INTERNATIONAL STANDARD

**ISO 15668**

First edition
1999-12-01

# Banking — Secure file transfer (retail)

*Banque — Transfert de fichier de sécurité (services aux particuliers)*



Reference number
ISO 15668:1999(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 734 10 79
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

# Contents

Page

**Foreword** ..... iv
**Introduction** ..... v
1 **Scope** ..... 1
2 **Normative references** ..... 3
3 **Terms and definitions** ..... 4
4 **Principles** ..... 5
5 **Application** ..... 6
6 **Authentication mechanisms** ..... 14
**Annex A** (informative) **Mechanism examples** ..... 15
**Annex B** (informative) **An example of implementation** ..... 23
**Annex C** (informative) **An example for ensuring file transfer integrity validation** ..... 28
**Annex D** (informative) **Graphics overview of security services with references** ..... 33

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

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.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

International Standard ISO 15668 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

Annexes A to D of this International Standard are for information only.

## Introduction

This International Standard describes how to secure file transfers in a retail banking environment. Typical use of such file transfers are those between a card accepting device and an acquirer, or between an acquirer and a card issuer.

# Banking — Secure file transfer (retail)

## 1 Scope

In contrast to file transfers in a wholesale banking environment characterised by exchanges of large volume, between mainframes, in a relatively high-security environment ("bulk file transfers"); those in a retail banking environment are characterised by low volumes and a lower degree of reliability of environment in which downloaded devices are operated. Such devices may be, but not limited to, an electronic point of sale terminal (EPOS), an automated vending machine (AVM), an automated teller machine (ATM), or a merchant server in communication with payment gateways.

It is assumed that a pre-established relationship exists between the entities involved in the secure file transfer, especially to cover the legal and commercial aspects related to the file transfer liabilities.

This International Standard applies to the different kinds of file transfer used in retail banking environment, but does not cover transaction messages identified in ISO 8583.

The transfer may require timeliness, and requires at least one of the following security services:



— message origin authentication;

— receiver authentication;



— integrity;

— confidentiality;

— non repudiation of origin;

— non repudiation of delivery;

— auditability.

It is assumed that all data forwarded by the originator shall have been confirmed as legitimate and correct prior to the transfer.

The different types of files to be transferred could contain:

— software;

— the retail transactions which have been performed and registered, (uploading);

— technical data related to an acquirer (access parameters...), (downloading);

— application data related to an acquirer (BIN list, hot list, ...), (downloading).

Characteristics of such file transfers are the following:

a) the type of data to be transferred can be

— non-secret data (collection of retail transactions, technical data and application data); or

— secret data.

b) the number of entities to receive the data can be:

— one;

— more than one (broadcast with even thousands of receivers).

c) the communication channels can consist of one or both of the following examples:

— telecommunication: public network, private network;

d) the nature of the transfer can be:

— direct-connect, real-time transfer (also known as circuit switching ); or

— store-and-forward transfer (also known as message switching).

NOTE This International Standard considers the security service during the transfer. Requirements to ensure that transferred files have not been altered after transfer achievement are outside the scope of this International Standard.



**Permissible forms of Secure File Transfer**

**Transfer of Secured Files**



The transfer function does not provide any security services but includes only communication services. In this case the file shall be secured prior to the transfer. Security is managed by the originator and the receiver themselves. They need not trust the lower levels. There is no security added by the communication level (sender and receiver).


SFT = Secure File Transfer

**Secured transfer of files**

In this case, the security is taken into account only from the sender to the receiver and the originator fully trusts the sender. One example is where the originator is the sender and the security is delegated to the transfer level. This is not end to end security as there is no security added by the originator. In this case, the transfer function fully includes the security services. The file need not be secured prior to the secured transfer taking place.

**Secured transfer of secured files**

The security functions can be split up between the security function and the transfer function. One example is where the originator creates a file, signs it with the private signature key, and enciphers the file with a key known only by the end user (the receiver).

The concern in this example is to prevent anyone within the senders organisation from seeing the content of the originators file. However, the originator trusts its agent(s) to process the transfer and to take into account the authentication, integrity, between the sender and the receiver.


## 2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 8372:1987, *Information processing – Modes of operation for a 64-bit block cipher algorithm*.



ISO 8583:1993, *Financial transaction card originated messages – Interchange message specifications*.

ISO 8731-1:1987, *Banking – Approved algorithms for message authentication – Part 1: DEA*.



ISO 9564-1:1991, *Banking – Personal Identification Number management and security – Part 1: PIN protection principles and techniques*.

