SWIFTNet messaging on TARGET2

Frequently asked questions

Status	Approved
Author	SWIFT
Date	June 2007
Version	13

Table of contents

1 SWIFT products and services for TARGET2

1.1 Q: What SWIFT messaging services will be used for TARGET2?

A: To access the TARGET2-SSP, the commercial banks will have to use standard SWIFT products and services; SWIFTNet FIN and MTs, FIN Copy, SWIFTNet InterAct and SWIFTStandards XML for Cash Management, SWIFTNet FileAct and SWIFTNet Browse. Depending on the SSP applications accessed, both real-time and Store & Forward modes may be needed.

> Back to questions

1.2 Q: What are FIN and FIN copy used for in TARGET2?

A: The customer transfers (MT103 and 103+), the bank transfer (MT202) and optionally the direct debit (MT204) will be used by the TARGET2 participants for payments initiation. TARGET2 participants can optionally use FIN for reporting purpose (e.g. MT 900, 910, 950). The FIN Copy mechanism will be used by the TARGET2 participants to transmit a euro payment to TARGET2 for settlement purpose.

> Back to questions

1.3 Q: What is SWIFTNet Browse used for in TARGET2?

A: SWIFTNet Browse provides TARGET2 direct participants secure browsing capabilities through the SWIFT MVIP Network. For example, by accessing the ICM via a SWIFTAlliance WebStation, the TARGET2 participant can view its current liquidity position, its payments queue or the system status.

> Back to questions

1.4 Q: What is SWIFTNet InterAct used for in TARGET2?

A: SWIFTNet InterAct provides real-time exchange of instructions between TARGET2 and its direct participants. For example, participants can instantaneously monitor their credit risk exposures or manage liquidity and collateral.

For the purpose of TARGET2, SWIFTNet InterAct will be used in real-time query/response mode. Real-time messaging for TARGET2 traffic only requires 64Kbps leased lines at a minimum (no economy line). This means that some of the future TARGET2 users might need a line upgrade. Ancillary systems using the ASI interface also may use the InterAct S&F mode, depending on the settlement option chosen.

These InterAct messages will be exchanged either automatically in Application-to-Application mode or transparently via SWIFTNet WebStation in the User-to-Application mode.

SWIFTNet InterAct is used with the SWIFTStandards XML for Cash Management. SWIFT has defined 24 Cash Management messages, out of which 16 will be used by TARGET2. Those standards are published in the TARGET2 specifications (book 4 of UDFS) and the schema files are available on the ECB website. TARGET2 is also using proprietary XML messages.

> Back to questions

1.5 Q: What is SWIFTNet FileAct used for in TARGET2?

A: SWIFTNet FileAct supports the exchange of large volumes of data. For example, SWIFTNet FileAct will be used for reporting purpose and distribution of the TARGET2 directory.

SWIFTNet FileAct will be used in two different modes: the real-time file downloads where TARGET2 user will pull information (for example to download the TARGET2 directory or to get long reports) and the store-and-forward mode when TARGET2 (or an Ancillary System) is the sender of the file (for example to send the weekly updates of the TARGET2 Directory).

➢ Back to questions

1.6 Q: Where to find information on XML Cash Management messages related to TARGET2

A: The book 4 of TARGET2 UDFS, contains the SWIFTStandards XML Cash Management messages to be used for TARGET2 as well as TARGET2 XML proprietary messages. These messages are aligned with the latest version of the SWIFTStandards MX Cash Management.

> Back to questions

1.7 Q: How participants can set-up Browse sessions with TARGET2?

A: The user authentication to the SSP is done transparently by sending an InterAct message, whilst the application is browsed with the HTTPS protocol. If the user requires the exchange of sensitive data, an InterAct message is used. This mechanism is transparent for the end user. This InterAct message will contain the user credentials to identify and authenticate the operator behind the client.

➢ Back to questions

1.8 Q: Do TARGET2 participants have to define dedicated Store & Forward queues for TARGET2?

A: No, but if a participant is already subscribed to another SWIFTNet FileAct Store & Forward service, then he can either use the generic queue or define additional queues for TARGET2. This choice is based on operational considerations.

> Back to questions

1.9 Q: What are the SWIFTNet parameters used for TARGET2?

A: TARGET2 will use RBAC and will communicate the defined roles to the community. RBAC roles will be appended to the message headers. The information related to the RBAC Roles can be found in the UDFS, ICM User Handbook section 3.

