



Messaging

FINCopy

## Service Description

This service description provides an overview of the FINCopy service, including the features and functions of the service as well as security and control considerations. In addition, the document covers the general terms and conditions, and the responsibilities and liabilities that apply to SWIFT, the service administrators, and the users. This document is for users of the FINCopy service, service administrators, and developers.

19 September 2008

# Table of Contents

<b>Preface</b> .....	4
<b>1 Introduction</b> .....	6
1.1 SWIFTNet and FIN Overview .....	6
1.2 FINCopy Overview .....	6
1.3 How FINCopy Works .....	7
1.4 Implementing FINCopy .....	9
1.5 Support for FINCopy .....	10
<b>2 Features and Functions</b> .....	11
2.1 FINCopy Service Parameters .....	11
2.2 FINCopy Service Modes .....	12
2.3 Service States .....	18
2.4 Service Messages .....	18
<b>3 Security and Control</b> .....	25
3.1 Closed User Groups .....	25
3.2 Double Authentication .....	25
<b>4 Service Administrator Responsibilities</b> .....	28
4.1 Implementation .....	28
4.2 Operational .....	30
4.3 General Responsibilities .....	32
<b>5 FINCopy User's Responsibilities</b> .....	34
5.1 Implementation .....	34
5.2 Operational .....	35
<b>6 Relationship between FINCopy and FIN</b> .....	39
6.1 Message Retrievals .....	39
6.2 Message Flow Integrity .....	39
6.3 Test and Training .....	43
<b>7 Ordering</b> .....	44
<b>8 SWIFT General Terms and Conditions and Liability</b> .....	45
8.1 Application of the SWIFT General Terms and Conditions .....	45
8.2 SWIFT Liability .....	45
<b>Appendix A FINCopy Service Profile</b> .....	46
A.1 FINCopy Service Profile .....	46
A.2 FINCopy Service Profile Parameters .....	47
<b>Appendix B Case Studies</b> .....	52
B.1 Purpose of this Appendix .....	52
B.2 Transaction Profile .....	53

---

---

B.3	Messages, Y-Copy Mode: Authorised Payment .....	54
B.4	Messages, Y-Copy Mode: Rejected Payment .....	59
B.5	Messages, Fallback to Bypass Mode .....	63
B.6	Messages, T-Copy Mode .....	65
<b>Appendix C Service Administrators Operations Guide .....</b>		<b>69</b>
C.1	General .....	69
C.2	Definition of Procedures .....	69
C.3	Data Maintenance .....	71
C.4	Processes and Procedures .....	72
C.5	Stress Testing FINCopy .....	77
C.6	Telephone Authentication Procedure .....	77
C.7	Forms .....	83
<b>Legal Notices .....</b>		<b>85</b>

# Preface

## Contents

This service description provides an overview of the FINCopy service, including the features and functions of the service as well as security and control considerations. In addition, the document covers the general terms and conditions, and the responsibilities and liabilities that apply to SWIFT, the service administrators, and the users.

Although FINCopy is an extension of FIN functionality, it is a separate service. Similarly, this service description is separate from FIN service publications.

---

**Note** This service description, together with the *SWIFT General Terms and Conditions* and other relevant service documentation, is an integral part of the contractual arrangements between SWIFT and its customers for the provision and the use of FINCopy.

---

## Intended readership

The information is intended for:

- current or prospective FINCopy users, service administrators, or other users that require a good understanding of this SWIFT service
- developers that require background information about elements of FINCopy

Readers of this document require a basic understanding of FIN messaging, as described in the *FIN Service Description*. A brief summary of FIN messaging is included in the Introduction of this service description.

## SWIFT-defined terms

This document contains terms that have a specific meaning in the context of SWIFT documentation (for example, customer, user, or SWIFT services and products). These terms, which are either defined in this document or in the *SWIFT Glossary*, are highlighted as shown in this example:

SWIFT provides secure, standardised messaging services and interface software to its customers.

## Related documentation

For a better understanding of FIN messaging, see:

- *FIN Service Description*
- *FIN Operations Guide*
- *FIN Error Codes*
- *FIN System Messages*
- *SWIFT Glossary*
- *SWIFT Data Retrieval Policy*
- *SWIFT General Terms and Conditions*
- *Support Service Description*
- *SWIFT Price List*

- *SWIFT Personal Data Protection Policy*

**Significant changes since the February 2007 edition**

Modifications due to the migration to the Relationship Management Application and minor clarifications.

# 1 Introduction

## General

This chapter introduces the FINCopy Service.

It provides the following information about FINCopy:

- what FINCopy is
- how FINCopy fits within FIN messaging
- how and why customers use FINCopy
- how FINCopy works
- how customers implement FINCopy

FINCopy is an independent and separate service that extends FIN functionality. For more information about the FIN service, see the *FIN Service Description*, the *FIN Operations Guide*, *FIN Error Codes*, and the *FIN System Messages*.

## 1.1 SWIFTNet and FIN Overview

### SWIFTNet

SWIFTNet is a secure, dedicated, global communication network that supports a range of financial messaging services, which includes the FIN store-and-forward message-processing service.

### FIN

FIN provides users with a wide range of message types for transaction and information processing and settlement.

FIN messages consist of structured headers, text, and trailers, and conform to internationally accepted standards. SWIFT protects the confidentiality, integrity, and authenticity of FIN messages as described in the *FIN Service Description*.

## 1.2 FINCopy Overview

### Introduction

FINCopy is a message duplication service. SWIFT developed FINCopy to assist financial communities in implementing centralised systems, for example, Real-Time Gross Settlement (RTGS) or netting systems.

RTGS and netting systems respond to risk management needs by separating funds transfers into:

- information processing between the sending institution and the receiving institution
- funds settlement, in which both institutions maintain accounts in the books of a controlling institution

## FINCopy

FINCopy, in combination with FIN, provides the *service administrator* with a simple, flexible, and secure way to monitor and control financial transactions. FINCopy uses the facilities of FIN, enhanced with a copy of selected information to the third party. This service can be used to clear, net or settle high-value payments, securities, and other financial transactions.

It is a Store-Copy-(Authorise)-and-Forward facility for users that participate in a closed user group.

A FINCopy closed user group comprises:

- users that participate in the FINCopy closed user group
- a *service administrator* that manages clearing, netting, or settlement tasks

The FIN interface of the *service administrator* usually connects with a settlement or other clearing system, which authorises the message delivery to the intended receiver. The decision to authorise and enable delivery is based on the following elements:

- the actual message contents
- dynamic business data about the parties involved, for example, the sender's account balance
- multilateral preagreements within the user community
- any combination of all or part of the preceding items

## 1.3 How FINCopy Works

### Copy modes

A normal FIN relationship is between the sender and the receiver of a FIN message. FINCopy involves a third party, a *service administrator*, in message flows, or modes, known as *Y-Copy* and *T-Copy*.

These illustrations show the information flows for:

- normal FIN service (Figure 1)
- FINCopy Y-Copy and T-Copy modes (Figure 2)

**Figure 1: FIN service Information Flow**

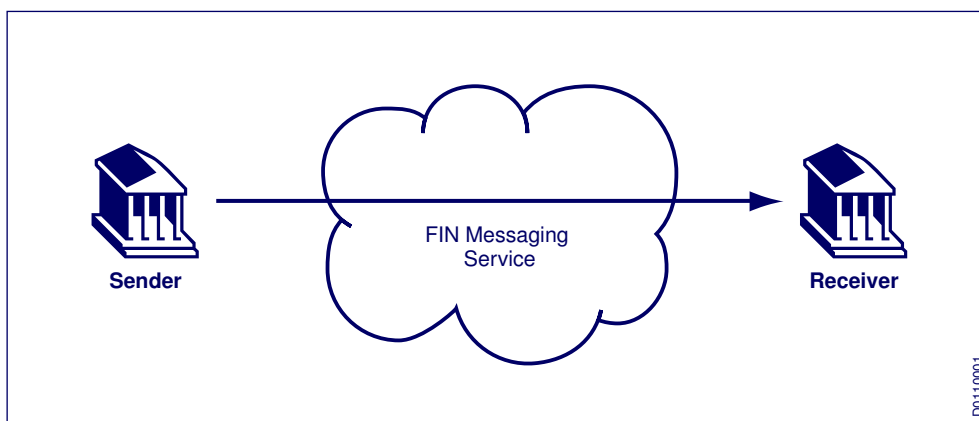
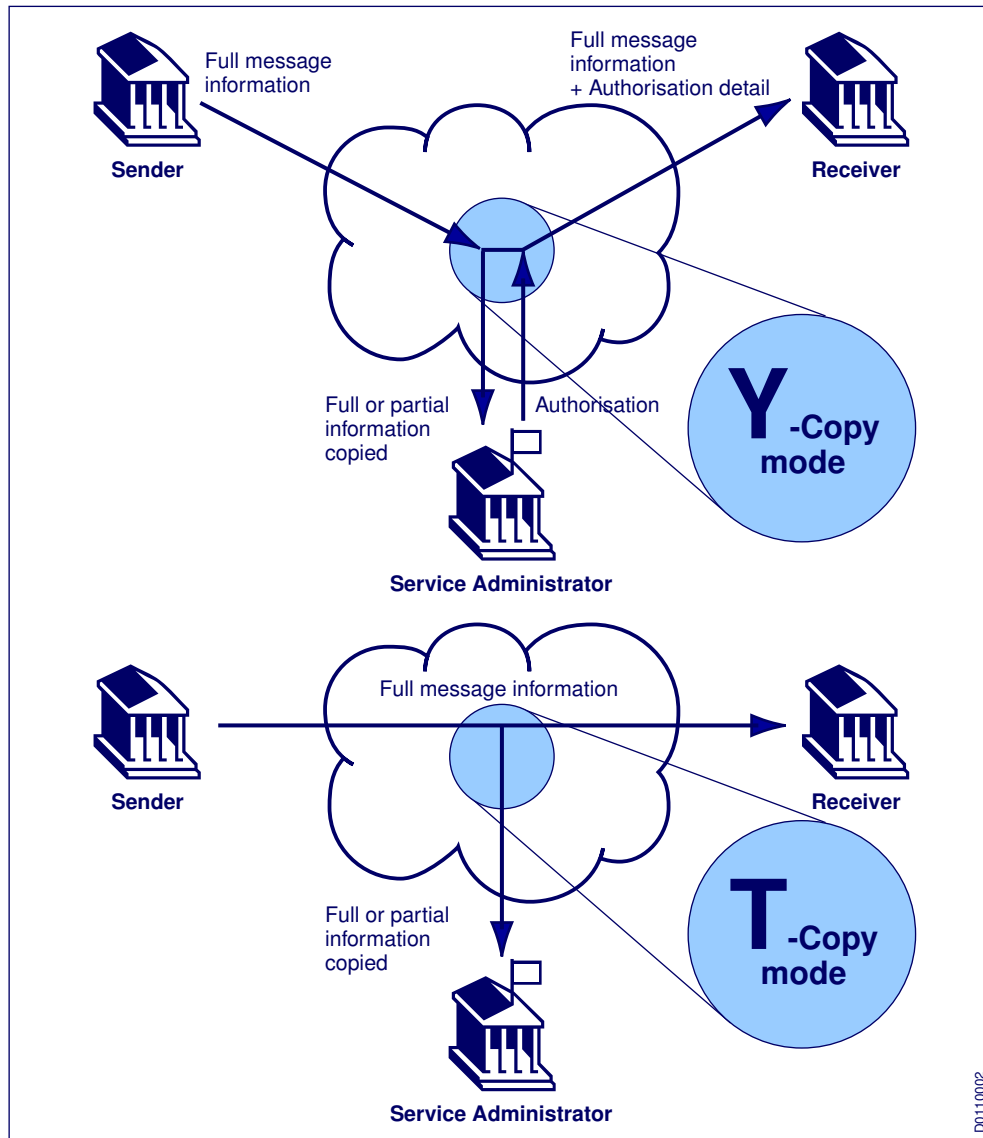


Figure 2: FINCopy service Information Flow



The sending institution uses FIN to prepare its message for transmission to the receiver, in the usual way. The sender adds a service code that indicates that it requires a copy of the message, and then transmits the message.

In Y-Copy mode, FINCopy intercepts the FIN message and copies some or all of the information to a *service administrator*. FINCopy holds the message in a temporary queue until the *service administrator* sends the appropriate authorisation or rejection. If the message is authorised by the *service administrator*, then FIN forwards it for delivery to the receiver, together with the authorisation code. Optionally, the *service administrator* can add information for the sender or the receiver of the original message, or both. If the message is rejected, then FIN aborts the message and notifies the sender.

In T-Copy mode, FINCopy copies some or all of the information to a *service administrator*. The FIN message is not held in a temporary queue, but is queued for delivery to the intended recipient in the normal way. The *service administrator* can advise the sender and the receiver of the status of the transaction by separate messages after the event.

The general principles of FIN, as described in the *FIN Service Description* and the *FIN Operations Guide*, apply to all messages involved in FINCopy.

## 1.4 Implementing FINCopy

### 1.4.1 Service Administrators

#### Aspects of implementation

Service administrators may implement FINCopy as part of a larger project, for example, to create or enhance a clearing, netting, or settlement system. For this, the service administrator may need to register as a SWIFT user, install a FIN interface, and connect to FIN.

The FINCopy implementation procedure consists of the following aspects:

- **administrative** - The service administrator establishes a closed user group, determines the message types and fields that FINCopy must copy, and decides which service code to use.
- **practical** - The service administrator ensures that its FIN Interface can receive copies of messages and send authorisations and rejections.
- **legal** - The service administrator establishes a FINCopy service agreement with SWIFT. The service administrator also establishes an agreement framework with its users (that is, the FIN users that participate in the closed user group).

### 1.4.2 FINCopy Users

#### FINCopy implementation

To implement FINCopy, the user must do the following:

- Confirm with its FIN interface supplier that the interface supports FINCopy.
- Establish agreements with the service administrator and with SWIFT to use the FINCopy service. The user must use the SWIFTNet Service Subscription Form to confirm the agreement to comply with SWIFT's requirements for the use of FINCopy.
- Enter a 3-character service code in the optional field 103 in block 3 to identify the FINCopy Service.

FINCopy supports access to multiple services by the same user, by using a unique code to identify each service.

- Automated message-generation systems must insert field 103 in the user header block when they create the FIN message that the FINCopy application copies.

Some FIN Interface implementations insert field 103 into the header block automatically. Users that participate in a FINCopy closed user group can confirm details with individual suppliers.

Field 103 is located in the user header block as follows:

```
{3:{103:<service-code>}{113:<banking-priority>}{108:<MUR>}}
```

---

**Note** Other fields may be present in the user header block. For a full description of the user header format, see *FIN System Messages*.

---

## 1.5 Support for FINCopy

### 1.5.1 Service Administrators

#### Support for service administrators

During the implementation phase, SWIFT helps the *service administrator* to define the service parameters and manage the FINCopy closed user group. See: "Features and Functions" on page 11.

When the FINCopy service is operational, SWIFT manages the FINCopy closed user group, based on input from the *service administrator*.

SWIFT provides operational support for FINCopy in the same way as it provides support for FIN. For information about the operational support for FIN, see the *Support Service Description*.

### 1.5.2 FINCopy Users

#### Support for FINCopy users

The FIN support available to *FIN users* is also available to users that participate in a FINCopy closed user group.

SWIFT implements the FINCopy closed user group and the *service administrator* enrolls or withdraws *users* in the FINCopy closed user group. The *service administrator* generally provides additional administrative support to the users that participate in the closed user group, for example, the local settlement helpdesk.

## 2 Features and Functions

### General

This chapter describes the following features and functions of the FINCopy Service:

- the FINCopy service parameters
- FINCopy service modes
- message flows within Y-Copy and T-Copy modes, including optional sender notification in Y-Copy mode
- FINCopy service states
- the structure and use of FINCopy Service messages MT 096 and MT 097
- the use of FINCopy Service messages MT 028 and MT 029

## 2.1 FINCopy Service Parameters

### Parameters

FINCopy enables a *service administrator* to operate another service, for example Real-Time Gross Settlement (RTGS), netting, or clearing. The *service administrator* must establish a unique set of parameters for each implementation to govern the provision of the FINCopy service.

The *service administrator* defines these parameters on the Service Profile Form:

- message selection
- message validation
- additional parameters for the service

The **message selection** criteria for FINCopy are as follows:

- the FINCopy service identifier code, which is a 3-character code used in field 103 of the user header
- the message types that FINCopy must copy
- other message types that users that participate in the FINCopy closed user group can exchange
- the participation of the sender and the receiver in the FINCopy closed user group. See "Closed User Groups" on page 25.

The **message validation** criteria is as follows:

- the currency code (optional)
- the authentication mode. See "Double Authentication" on page 25 for a description of the FINCopy Service double authentication mechanism.
- the usage definition - live or Test and Training service

The *service administrator* can define the following **additional parameters**:

- Full or partial copying of the message. If partial copy is selected, the service administrator will also define the specific field tags to be copied.

- The identification of the service administrator's live destination that will be used for signing operations. All Public Key Infrastructure signing operations will use a certificate associated with the service administrator's live destination, even if the traffic being signed is test and training traffic.
- The service mode profile - Y-Copy or T-Copy.
- The fallback service mode - Bypass or T-Copy mode, or closed-service state.
- Optional sender notification in Y-Copy mode. See: "Optional Sender Notification" on page 16.
- Whether certain messages that the service administrator sends to the users that participate in the FINCopy closed user group are billed to the user or the service administrator. If SWIFT bills the users that participate in the FINCopy closed user group, then this is known as reverse billing.
- If the messages that are to be copied (that is, those messages that contain field tag 103), require authorisation or not.

Before starting FINCopy operations, the service administrator must determine, in agreement with SWIFT, the parameters for that service. SWIFT provides support for the definition of these parameters.

From the parameters that the service administrator provides, SWIFT creates two FINCopy services: one for live operation and one for Test and Training purposes.

---

**Note** FINCopy services can use different parameters for live operation and Test and Training.

Before starting the operations, all FINCopy parties (that is, the service administrator and the users that participate in the FINCopy closed user group) must include the FINCopy service parameters in the FIN interface for both the live and the Test and Training services.

---

For a sample FINCopy service profile, see Appendix A, "FINCopy Service Profile" on page 46.

## 2.2 FINCopy Service Modes

### Introduction

The FINCopy service can operate in the following modes:

- Y-Copy
- T-Copy
- Bypass

In normal operations, FINCopy operates in either Y-Copy or T-Copy mode. SWIFT reserves Bypass mode for specific, abnormal situations.

In **Y-Copy mode**, FINCopy copies messages to the service administrator, and stores these messages until it receives authorisation or refusal from the service administrator.

In **T-Copy mode**, FINCopy copies messages to the service administrator and immediately forwards the messages for delivery to the receiver.

In **Bypass mode**, FINCopy does not copy the messages to the service administrator.

**Modes and Actions**

Mode	Message selected for FINCopy processing?	Message copied?	Wait for authorisation?
Y-Copy	yes	yes	yes
T-Copy	yes	yes	no
Bypass	yes	no	no

## 2.2.1 Y-Copy Mode

### Message flow

In Y-Copy mode, the message flow is as follows:

1. A user that participates in a FINCopy closed user group sends a user-to-user message, for example MT 103, to a receiver. To identify this message as a FINCopy user-to-user message, the sender adds field 103 to block 3, the user header. This field contains the service code of the requested FINCopy service. The service definition within FIN determines whether the message is Y-Copy or T-Copy.
2. FINCopy intercepts the user-to-user message and copies some or all fields into an MT 096 to the *service administrator*. MT 096 is equivalent to a request to execute the transaction. FINCopy holds the original user-to-user message until it receives the appropriate instruction from the *service administrator*.
3. The *service administrator's* decision to authorise the user-to-user message is based on the MT 096 information and other data, for example, the sender's balance. The *service administrator* may delay the authorisation if the system allows payments to be queued until balances are sufficient to enable processing.
4. The *service administrator* returns a delivery authorisation or refusal to the FINCopy service in the form of a FINCopy Message Authorisation/Refusal Notification MT 097.
5. Based on the information in MT 097, FINCopy either delivers the user-to-user message, or aborts it and sends an Abort Notification MT 019 to the sender.

See also: "Figure 3: Y-Copy message flow: sender phase", "Figure 4: Y-Copy message flow: service administrator phase: authorised message" and "Figure 5: Y-Copy message flow: service administrator phase: rejected message".

