INTERNATIONAL STANDARD

ISO 11568

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

© ISO 2023 – All rights reserved

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

© ISO 2023 – All rights reserved

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

© ISO 2023 – All rights reserved

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.

© ISO 2023 – All rights reserved

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.

© ISO 2023 – All rights reserved

Financial services — Key management (retail)

1 Scope

1.1 General

This document describes the management of symmetric and asymmetric cryptographic keys that can be used to protect sensitive information in financial services related to retail payments. The document covers all aspects of retail financial services, including connections between a card-accepting device and an Acquirer, between an Acquirer and a card Issuer, and between an ICC and a card-accepting device. It covers all phases of the key life cycle, including the generation, distribution, utilization, archiving, replacement and destruction of the keying material. This document covers manual and automated management of keying material, and any combination thereof, used for retail financial services. It includes guidance and requirements related to key separation, substitution prevention, identification, synchronization, integrity, confidentiality and compromise, as well as logging and auditing of key management events.

Requirements associated with hardware used to manage keys have also been included in this document.

1.2 Scope exclusions

This document does not specifically address internet banking services offered by an Issuer to their own customers through that financial institution's website or applications.

This document does not address using asymmetric keys to encrypt the Personal Identification Number (PIN) or any other data and does not address asymmetric keys managed with asymmetric keys.

This document is not intended to apply to the management of the keys installed in an ICC during manufacturing or the initial key established in an ICC during card personalization.

This document is not intended to address post-quantum encryption considerations. Key management using quantum technologies is out of scope of this document.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

ISO/IEC 11770 (all parts), *Information security — Key management*

ISO 13491 (all parts), *Financial services — Secure cryptographic devices (retail)*

ISO 16609, *Financial services — Requirements for message authentication using symmetric techniques*

ISO/IEC 18031, *Information technology — Security techniques — Random bit generation*

ISO/IEC 18032, *Information security — Prime number generation*

ISO/IEC 18033 (all parts), *Information security — Encryption algorithms*

ISO/IEC 19592-2, *Information technology — Security techniques — Secret sharing — Part 2: Fundamental mechanisms*

© ISO 2023 – All rights reserved

ISO/IEC 19772, *Information security — Authenticated encryption*

ISO 20038, *Banking and related financial services — Key wrap using AES*

ISO 21188:2018, *Public key infrastructure for financial services — Practices and policy framework*

ANSI X9.63, *Public Key Cryptography for the Financial Services Industry — Key Agreement and Key Management Using Elliptic Curve-Based Cryptography*

ANSI X9.143, *Retail Financial Services — Interoperable Secure Key Block Specification*

RFC 3647, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Internet Request for Comments 3647, S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, November 2003*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
Acquirer
institution (or its agent) which acquires from the card acceptor the data relating to the *transaction* (3.84) and initiates the data into an *Interchange* (3.47) system

[SOURCE: ISO/IEC 7812-1:2017, 3.1]

3.2
Advanced Encryption Standard
AES
16-byte block *cipher* (3.3)

Note 1 to entry: This is defined in ISO/IEC 18033-3.

3.3
algorithm
specified mathematical process for computation or set of rules which, if followed, will give a prescribed result

[SOURCE: ISO 16609:2022, 3.1]

3.4
archived key
inactive *cryptographic key* (3.28) that is being stored in a secure manner for a non-operational purpose

3.5
asymmetric algorithm
cryptographic algorithm (3.27) that uses two related keys, a *public key* (3.71) and a *private key* (3.69), where the two keys have the property that, given the public key, it is *computationally infeasible* (3.25) to derive the private key

3.6
asymmetric cryptosystem
cryptosystem using *asymmetric algorithms* (3.5)

© ISO 2023 – All rights reserved

3.7
authentication
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

3.8
authentication element
message element that is to be protected by *authentication* (3.7)

[SOURCE: ISO 16609:2022, 3.12, modified — Term revised.]

3.9
Base Derivation Key
BDK
key used in *derivation* (3.32) to generate *initial DUKPT keys* (3.45) for installation into transaction originating *secure cryptographic devices* (3.75) and for transaction processing

3.10
BDK ID
32-bit value that identifies the *Base Derivation Key* (3.9)

Note 1 to entry: This was formerly known as the *Key Set Identifier* (*KSI*) (3.57) in the TDEA DUKPT specification.