Non-repudiation of emission is mandatory for some requests, for other requests it is optional. The message validation (MVAL) feature has not been chosen.

TARGET2 has not set any specific rules for the DN tree structure. TARGET2 will link, during the registration process a participant DN to a TARGET2 account reachable by the DN. However, it is strongly recommended to adapt the DN naming to the new SWIFTNet Phase2 rules; this will be emphasized in the "getting started" document.

> Back to questions

1.10 Q: Is there a TARGET2 Directory?

A: The TARGET2 Directory is based on the static data from the SSP and on the BIC/BIC+ directories produced by SWIFT. The service administrator will publish weekly updates/new versions of the TARGET2 directory.
It will be distributed via FileAct to TARGET2 direct members only, they are not allowed to send it to other parties such indirect participants.

1.11 Q: Which directories will be used during and after the migration to TARGET2 ?

BIC directory products and the current paper TARGET directory will continue to contain all the current service codes (eg RTP, BRL, and TBF) up to the end of the migration of **all** services.

The TGT/TG+ service codes will be introduced at the end of the migration and only at this stage will replace the current codes in the BIC products.
The current TARGET directory will disappear at the end of the migration.

Customers do not need to register TGT/TG+ at SWIFT for publication in the BIC products as these codes will be automatically be derived from the TARGET2 directory.
The Direct Participant must request publication in the TARGET2 Directory at his selected Central Bank, for him and all his Indirect Participants.

The TARGET2 directory is the tool for migrated users to route their payments to other migrated users and/or to non migrated users. Migrated users use exclusively the TARGET2 directory, while non migrated users use as today the TARGET directory and the BIC products.

2 Technical access to TARGET2

2.1 Q: How can a SWIFT user re-use his existing SWIFTNet connection?

A: SWIFTNet FIN users will have to upgrade their infrastructure to allow, SWIFTNet FIN Copy, SWIFTNet Browse, InterAct and FileAct.
The user already accessing non-FIN services (SWIFT solutions), might have to update the current set-up; depending on each specific solution, the set-up must be evaluated.
Participants wanting to automate their non-FIN traffic handling have to develop or purchase an appropriate application or adapt an existing application.

> Back to questions

2.2 Q: What are the technical modes for accessing TARGET2?

A: SWIFTNet FIN and SWIFTNet FIN Copy are used to access the PM module. There are two different technical modes for accessing the ICM module: the Application-to-Application mode and the User-to-Application mode. Those two modes are very often used in parallel. Third-party application vendors can offer applications that support TARGET2 requirements by integrating the necessary SWIFTNet services and XML standards. SWIFT provides vendors with SWIFTNet Developer kits and the Eurosystem provides additional specifications as well as the TARGET2 standards.

Application-to-application mode
Information and messages are transferred between the SSP and the individual participants' internal application, automatically, without human intervention. Therefore, the participant has to develop its own application, adapt an existing one or purchase an appropriate solution. SWIFTAlliance Gateway Single Window licence provides automated application-to-application communication. Should you need more information on the licensing please contact your Account Manager

User-to-application mode
This mode allows direct communication between a participant's user and ICM, using SWIFTNet Browse. The information is displayed in a browser running on the SWIFTAlliance WebStation. The SWIFTAlliance WebStation provides browser-based and interactive person-to-application communication. As the majority of the future TARGET2 users are SWIFTAlliance Access and Entry users, the SWIFTAlliance Starter Set might be more appropriate than the Standalone WebStation.

For additional info on technical access mode, please consult the "Getting Started" on www.swift.com

> Back to questions

2.3 Q: What are the alternatives besides SWIFTNet to connect to TARGET2?

A: No alternative, SWIFTNet is the unique channel of communication to access TARGET2.
To connect to TARGET2, the participants have to fulfill some technical prerequisites:
• They need a connection to SWIFT's Secure IP Network
– Directly with their own SWIFTNet infrastructure
– Via a SWIFT Service Bureau
• They need 8- or 11-digit published SWIFT BIC.
– Full SWIFT membership
– Limited SWIFT membership (this is: PSPA - Payment system participants)
• They have to successfully complete a series of tests to prove their technical and operational competence before taking part in the PM. (More details about the test are published by Eurosystem)

> Back to questions

2.4 Q: What steps must a customer take to connect to TARGET2?

A: Following issues must be taken into account:
• Set up the necessary project organization
• Decide on the type of participation in SSP (direct or indirect)
• Identification of the in-house infrastructures and applications that may need adjustment
• Carry out a matching check with other projects that are either planned or under way.
• Inclusion in the budget plan
• If not already done, acquisition of a comprehensive SWIFTNet knowledge of the SWIFTNet Services (Browse, InterAct and FileAct) as well as in SWIFTNet FIN in Y-copy mode.
In the period 2006-2007, participants will receive close support from their NCBs on the type and timing of actions to take.