Figure 3: Y-Copy message flow: sender phase

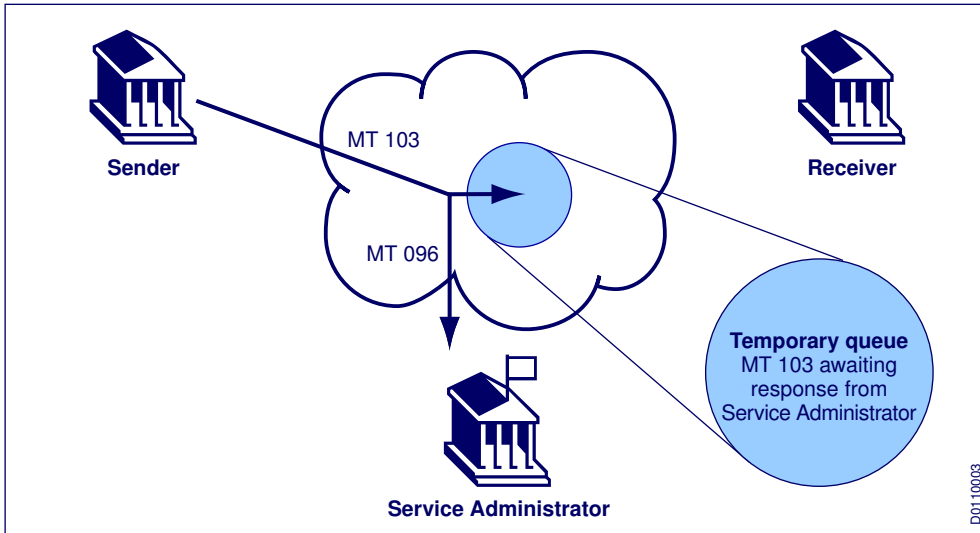


Figure 4: Y-Copy message flow: service administrator phase: authorised message

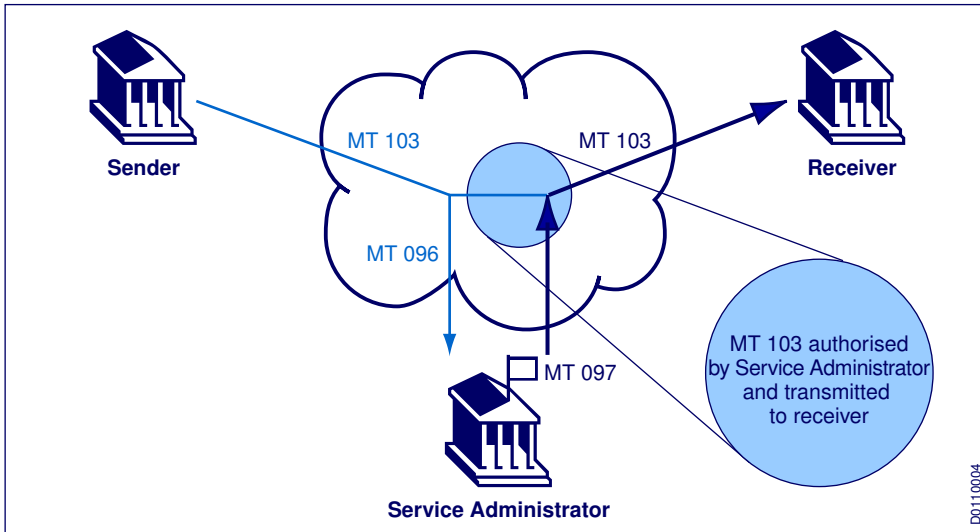
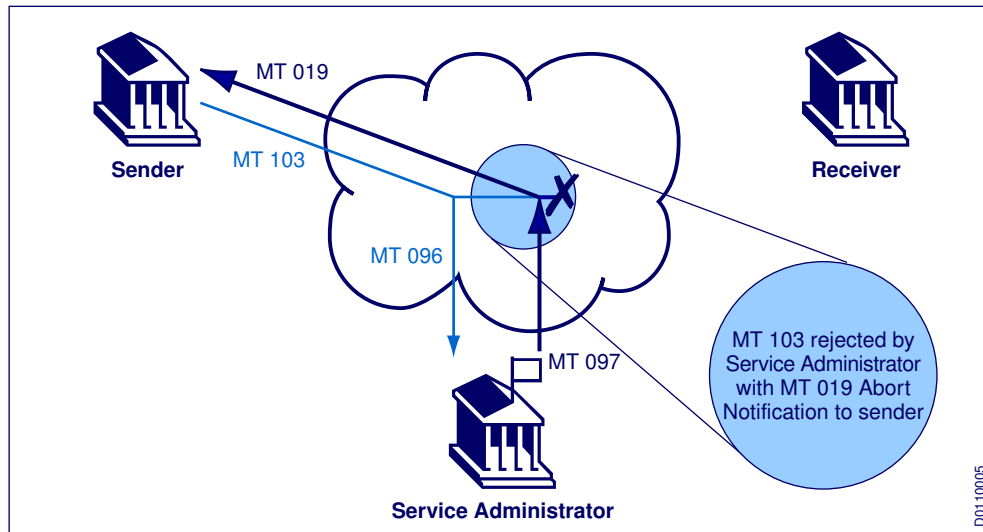


Figure 5: Y-Copy message flow: service administrator phase: rejected message



### 2.2.1.1 Monitoring Messages

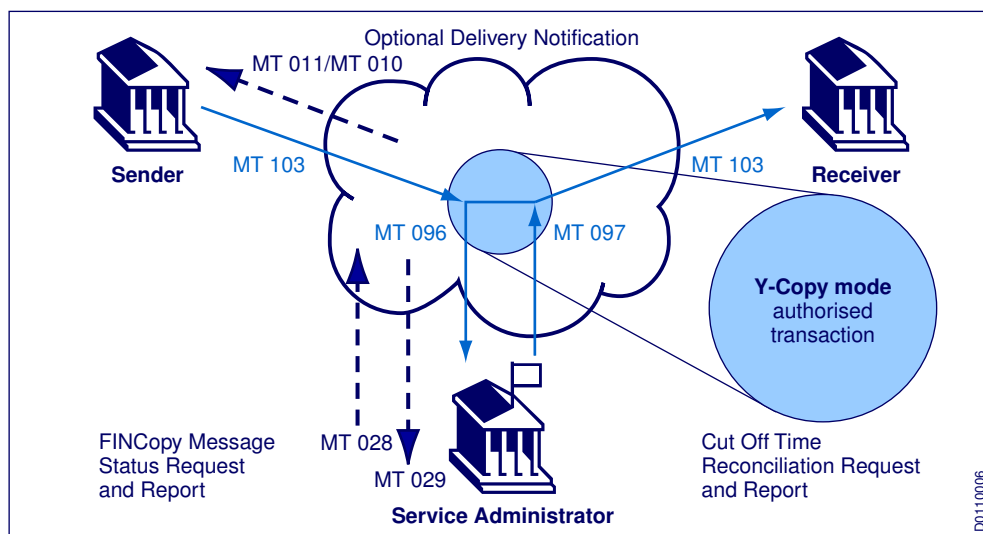
#### Available message types

The following monitoring capabilities are also available:

- As part of the normal FIN Service, the sender can request that FIN monitors the delivery of sent messages. In this case, FIN returns a Delivery Notification MT 011 and, or a Non-delivery Warning MT 010 to the sender, as appropriate. These notifications are based on the delivery of the original message to its receiver, and not on the delivery of the copy to the service administrator.
- To examine the FINCopy hold queue, the service administrator can send a FINCopy Message Status Request MT 028. FINCopy responds with a FINCopy Message Status Report MT 029.

See: "Figure 6: Monitoring messages: authorised transaction: optional messages".

Figure 6: Monitoring messages: authorised transaction: optional messages



**Note** For more information about the FIN system and service messages, see the *FIN System Messages*.

### 2.2.1.2 Optional Sender Notification

#### Use of MT 012

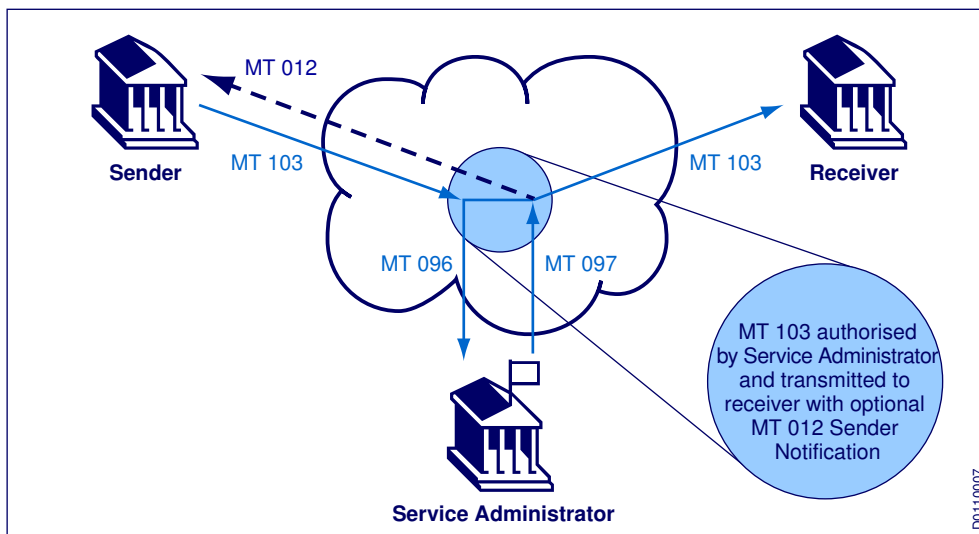
An optional feature of Y-Copy mode is MT 012 for Sender Notification. This feature, which the service administrator selects during the implementation phase, conveys information to the sender of the original user-to-user message. The service administrator inserts field 114<payment-release-information-sender> into the *MT 097 FIN copy message authorisation/refusal notification*. FINCopy then transmits an *MT 012 sender notification* to the sender of the original message identified in field 114.

**Note** The service administrator can only use *MT 012 sender notification* when MT 097 is an authorisation message. FINCopy does not generate MT 012 when MT 097 is a rejection message, even if MT 097 contains field 114.

For more information about this optional feature, see "Relationship between FINCopy and FIN" on page 39.

The modified message flow using Sender Notification is illustrated in "Figure 7: Y-Copy message flow with sender notification".

**Figure 7: Y-Copy message flow with sender notification**



**Note** The service administrator decides whether to offer this feature for the service. It can be applied to all or some messages, based on message type, amount, or other criteria.

### 2.2.1.3 Optional Receiver Notification

#### Use of Field 115

Another optional feature of Y-Copy is Receiver Notification. It only applies to authorised messages. This feature, which is always available to the service administrator, conveys information to the intended receiver of the authorised user-to-user message.

The service administrator inserts field 115 <payment-release-information-receiver> in the *MT 097 FIN copy message authorisation/refusal notification*. If the MT 097 is an authorisation notification, FINCopy adds the field and its contents to the user header block of the user-to-user message, then forwards the message to the receiver.

## 2.2.2 T-Copy Mode

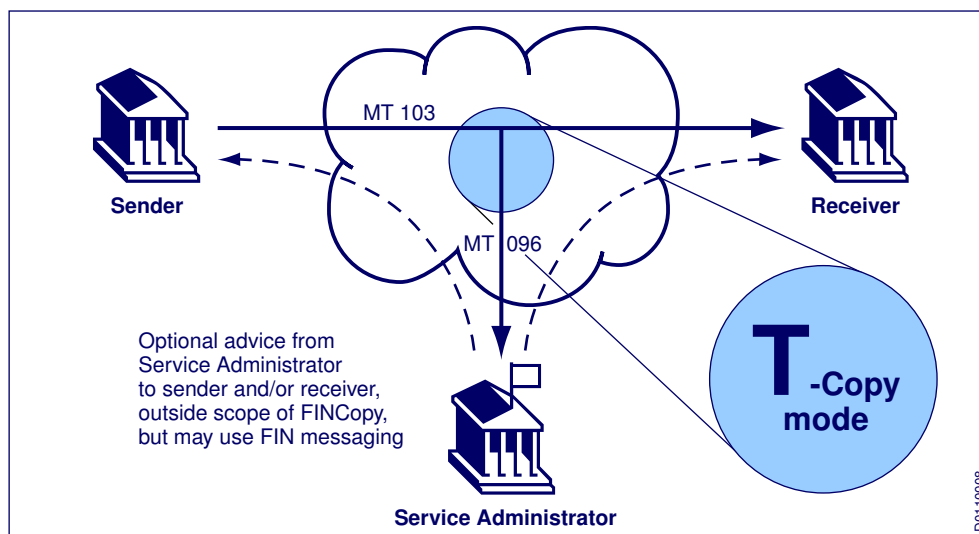
#### Message flow

As with Y-Copy, the service administrator determines the range of messages available in T-Copy mode for the users that participate in the FINCopy closed user group.

The message flow in "Figure 8: T-Copy message flow" is as follows:

- The sender transmits a user-to-user message, for example, an MT 103, to a receiver. To identify this message as a FINCopy user-to-user message, the sender adds field 103 to block 3, the user header. This field contains the identification of the requested FINCopy service. The service definition within FIN determines whether the message is Y-Copy or T-Copy.
- FINCopy intercepts the user-to-user message, and copies some or all of its fields into an MT 096 to the service administrator. Unlike Y-Copy mode, FINCopy does not hold the user-to-user message for service administrator approval. The message is treated as a normal FIN message, and is forwarded directly to the receiver.
- The service administrator uses the information copied in the MT 096 for whatever service it provides. If that service involves an information flow between the service administrator and either the sender or receiver, then the service administrator advises the sender or the receiver (or both) of the message status outside of the FINCopy message dialogue, as there is no *MT 097 FIN copy message authorisation/refusal notification*.

Figure 8: T-Copy message flow



## 2.2.3 Bypass Mode

### Emergency mode

The service administrator can ask SWIFT to operate an active Y-Copy service in **Bypass mode**. This emergency mode is only appropriate in disaster situations, not during normal operations.

Bypass mode operates as follows:

- The sender transmits a user-to-user message, for example, an MT 103 to a receiver. To identify this message as a FINCopy user-to-user message, the sender adds field 103 to block 3, the user header. This field contains the identification of the requested FINCopy service. The service definition within FIN determines whether the message is Y-Copy or T-Copy.
- FINCopy intercepts the user-to-user message, but cannot copy anything to the service administrator. FINCopy treats the user-to-user message as a normal FIN message, and forwards it directly to the receiver. If the service uses double authentication, FINCopy will add a PAC trailer to indicate that the service is operating in bypass mode. The PAC trailer will be empty. See "FINCopy Service Fallback" on page 42.

---

**Note** When the service is in emergency Bypass mode, the service administrator must advise users that participate in the FINCopy closed user group that messages are not copied.

---

## 2.3 Service States

### Open and closed states

A FINCopy Service operating in one of the three modes (that is, Y-Copy, T-Copy, or Bypass) is either in an *open* or *closed* state.

During normal operations, the service state is *open*.

SWIFT can only change service modes if the service state is closed. If a service administrator asks SWIFT to operate its declared fallback mode in an emergency, SWIFT closes the state, changes the mode, then reopens the service.

In the absence of problems, the implementation time for emergency changes to FINCopy parameters (change of mode, withdrawal of a user) is 45 minutes. This period starts from the time that the SWIFT Customer Support Centre has authenticated the service administrator, and has received a confirmation fax from the service administrator.

In some circumstances, fallback may only require SWIFT to close the service state.

---

**Note** A message requesting a FINCopy service when the service is *closed* receives a negative acknowledgement (NAK), with an appropriate error code. For explanations of FIN Error Codes, see the *FIN Error Codes*.

---

## 2.4 Service Messages

### How FINCopy monitors message traffic

The FIN system monitors message traffic between users that participate in a FINCopy closed user group and selects the messages that fulfil the following requirements:

- The message contains a valid FINCopy service identifier code.

- The message type is defined in the FINCopy service parameters.
- The sender and the receiver both participate in the FINCopy closed user group.
- The message passes standard input validation.
- The message passes specific but optional FINCopy validation that is based on currency code or dual authentication, or both.
- The message passes service-specific validation.

From each message that FINCopy selects, certain information is copied into the envelope *MT 096 FIN copy to Central Institution message*. In Y-Copy, the service administrator's response is the *MT 097 FIN copy message authorisation/refusal notification*.

## 2.4.1 MT 096 FIN Copy to Central Institution Message

### Message from system to the service administrator

FINCopy sends an MT 096 to the service administrator. FINCopy generates this message when a user that participates in a FINCopy closed user group places the appropriate FINCopy service identification code in the user header field 103 of a user-to-user message that is addressed to a user that participates in the same FINCopy closed user group. This service code instructs FINCopy to copy the message, according to the definition of the specified FINCopy service.

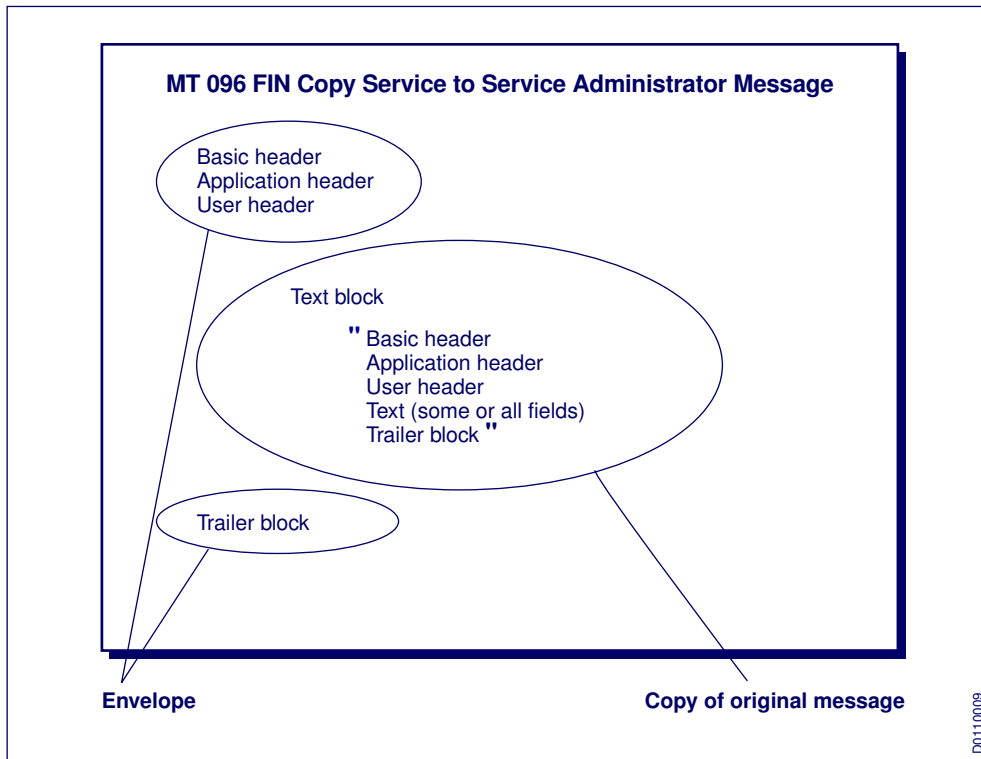
As shown in "Figure 9: MT 096 structure", the *MT 096 FIN copy to Central Institution message*, is a system-to-user message that envelopes information from the original user-to-user message. The text block of the MT 096 contains all the blocks of the original message (that is, basic header, application header, user header, text, and trailer blocks), including a dedicated user Message Reference trailer that FINCopy inserts to specify the message reference of the original user-to-user message. The format of this trailer is as follows:

```
<yyymmdd><hhmmss><mir>
```

where <yyymmdd><hhmmss> represents the input message acceptance date and time (GMT) and <mir> is the 28-character original user-to-user message input reference.

The specific FINCopy Service Profile determines which fields of the original message text block are copied.

**Figure 9: MT 096 structure**



The message reference is specific to FINCopy. The sole purpose of the message reference is to enable FINCopy to identify the MT 096 to which the MT 097 is a response. The message reference is an automatically generated trailer in the MT 096 and can only be reused in field 109 of the MT 097. The format of the message reference may change without prior notice.

If the institution that sent the original message is a synonym, then its master BIC8 appears in the message reference.

**Main Use**

The MT 096 is a FIN system message from FINCopy to the service administrator. See the *FIN System Messages* for details of the MT 096 header and trailer blocks. For MT 096 examples, see Appendix B, "Case Studies" on page 52.

The following table describes the block format of the MT 096.

**Table 2 - MT 096 format**

Block	Content or comment
1,2, and 3	Standard header blocks for a FIN system message. FINCopy puts the FINCopy service identifier code that it has copied from the original user-to-user message, into Field 103 in Block 3.
4	Text block, containing the header blocks, some or all of the text fields, and the trailer block of the original user-to-user message.
5	Standard trailer block for a FIN system message.

---

## 2.4.2 MT 097 FIN Copy Message Authorisation/Refusal Notification

### Message from service administrator to system

In Y-Copy, the service administrator sends the MT 097 to FINCopy. Each MT 097 is a response to an MT 096 from FINCopy.

The decision to allow or refuse delivery of the original user-to-user message is based on:

- information in the MT 096
- any additional available information the service administrator has about the sender and the receiver

The service administrator uses the *MT 097 FIN copy message authorisation/refusal notification* to convey the decision to authorise or refuse the original user-to-user message to FINCopy.

As shown in "Figure 10: MT 097 structure", the text block of the MT 097 contains the following:

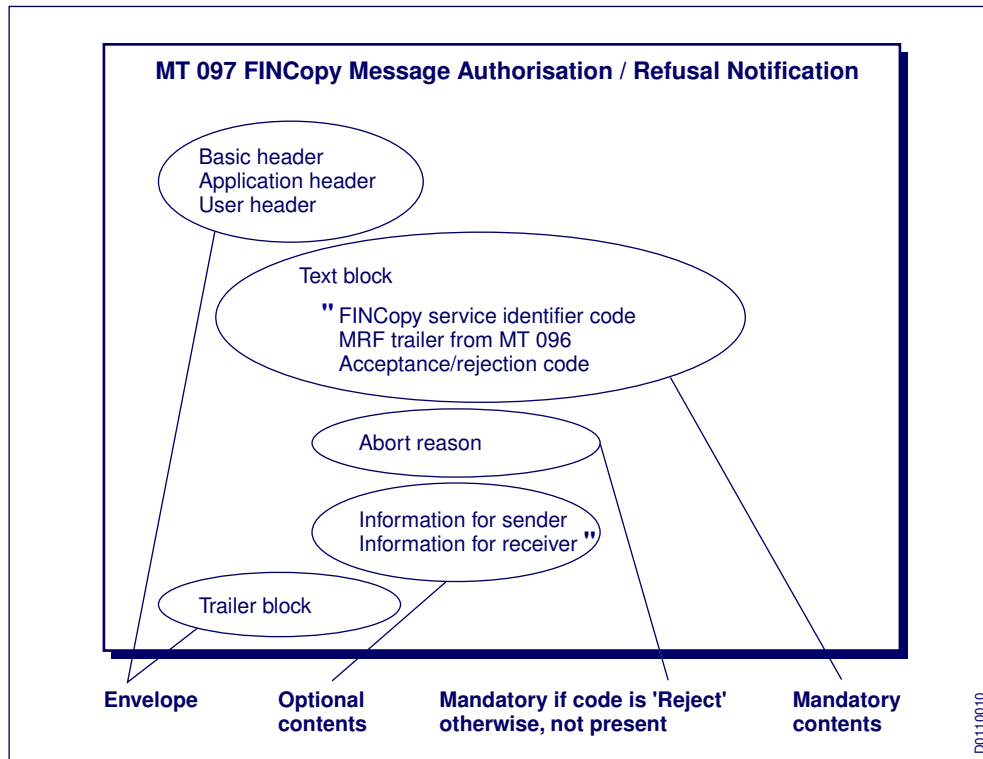
- the original FINCopy service identifier code
- the Message Reference trailer from the MT 096
- an indication of authorisation or rejection

When a message is rejected, the service administrator must add a code in field 432 `<abortreason>` of the MT 097 that indicates the reason for the abort.