3.11
card acceptor
party accepting the card for the purpose of presenting transaction data to an *Acquirer* (3.1) or intermediary facilitating the transaction flow

[SOURCE: ISO/IEC 7812-1:2017, 3.3]

3.12
certificate
digitally signed statement that binds the value of a public key to the identity of the person, device or service that holds the corresponding private key

[SOURCE: ISO 20415:2019, 3.15, modified — Term revised.]

3.13
certificate authority
CA
entity that vouches for the binding between a device's identity, its public key and associated keying material

[SOURCE: ISO/IEC/IEEE 8802-11:2022, definition modified.]

3.14
certificate authority system
CA system
infrastructure required to manage, maintain and secure the key pairs and certificates of the *certificate authority* (3.13)

Note 1 to entry: A CA system will typically include one or more *Hardware Security Modules* (3.42), firmware, computer equipment, operating systems and software

3.15
certificate policy
CP
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

[SOURCE: ISO 21188:2018, 3.13]

© ISO 2023 – All rights reserved

3.16
certificate practice statement
CPS
statement of the practices which a *certificate authority* (3.13) employs in issuing *certificates* (3.12) and which defines the equipment, policies and procedures the certificate authority uses to satisfy the requirements specified in the *certificate policies* (3.15) that are supported by it

3.17
certificate subject
entity identified in a *certificate* (3.12)

EXAMPLE *Secure cryptographic device* (3.75).

3.18
chain of custody
demonstrable possession, movement, handling and location of material from one point in time until another

[SOURCE: ISO/IEC 27050-1:2019, 3.1]

3.19
check value
key check value
KCV
component check value
CCV
non-secret value that is cryptographically related to the key (or component) and is used to verify that the underlying value is as expected

Note 1 to entry: It is possible for different keys or components to have the same check value.

3.20
cipher
method for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

3.21
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 18033-1:2021, 3.7]

3.22
cleartext
plaintext
unencrypted information

[SOURCE: ISO/IEC 18033-1:2021, 3.20]

3.23
communicating pair
two parties (usually institutions) sending and receiving transactions

Note 1 to entry: This includes alternate processing sites either owned or contracted by either communicating party.

© ISO 2023 – All rights reserved

3.24
compromise
<cryptography> breach or failure of the security of a process or system used to protect the confidentiality or integrity of sensitive information

Note 1 to entry: Compromise includes situations in which either unauthorized disclosure of sensitive information could have occurred or appropriate control is not demonstrable.

3.25
computationally infeasible
property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it

3.26
credentials
identification data for an entity, incorporating at a minimum the entity's distinguished name and public key

3.27
cryptographic algorithm
algorithm (3.3) for the transforming of data using a *cryptographic key* (3.28)

Note 1 to entry: Data transformation includes operations such as *encryption* (3.40), *decryption* (3.31), synchronized generation of keying material and computation or verification of a digital signature or Message Authentication Code.

3.28
cryptographic key
key
sequence of bits that determine the outcome of a cryptographic operation

Note 1 to entry: See cryptographic algorithm for further details.

Note 2 to entry: Examples of cryptographic operations include encryption, decryption, check function computation, derivation, signature generation or verification, and authentication.

3.29
cryptographic strength
strength
computational cost of the most effective known attack against a given cryptographic algorithm and key size

Note 1 to entry: The cryptographic strength is usually a function of key size, but different algorithms can have different cryptographic strengths even though their key sizes are the same.

Note 2 to entry: The strength of a given algorithm and key size can vary depending on the use of the algorithm. For example, uses with few or no plaintext-ciphertext pairs could be more resistant to attack than uses with many pairs under a given key.

3.30
cryptoperiod
defined period of time during which a specific *cryptographic key* (3.28) is authorized for use or during which the cryptographic keys in a given system may remain in effect

[SOURCE: ISO 16609:2022, 3.9]

3.31
decryption
process of transforming *ciphertext* (3.21) data into *cleartext* (3.22) data

© ISO 2023 – All rights reserved

3.32
derivation
cryptographic transformation process that is used to derive one value from another value

Note 1 to entry: This is typically used to produce new *cryptographic keys* (3.28), which can potentially be used for different purposes, from a single key.

