First edition
2023-02

Financial services — Key management (retail)

Services financiers — Gestion de clés (services aux particuliers)

Reference number
ISO 11568:2023(E)

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

Contents

Page

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.