Optionally, in authorised messages, the text block of the MT 097 also contains the following:

- information for the sender (in field 114). This information is returned to the sender in an MT 012.
- information for the receiver (in field 115). This information is added to the authorised user-to-user message when it is sent to the receiver.

**Figure 10: MT 097 structure**



The MT 097 is a FIN system message from the *service administrator* to FINCopy. This message applies to the FINCopy service only. For details of the MT 097 header and trailer blocks, see the *FIN System Messages*. For examples of the MT 097, see Appendix B, "Case Studies" on page 52.

**Note** For each MT 096 received from FINCopy in Y-Copy mode, a *service administrator* must send a response to FINCopy using the MT 097. The MT 097 can be sent at a later time but must be sent from the server destination that received the MT 096.

The following table shows the text block format of the MT 097.

**Contents of the MT 097 text block**

**MT 097 format**

Tag	Field	Content or comments
103	service-code	FINCopy service identifier code.
109	original-user-message-reference	Contents of the Message Reference trailer present in the corresponding MT 096.
451	accept-reject	0 = Accepted 1 = Rejected
432	abort-reason	Message rejection code: FINCopy service-specific within the range 50-ZZ.  (If Field 451 contains an acceptance code, then <i>service administrators</i> must not use this field. If Field 451 contains a rejection code, then this field must be present.)

Tag	Field	Content or comments
114	payment-release-information-sender	Information from <i>service administrator</i> to sender of payment message. (The presence of tag 114 generates an MT 012 to the sender of the original message. The contents of tag 114 are copied into the MT 012) (The contents of this field are ignored if Field 451 contains a rejection code.)
115	payment-release-information-receiver	Information from <i>service administrator</i> to receiver of payment message. This is added to the original message when it is output. (The contents of this field are ignored if Field 451 contains a rejection code.)

## 2.4.3 MT 028 FIN Copy Message Status Request

### Service administrator: information request

A *service administrator* uses the *MT 028 FIN copy message status request* to request information about messages that are awaiting authorisation.

#### MT 028 text block format

Tag	Field	Content or comments
103	service-code	FINCopy service identifier code.
243	hold-queue-request-type	Type of hold queue report, where: 1 = Counts and message input references 2 = Counts only
177	date-time	Start time local to the FINCopy <i>service administrator</i> .
177	date-time	Cut-off or end time local to the FINCopy <i>service administrator</i> .

This message always requires the first two fields. The *service administrator* must specify the FINCopy service identifier code and the type of report it requires, as follows:

- 1 = the number of messages in the queue and the message input reference for each message
- 2 = only the number of messages in the queue

The remaining two fields 177 define the time period of the report, as follows:

- if these fields are absent, then FINCopy assumes that the current date and time represent the cut-off for the report
- if only one field 177 is present, then FINCopy assumes that it states the cut-off time
- if both fields are present, then FINCopy assumes that the first field is the start time and the second field is the cut-off time

All times are local to the *service administrator*.

See *FIN System Messages* for more details.

## 2.4.4 MT 029 FIN Copy Message Status Report

### Response to service administrator

In response to a service administrator's *MT 028 FIN copy message status request*, FINCopy generates an *MT 029 FIN copy message status report*. The report contains the information that the service administrator has requested.

### MT 029 text block format

Tag	Field	Content or Comments
202	section-number	Number of the section in a multi-section message, starting with "0001".
203	total-sections	Total number of sections in a multi-section message.
177	date-time	Start time local to the FINCopy service administrator.
177	date-time	Cut-off or end time local to the FINCopy server.
103	service-code	FINCopy service identifier code.
343	cut-off-time-count	See explanation.
106	mir	Message Input Reference. The FINCopy report can contain up to 40 message input references, describing the messages that FINCopy has on hold for that service.

Fields 202 and 203 are always present in the report. The two fields 177 are present in the first section of the report, if present in the original MT 028 request. The final part of the report contains the FINCopy service identifier code and a combination of the final two fields in the preceding table. The last two fields depend on the type of request in the MT 028.

Field 343, <cut-off-time-count>, shows the number of urgent and normal user-to-user messages queued in FINCopy, within the date-time range specified in the MT 028.

FINCopy holds the messages for either of the following reasons:

- The sender marked them as copy messages in a Y-Copy service, so FINCopy copied them to the service administrator but the MT 096 has not yet been delivered to the service administrator.
- The MT 096 has been delivered but FINCopy has not had an MT 097 back from the service administrator.

## 2.4.5 MT 030 Cut-off Time Reconciliation Request

### Cut-off time reconciliation request

Customers use the MT 030 FIN system message to reconcile messages queued for delivery in relation to the receiver's cut-off time. To use this message, the delivery subsets of the receiver's destination must be configured for value-date-sensitive queuing.

## 3 Security and Control

### Introduction

This chapter describes the use within FINCopy of aspects of the FIN messaging service.

The chapter covers the following topics:

- closed user groups
- double authentication

## 3.1 Closed User Groups

### FINCopy closed user groups

SWIFT implements FINCopy on the basis of closed user groups. The *service administrator* defines the types of messages which users that participate in the closed user group can use within that FINCopy service. Closed user group characteristics form part of the FINCopy service parameters.

Users that participate in the closed user group exchange certain types of messages between themselves. Communication for these messages or these services is not possible with other users that do not participate in the closed user group.

Changes related to users that participate in a closed user group take effect following an allowable downtime window, provided that End-to-End Ordering has received the correct update information from the *service administrator* at least 14 days before the required update time.

All FINCopy services use the same copy mechanism within FIN. However, each FINCopy service is defined individually.

## 3.2 Double Authentication

### Sender of original message

FIN messages use an authentication mechanism that uses Public Key Infrastructure-based digital signatures.

FINCopy supports an optional double authentication mechanism which enables the *service administrator* to verify the origin and integrity of the copied data. It also enables the recipient of a user-to-user Y-Copy message to verify the identity of the *service administrator* that has authorised the message.

### Double authentication

#### Double authentication

In support of message authentication and integrity, if the *service administrator* has specified the use of double authentication in the service profile, then SWIFT enforces its use between the sender and the *service administrator* (for T-copy and Y-copy), and between the *service administrator* and the receiver (for Y-copy).

For more information about message authentication, see "Authentication Mode" on page 47.

**Note** Message authentication only applies to certain messages. Double authentication may apply to any FINCopy message. This means a message may carry a signature between the participants and the service administrator, but not between the sender and the receiver.

### SWIFT BIC8 address

The service profile contains the service administrator destination formerly known as the central institution destination. It is the Public Key Infrastructure certificate associated with the central institution destination that will be used for double authentication of FINCopy messages. When operating in Test and Training mode, a certificate associated with the live central institution destination must be used for all signing operations.

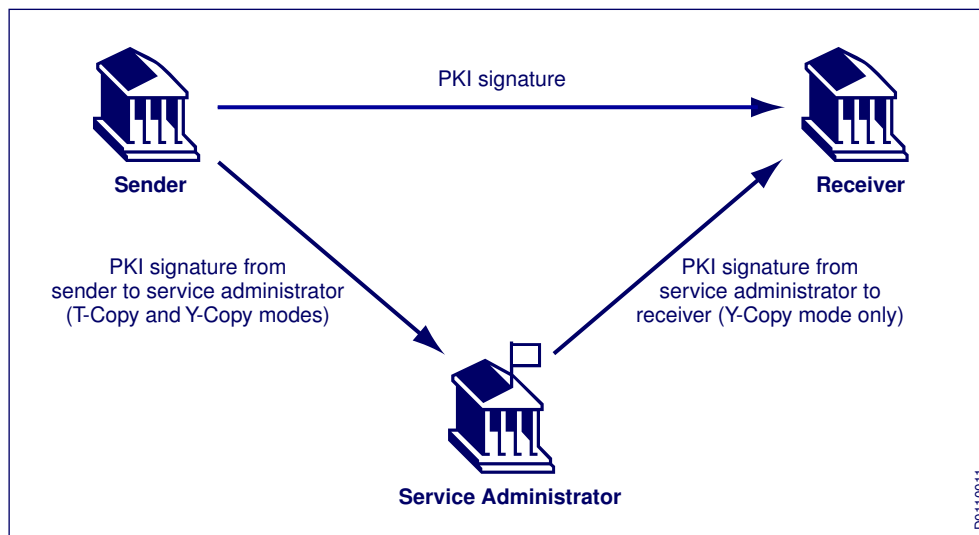
For Y-Copy, there may be two or three authentication results as shown in "Figure 11: Double authentication mechanism".

When the authentication parameters are added to the FIN Interface configuration, the double authentication process is automatic.

### Central institution

If double authentication is defined for the FINCopy service, then the service administrator must generate a PKI-based signature when generating the *MT 097 FIN copy message authorisation/refusal notification*. The user-to-user message that FIN forwards to the receiver contains the authentication elements calculated by the sender and by the service administrator.

**Figure 11: Double authentication mechanism**



Double authentication results in the following:

- The sender generates the required PKI-based signature. FINCopy copies this digital signature in the message when it queues the copy message to the service administrator. The receiver of the original message will receive a digital signature from the sender.
- In Y-Copy mode, the service administrator also generates a Public Key Infrastructure signature. FINCopy includes the digital signature when it queues the message to the receiver.

In T-Copy there is no second signature, even when double authentication is specified, as there is no service administrator-to-receiver message involved.

**Bypass mode**

When FINCopy service is in Bypass mode and the FINCopy service profile specifies double authentication, FINCopy appends an empty PAC trailer to the message queued to the receiver. This indicates to the receiver that the *service administrator* has not authorised the message.

## 4 Service Administrator Responsibilities

### Introduction

This chapter describes the specific role and responsibilities of the service administrator.

The chapter covers the following topics:

- creation of the contractual relationship with SWIFT for FINCopy
- definition of the FINCopy Service Profile
- communication with users that participate in the FINCopy closed user group
- day-to-day operations
- administration of the FINCopy closed user group
- other service administration responsibilities

### Further details

Appendix C, "Service Administrators Operations Guide" on page 69 contains a more detailed description of administrative and technical procedures that the service administrator and SWIFT perform. These procedures form the implementation and operation of a FINCopy Service.

## 4.1 Implementation

### 4.1.1 Procedure

#### 4.1.1.1 Service Administration Agreement

##### Actions to take

Before a FINCopy service is set up, the service administrator and SWIFT must execute a *Service Administration Agreement*. To execute a *Service Administration Agreement*, the service administrator must be a duly registered SWIFT user. The service administrator must also complete and return a signed *Service Approval Request Form*.

##### Service administrator authority

Without prejudice to its other obligations, the service administrator warrants the following points to SWIFT:

- The service administrator has the necessary capacity and authority to instruct SWIFT to set up a FINCopy service as per the service parameters that the service administrator defines from time to time.
- The use of the FINCopy service (as per the service parameters defined, and other instructions given, by the service administrator) complies with all applicable laws and regulations and does not infringe any third-party rights.

### 4.1.1.2 Service Profile

#### Operational parameters

When the implementation timetable is established, the service administrator must define the parameters to govern the operation of the FINCopy service. This comprises the FINCopy service profile for the live and Test and Training services. In particular, the service administrator must do the following:

- Agree a FINCopy service identifier code with SWIFT, to be uniquely used for the new service. Users that participate in this FINCopy closed user group place this code in the header field 103 to indicate the messages for FINCopy to copy. It can be any three alpha characters, except where this can lead to confusion. The first two characters must be unique, that is, no other financial community can use the same first two characters as a FINCopy service identifier code. The third character must not be the letter X.
- Define the FINCopy service parameters, see "Example of FINCopy service parameters" on page 46:
  - The service administrator destination (central institution destination): The central institution destination is used to authenticate the service administrator authorisation/refusal notification. See "Double Authentication" on page 25.
  - The other message types which users that participate in the FINCopy closed user group can exchange.
  - The BIC8 address for the FINCopy server destination: This destination forms part of the FINCopy service profile. FINCopy and the service administrator use them for the MT 096 and MT 097 dialogue. Services with high traffic volumes may need to operate with two FINCopy server destinations. The service administrator and SWIFT will agree this in advance. If two server destinations are used then the service administrator must send each MT 097 from the same address as that which received the corresponding MT 096.
  - The numeric codes: Ranging from 50 to 99, and any alphanumeric codes for use as abort reason codes in field 432 of MT 097 and MT 019. In the same manner, any message status codes for use in field 431 for non-delivery warnings, undelivered message reports, and retrieved messages. See *FIN Error Codes*.
  - Decide whether copy messages require authorisation or not.

The service administrator instructs SWIFT of the applicable service parameters through the service profile. SWIFT publishes the service parameters of each FINCopy service at [www.swift.com](http://www.swift.com) > Support > Knowledge base > Tip2135221. The service administrator has, however, the ultimate responsibility to ensure that all users participating in the FINCopy closed user group know the service parameters that are relevant to them. For more information about the service profile, see Appendix A, "FINCopy Service Profile" on page 46.

---

**Note** When the service is in live operation, the service administrator must ensure that the communication methods are adequate for **routine and emergency** situations. This is to enable communication to some or all users that participate in the FINCopy closed user group, for any day-to-day operational matters that affect both FINCopy and the underlying service.

---

## References

### FINCopy service information

Topic	Reference
Abort reason codes and message status codes	"Relationship between FINCopy and FIN" on page 39
The service profile and parameters	Appendix A, "FINCopy Service Profile" on page 46
Operational procedures	Appendix C, "Service Administrators Operations Guide" on page 69

### 4.1.1.3 Operations Guide

#### Overview

The service administrator must abide by the procedures in Appendix C, "Service Administrators Operations Guide" on page 69, summarised in this chapter.

## 4.1.2 FIN Interfaces

### Suitability for FINCopy

A service administrator, which is already a FIN user and has a FIN interface, must confirm with the supplier that the interface supports FINCopy. The FIN interface configuration must be modified to include the FINCopy server destinations that the service administrator defines. The service administrator must also ensure the FIN Interface has adequate connectivity to support the service needs.

Service administrators without a FIN Interface must acquire one for each of the defined FINCopy server destinations. The interface must be able to send and receive the FINCopy Service messages and any other messages that are necessary to operate the specified service.

## 4.2 Operational

### Message exchange

For each user-to-user message sent between the users that participate in a FINCopy closed user group, FINCopy copies specific information from the user-to-user message into an *MT 096 FIN copy to Central Institution message*. FINCopy sends the MT 096 to the service administrator.

In Y-Copy mode, the service administrator must respond with an *MT 097 FIN copy message authorisation/refusal notification* for each MT 096 received. This applies for both live and Test and Training messages. In each MT 097, the service administrator must approve or refuse the underlying transaction.

---

**Note** Service administrators must ensure that the MT 097 is sent from the same FINCopy server destination that received the MT 096.

---

## Authentication

If double authentication has been defined in the FINCopy service profile, then the service administrator must be able to calculate and verify the Public Key Infrastructure-based signature. The service administrator must also be able to calculate and insert Public Key Infrastructure signature in the MT 097.

The service administrator's responsibilities for message authentication are given in the *FIN Security Guide*.

If the service administrator has defined that an *MT 012 sender notification* is required for the FINCopy service, then the service administrator can add text in field 114 of the MT 097. The service administrator can always place a text message for the receiver in field 115 of the MT 097.

If the MT 097 contains a rejection code then:

- FINCopy does not generate an MT 012, even if field 114 is present in the MT 097.
- FINCopy aborts the original user-to-user message and notifies the sender. FINCopy does not notify the receiver and does not pass the contents of field 115 to the receiver.

## Additional service administrator message exchange

The service administrator's FIN Interface can request FINCopy message status reports and cut-off time reconciliation reports from FIN. To do this, the interface sends an *MT 028 FIN copy message request*. FIN responds with an *MT 029 FIN copy message status report*.

The service administrator can also use the normal FIN message retrieval functionality. This includes the retrieval of MT 096 and MT 097 messages.

---

**Note** For full details of the system messages MT 028 and MT 029, see *FIN System Messages*.

---

## The service administrator's operational responsibilities

The service administrator must ensure that its FIN interface and other systems can handle the predicted maximum traffic volume without causing undue delays to FINCopy messages queued in Y-Copy mode.

The service administrator must be able to send and receive the types of messages that are defined in the service definition.

The service administrator must ensure that the system can handle the declared fallback procedure, for example, operating in Bypass mode, followed by the return to Y-Copy mode. To initiate the fallback procedure, the service administrator must contact the Customer Support Centre to request the closure, mode change, and re-opening of the service. When the problem that caused the fallback is solved, the service administrator must repeat the fallback procedure to revert to live.

For details of emergency procedures, including fallback procedures, see Appendix C, "Service Administrators Operations Guide" on page 69.

### Valid FINCopy service mode and state changes

Current service mode	Next service modes or states available	Reason for change
Y-Copy	T-Copy, Bypass, Closed state	fallback as specified in the FINCopy Service Profile
T-Copy	Closed state	fallback as specified in the FINCopy Service Profile

Current service mode	Next service modes or states available	Reason for change
T-Copy	Y-Copy	recovery from fallback
Bypass	T-Copy, Y-Copy	recovery from fallback

**Note** Bypass mode is available only from services in Y-Copy mode.

**Note** For services operating in Test and Training mode, the service administrator must accommodate and manage the choice of mode (current or future) for the users that participate in the FINCopy closed user group.

The MT 096, being a system message, is not dependent upon current or future modes. It contains FINCopy information appropriate to the mode that the sender of the original Test and Training user-to-user message selected. In Test and Training, a service administrator can receive MT 096s from users that participate in the FINCopy closed user group that contain either the current or future version of the same user-to-user message. SWIFT recommends that the service administrator declares the mode for the Test and Training session to the users that participate in the closed user group, and manages it manually.

## 4.3 General Responsibilities

### Service administrator

In addition to the implementation procedures outlined in "Procedure" on page 28 and the operational responsibilities in "Operational" on page 30, and without prejudice to other responsibilities set out in the *Service Administration Agreement* or the *Service Approval Request Form* a service administrator has the following responsibilities:

1. Administer the FINCopy closed user group(s).

This responsibility includes the following actions:

- Define the rules that govern the participation in the FINCopy service, and inform SWIFT thereof (and any subsequent change thereto).
- Instruct SWIFT of those users that may participate in the FINCopy service. In particular, the service administrator is solely and exclusively responsible for promptly confirming to SWIFT the approval or, as the case may be, the rejection of FINCopy user subscriptions. The service administrator is also solely and exclusively responsible for requesting the withdrawal of users from the FINCopy service.

2. Serve as the primary SWIFT contact for the provision of the FINCopy service.

3. Instruct SWIFT without delay of the service parameters for the provision of the FINCopy service through the service profile.

4. Ensure that all users know the service parameters that are relevant to them.

The objective is to enable these users to take the following actions:

- investigate and understand any consequences on their operations
- comply with their responsibilities, see "FINCopy User's Responsibilities" on page 34

5. Have the necessary capacity and authority to perform the obligations of the *service administrator*. These obligations include, without limitation, the authority to allow, refuse, or withdraw FINCopy users in, or from, the FINCopy closed user groups.

**Related procedures**

For more information about the related procedures, see Appendix C, "Service Administrators Operations Guide", and "Procedures".

The *service administrator* must be able to communicate with SWIFT by means of the MT 999 at all times.

# 5 FINCopy User's Responsibilities

## Introduction

This chapter describes the FINCopy procedures which users that participate in a FINCopy closed user group must perform.

It covers the following topics:

- implementation procedures
- technical requirements
- day-to-day operations

## 5.1 Implementation

### 5.1.1 Procedures

#### Prerequisites to participate in a FINCopy service

To participate in a FINCopy service, the user must be a duly registered SWIFT user.

#### Ordering procedure to participate in a FINCopy service

The procedure to participate in a FINCopy service is as follows:

1. The applicant FINCopy user subscribes to the relevant FINCopy service through SWIFT's e-ordering tool that is available on [www.swift.com](http://www.swift.com).
2. The service administrator approves the subscription to the FINCopy service.
3. Once approved, SWIFT confirms the subscription to the service administrator and to the SWIFT user, by e-mail.

### 5.1.2 FIN Interface

#### Requirements

The user that participates in a FINCopy closed user group must have a FIN Interface that can send and receive FIN message traffic. Users that participate in a FINCopy closed user group must confirm with the interface supplier that their FIN interface supports FINCopy.

To send and receive FINCopy messages, the FIN Interface of a user that participates in a FINCopy closed user group must also be able to do the following:

- accept the use of Field 103 (the FINCopy service Identifier Code) in the user header of any message type that the FINCopy service profile specifies as a FINCopy user-to-user message
- receive messages that the service administrator has authorised, and for which the service administrator may have supplied information in Field 115
- add the Public Key Infrastructure-based digital signature, if the service administrator has specified double authentication in the FINCopy service profile

- receive and process the Public Key Infrastructure-based digital signature equivalent, on an incoming message, if the service administrator has specified double authentication in the FINCopy service profile
- receive and process a message with an empty PAC trailer, if the service administrator has specified double authentication in the FINCopy service profile, and the FINCopy service is in Bypass mode

---

**Note** All FIN users that join a FINCopy closed user group receive, from the service administrator (not from SWIFT), the FINCopy service profile for the specific FINCopy service. This enables the user that participates in the FINCopy closed user group to configure the FIN interfaces for that service.