3.33
Derivation Identifier
Derivation ID
DID
32-bit value that identifies the specific *initial DUKPT key* (3.45) derived using the *Base Derivation Key* (3.9)

Note 1 to entry: This was formerly known as the 19-bit value Device ID (DID) or TRSM ID in the TDEA DUKPT specification.

3.34
derivation key
cryptographic key (3.28) that is used to cryptographically compute another key using *derivation* (3.32)

3.35
derived unique key per transaction
DUKPT
key management method that uses a unique key for each *transaction* (3.84) and prevents the disclosure of any past key used by the *transaction originating SCD* (3.86)

Note 1 to entry: The unique *transaction keys* (3.85) are derived from a *Base Derivation Key* (3.9) and non-secret data transmitted as part of each transaction.

3.36
digital certificate
asymmetric cryptosystem that provides for the creation and subsequent verification of *digital signatures* (3.37)

3.37
digital signature
cryptographic transformation of data which, when associated with a data unit and accompanied by the corresponding public-key certificate, provides the services of origin authentication, data integrity and signer non-repudiation

3.38
double-length TDEA key
TDEA key having a length of 128 bits, consisting of 112 key bits and 16 parity bits, which is typically represented in 32 hexadecimal digits

3.39
dual control
process of utilizing two or more separate individuals operating in concert to protect sensitive functions or information whereby no single individual is able to use the function or access all the information alone

Note 1 to entry: A *cryptographic key* (3.28) is an example of the type of material protected using dual control.

Note 2 to entry: For protecting cryptographic keys and other sensitive data, this concept is closely related to *split knowledge* (3.77).

[SOURCE: ISO 9564-1:2017, 3.10, modified — Definition revised and notes to entry added.]

© ISO 2023 – All rights reserved

3.40
encryption
encipherment
process of transforming *cleartext* (3.22) data into *ciphertext* (3.21) data for the purpose of security or privacy

3.41
exclusive-or
XOR
mathematical operation defined as: 0 XOR 0 = 0 0 XOR 1 = 1 1 XOR 0 = 1 1 XOR 1 = 0

Note 1 to entry: Equivalent to binary addition without carry (modulo-2 addition).

3.42
Hardware Security Module
HSM
secure cryptographic device (3.75) that provides a set of secure cryptographic services including, but not limited to, key generation, cryptogram creation, PIN translation and certificate signing

[SOURCE: ISO 13491-1:2016, 3.23]

3.43
hash function
one-way function that maps a set of strings of arbitrary length on to a set of fixed-length strings of bits

Note 1 to entry: The output is generally relatively small.

Note 2 to entry: A collision-resistant hash function has the property that it is computationally infeasible to construct distinct inputs that map to the same output.

3.44
independent communication
process that allows an entity to counter-verify the correctness of a credential and identification documents prior to producing a certificate

EXAMPLE Call-back, visual identification.

3.45
initial DUKPT key
IK
unique *cryptographic key* (3.28) loaded into a *secure cryptographic device* (3.75) that has been derived from a *Base Derivation Key* (3.9)

3.46
Initial Key ID
64-bit value that identifies the specific *initial DUKPT key* (3.45) derived under the *Base Derivation Key* (3.9)

Note 1 to entry: It is a concatenation of the *BDK ID* (3.10) and the *Derivation ID* (3.33)

3.47
Interchange
mutual acceptance and exchange of messages between institutions for card payment transactions

3.48
Issuer
institution holding the account identified by the Primary Account Number (PAN)

Note 1 to entry: See Annex J for additional information on the role an Issuer plays in the payment environment.

© ISO 2023 – All rights reserved

3.49
key agreement
process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key

Note 1 to entry: By predetermine, it is meant that neither entity A nor entity B can, in a computationally efficient way, choose a smaller key space and force the computed key in the protocol to fall into that key space.

[SOURCE: ISO/IEC 11770-4:2017, 3.13]

3.50
key component
component
one of at least two values that are combined using XOR to form a symmetric *cryptographic key* (3.28)

Note 1 to entry: Each component has the same format (including length) as the cryptographic key.