ISO/IEC 9796:1991, *Information technology – Security techniques – Digital signature scheme giving message recovery*.

ISO/IEC 9796-2:1997, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function*.

ISO/IEC 9797:1994, *Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*.

ISO/IEC 9798-1:1991, *Information technology – Security techniques – Entity authentication mechanisms – Part 1: General model*.

ISO/IEC 9798-2:1994, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms*.

ISO/IEC 9798-3:1993, *Information technology – Security techniques – Entity authentication mechanisms – Part 3: Entity authentication using a public key algorithm*.

ISO/IEC 9798-4:1995, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function*.

ISO 9807:1991, *Banking and related financial services – Requirements for message authentication (retail).*

ISO/IEC 10116:1993, *Information technology – Modes of operation for an n-bit block cipher algorithm*.

ISO/IEC 10118-1:1994, *Information technology – Security techniques – Hash-functions – Part 1: General*.

ISO/IEC 10118-2:1994, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm*.

ISO 11568 (all parts), *Banking – Key management (retail).*

ISO/IEC 13888-2:1998, *Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques*.

ISO/IEC 13888-3:1997, *Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques*.

NIST FIPS PUB 180-1, *Secure Hash Standard (Secure Hash Algorithm SHA-1).*

## 3 Terms and definitions

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

**3.1**
**hot list**
a list of Primary Account Numbers (PAN) which are arranged according to the card issuer or its agent, not valid for transaction use

**3.2**
**digital signature**
data appended to, or a cryptographic formation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient



**3.3**
**File Validation Value (FVV)**
a derived value used for file validation purposes



**3.4**
**hash code**
the result of applying hash-function to data bits

**3.5**
**hash-function**
a (mathematical) function which maps values from a (possibly very) large set of values into smaller range of values, satisfying the following two properties within this International Standard:

— it is computationally infeasible to find for a given output an input which maps to this output;

— it is computationally infeasible to find for a given input a second input which maps to the same output.

**3.6**
**application manager**
the part of the software of a terminal which is in charge of verifying the secure downloading of the intended executable object

**3.7**
**Message Authentication Code (MAC)**
a code in a message between the originator and the receiver used to validate the source and part or all of the text of the message

NOTE The code is the result of an agreed calculation.

**3.8**
**originator**
the entity that creates the file that has to be transferred to the receiver and is responsible for its security

**3.9**
**receiver**
the entity that receives the file

**3.10**
**sender**
the entity that sends the file

**3.11**
**sponsor**
the entity that evaluates the risk of the file transfer

## 4 Principles

### 4.1 Message Origin Authentication

The purpose of message origin authentication is to provide assurance to the receiver that the alleged originator is the legitimate originator. It may also provide assurance to the receiver that the alleged file is the actual file, in the event that the receiver is authorised to receive certain files from only a subset of its authorised originators.



Message origin authentication may occur concurrent with the file transfer, though it may also occur before the transfer in a connection mode. If a store and forward transfer is used, the message origin authentication shall occur after the transfer, when the file is retrieved by the receiver. (Note: transfer of secured files in the model).



Techniques that provide content authentication may provide message origin authentication, but these techniques require the transfer of the entire file before the authentication can be verified. There may be situations in which it is desirable to perform message origin authentication prior to initiating the actual transfer. As an example, it may be desirable to prevent an impostor from masquerading as a legitimate file-provider and tying up a communications channel for an extended time in transferring a long file, even though the illegitimacy of the originator would eventually be detected and the transferred file rejected.

### 4.2 Receiver authentication

This security service authenticates the identity of the receiver prior to initiating the transfer, so that the transfer will not occur unless the receiver's identity has been verified.

Some receivers (POS terminals) are allowed to receive only some types of files. Part of the authentication process is the control by the originator of the rights for the receiver to receive some file-type.

Another possible reason for using "receiver authentication" is to prevent an unauthorised party from impersonating a legitimate receiver and tying up the originator's communications capabilities while the originator transfers a perhaps-lengthy file to the impersonator.

Receiver authentication does not prevent an unauthorised party from ascertaining the file contents (by "listening in"). Without this security service, and without the security service of confidentiality, anyone could easily impersonate the legitimate receiver and thus obtain the file. If it is essential that only the authorised receiver(s) of a file actually receive the file, then the security service of confidentiality must be used. Only in this way can it be ensured that an unauthorised party has not "listened in" on the communications channel and thus obtained a copy of the file.