---

## 5.2 Operational

### 5.2.1 Sender's Perspective

#### Event sequence

The process from the sender's perspective ("Figure 12: Payment message process from the sender's perspective" on page 37) is as follows:

#### 1. Mark the message for FINCopy

If the sender wants to copy a message to the service administrator, then the sender must insert the FINCopy service Code specified by the service administrator in Field 103 of Block 3 (user header) of its FIN user-to-user message.

If there is no field 103 containing a service code, then FINCopy does not copy the original message to the service administrator. In this case, FINCopy delivers the message directly to the receiver, unless the service administrator has specifically requested that FINCopy must copy all messages exchanged within the FINCopy closed user group.

#### 2. Generate the digital signature

If the service administrator has specified double authentication in the FINCopy service profile, then the sender's FIN Interface uses relevant information to calculate the digital signature. For detailed information, refer to section A.2.4, "Authentication Mode".

#### 3. Send the message to the receiver

The sender transmits the message through FIN. FIN detects that the message is a FINCopy user-to-user message, places it in a temporary queue, and generates the MT 096 to the service administrator. The MT 096 contains the elements of the original message that the service administrator defined to be copied in the FINCopy service profile.

#### 4. Receive information about the message

If FIN positively acknowledges (ACKs) the message, then the sender may receive the following information:

- If the service definition includes Sender Notification, then the sender may receive an *MT 012 sender notification* when the payment is authorised.
- The sender may receive an *MT 019 abort notification* for one of the following reasons:
  - The MT 096 copy message is aborted.

- The service administrator's response to the copy of the message is an MT 097 rejection that causes FIN to reject the queued user-to-user message.
- FIN has aborted the user-to-user message for a technical reason, outside the scope of FINCopy, after the service administrator authorised the message.

This means that the sender may receive this message after it has received the MT 012. Field 432 in the MT 019 contains an abort reason code that explains why FIN or FINCopy aborted the original user-to-user message. The sender can use the code to determine which service aborted the message. See "FINCopy Abort Notification" on page 40 for a list of abort reason codes.

The MT 019 also contains the relevant service identifier code.

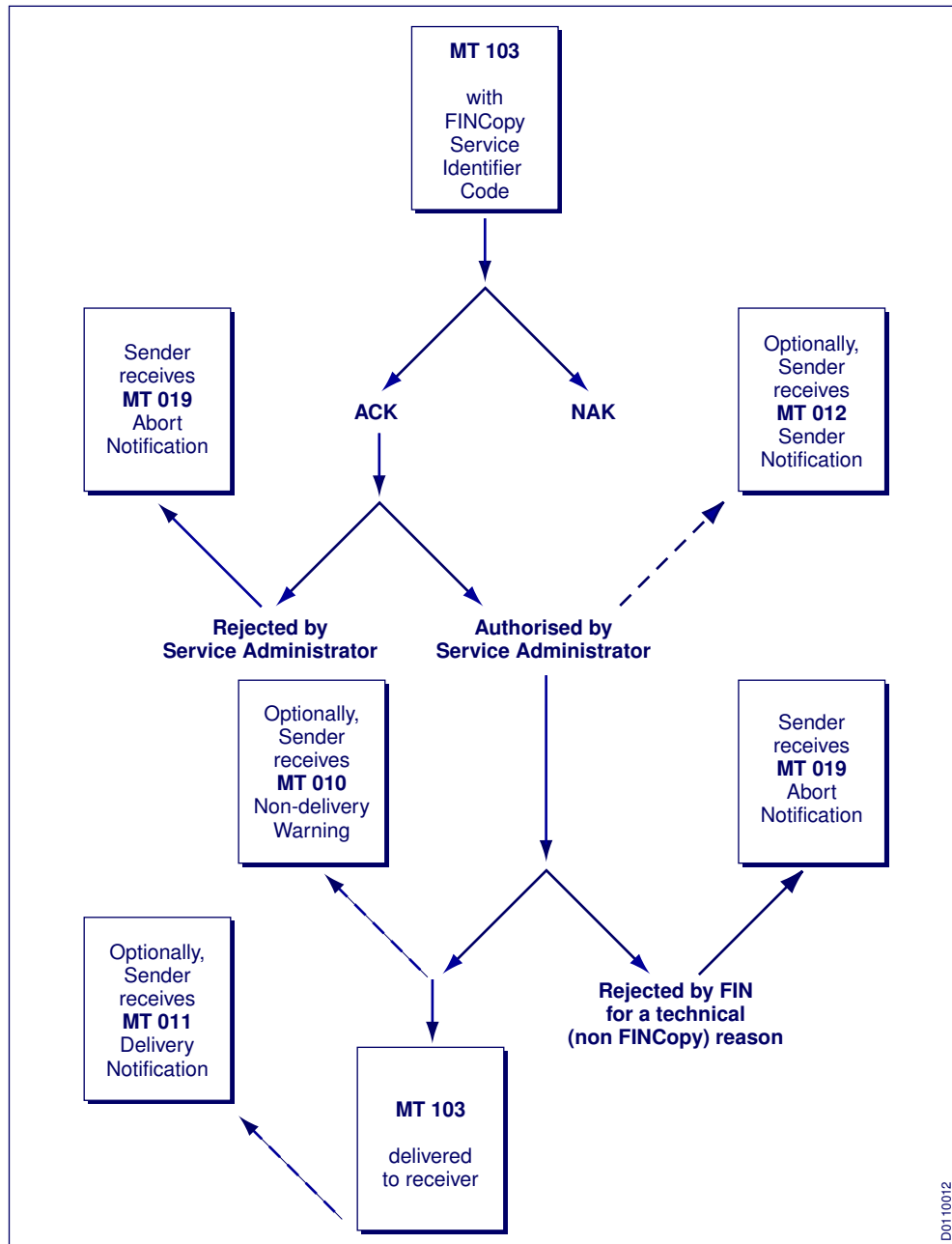
- The message aborts because the service administrator has not authorised delivery of the original message for more than 14 days (four days in Test and Training).

If FIN negatively acknowledges (NAKs) the message, then FINCopy does not copy the message. The sender can correct the error and re-send the message.

#### 5. **Exchange message with the service administrator**

If the service allows the exchange of a particular message type with the service administrator, then the sender must be able to process this message type.

Figure 12: Payment message process from the sender's perspective



D0110012

## 5.2.2 Receiver's Perspective

### Event sequence

The receiver is involved in FINCopy in the following way:

#### 1. Receive FINCopy user-to-user messages

User-to-user messages for the receiver contain the following:

- Field 103 in Block 3 (of the user header)
- optionally, Field 115 (in block 3), which contains information from the service administrator

- two digital signatures if the service administrator has specified double authentication in the FINCopy service profile.

## 2. **Verify the digital signature**

If the FINCopy service is in T-Copy mode, and the service profile specifies double authentication, then there cannot be a digital signature from the service administrator for the receiver. This is because there is no communication between a service administrator and a receiver in this mode.

If the message received contains an empty PAC, then the receiver knows that the fallback solution agreed amongst the FINCopy closed user group participants applies. For information about the different fallback modes, see "FINCopy Service Fallback" on page 42.

## 3. **Exchange a message with the service administrator**

If the Service Profile allows the exchange of a particular message type with the service administrator, then the receiver must be able to process this message type.

## 6 Relationship between FINCopy and FIN

### General

This chapter describes the impact of the FINCopy Service on aspects of the FIN messaging service.

The chapter covers the following topics:

- message retrievals
- the FINCopy trigger mechanism
- delivery monitoring and message abort notifications
- FINCopy abort notifications
- duplicate message avoidance
- payment release information
- message status reporting
- fallback processing
- Test and Training

### 6.1 Message Retrievals

#### FINCopy Service and user-to-user messages

Users that participate in a FINCopy closed user group can retrieve user-to-user messages, and the *service administrator* can retrieve FINCopy Service messages (for example, the MT 096 and the MT 097), up to 124 days after SWIFT has acknowledged the messages, as described in the *FIN Service Description*, the *FIN Operations Guide*, and as per the *SWIFT Data Retrieval Policy*.

---

**Note**      The *service administrator* must retrieve a service message from the same server destination that sent or received the message.

---

### 6.2 Message Flow Integrity

#### 6.2.1 FINCopy Service Trigger Mechanism

##### FINCopy service code

The presence of the FINCopy service code in Field 103 in Block 3 (of the user header) of the original message triggers the FINCopy mechanism.

FINCopy accepts a copy instruction for a message only if the message contains a valid FINCopy service code and a valid combination of message parameters (including sender, receiver, and message type), according to the *service administrator's* definitions in the service profile for that service code.

If there is no field 103 containing a service code, then FINCopy does not copy the original message to the *service administrator*. Instead, FIN delivers the message directly to the receiver, unless the *service administrator* has specifically requested in the service profile that all messages exchanged

in the FINCopy closed user group must be copied. If all messages exchanged within the closed user group must be copied, then SWIFT mandates the use of tag 103.

The service-code in Field 103 of Block 3 of the sent message must match the service Identifier of a valid FINCopy Service to which the sender and the receiver subscribe. The service profile must contain the message type. Otherwise, the message receives a negative acknowledgement (NAK).

## 6.2.2 Delivery Monitoring and Message Abort Notifications

### Abort conditions

FIN monitors message delivery for the original message. SWIFT does not provide the *service administrator* with a message delivery control mechanism (MT 010 and MT 011) for the delivery of the authorisation and refusal messages.

FIN aborts the delivery of the message or the copy if any of the conditions given in the following table is true.

### Abort conditions

Service	Condition
FINCopy	The <i>service administrator</i> has rejected the FINCopy service message.
FIN	The receiver has not logged on to SWIFT and selected FIN, for a period of 14 days in live mode, or four days in Test and Training mode (this applies to both the MT 096 and the original message).
FIN	After 11 unsuccessful delivery attempts (this applies to both the MT 096 and the original message).
FINCopy and FIN	The <i>service administrator</i> has not sent an authorisation or refusal message for live copy messages within 14 days, or for test and training copy messages within 4 days.

If the message aborts, whether for a FINCopy reason or a FIN reason, then SWIFT uses normal FIN functionality to notify the sender, by means of the *MT 019 abort notification*. This notification contains the appropriate abort reason codes and the relevant service identifier code. To mitigate operational risks, the receiver of an abort notification message should take appropriate action with all involved parties in line with the procedures communicated by the *service administrator*.

## 6.2.3 FINCopy Abort Notification

### Abort reasons

If the *service administrator* rejects a user-to-user message by means of the MT 097, then FINCopy sends an *MT 019 abort notification* to the sender of the original message. The MT 019 contains an appropriate error code in Field 432, and the relevant service identifier code. FIN does not deliver the original message to the receiver.

For a full list of message rejection codes (abort reasons) that apply to field 432 of the MT 019, see the *FIN System Messages*.

The *service administrator* is responsible for keeping the users that participate in its FINCopy closed user group informed of the codes used.

## 6.2.4 Duplicate Message Avoidance

### Possible Duplicate Emission and Possible Duplicate Message trailers

FIN protects users against message duplication by means of the Possible Duplicate Emission and Possible Duplicate Message trailers. These indicators warn a receiver that a message is possibly a duplicate of a previous one.

Because these indicators form part of the message trailer, FINCopy includes them in the information that it copies in the *MT 096 FIN copy to Central Institution message*. In this way, FINCopy also warns the service administrator of the possible duplicates.

These trailers are part of FIN functionality and are not specific to FINCopy. For full details see the *FIN Service Description*.

## 6.2.5 Payment Release Information

### MT 097

When the service administrator sends an authorisation message (MT 097), it has the opportunity to specify service-administrator-to-sender or service-administrator-to-receiver information (or both). The service administrator places this information in fields 114 and 115.

The service administrator must select the option to use field 114 during FINCopy implementation, because the use of this field generates a separate message, which has message charge implications. The option to use Field 115, which causes information to be added to an existing message by the FINCopy application, is always available to a service administrator.

If a service administrator places a text message in the optional Field 114 of the authorisation message MT 097, to provide information for the sender of the original user-to-user message, then FINCopy issues a Sender Notification (MT 012), which includes this information. FINCopy sends the MT 012 to the sender of the original user-to-user message.

If the service administrator uses field 115 to specify service-administrator-to-receiver information, then SWIFT includes the information in block 3 of the user-to-user message.

---

**Note** If the MT 097 contains a rejection code, then the presence of field 114 does not generate an *MT 012 sender notification*. Also, if the service administrator includes field 115 in a rejection message, then FINCopy **ignores** the information, because there is **no** notification to the receiver of a rejected message.

---

### Duplicate MT 097

If a service administrator sends a duplicate MT 097, then the following occurs:

- if there is a Possible Duplication Emission trailer, then FINCopy ignores the second message provided it received the first MT 097
- If there is no Possible Duplication Emission trailer, then the following occurs:
  - if the service administrator had already authorised the user-to-user message, then FIN sends an *MT 015 Delayed NAK* to the service administrator, with error code X37
  - if the service administrator had already refused the user-to-user message, then FIN sends an *MT 015 Delayed NAK* to the service administrator, with error code X36

## 6.2.6 Message Status Reporting to Sender

### Error and reason codes

FIN System Messages that provide message, error, or reason codes include specific FINCopy codes, as well as codes that refer to reasons outside the scope of FINCopy, but within the scope of FIN processing.

The system messages specifically include the following:

- non-delivery warnings (MT 010), if the message remains undelivered to the receiver at the end of the obsolescence period
- solicited and unsolicited undelivered message reports (MT 066, MT 082, MT 083)
- message retrievals, including delivery history (MT 021, MT 023)
- abort notifications (MT 019)

FIN reports the status of a message in Field 431 of non-delivery warnings, undelivered message reports, and retrieved messages.

For a full list of the message status codes in field 431, see the *FIN System Messages*.

The service administrator must keep the users that participate in its FINCopy closed user group informed of the current codes.

## 6.2.7 FINCopy Service Fallback

### Fallback modes

The service administrator must decide upon the fallback mode when it first defines the service. (See "FINCopy Service Profile Parameters" on page 47).

The fallback modes are:

- **Fallback from Y-Copy mode to closed service state**

In this situation, messages that FINCopy holds while it awaits a response from the service administrator remain in the temporary queue. New user-to-user FINCopy messages, which users that participate in the FINCopy closed user group send while the service is closed, receive a negative acknowledgement (NAK).

- **Fallback from T-Copy mode to closed service state**

Because FINCopy does not queue messages in T-Copy mode, the impact of this fallback situation is that new user-to-user FINCopy messages, which users that participate in the FINCopy closed user group send while the service is closed, receive a NAK.

- **Fallback from Y-Copy mode to bypass mode**

A service administrator can bypass the FINCopy service mechanism in Y-Copy mode. To do this, the service administrator must ask SWIFT to change the service mode to Bypass.

SWIFT can only make mode changes if the service state is closed. FIN NAKs new user-to-user FINCopy messages which users that participate in the FINCopy closed user group send while the service is closed. If SWIFT reopens the service state in Bypass mode, then it forwards new and existing FINCopy messages to the receiver, and replaces digital signatures generated by the central institution destination with empty PACs.

---

**Note** An empty PAC trailer indicates to the receiver that the service administrator has not authorised, or received a copy of, the message. Empty PAC trailers are only used to indicate bypass mode for services that use double authentication.

---

- **Fallback from Y-Copy mode to T-Copy mode**

If the service administrator had chosen to use T-Copy mode for fallback from Y-Copy mode, then SWIFT must still close the service to change the mode. FIN NAKs new user-to-user FINCopy messages that SWIFT receives while FINCopy is closed. Within FINCopy, SWIFT continues to queue messages that require authorisation. Once SWIFT reopens the service in T-copy mode, it forwards new SWIFT FINCopy messages to the receiver with no digital signature from the service administrator. This is because T-Copy mode allows only the digital signature between sender and service administrator. If the service operates in double authentication mode, then SWIFT forwards existing FINCopy messages with empty PAC trailers. This indicates that the messages have not undergone the authorisation process, even though FINCopy originally received the messages in Y-Copy mode.

---

**Note** Absence of a PKI signature from the service administrator if the service profile specifies double authentication, is an indication to the receiver that the service is operating in T-Copy mode.

---

## 6.3 Test and Training

### Test and Training within a FINCopy Service Closed User Group

All users that participate in a FINCopy Service closed user group benefit from a full Test and Training environment to exchange test FINCopy user-to user messages. In such an environment, FINCopy copies messages to a service administrator Test and Training destination.

The service administrator must take note that FINCopy copies MT 096 and MT 097 system messages in Test and Training mode, regardless of the following circumstances:

- whether the service administrator is operating the service in current or future mode
- whether the sender sent the original FINCopy message in current or future mode

The service administrator must manage the choice of mode for such Test and Training sessions. The MT 096, being a system message, is not dependent upon current or future mode, and contains information that FINCopy has copied, that is appropriate to the mode that the sender of the original Test and Training user-to-user message has selected. For this reason, in Test and Training, a service administrator can receive information that FINCopy has copied from different users that participate in the FINCopy closed user group, in both current and future modes.

---

**Note** For more information about Test and Training, see the *FIN Service Description* and the *FIN Operations Guide*.

---

# 7 Ordering

## **Order SWIFT services and products**

To use SWIFT services and products, a customer must subscribe to, or order, the relevant services and products.

## **Related information**

For information about SWIFT's online ordering facility and how to order, see [www.swift.com](http://www.swift.com) > Ordering.

## 8 SWIFT General Terms and Conditions and Liability

### 8.1 Application of the SWIFT General Terms and Conditions

#### SWIFT General Terms and Conditions

The *SWIFT General Terms and Conditions* govern the provision and the use of the FINCopy service. For the latest available version of the *SWIFT General terms and Conditions*, see [www.swift.com](http://www.swift.com) > About SWIFT > Legal > SWIFT contracts.

### 8.2 SWIFT Liability

#### Liability for FINCopy messaging

SWIFT accepts liability (whether in contract, tort, or otherwise) to the service administrator and users that participate in the FIN closed user group, in connection with the provision and the use of the FINCopy service, as set out in the *SWIFT General Terms and Conditions*, to the extent supplemented or varied by the terms of this chapter.

SWIFT's liability for FIN messages shall apply *mutatis mutandis* to the FINCopy message processing. This takes into consideration, however, that FINCopy message processing is deemed to consist of the delivery of two user-to-user FIN messages (that is, one from the sending user that participates in the FINCopy closed user group to the service administrator and, if so authorised by the service administrator, one from the sending user that participates in the FINCopy closed user group to the receiving user that participates in the FINCopy closed user group).

Also, and for the purposes of FINCopy message processing, timing is defined as follows:

1. For the delivery of the full or partial copy to the service administrator, the delivery time is defined as the time elapsed between the acknowledgement of receipt of the original message by FIN to the sending user that participates in the FINCopy closed user group and the availability of the full or partial copy that FINCopy forwards to the service administrator.
2. For the delivery of the original message and approval stamp to the receiver in Y-Copy mode, the delivery time is defined as the time elapsed between the acknowledgement of receipt of the delivery authorisation by SWIFT to the service administrator, and the availability of the original message that FINCopy forwards to the addressee.
3. For the delivery of the optional sender notification in Y-Copy mode, the delivery time is defined as the time elapsed between the acknowledgement of receipt of the delivery authorisation by SWIFT to the service administrator, and the availability of the sender notification that SWIFT forwards to the sender of the user-to-user message.

To avoid any doubt, the responsibilities of the SWIFT user, as a sender or as a receiver of a FIN message, as laid down in the FIN service documentation and, in particular, the *FIN Service Description*, shall also apply *mutatis mutandis* either to the service administrator or the user that participates in the FINCopy closed user group (or both, as the case may be) for messages exchanged in relation to, or in connection with, FINCopy.

## Appendix A

# FINCopy Service Profile

## A.1 FINCopy Service Profile

This example is for a FINCopy Service with the service code *COP*.

### Example of FINCopy service parameters

Parameter	Value
FINCopy service code	COP
Live Service flag (Live = Y, Test and Training = N)	Y
Service administrator destination (central institution destination)	COPYCCLL
Authentication mode (normal = 1, double = 2)	2
Full copy flag (full copy = Y, partial copy = N)	N
Currency code	CCD
Y-Copy Sender Notification (MT 012) (G=Global, I=Individual, N=None)	I
----	----
Message type (repeat next three parameters for each MT)	MT103
List of field tags that FINCopy copies	20, 32A
Field tag containing the value date	NA
Field tag containing the currency	32A
Message type	MT 202
List of field tags that FINCopy copies	20, 32A
Field tag containing the value date	NA
----	----
FINCopy service mode	Y-Copy
FINCopy fallback service	Close the service
FINCopy server destination	COPYCCLA
RMA bypass	Y
FINCopy server destination	COPYCCLA

FINCopy and the service administrator use the FINCopy server destination to exchange FINCopy service messages.

The users that participate in the FINCopy closed user group may not see, or require notification about, FINCopy service messages for a particular FINCopy service. For all operational purposes or verification of digital signatures, users that participate in a FINCopy closed user group must use the service administrator destination (central institution destination), which is the third parameter in this example.

## A.2 FINCopy Service Profile Parameters

### A.2.1 FINCopy Service Code

#### Field 103

The FINCopy service code parameter is a unique Identifier which the user that participates in a FINCopy closed user group inserts into field 103 of the user header, to identify a message for FINCopy. FIN also uses this parameter in undelivered message reports, for the same purpose. Live and Test and Training profiles must share the same FINCopy service code. Once the service administrator has defined this parameter, it cannot be changed.

### A.2.2 Live Service Flag

#### Live or Test and Training

The live service flag indicates whether the given service definition is for a live copy service or for a Test and Training service.

### A.2.3 Service Administrator Destination (Central Institution Destination)

#### SWIFT BIC8

The Service Administrator Destination, formerly known as the central institution destination is a valid SWIFT BIC8 that SWIFT assigns to the service administrator. The central institution destination is for the calculation of digital signatures. The central institution destination can be the same as the server destination.

