial services environment, for example in messages between a card acceptor and an Acquirer. Typical services in the retail financial services domain include point-of-sale (POS) debit and credit authorizations and automated teller machine (ATM) transactions. While it is designed with these environments in mind, it may also be used in unrelated applications. For example, such keys could be used for:

- encrypting Personal Identification Numbers (PIN) (see ISO 9564-1);
- authenticating messages;
- encrypting other data;
- encrypting or deriving cryptographic keys;
- automated symmetric key distribution using asymmetric techniques.