3.51
key distribution host
KDH
host distributing keys in the *SKDAT* (3.79) key distribution methodology

Note 1 to entry: See Annex K for more details on the role a KDH plays in SKDAT.

3.52
key encryption key
KEK
key used exclusively to encrypt and decrypt other keys

3.53
key receiving device
KRD
device receiving keys in the *SKDAT* (3.79) key distribution methodology

3.54
key separation
method for ensuring that a key is used for only its intended purpose

3.55
Key Serial Number
KSN
concatenation of the *Initial Key ID* (3.46) and the transaction counter used in *DUKPT* (3.35)

3.56
key set
group of keys that are all determined by a common cryptographic procedure and differentiated by non-secret input such that knowledge of one key does not disclose any other key in the group

3.57
Key Set Identifier
KSI
non-secret value that uniquely identifies a *key set* (3.56)

3.58
key share
result of dividing a *cryptographic key* (3.28) into some number (n) of pieces (shares), such that a designated minimum number (m) of pieces are required to reconstitute the key

Note 1 to entry: Each key share is constructed in such a manner that access to fewer than m shares does not disclose any information about the key. In all cases, m is greater than 1 and less than or equal to n.

Note 2 to entry: A secret sharing scheme involving key shares is often referred to as an "m of n scheme".

© ISO 2023 – All rights reserved

3.59
keying material
data that comprise a complete *cryptographic key* (3.28) and its relevant metadata

EXAMPLE Keys, attributes, initialization vectors.

3.60
master key
highest level of key encrypting key in a hierarchy of *key encryption keys* (3.52) and *transaction keys* (3.85)

3.61
message authentication
verification that a message was sent by the purported originator to the intended recipient and that the message was not changed in transit

[SOURCE: ISO/IEC 20944-1:2013, 3.11.1.9]

3.62
Message Authentication Code
MAC
cryptographic value used to confirm that the message came from the stated sender and has not been changed in transit

3.63
node
point in a network that does some form of processing of data

EXAMPLE Terminal, Acquirer, switch.

3.64
non-repudiation
service that provides verifiable evidence to substantiate integrity and origin of data, thereby eliminating successful deniability

3.65
parity
result of a calculation of the number of '1' bits in a string of '0' and '1' bits that indicates whether the number of '1' bits is odd or even

3.66
payment instrument
physical payment card, electronic equivalent or other electronic instrument or order used for the transmission or payment of money, sold or issued to one or more persons, whether or not the instrument is negotiable

Note 1 to entry: This does not include any credit card voucher, any letter of credit or any instrument that is redeemable by the Issuer in goods or services.

3.67
Personal Identification Number
PIN
string of numeric digits established as a shared secret between the account owner and the *Issuer* (3.48), for subsequent use to validate authorized card usage

[SOURCE: ISO 9564-1:2017, 3.19, modified]

© ISO 2023 – All rights reserved

3.68
Primary Account Number
PAN
assigned number, composed of an Issuer identification number, an individual account identification and an accompanying check digit that identifies the card Issuer and account owner (who is the cardholder for physical cards)

Note 1 to entry: The accompanying check digit is specified in ISO/IEC 7812-1.

[SOURCE: ISO 9564-1:2017, 3.22, modified]

3.69
private key
key in an asymmetric key pair which is known only by that entity

3.70
pseudo-random process
process that produces a value which is statistically random and essentially unpredictable even though it was generated by a deterministic algorithm

3.71
public key
key of an entity's asymmetric key pair which can usually be made public without compromising security

[SOURCE: ISO/IEC 11770-1:2010, 2.36]

3.72
random
value in a set that has an equal probability of being selected from the total population of possibilities, hence is unpredictable

3.73
recipient
person, institution or other party that is responsible for and authorized to receive a message or package

3.74
replay
process of sending a message which contains all or part of a previously sent message, as a method of perpetrating a fraud

3.75
secure cryptographic device
SCD
device that provides physically and logically protected cryptographic services and storage and which can be integrated into a larger system such as an ATM or POS terminal

EXAMPLE entry device (PED), Hardware Security Module (HSM).