---

**Note** If the service administrator is also a user that participates the FINCopy closed user group, then it must use a separate BIC8. If the participation is in test mode only, then an additional Test and Training destination is required.

---

### A.2.4 Authentication Mode

#### Single or double

The authentication mode parameter indicates whether the FINCopy service is in single or double authentication mode. Double authentication mode requires digital signatures in FINCopy messages and (in Y-Copy mode) in message authorisations and refusals from the service administrator.

### A.2.5 Digital Signature Generation

#### Sender authentication

Because of the way Public Key Infrastructure has been implemented, the sender of the original message only needs to calculate one PKI signature. This signature covers two sets of data, one for the receiver of the original message and one for the service administrator. The service administrator and the receiver of the original message use the PKI signature to authenticate the sender.

### User-to-user message

The following message data will be used:

- **Sender BIC8** - the eight character BIC code of the sender of the message.
- **Receiver BIC8** - the eight-character BIC code of the receiver of the message.
- **Full block 4** - the full content of block 4 of the FIN message.
- **Random value** - this element is mandatory in the case of double authentication, that is, when the sender generates two digests. In all other cases, it is not allowed. The purpose of this element is to ensure that, in the case of partial copy, it is not possible for the service administrator to derive the full block 4 contents.

### Sender to service administrator

To create the message digest that is signed for the service administrator, the sender's application uses the following message data:

- **Sender BIC8** - the eight character BIC code of the sender of the message
- **Central institution destination BIC** - the eight-character BIC code of the FINCopy central institution destination as defined in the FINCopy Service Profile for the service.
- **The to-be-copied part of block 4** (full or partial). These are the fields that will be copied to the Service Administrator in the *MT 096 FIN copy to Central Institution message*.

### Service administrator to receiver

The service administrator calculates a PKI signature based on the following input data:

- **Central Institution destination BIC** - the eight-character BIC code of the central institution destination as defined in the FINCopy Service Profile for the service.
- **Receiver BIC8** - the eight-character BIC code of the receiver of the original message.
- **Field 115** (if present) - the contents of the optional field tag 115 (Payment Release Information) from the Service Administrator to the receiver.
- The fields copied from block 4 of the original message and received in the *MT 096 FIN copy to Central Institution message*.
- The signature value of the original message if the original message contained a digest for the user-to-user message.

The service administrator signs using the certificate associated with the central institution destination, as identified in the *service profile form*.

### Data covered by the PKI signature between the sender and the receiver

```
{1:F01BCITITMMAXXX0012000123}
{2:01030950040322BNPAFRPPXXX00120078960403221051U3}
{4:CrLf
:20:1234567890CrLf
:23B:CREDCrLf
:32A:040322EUR450,00CrLf
:50K:MASTERS IMPORTCrLf
RUE DES ARBRES 119CrLf
CAMBRAICrLf
:52A:BNPAFRPPCAMCrLf
:53A:POCIITMM680CrLf
:57A:BCITITMM680CrLf}
```

```

:59:/P03452032022819 30CrLf
GRAND IMPORTCrLf
PESCARACrLf
:70:/RFB/INV 5591CrLf
:71A:BENCrLf
-}
{5:{CHK:123456789ABC}}

```

### Data covered by the PKI signature between the sender and the service administrator

The signature is calculated on the fields marked in **bold** in the following message plus the central institution BIC9, ie the BIC8 plus the logical terminal identifier:

```

{1:F01BCITITMMAXXX0012000123}
{2:O1030950040322BNPAFRPPXXX00120078960403221051U3}
{4:CrLf
:20:1234567890CrLf
:23B:CREDCrLf
:32A:040322EUR450,00CrLf
:50:MASTERS IMPORTCrLf
RUE DES ARBRES 119CrLf
CAMBRAICrLf
:52A:BNPAFRPPCAMCrLf
:53A:POCIITMM680CrLf
:57A:BCITITMM680CrLf
:59:/P03452032022819 30CrLf
GRAND IMPORTCrLf
PESCARACrLf
:70:/RFB/INV 5591CrLf
:71A:BENCrLf
-}
{5:{CHK:123456789ABC}}

```

## A.2.6 Full Copy Flag

### Full or partial copy service

The full copy flag parameter indicates whether the service administrator has defined the FINCopy service as a full copy service or a partial copy service. The mode applies to the entire service (that is, for all message types copied).

If the service is a partial copy service, then the FINCopy service copies only the specified field tags to the server. If the service is a partial copy service, then the service administrator must specify the list of field tags for each message type in the service profile. FINCopy can copy up to 32 different field tags per message type.

---

**Note** Full copy service mode must be used for ISO 15022 message types.

---

## A.2.7 Currency Code

### Currency code check

The currency code check parameter indicates whether the FINCopy Service must make a currency code check on the FINCopy messages. If the check is required, then the service administrator must specify a field tag that contains the currency code for each message type in the service profile.

---

**Note** Service administrators must not specify currency code checks to ISO 15022 message types when defining the service profile.

---

## A.2.8 MT 012 Y-Copy Sender Notification

### Sender notification

The sender notification parameter indicates, for Y-Copy mode, whether FINCopy uses the MT 012 to convey information to the sender of the original user-to-user message. If the *service administrator* selects this option, then either all, or selected users that participate in the FINCopy closed user group, in agreement with the *service administrator*, receive this message.

The options that are available to the *service administrator* are as follows:

- **General use**

FINCopy always uses the MT 012

- **Individual use**

The *service administrator* decides under which circumstances FINCopy sends an MT 012.

- **Not used**

The MT 012 is not available for the specific FINCopy Service.

## A.2.9 Message Types Selected for Copying

### Message types

For each FINCopy service, the *service administrator* can select up to 25 message types to be copied.

## A.2.10 FINCopy Service Mode

### Normal service mode

The FINCopy service mode parameter indicates the normal service mode, Y-Copy, or T-Copy. In Y-Copy mode, FINCopy delivers the original message to the receiver only after receipt of an authorisation message from the *service administrator*. In T-Copy mode, FINCopy delivers the original message to the receiver, and sends a full or partial copy to the *service administrator*.

## A.2.11 FINCopy Fallback Service Mode

### Emergency service

FINCopy fallback service mode is the mode in which the service can operate if there is a disaster or emergency. For more information about the different types of fallback modes, see "FINCopy Service Fallback" on page 42.

## A.2.12 FINCopy Server Destination

### Service administrator server destination

The FINCopy server destination parameter is the service administrator server destination to which FINCopy forwards *MT 096 FIN copy to Central Institution messages*. Each FINCopy service requires one server destination. High volume services may require two server destinations. SWIFT will agree this with the service administrator in advance. Live and Test and Training services must have separate server destinations.

---

**Note** If a service has two server destinations, then the server destination (that is, the BIC8) that received the MT 096 must always issue the corresponding *MT 097 FIN copy message authorisation/refusal Notification*.

---

## Appendix B

# Case Studies

## B.1 Purpose of this Appendix

### Sample transaction messages

This appendix contains the messages that relate to a sample transaction that is profiled in "Transaction Profile" on page 53. The sample transaction shows the various extra fields and trailers for the different FINCopy conditions described in sections "Messages, Y-Copy Mode: Authorised Payment" on page 54 to "Messages, T-Copy Mode" on page 65.

To explain the processes, these case studies show all the messages involved in the various FINCopy modes. In reality, users that participate in the FINCopy closed user group and the service administrator, have different perspectives on the FINCopy service, as "Figure 29: FINCopy user's perspective" and "Figure 30: Service administrator's perspective" illustrate. Users that participate in the FINCopy closed user group see the payment message process. The service administrator sees the system message dialogue with FINCopy.

**Figure 29: FINCopy user's perspective**

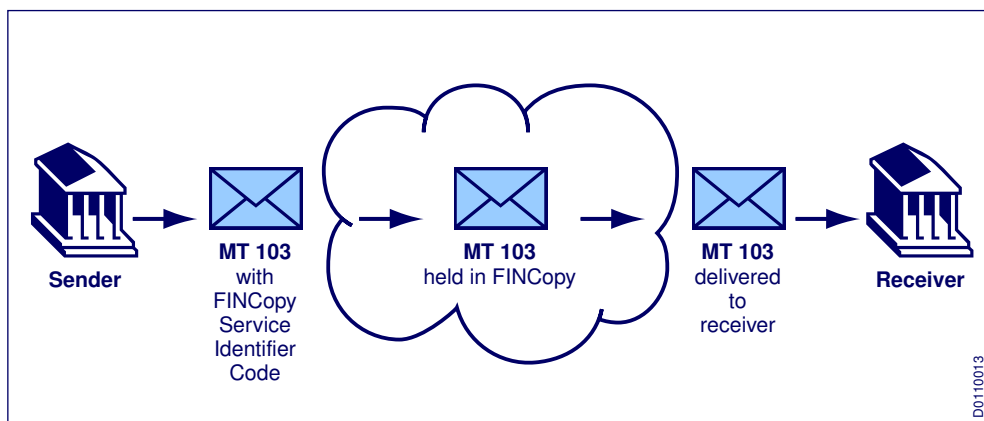
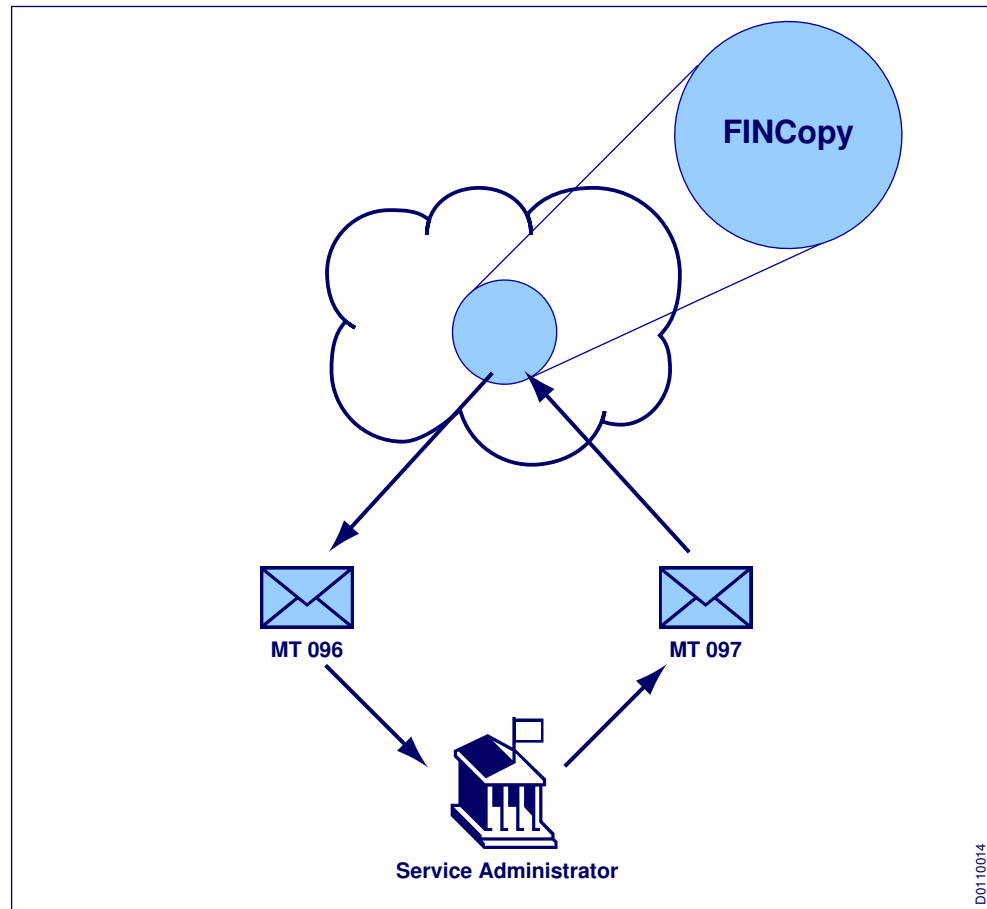


Figure 30: Service administrator's perspective



**Note** The messages shown in this appendix have some header and trailer block fields on separate lines. This is only for purposes of illustration and must not be taken as indications of <carriage return - line feed> within the messages.

## B.2 Transaction Profile

### Case study parameters

Sections "Messages, Y-Copy Mode: Authorised Payment" on page 54 to "Messages, T-Copy Mode" on page 65 show the messages that result from the following transaction processed by various FINCopy services.

For this purpose, the following is assumed:

- that the transaction takes place in a country with country code *CC*
- that the currency in the country is *CC Dollars*, with a currency code of *CCD*
- that a *service administrator* with primary server destination *INSTCC2AXXX* has established an RTGS system that uses FINCopy
- that two users that participate in the FINCopy closed user group are Senderbank *SNDRCC2AXXX* and Receiverbank *RCVRCC2AXXX*

- that on 01 September 2007, Senderbank, on behalf of its customer A. Payer Inc., effects a same-day-value payment of CCD 10,000.00 in favour of A. Payee Inc., in account with Receiverbank.

In these case studies, the FINCopy service profile contains the following parameters:

- the FINCopy service Identifier code is *COP*
- double authentication
- partial copy
- FINCopy must copy fields 20 and 32A in the MT 103.

RMA authorisation is not required for messages that are to be copied.

Other FINCopy service profile parameters vary according to the different case studies.

## B.3 Messages, Y-Copy Mode: Authorised Payment

### Y-Copy mode example

In this case study, the *service administrator* has specified Y-Copy mode in the FINCopy service profile. The FINCopy service is in normal operations mode, and the *service administrator* has authorised the payment message.

The following figures show the sequence of messages:

- "Figure 31: MT 103 single customer credit transfer - that Senderbank has prepared and transmitted to FIN." and transmitted to FIN.
- "Figure 32: MT 096 FIN copy to Central Institution message".
- "Figure 33: MT 097 FINCopy message authorisation/refusal notification", that the *service administrator* has returned. It shows the authorisation code, and contains information for both the sender and the receiver.
- "Figure 34: MT 103 single customer credit transfer message as delivered - to Receiverbank". The message contains additional information in the header block from the *service administrator*.
- "Figure 35: MT 012 sender notification". This message contains information for Senderbank from the *service administrator*.

**Figure 31: MT 103 single customer credit transfer - that Senderbank has prepared and transmitted to FIN.**

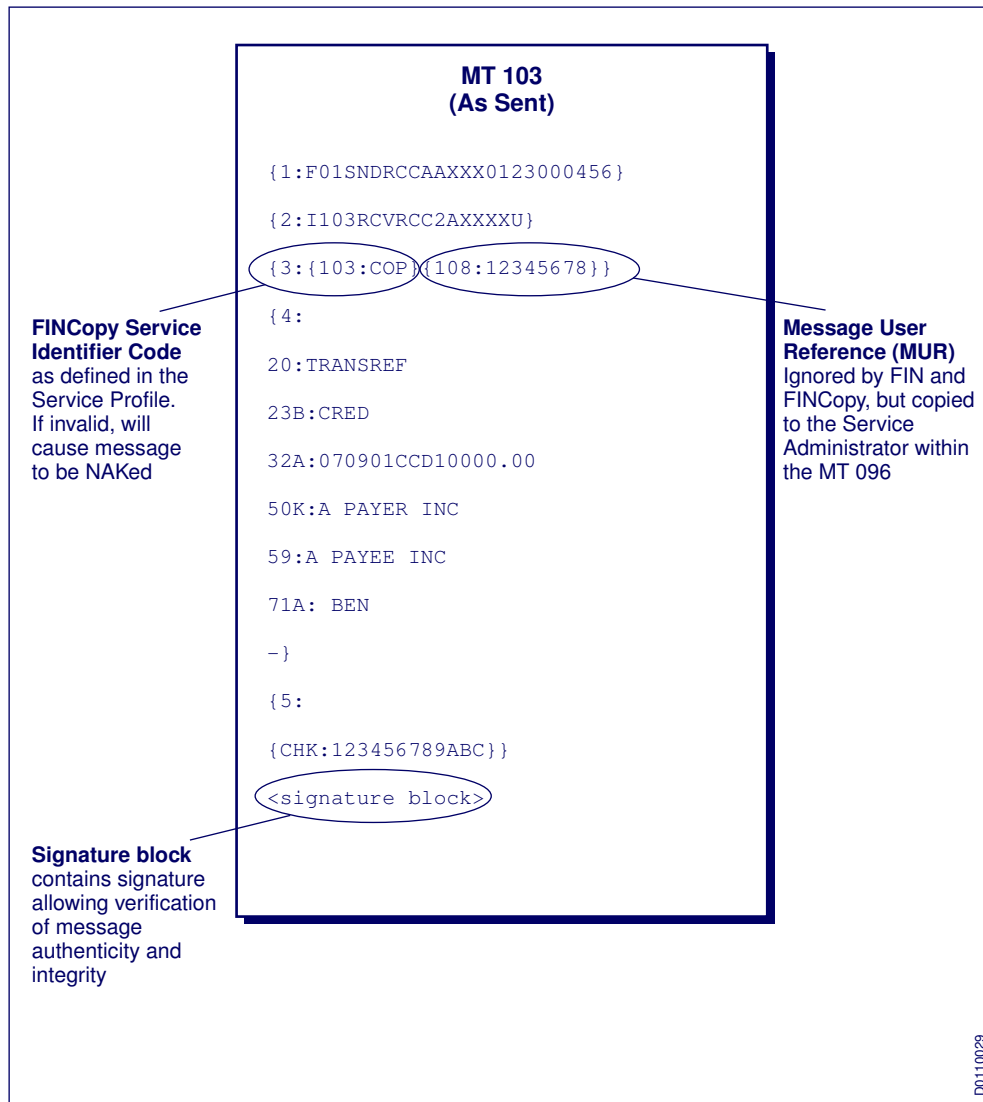


Figure 32: MT 096 FIN copy to Central Institution message

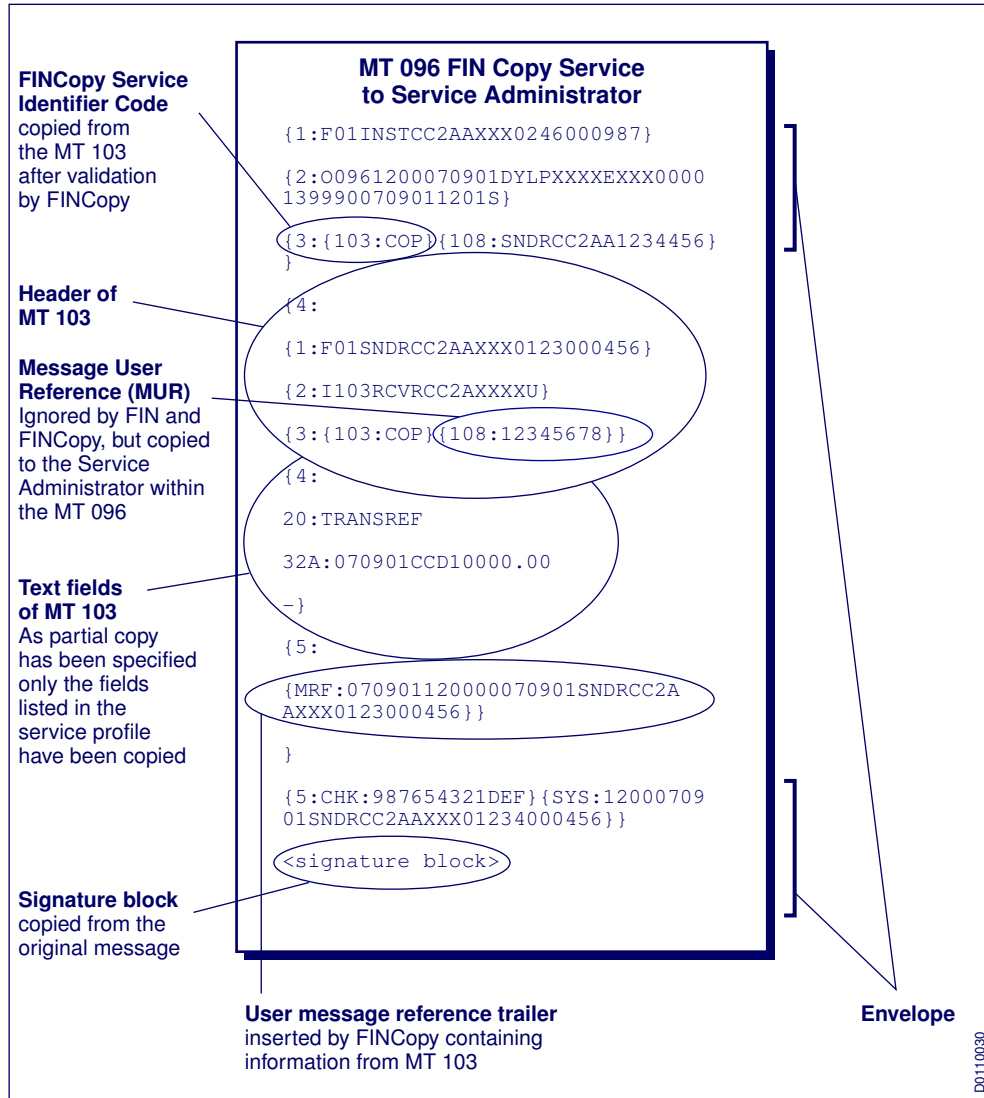
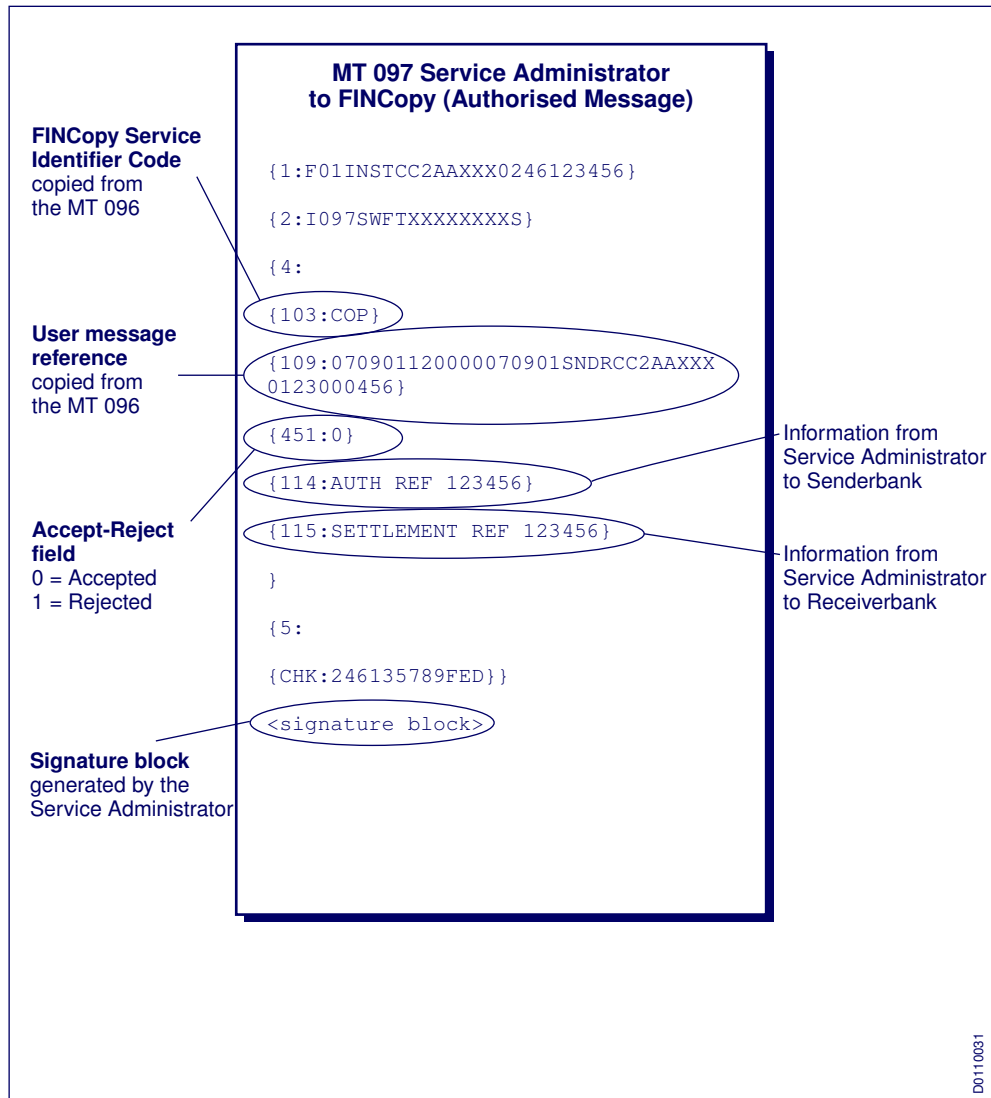