Note that there is a related security service, non repudiation of delivery, that confirms, after the completion of the transfer, that the authorised party has successfully received the file.

### 4.3 Integrity

Accidental or unauthorised alteration of the transferred file, or, at a minimum, selected portions of the transferred file, shall be detected during and after the transfer process. Integrity services may control the entire file in a single process, or they may individually control segments of the file.

### 4.4 Confidentiality

When necessary, the confidentiality of the transferred files shall be ensured and shall be applied to either the whole file or those file portions that actually require confidentiality.

### 4.5 Non repudiation of origin

This security service provides evidence that the claimed originator actually originated the transferred file. (Without such evidence, the originator might falsely claim that the receiver created the file, or else the receiver might have created the file, and then falsely claimed that it came from the originator.)

### 4.6 Non repudiation of delivery

This security service provides evidence that the claimed receiver actually received the transferred file. Without such evidence, the receiver might claim non-receipt of the file. This service is achieved by mechanisms identified in annex A. The receiver sends to the originator a non repudiation token message proving that:

1) the intended receiver received the file;

2) the file contents were received unaltered.



NOTE The extent of non repudiation may be determined by domestic laws or local banking regulations.



### 4.7 Auditability

If required by the application, it may be necessary for the sender/originator and/or the receiver to log appropriate details of the transfer (time and date, nature of the files, volume of the files, version number...). Such logs may include failed attempts to transfer data, as well as successful attempts. In the event of attempted fraud, a log of failed transfers may assist in identifying the source of the attempt.

## 5 Application

### 5.1 Software downloading

#### 5.1.1 Definition

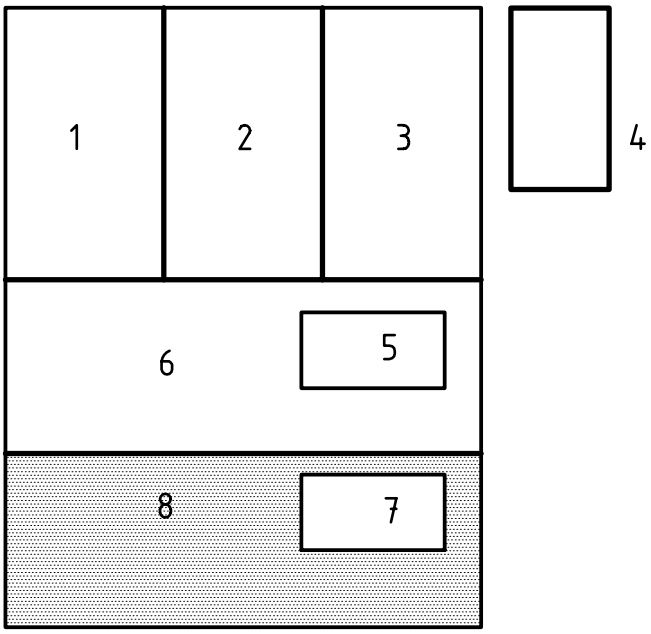
The software of a terminal is composed of distinct functional layers:

a) a trusted and fixed software, pre-loaded before secure file transfer, which is in charge of implementation of security mechanisms for downloading the application manager and its secure execution;

b) an application manager which is in charge of implementation of security mechanisms for downloading the different applications and their secure execution;

c) different applications, which consist of either executable objects or interpreted objects.

NOTE The above are representative of different layers within the device. Only layers 2 and 3 are downloadable The security of layer 1 is outside the scope of this International Standard.




**Key**



1 Application 1
2 Application 2
3 Application 3
4 Executable objects or interpreted objects
5 Keys
6 Application manager
7 Trusted, fixed and preloaded software (bootstrap)



**Figure 1 — Representation of the software of a terminal**

Security services required for software downloading are:

— mutual authentication or unilateral authentication of the originator/sender;

— integrity verification of the transferred file.

Confidentiality may be required for sensitive data when appropriate (e.g. keys).

Prior authentication of the sender by the device may not be required when the downloading is processed in a specific buffer and integrity checking is performed prior to accepting the software, achieving implicit authentication of the sender.

For each layer, the sequence of the operations shall be: mutual authentication, software transfer, integrity verification. In the case of mutual authentication failure, the software transfer shall not be performed. In the case of integrity failure, the software shall not be accepted by the device and the whole sequence shall be performed again.

NOTE It is not always necessary to authenticate the receiver. It may be sufficient for the receiver to have message origin authentication for downloaded software.