[SOURCE: ISO 13491-1:2016, 3.28]

3.76
sender
person, institution or other entity transmitting a message or package

3.77
split knowledge
condition under which two or more individuals separately and confidentially have information that, individually, convey no knowledge of the resulting combined information

EXAMPLE *Components* (3.50) of a *cryptographic key* (3.28) managed under strict custody separation such that no one person can gain access to the entire set.

© ISO 2023 – All rights reserved

[SOURCE: ISO 9564-1:2017, 3.28, modified — Definition revised and example added.]

3.78
symmetric key
secret *cryptographic key* (3.28) that is used in a symmetric *algorithm* (3.3)

3.79
symmetric key distribution using asymmetric techniques
SKDAT
key distribution method that uses asymmetric cryptography to protect the keys during transport

Note 1 to entry: See Annex K.

3.80
switch
node that can route data from a node to other nodes

3.81
tamper evident and authenticable bag
TEA bag
one-time use packaging that is designed in such a way as to make it infeasible to access the contents without detection and has a pre-printed unique identifier that cannot be changed without detection to allow for authentication

Note 1 to entry: The form of the packaging is not necessarily restricted to a bag.

3.82
tampering
unauthorized modification that compromises the security properties of a device or security container

EXAMPLE 1 Insertion of active or passive tapping mechanisms into a device to determine, record or modify secret data.

EXAMPLE 2 An attempt to penetrate or open a security container, TEA bag or device.

3.83
terminal
device or system that initiates a *transaction* (3.84) and is, contains or interfaces with a *transaction-originating SCD* (3.86) for cryptographic functions

3.84
transaction
series of messages to perform a predefined function

EXAMPLE Payment transaction.

3.85
transaction key
key used to cryptographically protect the transaction data elements between nodes

Note 1 to entry: If more than one key is used for different cryptographic functions, each key can be a variant or derivative of the transaction key.

Note 2 to entry: A transaction key is sometimes referred to as a data key, communications key, session key or working key.

3.86
transaction-originating SCD
secure cryptographic device (3.75) that is, is integrated in or is used by the *terminal* (3.83) that initiates the financial *transaction* (3.84)

EXAMPLE PIN entry device.

© ISO 2023 – All rights reserved

Note 1 to entry: An intermediate device that processes the transaction, such as a *Hardware Security Module* (3.42), is not a transaction-originating SCD.

3.87
Triple Data Encryption Algorithm
TDEA
symmetric *algorithm* (3.3)

Note 1 to entry: The TDEA is specified in the ISO/IEC 18033 series.

3.88
triple-length TDEA key
Triple Data Encryption Algorithm (3.87) key having a length of 192 bits, consisting of 168 key bits and 24 parity bits, that is typically represented in 48 hexadecimal digits

3.89
verification
process of associating and/or checking a unique characteristic

4 Key management requirements

4.1 General

4.1.1 Key management strategy

Key generation, storage, loading, transport, use and destruction are points at which a key management policy is applied to ensure the secrecy of the keys. For an illustration of the symmetric key life cycle, see Annex D; for the asymmetric key life cycle, see Annex E.

The impact of a compromise of a given key should be taken into consideration when deciding the policy for management.

It is necessary to employ mechanisms that detect or prevent the unauthorized use of a key, the use of modified or substituted keys or the replay of keys.

This subclause includes general requirements that apply to the management of keys.

4.1.2 Dual control and split knowledge of secret or private keys

The management of cleartext components or shares of symmetric (secret) and asymmetric private keys shall ensure dual control and split knowledge of the resulting key. Throughout the life cycle of a key, an individual shall not have (or have had) access to all cleartext components or a sufficient number of shares to form the key. Each person or group of persons (e.g. custodian) responsible for each key component or share shall have received adequate training and shall have signed an acknowledgement of their responsibilities to keep secret the key component or share entrusted to them.

The chain of custody for each cleartext component or share shall be documented and such documentation shall be maintained.

Access to fewer than the number of shares required to reconstruct the plain text symmetric or private key or components required to reconstruct a symmetric key shall give no information about the overall key.

A cleartext key share or component of a symmetric or private key shall be accessible only to the person or group of persons to whom it has been entrusted and only for the minimum duration required.

© ISO 2023 – All rights reserved