Figure 33: MT 097 FINCopy message authorisation/refusal notification



**Figure 34: MT 103 single customer credit transfer message as delivered - to Receiverbank**

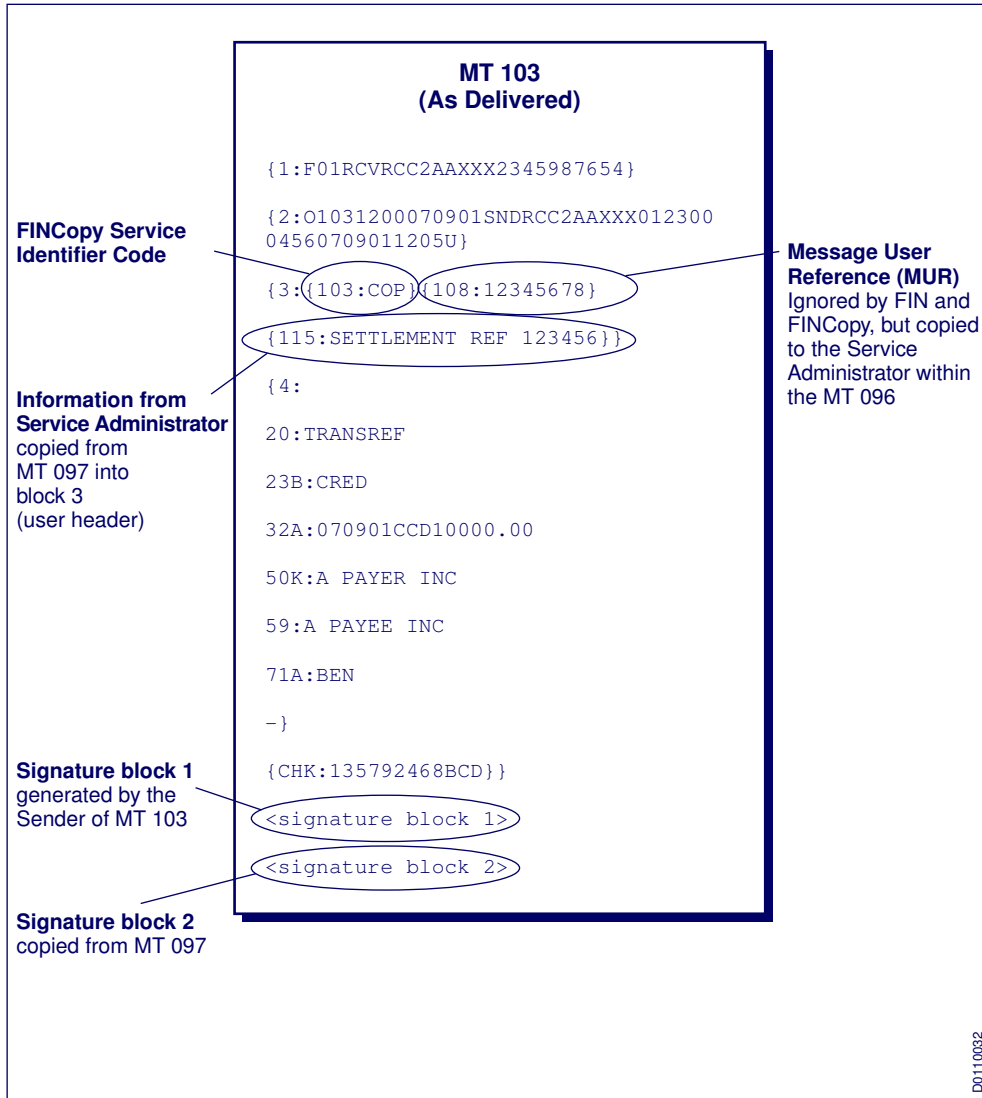
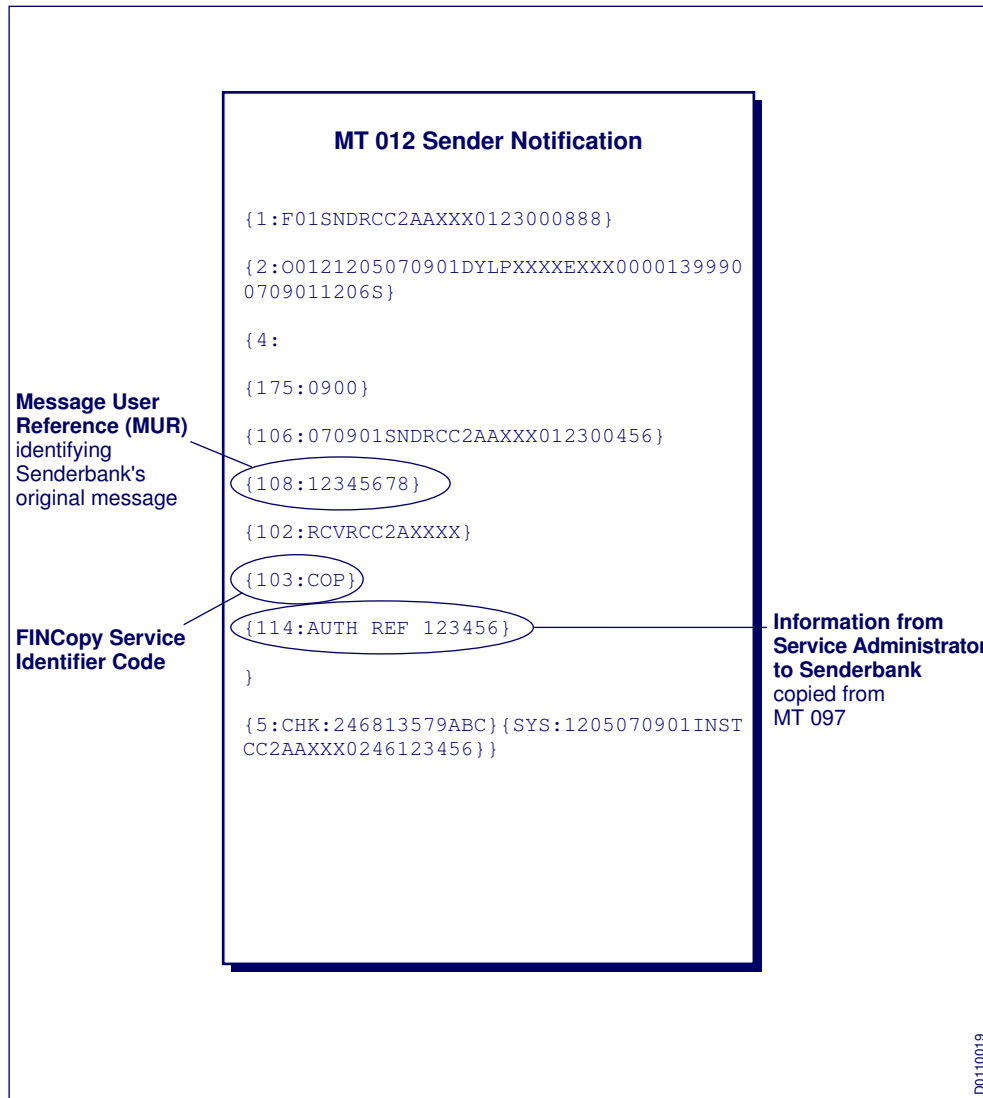


Figure 35: MT 012 sender notification



**Note** Because FINCopy service profiles for the case studies in this appendix specify *partial copy*, the MT 103 trailers copied in the MT 096, and illustrated in figures 32, 37, and 43, do not include the Checksum trailer. However, if the service profiles had specified *full copy*, then the Checksum trailer would be present.

## B.4 Messages, Y-Copy Mode: Rejected Payment

### Message sequence

In this case study, the FINCopy service is still in Y-Copy mode, but the service administrator decides to reject the payment message.

The message sequence is as follows:

- "Figure 36: MT 103 single customer credit transfer message - from Senderbank".
- "Figure 37: MT 096 FIN copy to Central Institution message".

**Note** These messages are identical to those in the case study in "Messages, Y-Copy Mode: Authorised Payment" on page 54.

- "Figure 38: MT 097 rejection message" shows the MT 097, in which Field 451 indicates that the service administrator has rejected the proposed transaction, and that FINCopy must delete the payment message and not deliver it to Receiverbank. This message also contains a code, in Field 432, giving the abort reason.
- "Figure 39: MT 019 abort notification - to Senderbank".

**Figure 36: MT 103 single customer credit transfer message - from Senderbank**

**MT 103 (As Sent)**

```

{1:F01SNDRCC2AAXXX0123000456}
{2:I103RCVRCC2AXXXU}
{3:{103:COP}{108:12345678}}
{4:
20:TRANSREF
23B:CRED
32A:0709012CCD10000.00
50K:A PAYER INC
59:A PAYEE INC
71A:BEN
-}
{5:
{CHK:123456789ABC}}
<signature block>
    
```

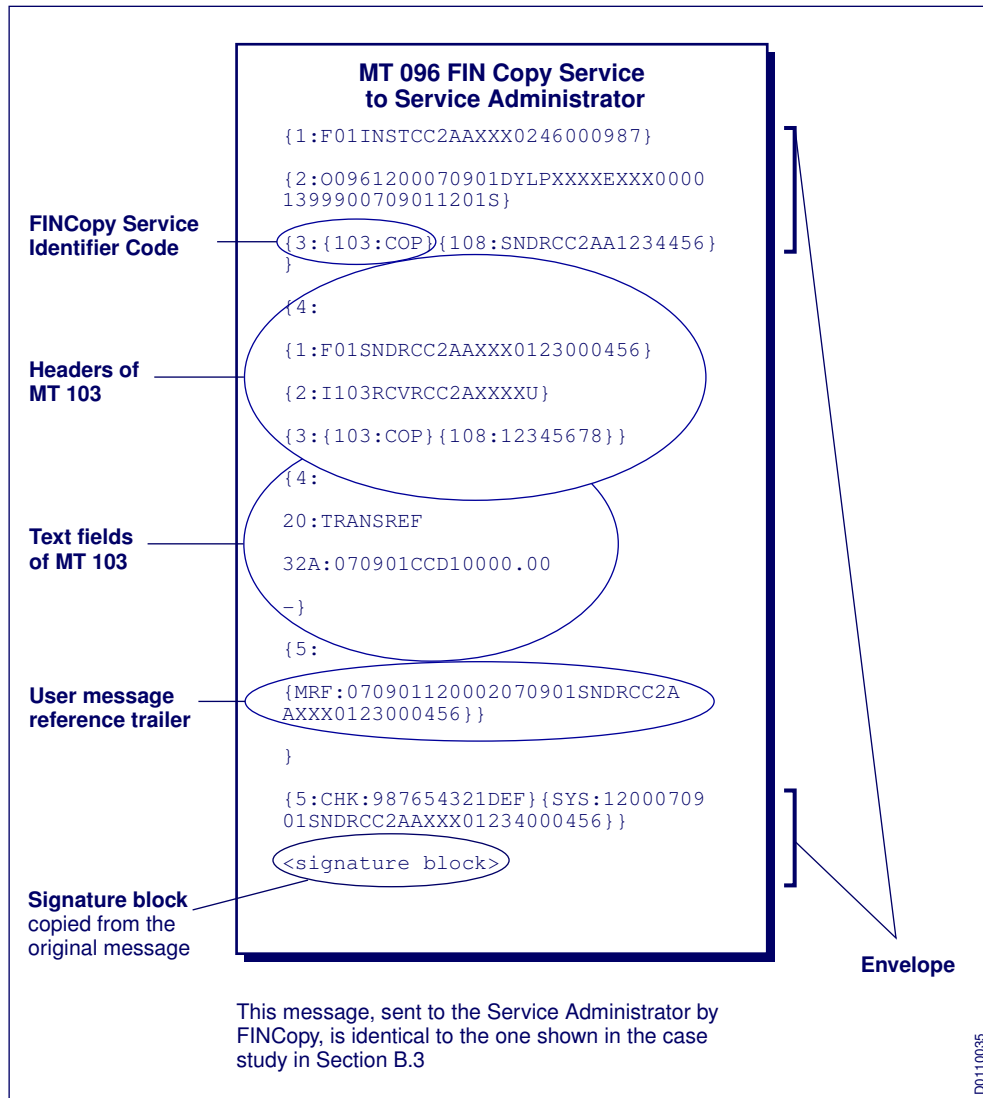
**FINCopy Service Identifier Code,**  
as shown in Figure 31.

**Signature block**  
contains signature allowing verification of message authenticity and integrity

As Senderbank is unaware that this message will be rejected by the Service Administrator, this message is identical to the one shown in the case study in Section B.3

D0110034

Figure 37: MT 096 FIN copy to Central Institution message



**Figure 38: MT 097 rejection message**

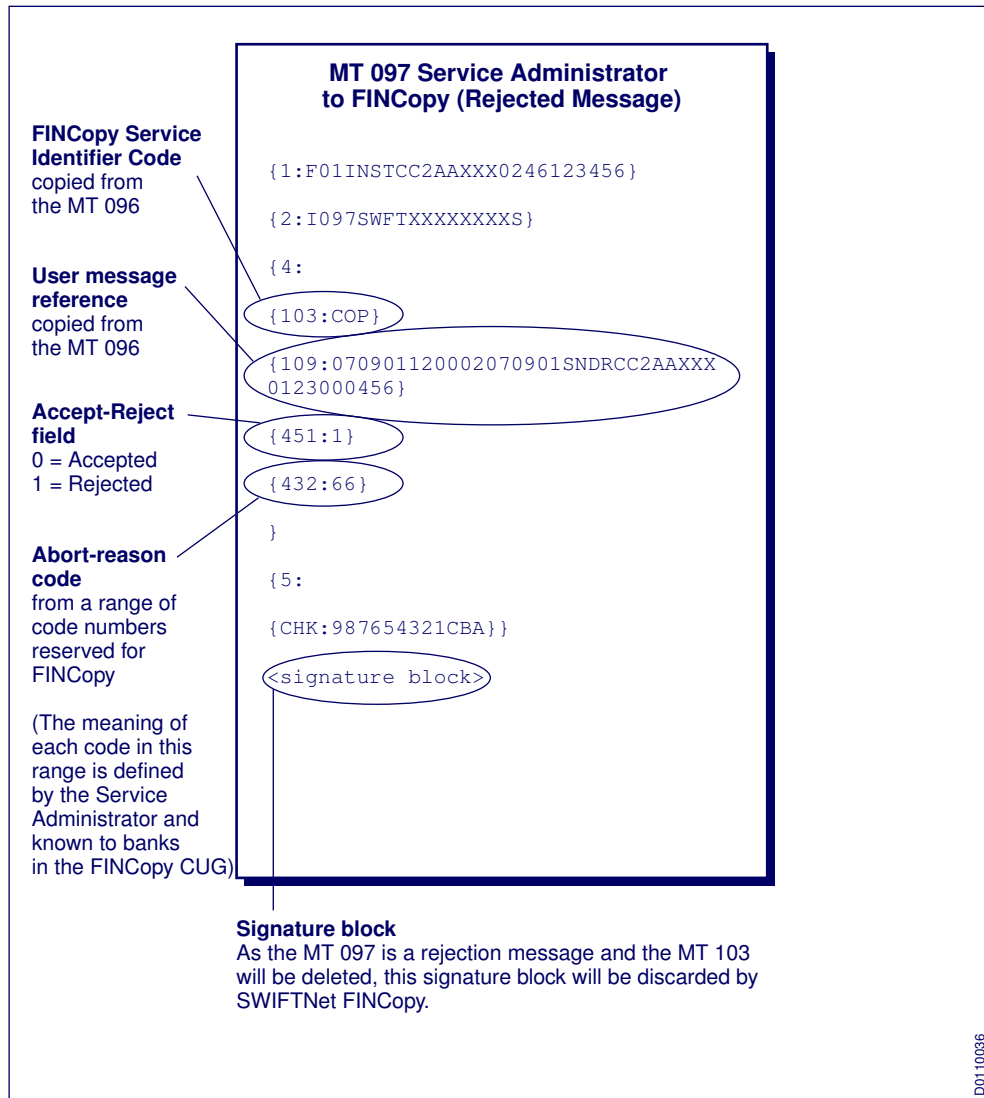
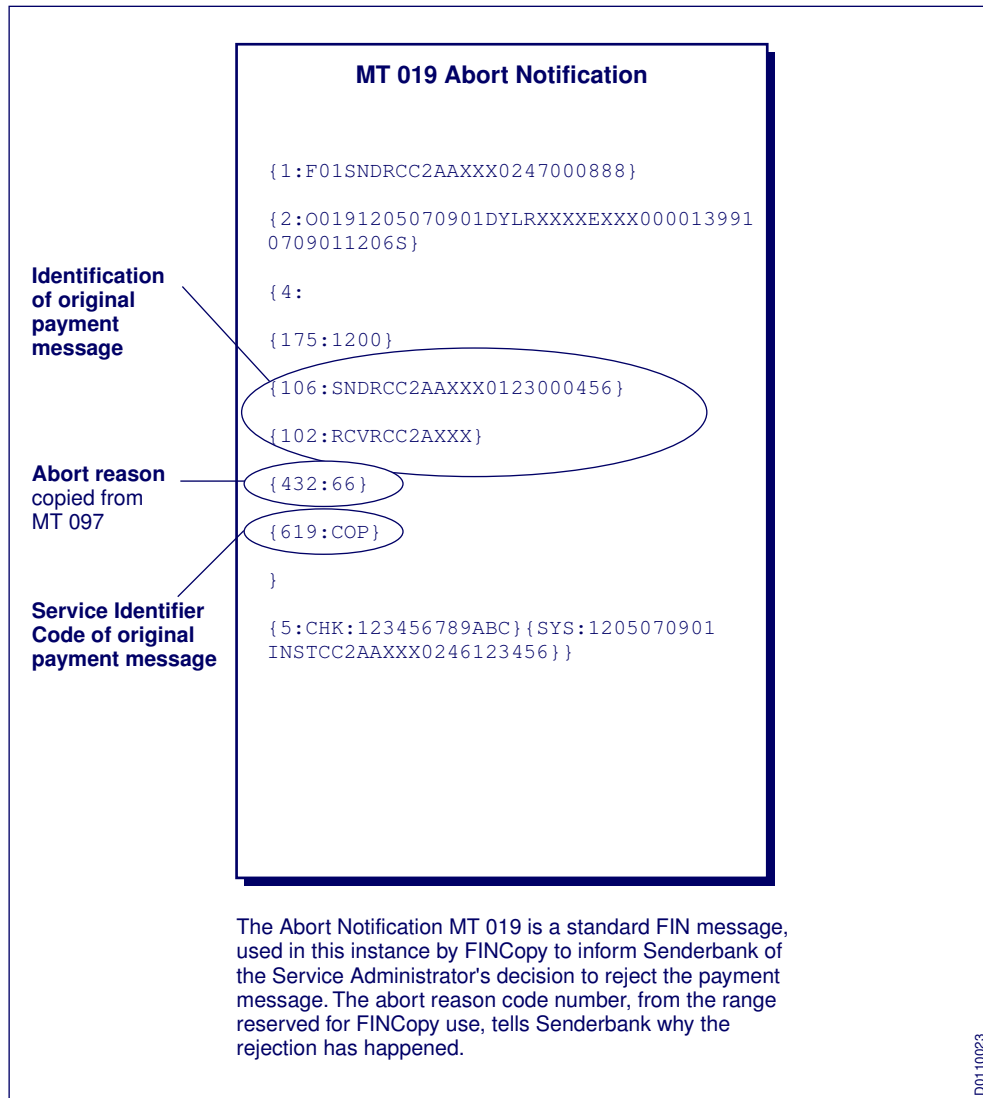


Figure 39: MT 019 abort notification - to Senderbank



## B.5 Messages, Fallback to Bypass Mode

### Fallback service mode

This case study shows the operation of the FINCopy service in one of the fallback service modes. The service administrator has already, as an emergency procedure, requested SWIFT to switch to the declared fallback mode. SWIFT has closed the service state, changed the mode from Y-Copy mode to Bypass mode, and reopened the service state.

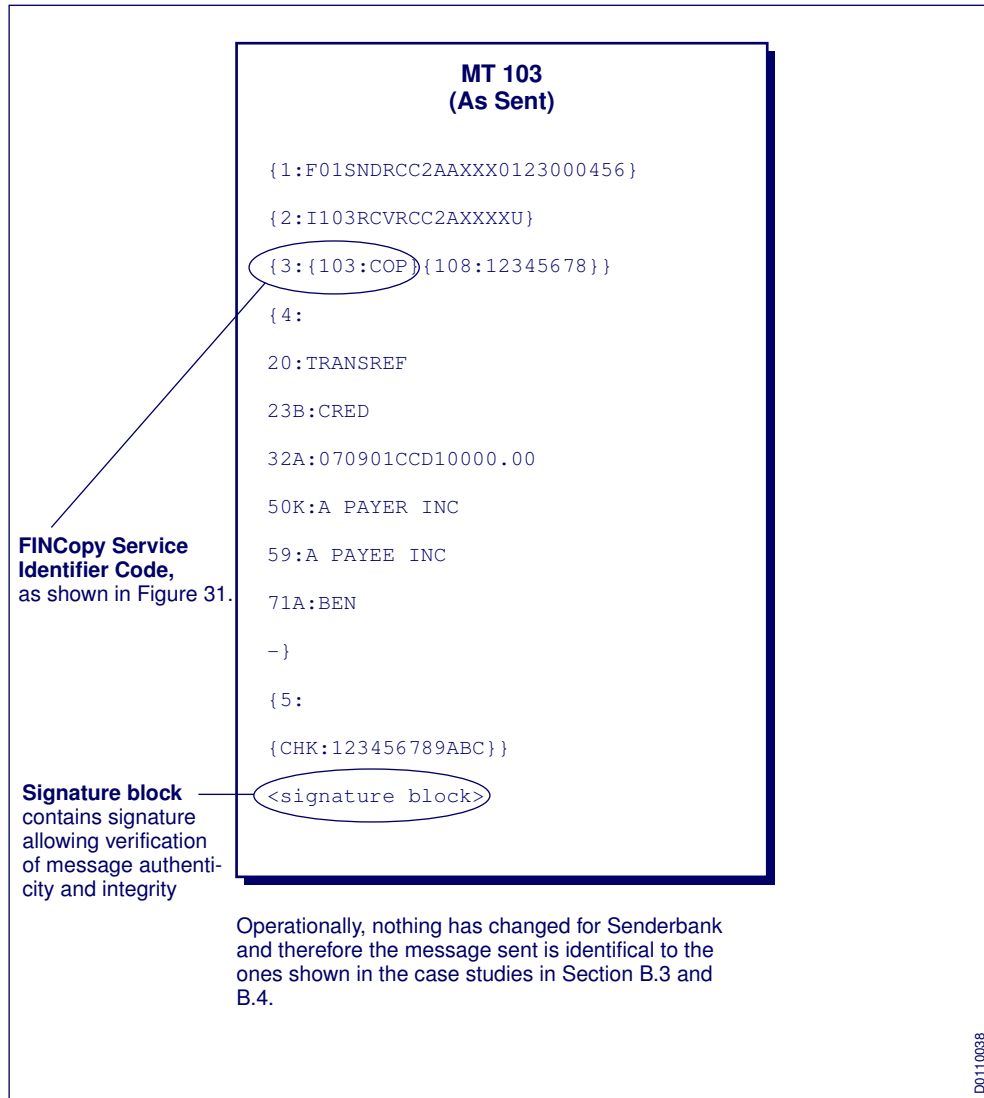
The message sequence is as follows:

- "Figure 40: MT 103 single customer credit transfer message - from Senderbank". This MT 103 is identical to those in sections "Messages, Y-Copy Mode: Authorised Payment" on page 54 and "Messages, Y-Copy Mode: Rejected Payment" on page 59, because a FINCopy mode change has no impact on the sender. Indeed, the sender does not need to know that SWIFT has changed the mode.

However, if Senderbank had sent the MT 103 when the service state was closed for the mode change, Senderbank would have received a negative acknowledgement (NAK) for the message.

**Note** The change to a fallback mode may, however, have significant impact on the real-time gross settlement or netting service for which the customer uses the FINCopy service. The service administrator must ensure that all users that participate in the FINCopy closed user group receive appropriate notification.

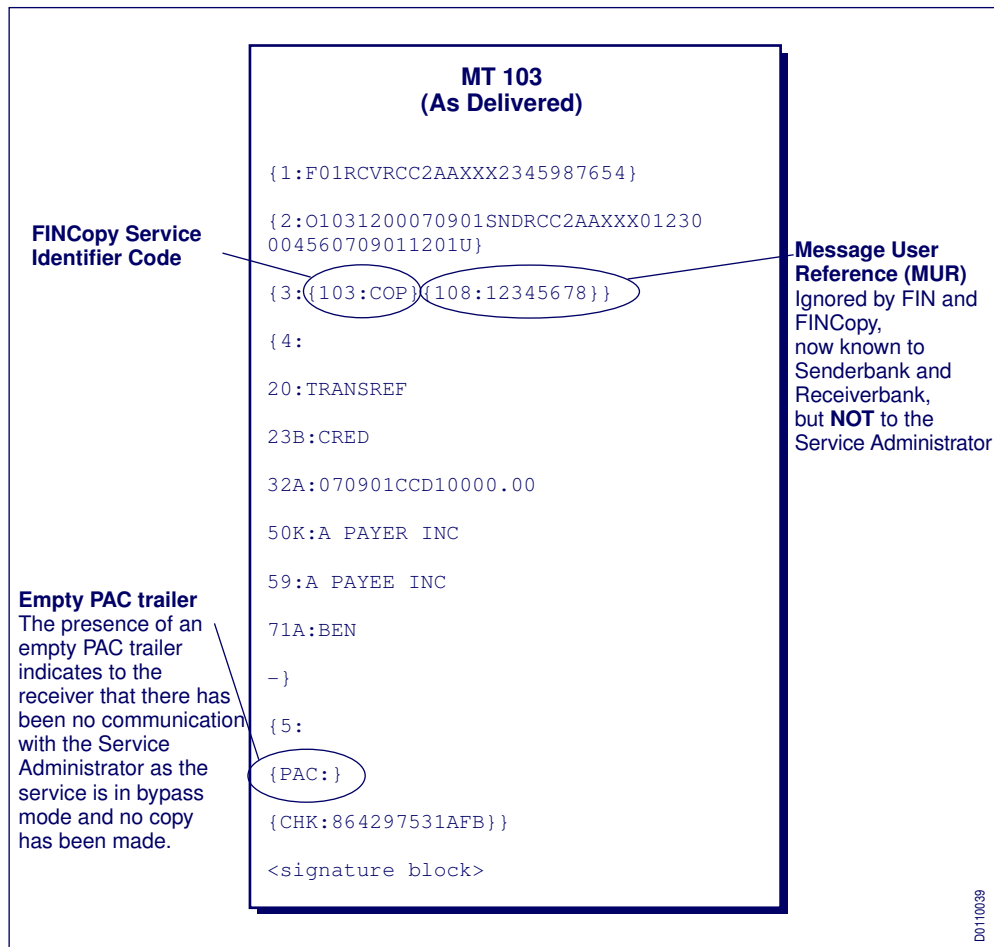
**Figure 40: MT 103 single customer credit transfer message - from Senderbank**



- "Figure 41: MT 103 as delivered - to Receiverbank" shows the MT 103 that FINCopy has forwarded and FIN has delivered directly to Receiverbank. The message has not been held in a temporary queue. The presence of an empty PAC trailer indicates to the receiver that there has been no communication with the service administrator as the service is in bypass mode

and no copy has been made. For the same reason, field 115 is not added to the header block of the MT 103.

**Figure 41: MT 103 as delivered - to Receiverbank**



## B.6 Messages, T-Copy Mode

### T-Copy mode

This case study shows the operation of the FINCopy service in T-Copy mode. This can be either the normal mode, as specified in the FINCopy service profile, or the fallback mode for a service that normally operates in Y-Copy mode.

The message sequence is as follows:

- "Figure 42: MT 103 single customer credit transfer message - from Senderbank" (identical to those in the preceding sections).
- "Figure 43: MT 096 FIN copy to Central Institution message" (also identical to those in preceding sections).
- "Figure 44: MT 103 single customer credit transfer message - as delivered" (forwarded to Receiverbank by FINCopy). FINCopy forwards this message as soon as it has copied the information required for the MT 096.

**Figure 42: MT 103 single customer credit transfer message - from Senderbank**

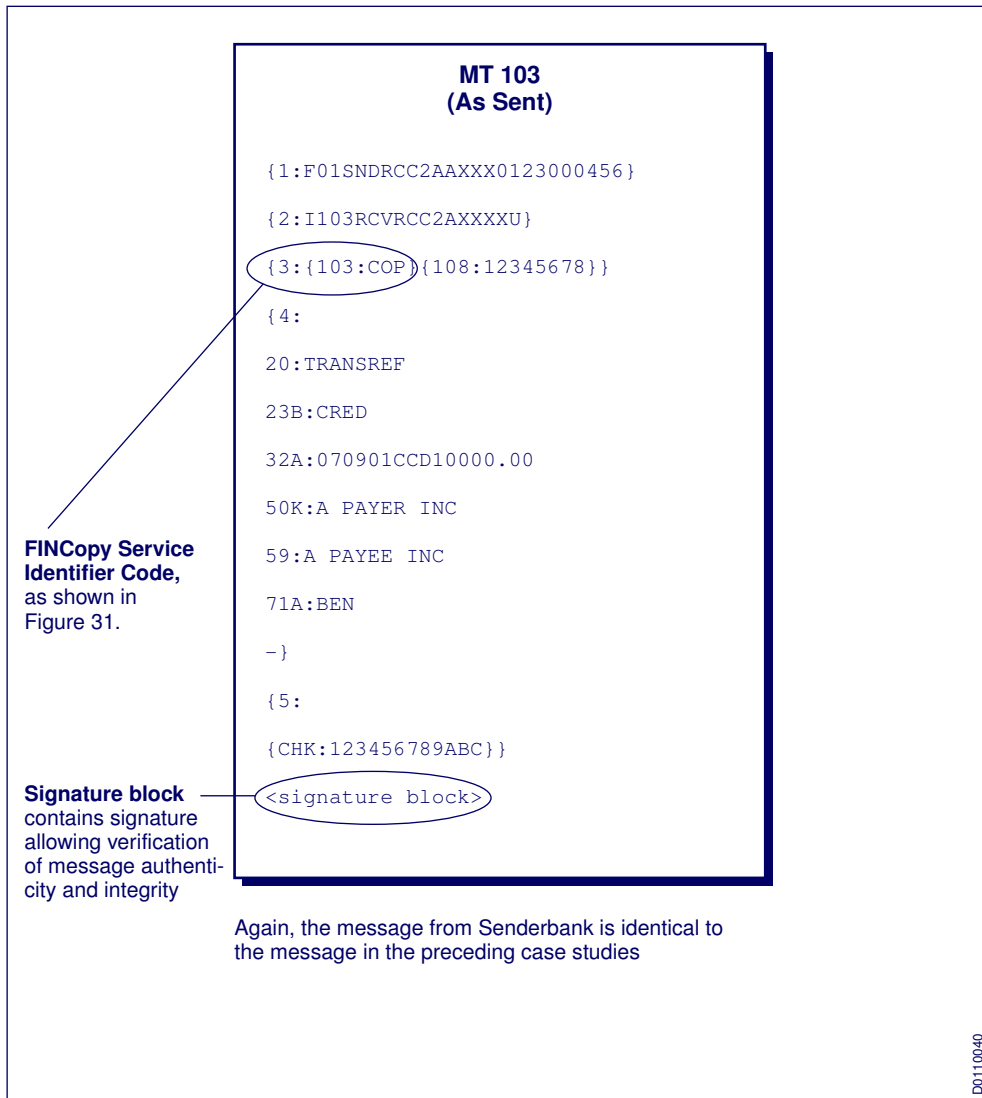
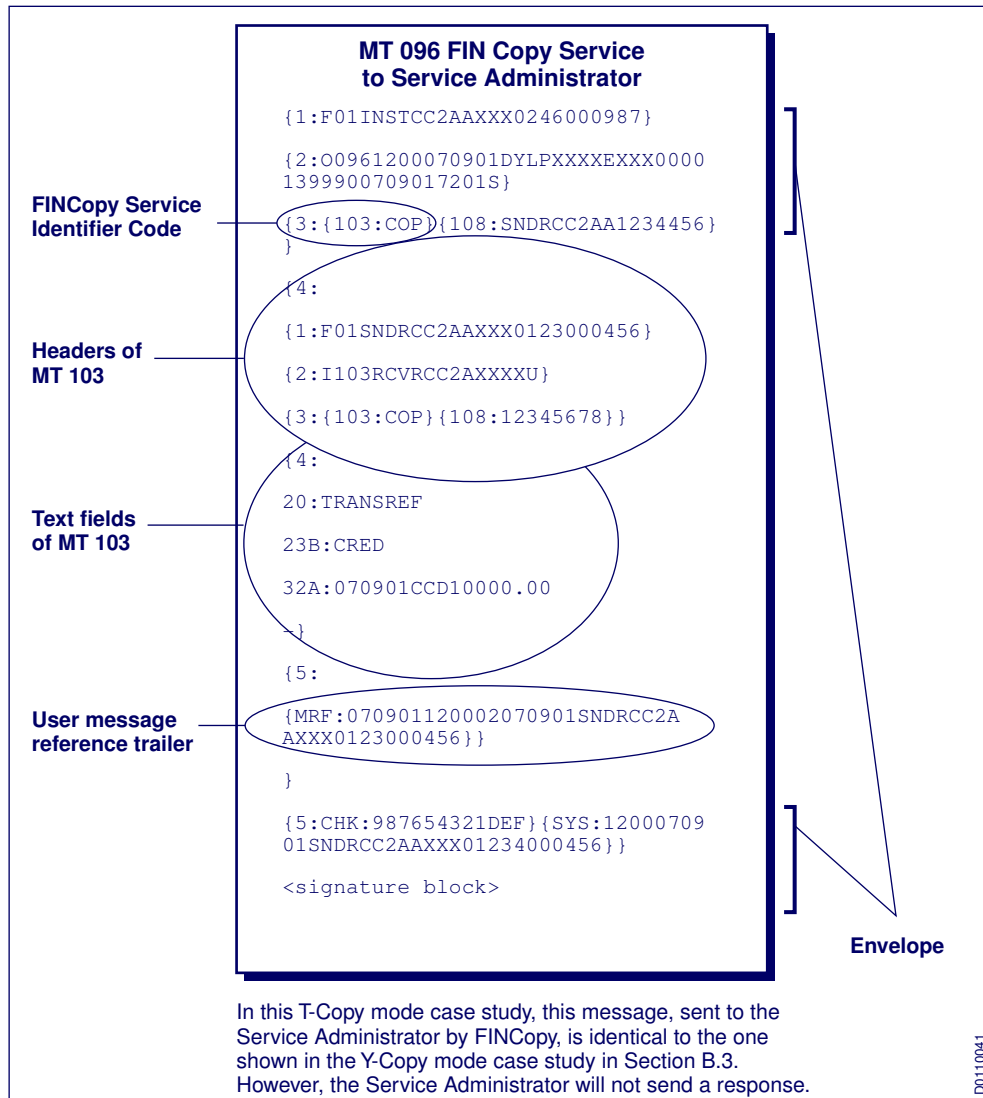


Figure 43: MT 096 FIN copy to Central Institution message



**Figure 44: MT 103 single customer credit transfer message - as delivered**

**MT 103  
(As Delivered)**

**FINCopy Service Identifier Code**

```

{1:F01RCVRCC2AAXXX2345987654}

{2:O1031200070901SNDRCC2AAXXX01230
004560709011201U}

{3:({103:COP}){108:12345678}}

{4:

20:TRANSREF

23B:CRED

32A:070901CCD10000.00

50K:A PAYER INC

59:A PAYEE INC

71A:BEN

-}

{5:

{CHK:249765318DAB}}

<signature block>
                
```

Since there is no communication between the Service Administrator and Receiverbank in T-Copy mode, there is no sign from the Service Administrator for Receiverbank.

**This message has not been held in a temporary queue but forwarded by FINCopy for delivery to Receiverbank once the information needed for the MT 096 to the Service Administrator has been copied.**

D0110042

## Appendix C

# Service Administrators Operations Guide

## C.1 General

### C.1.1 Scope of this Appendix

#### FINCopy procedures

This appendix describes the procedures that are relevant to FINCopy. For more information about SWIFT Support, see [www.swift.com](http://www.swift.com) > Support. For more information about the ordering process, see [www.swift.com](http://www.swift.com) > Ordering.

## C.2 Definition of Procedures

#### Procedures

This section lists the following types of procedures in alphabetical order:

- FINCopy service: normal procedures
- FINCopy service: emergency procedures

### C.2.1 FINCopy Service: Normal Procedures

#### Normal procedures

#### Procedures

Procedure	Explanation
Add FINCopy user	To add a SWIFT user to a new or existing FINCopy closed user group.
Define FINCopy Service Parameters	To set up a FINCopy service profile.
Modify FINCopy Service Parameters	To modify an existing FINCopy service profile.
Open FINCopy Service	The request from a service administrator for SWIFT to activate a FINCopy service, for either live or Test and Training operation, in the agreed mode (Y-Copy, T-Copy, or Bypass).
Order FIN Interface Software	To order FIN interface software.
Order Documentation	To order the documentation that users require to operate a FINCopy service.
Report Ordering Problem	To report delays or misunderstandings about a purchase order that needs a follow-up or a solution (or both).
Report Technical Problem	To report difficulty or inability to connect to the SWIFT network, or any other technical or operational problem.

Procedure	Explanation
Withdraw FINCopy user	To remove a FINCopy user from the closed user group at a specific date, at the request of the service administrator.

## C.2.2 FINCopy Service: Emergency Procedures

### Restrictions

The use of emergency procedures is restricted to either of the following:

- unforeseen critical events with severe time constraints
- planned contingency testing

Emergency procedures apply to exceptional circumstances. At all other times, users that participate in a FINCopy closed user group must follow normal procedures.

### Allowable downtime window

Emergency modifications to the FINCopy service cannot take place during an allowable downtime window. An allowable downtime window is a scheduled period during which SWIFT does not guarantee service availability. SWIFT normally uses allowable downtime windows for planned changes, with the consequent interruption of services. SWIFT usually schedules allowable downtime windows outside business hours, at weekends.

### C.2.2.1 FINCopy Service: Unforeseen Critical Emergency Events

#### Exceptional procedures

##### Procedures

Procedure	Explanation
Emergency Modify FINCopy Mode or State	An emergency request by a service administrator for a change of FINCopy mode for the live or Test and Training FINCopy service. This means a change from the mode in which the FINCopy service is working (for example, from Y-copy mode to Bypass mode).
Emergency Withdraw FINCopy user	An emergency request by a service administrator to remove a FINCopy user from the closed user group, with immediate effect.

### C.2.2.2 FINCopy Service: Planned Contingency Testing

#### Exceptional procedures

There are two types of planned contingency testing, as follows:

- mode change to perform system trial tests
- mode change to perform emergency tests

The service administrator must notify SWIFT of these tests beforehand as indicated in the following table.

**Procedures**

<b>Procedures</b>	<b>Explanation</b>
Mode Change for System Trialing	<p>A service administrator wants to test the ability of itself and the users that participate in its FINCopy closed user group to operate in fallback mode.</p> <p>The service administrator must send a fax to its owning Customer Support Centre, at least four business days before the test, and must indicate the local date and time of the requested mode change.</p> <p>On the day of the mode change, the service administrator must telephone its owning Customer Support Centre and follow the emergency procedures described in procedure P5. (See C.4, "Processes and Procedures".)</p>
Mode Change to Perform Emergency Tests	<p>A service administrator wants to simulate an emergency situation and test the emergency procedures.</p> <p>On the day of the mode change, the service administrator must telephone its owning Customer Support Centre and follow the standard emergency procedures. In this case, no prior warning is required.</p> <p>SWIFT recommends regular testing, as follows:</p> <ul style="list-style-type: none"> <li>• 3 tests during service deployment per Customer Support Centre</li> <li>• 2 tests per year, after the service has gone live</li> </ul>

For more information about this procedure, see "Telephone Authentication Procedure" on page 77.

## C.3 Data Maintenance

### Table contents

"Table 12: FINCopy service data maintenance" and "Table 13: FINCopy user administration data maintenance" provide information about the different types of requests which users that participate in a FINCopy closed user group and service administrators make to SWIFT. These requests fall into the following categories:

- ordering and data maintenance
- technical problems

For each request type, the table shows the procedure number in the second column. See section "Processes and Procedures" on page 72 for details of these procedures.

If applicable, the table also shows the form which the user that participates in a FINCopy closed user group, or the service administrator must use, and the time that SWIFT requires to implement the request.

---

**Note** This section does not cover connectivity equipment. However, for planning purposes, customers must consider the time to install and commission such equipment, together with the timing of any configuration changes to interface software.

---

## C.3.1 Ordering and Data Maintenance

### FIN

For information about the FIN messaging service, see the FIN documentation, and [www.swift.com](http://www.swift.com).

Customers can order documentation and interface software on [www.swift.com](http://www.swift.com).

### FINCopy service

**Table 12: FINCopy service data maintenance**

Request	Procedure to follow	Request form to use	Estimated time to implement
define FINCopy service parameters	P3	Service Profile Form (Service Administrator)	84 days
modify FINCopy service parameters	P3	SWIFTNet Service Profile Form (Service Administrator)	2 to 8 weeks (depending on the type of change required)
open FINCopy service	P3	by e-mail from one of the authorised approvers	14 days
emergency modify FINCopy mode	P5	Telephone Authorisation Procedure plus Emergency Request Confirmation	45 minutes

### FINCopy user administration

**Table 13: FINCopy user administration data maintenance**

Request	Procedure to follow	Request form	Estimated Time to implement
add FINCopy user	P1	SWIFTNet Service Subscription Form (e-MSSF)	14 days changes are effected at weekends
withdraw FINCopy user	P2	SWIFTNet Terminate Market Infrastructure Subscription Form	14 days changes are effected at weekends
emergency withdraw FINCopy user	P5	Telephone Authorisation Procedure plus Terminate Market Infrastructure Subscription Form	45 minutes

## C.4 Processes and Procedures

### Introduction

This section explains the generic processes and procedures identified in the preceding section. For each generic process and procedure, this section lists and explains the specific steps involved.

## C.4.1 P1: Order from a FINCopy User approved by the Service Administrator, to End-to-End Ordering by Form

### Process

The process for adding a user to a FINCopy closed user group is as follows:

1. The SWIFT user completes the SWIFTNet Service Subscription Form (e-MSSF).
2. SWIFT sends an approval request to the service administrator.
3. One of the service administrator authorised approvers must approve the e-MSSF and send it back to End-to-End Ordering.
4. End-to-End Ordering implements the service subscription and confirms implementation to the service administrator and to the SWIFT user, by e-mail.

---

**Note** End-to-End Ordering cannot process a request for activation unless it meets the following criteria:

- End-to-End Ordering has received the required e-MSSF duly approved by the service administrator
  - the SWIFT user is allowed to send and receive the messages exchanged within the FINCopy closed user group
- 

### Implementation timetable

Implementations always occur during the weekend. The earliest possible implementation of an order is the second weekend following the date of submission. SWIFT must validate orders as being correct and approved by the service administrator. SWIFT must receive duly approved e-MSSF forms at the latest by 10:00 GMT on the Tuesday preceding the requested implementation date.

### Example

If SWIFT receives the approved e-MSSF on Tuesday 6 November 2007, before 10:00 GMT, then SWIFT will activate the user in the FINCopy closed user group during the allowable downtime window on 10 November 2007. If SWIFT receives the approved e-MSSF on Tuesday 6 November 2007, after 10:00 GMT, then SWIFT will activate the user in the FINCopy closed user group during the allowable downtime window on 17 November 2007.

## C.4.2 P2: Order from a Service Administrator to End-to-End Ordering by Form

### Process

The process for withdrawing a user from a FINCopy closed user group is as follows:

1. The service administrator or the user completes the SWIFTNet Terminate Subscription Form.
2. If a user has completed the SWIFTNet Terminate Subscription Form, then one of the service administrator's authorised approvers must approve this form.
3. End-to-End Ordering implements the procedure and confirms implementation to the service administrator and to the customer by e-mail.

---

**Note** Service administrators must use process P1 to arrange for SWIFT to readmit a previously withdrawn user to the FINCopy closed user group.

---

### Implementation timetable

Implementations always occur during the weekend. The earliest possible implementation of an order is the second weekend following the date of submission. SWIFT must validate orders as being correct and approved by the service administrator. Duly approved SWIFTNet Terminate Subscription Forms must be received at the latest by 10:00 GMT on the Tuesday preceding the requested implementation date.

### Example

If SWIFT receives the approved SWIFTNet Terminate Subscription Form on Tuesday 6 November 2007, before 10:00 GMT, then SWIFT will activate the user in the FINCopy closed user group during the allowable downtime window on 10 November 2007. If SWIFT receives the approved SWIFTNet Terminate Subscription Form on Tuesday 6 November 2007, after 10:00 GMT, then SWIFT will activate the user in the FINCopy closed user group during the allowable downtime window on 17 November 2007.

## C.4.3 P3: Order from a Service Administrator to Market Infrastructures Service Management by Form

### Introduction

Customers use the P3 order form to do the following:

- define and modify SWIFT FINCopy service parameters
- order telephone authentication cards
- notify the start-up date of a new FINCopy service

### C.4.3.1 P3: To Define or Modify FINCopy Service Parameters

#### Process

The following process defines or modifies FINCopy service parameters:

1. The service administrator and SWIFT Payments Clearing Business Management agree the definition or change.
2. The service administrator completes the Service Profile Form and sends or faxes it to Global Sales Services. The order must arrive in good time.
3. Global Sales Services, together with Payments Clearing Business Management, reviews the content of the order.
4. Global Sales Services confirms receipt of the form to the service administrator by MT 999, fax, or mail, and, in the case of a modification, confirms the time needed for implementation.
5. Ordinarily, SWIFT implements modifications to FINCopy parameters within two to eight weeks (depending on the type of change required), during an allowable downtime window.

---

**Note** Customers cannot modify the following FINCopy service parameters:

- the server destinations
  - the service administrator destination (central institution destination)
  - the FINCopy service identifier code
- 

6. If changes affect the users in a FINCopy closed user group, then the service administrator must allow the users sufficient time to change the appropriate parameters in their own systems.

### C.4.3.2 P3 - To order telephone authentication cards

#### Process

The process for ordering a telephone authentication card is as follows:

1. The service administrator completes the FIN Security Equipment Order Form.
2. SWIFT confirms receipt of the form to the service administrator by MT 999, fax, or mail.

---

**Note** For more information about this process, see "Telephone Authentication Cards" on page 78 for further details.

---

### C.4.3.3 P3: To Open the FINCopy Service

#### Process

The process for opening the FINCopy service is as follows:

1. The service administrator and SWIFT Payments Clearing Business Management agree a date to open the live, or Test and Training FINCopy service.
2. The service administrator completes a written request, and sends or faxes the request to Payments Clearing Business Management and Customer Projects.
3. SWIFT confirms receipt of the request to the service administrator by MT 999, fax, or mail.
4. SWIFT activates the FINCopy service, and confirms activation to the service administrator by MT 999, fax, or mail.

---

**Note** SWIFT activates FINCopy services only during allowable downtime windows.

---

## C.4.4 P4: Problem Report to Customer Support Centre

#### Process

Standard Support processes should be used for FINCopy service-related issues:

- For more information, see the *Support Service Description*.

## C.4.5 P5: Emergency Request from the Service Administrator to Customer Support Centre by Authenticated Telephone Call

### Introduction

This procedure enables the following:

- emergency modification of FINCopy mode
- emergency modification of multiple server mapping
- emergency withdrawal of a user from a FINCopy closed user group

---

**Note** The service administrator uses this procedure for emergency changes only (that is, critical events or time constraints).

---

To ensure that only the service administrator can request emergency updates, SWIFT uses exchanged passwords to authenticate the service administrator calling the SWIFT Customer Support Centre.

For more information about this procedure, see "Telephone Authentication Procedure" on page 77, for more details.

### Emergency request from the service administrator to the Customer Support Centre

The process for processing an emergency request from the service administrator to Customer Support Centre is as follows:

1. The service administrator calls the Customer Support Centre with the emergency request.
2. The parties identify each other by means of a password exchange.
3. The Customer Support Centre gives the service administrator a case reference number.
4. The service administrator also confirms the request by fax to Customer Support Centre stating in capital letters at the start of the fax: **EMERGENCY REQUEST CONFIRMATION**.

---

**Note** SWIFT provides a template for emergency request confirmations.

---

5. The Customer Support Centre confirms the change to the service administrator by fax.

## C.4.6 P6: Problem Report from a FINCopy User to the Local Settlement Help Desk by Telephone

### Procedure

This procedure is specific to particular FINCopy services:

- For more information, contact the relevant service administrator.

## C.5 Stress Testing FINCopy

### Individual and global stress testing

There are two types of FINCopy stress tests, as follows:

- Stress tests for individual users that participate in a FINCopy closed user group. As part of its Test and Training qualification, a service administrator may request users that participate in a FINCopy closed user group to prove that they can achieve their respective peak hour throughput. The service administrator plans and runs these tests at its best convenience. Individual user stress tests must also respect the rules about peak message volumes at the service administrator level that are defined in the remainder of this section.
- Global system stress testing. This means that all users that participate in a FINCopy closed user group are testing the closed user group's peak hour throughput, which can have a significant impact on the SWIFT network (especially at the service administrator level), depending on the volumes.

For all types of stress testing, the following rules apply:

- Peak hour under 5,000 messages (at the service administrator level)

The service administrator is free to organise these tests on its own (no need to co-ordinate with SWIFT).

- Peak hour between 5,000 and 10,000 messages (at the service administrator level)

The service administrator must request a testing date and time from SWIFT Capacity Planning. The service administrator must make this request at least eight weeks before the desired period, and must send the request by fax or MT 999. Capacity Planning issues, by fax or MT 999, a time to perform the tests. (Depending on network load, it may be necessary for tests to take place during weekends). Exceptionally, the service administrator can arrange a notification period of less than eight weeks on a best-effort basis.

- Peak hour over 10,000 messages (at the service administrator level)

The service administrator must request a testing date and time from SWIFT Capacity Planning. The service administrator must send the request, by fax or MT 999, to SWIFT Capacity Planning, with at least 8-weeks notice. Capacity Planning notifies the service administrator, by fax or MT 999, of the date on which the tests can take place. Exceptionally, the service administrator can arrange a notification period of less than eight weeks on a best-effort basis.

---

**Note** Capacity Planning reserves the right to cancel tests (for example, if a major, unexpected problem arises).

---

## C.6 Telephone Authentication Procedure

### Introduction

This section explains the authentication part of procedure P5. Service administrators use this procedure for emergency telephone requests to the SWIFT Customer Support Centre.

### Recommendation

As with all emergency procedures, SWIFT recommends regular testing of this authentication procedure.

## C.6.1 Telephone Authentication Cards

### C.6.1.1 Introduction

#### Password cards

SWIFT authenticates the telephone call by means of a hexadecimal password that is used only once. This password, called Phone Key (PK), is the result of a calculation based on several parameters, entered by the user, and stored inside the telephone authentication card.

To authenticate telephone calls, the service administrator must have a Basic Card Reader (BCR) and USER integrated circuit cards. These enable the service administrator to do the following:

- to prove to its counterpart, the Customer Support Centre, that the requester of the change is an authorised person at the service administrator's location (that is, that the request is genuine)
- to check that the other party is the Customer Support Centre

### C.6.1.2 Definitions

#### Terms

##### List of terms

Authentication Security Officer	One or more security officers at the service administrator's location, that are responsible for the control and the management of telephone authentication cards and BCRs, and for liaison with the owning Customer Support Centre.
Owning Customer Support Centre	The Customer Support Centre that is responsible for the customisation of all sets of telephone authentication cards for the service administrator and other Customer Support Centres.

For further explanations about authentication security officers and owning Customer Support Centres, see the *FIN Security Guide*.

### C.6.1.3 Administration

#### Terms

For a service administrator, administration of telephone authentication cards is straightforward.

SWIFT gives ownership of a set of telephone authentication cards to the owning Customer Support Centre, which administer and maintain the cards according to the service administrator's requirements.

---

**Note** In these circumstances, a set of telephone authentication cards contains at least one user security officer card) and one User card.

---

#### Further Details

The owning Customer Support Centre and the service administrator agree dates for testing the authentication procedure, for Test and Training and, subsequently, for live operation.

## C.6.1.4 Ordering Procedures

### Security officer and user cards

The service administrator determines, with the assistance of Global Sales Services, the number of user security officer and user cards to order.

---

**Note** For security and operational reasons, SWIFT advises the service administrator to order a backup card for each card that it requests.

---

### Order quantity

SWIFT recommends that the service administrator orders at least the following cards:

- six user security officer cards (2 for each Customer Support Centre)
- eight or 12 user integrated circuit cards, according to the following options:
  - 2 for each Customer Support Centre (2 x 3 = 6), plus 2 for the service administrator
  - 3 for each Customer Support Centre (3 x 3 = 9), plus 3 for the service administrator

The owning Customer Support Centre ships USER cards to the Authentication Security Officers at the service administrator's location, and user security officer and USER cards to the other Customer Support Centres.

The Authentication Security Officers, and the other Customer Support Centres, must acknowledge receipt of the cards to the owning Customer Support Centre by MT 999, fax, mail, or internal electronic mail (between the Customer Support Centres).

On receipt of the acknowledgements, the owning Customer Support Centre ships the two PIN mailers for the USER cards to the authentication security officers. The owning Customer Support Centre also ships the PIN mailers for the user security officer cards to the other Customer Support Centres.

Each Customer Support Centre starts a service administrator file for the cards, and keeps the PINs in a secure place.

## C.6.1.5 Operational Procedures

### Phone-key generation

The following step-by-step procedure for Phone Key generation must be conducted simultaneously at the calling service administrator's location **and** at the called Customer Support Centre.

If a sensitive update is necessary, then the service administrator must call the owning Customer Support Centre and give customer identification.

---

**Note** If the service administrator calls outside the owning Customer Support Centre's normal working hours, then SWIFT automatically routes the telephone call to another Customer Support Centre.

---

### Activation sequence

The service administrator activates the BCR by inserting the USER card and the correct PIN code. See "Table 14: phone key generation, steps 1 to 7" in the Phone Key (PK) generation procedure.

The owning Customer Support Centre asks the service administrator to provide the next PK challenge (that is, a random 4-digit number). "Table 15: Phone key generation, step 8" shows step 8 of this process.

Customer Support Centre staff ask the service administrator to read out the characters displayed on the first line of the Basic Card Reader (BCR) display. If the characters match the display on the Customer Support Centre reader, then the service administrator has successfully authenticated itself.

**Table 14: phone key generation, steps 1 to 7**

Step	Action	Display
1	Insert the user integrated circuit card into the BCR The BCR displays ->	<b>CONNECTED MODE?</b>
2	Press the following keys in sequence The BCR displays ->	<b>D A E A #</b> <b>ENTER PIN 1</b> <b>1st TRY:.....</b>
3	Type the PIN 1 associated with the user integrated circuit card inserted in the BCR, followed by -> The BCR displays -> Type the PIN 2 associated with the user integrated circuit card inserted in the BCR, followed by -> Once you have typed the PIN 2 and #, the BCR displays ->	<b>#</b> <b>ENTER PIN 2</b> <b>1st TRY:.....</b> <b>#</b> <b>SWIFT SLS MANAGEMENT</b>
4	Press -> and the BCR displays ->	<b>#</b> <b>SLS MANAGEMENT</b> <b>SK GENERATION</b>
5	Press -> and the BCR displays ->	<b>#</b> <b>LOGICAL TERMINAL</b> <b>BANKCCLLZ (example)</b>
6	Press -> and the BCR displays ->	<b>#</b> <b>APPLICATION</b> <b>LOGIN</b>
7	Press -> and the BCR displays ->	<b>#</b> <b>LSN:</b>

The owning Customer Support Centre then reads out next eight characters, characters, from the second line of the BCR display, to authenticate itself to the service administrator.

After successful authentication of both parties, the service administrator makes its request.

**Note** The owning Customer Support Centre informs the other Customer Support Centres of the next PK sequence number they must use.

### Authentication process failure

If the characters do **not** match the Customer Support Centre display, then the authentication process has failed. The two parties can restart the procedure at their discretion.

**Table 15: Phone key generation, step 8**

Step	Action	Display
8	Type the 4-digit challenge as given by the Customer Support Centre staff -> followed by -> The BCR then displays the phone key as follows: ->	<b>NNNN</b> <b># SK: 5977 B45C</b> <b>1/2 741E A8E0</b> (example)

**Note** To avoid misinterpretation of alphabetic characters, SWIFT recommends the use of international spelling (for example, A Alpha, B Bravo, C Charlie, as listed in Table 16).

### Recommended code words

**Table 16: International spelling code words**

Letter	Code word
A	ALPHA
B	BRAVO
C	CHARLIE
D	DELTA
E	ECHO
F	FOXTROT

**Note** Each telephone call relating to an emergency request should be authenticated.

## C.6.1.6 Troubleshooting

### Introduction

The purpose of this section is to provide the *service administrator* with some guidance if the BCR fails to operate correctly. The following examples describe some problems that may occur when the BCR is used to authenticate the telephone call.

**Note** The Basic Card Reader (BCR) and integrated circuit cards are robust and reliable devices, and, whatever operational difficulties the *service administrator* may incur, the owning Customer Support Centre staff are always available to assist customers to find the correct solution.

For more detailed information, see the SWIFT Manual *Card Readers User Guide* .

### Examples

The following are sample authentication problems:

#### 1. Unsuccessful authentication

The Phone Key (PK) that the BCR generates may not be the same as the one that the owning Customer Support Centre expects. This results in an authentication failure, which occurs because the card reader has stored the incorrect integrated circuit card kernel version.

The service administrator must immediately update this parameter to its correct value. If the service administrator does not know this value, then it must contact the owning Customer Support Centre.

## 2. **BCR refuses to generate a PK**

Either of the following reasons can explain this:

- No PIN code was entered.
- The PIN code is not correct.
- The integrated circuit card is blocked (following more than three unsuccessful attempts to enter the PIN code). In this case the service administrator must use the backup card and send the blocked integrated circuit card to the owning Customer Support Centre.
- The BCR battery must be replaced.

## 3. **Lost or stolen BCR**

The BCR contains no secret information. Therefore, following the loss of a BCR, the service administrator simply replaces it with the backup card and orders a new one from SWIFT.

The act of moving to a new BCR implies the need to update, and possibly modify for security reasons, the kernel version on the replacement card reader.

## 4. **Lost or stolen cards**

Should any USER card be lost or stolen, the service administrator, or Customer Support Centre, must immediately take protective action to prevent that integrated circuit card from use by unauthorised persons.

For user integrated circuit cards, access codes are calculated from secret information stored in the integrated circuit cards, and known as integrated circuit card Kernels. Eight integrated circuit card Kernels are defined for each user integrated circuit card.

The owning Customer Support Centre manages the integrated circuit card kernel version in current use, and must make the kernel version information known to every other involved party (that is, the service administrator and the other Customer Support Centres). To notify the service administrator, the owning Customer Support Centre sends an MT 999, fax, or mail, to the two nominated security officers.

If cards are lost, then one of the parties (either the service administrator or the owning Customer Support Centre) calls the other and states that the kernel version must be changed to the next version number.

One of the parties (either the service administrator or the owning Customer Support Centre) asks the other to provide confirmation of the necessary change of kernel version from a second person (for example, the second authentication security officer at the service administrator's location).

The owning Customer Support Centre updates the kernel version and notifies all other involved parties of the new kernel version for the service administrator's USER cards.

---

**Note** To avoid a situation in which there is no backup USER card, the service administrator must order new cards before only one USER card remains.

---

## C.7 Forms

### Introduction

All necessary forms, including the SWIFTNet Service Subscription Form (e-MSSF), are available from SWIFT's Regional Commercial Administrators or [www.swift.com](http://www.swift.com).

### C.7.1 SWIFTNet Service Profile

#### FINCopy operational parameters

The service administrator uses the Service Profile Form to communicate to SWIFT general information about itself, and some FINCopy operational parameters, including the following:

- definition of the message types and fields to be copied, routing restrictions, and other service profile parameters
- message billing
- details of the service administrator and two or three authorised approvers at the service administrator's location (the approvers are responsible for the service's implementation and operation)
- addition of dedicated server destinations

---

**Note** Although this form is intended for the service administrator to confirm the FINCopy service profile that it has agreed with SWIFT, the service administrator **must** also arrange for all users that participate in the FINCopy closed user group to receive this information. All users that participate in a FINCopy closed user group must configure the service profile parameters correctly in the FIN interfaces.

---

### C.7.2 Emergency Request Confirmation

#### Confirmation of verbal request

The service administrator uses the Emergency Request Confirmation Form only to confirm to SWIFT the emergency withdrawal of a user from a FINCopy closed user group, or the modification of the FINCopy service mode. The service administrator must fax the form to the appropriate Customer Support Centre after it has made a verbal request by authenticated telephone call.

### C.7.3 SWIFTNet Subscription Form

#### Permission to use FINCopy

A SWIFT user uses the FINCopy Subscription Form (e-MSSF) to notify SWIFT that it wants to do the following:

- join a FINCopy closed user group
- acknowledge and agree with the terms and conditions of its use of the FINCopy service.

## C.7.4 SWIFTNet Terminate Subscription Form

### FINCopy user withdrawal

The service administrator uses the SWIFTNet Terminate Subscription Form to notify SWIFT of the withdrawal of a user from a FINCopy closed user group.

# Legal Notices

## Copyright

Copyright © S.W.I.F.T. SCRL ("SWIFT"), Avenue Adèle 1, B-1310 La Hulpe, Belgium, or its licensors, 2008. All rights reserved.

You may copy this publication within your organisation. Any such copy must include these legal notices.

## Confidentiality

This publication contains SWIFT or third-party confidential information. Do not disclose this publication outside your organisation without the prior written consent of SWIFT.

## Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

## Translations

The English version of SWIFT documentation is the only official and binding version.

## Trademarks

SWIFT, S.W.I.F.T., the SWIFT logo, Sibos, SWIFTNet, SWIFTReady, and Accord are trademarks of S.W.I.F.T. SCRL. SWIFT is the trading name of S.W.I.F.T. SCRL. Other product, service, or company names in this publication are tradenames, trademarks, or registered trademarks of their respective owners.