➢ Back to questions

2.5 Q: How must a customer configure FTA for the TARGET2 directory updates in Store & Forward mode?

To automatically download the TARGET2 directory updates in Store & Forward mode using the SWIFTAlliance Gateway FTA, you have to define the Store & Forward queue in the FTA application (see Q.1.8).
See *SAG File Transfer Interface Guide*, Section *4.2.6 The Queue Definition Details Window*

- Queue Name:
The name of the store-and-forward queue as supplied by you on the order form when subscribing to the TARGET2 services.

- Queue Description:

A free-text field into which you can put any useful information about the queue.

- Security DN

The distinguished name that is used to authorise and sign operations on the queue. The Security DN must have an SnFRequestor RBAC role assigned, giving permission for online queue acquisition. In addition, it must have a certificate defined in relaxed mode on the SAG.

- Order of Delivery

FIFO (First In First Out): This is the default option.

2.6 Q: For Ancillary Systems only: How to receive Store&Forward InterAct and FileAct traffic in different queues ?

The data sent by the SSP to Ancillary Systems is sent via InterAct or FileAct Store&Forward. To receive the traffic in different queues (so that the InterAct messages and the FileAct files can be processed by different interfaces/applications) two MRR rules must be created.
This can be done by clicking the "Advanced" button in the Traffic Routing section of the e-order form.

SSP uses a different Requestor DN for sending InterAct and FileAct traffic.

This is an example of the two MRR rules for the pilot service.

Rule Order	Queue Name	Requestor DN	Responder DN	Request Type
10	bankccll_msg!p	cn=interact,ou=tet,o=trgtxepm,o=swift	o=bankccll,o=swift	*
20	bankccll_file!p	cn=fileact,ou=tet,o=trgtxepm,o=swift	o=bankccll,o=swift	*

For the production service the following DNs are used:

cn=interact,ou=prod,o=trgtxepm,o=swift and

cn=fileact,ou=prod,o=trgtxepm,o=swift.

Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: (Default) Times New Roman, 12 pt
Formatted: Font: 12 pt
Formatted: Font: (Default) Times New Roman
Formatted Table
Formatted: Font: (Default) Times New Roman
Formatted: Font: (Default) Times New Roman
Formatted: Font: (Default) Times New Roman, 12 pt
Deleted:
Formatted: Font: (Default) Times New Roman, 12 pt
Deleted: .

2.7 Q: On average, how many times will a SAB user have to logon to the ICM server and in how many InterAct messages will this result?

A: The ICM server triggers an automatic disconnect after several minutes (the final time has not been decided yet by 3CB). This means that all users will probably have to redo their logon several times a day. For customers connected to SWIFTNet via a dial-up line, there is also the VPN box time-out (7 minutes).

Each logon generates one InterAct 'swlogon' message and several HTTPS exchanges, but the 'swlogon' is the only message flow that is chargeable on a per-message basis. The HTTP flows are not chargeable per flow, but are included in the monthly Browse fee. Conclusion: the user will be charged one InterAct message per logon.

> Back to questions

2.8 Q: Which SWIFT form to fill in to subscribe to TARGET2?

A: A participant should fill in two (one for test and one for live) specific TARGET2 e-MSSF forms be completed with the help of its NCB. Only direct participants and multi-addressees (including ancillary systems) must do so, as far as SWIFT forms are concerned.

List of services:

TGT (FIN Copy)
TGC (FIN Cug for CBC)
TGH (FIN Cug for HAM)
trgt.papss!p and trgt.papss (InterAct and FileAct, Real-Time)
trgt.sfpapss!p and trgt.sfpapss (InterAct and FileAct, Store-and-Forward)

> Back to questions

2.9 Q: Can a SWIFT Service Bureau implement TARGET2 for its clients?

A: A Service Bureau can offer the required SWIFTNet infrastructure to its customers, both in application-to-application and in user-to-application mode.

InterAct and FileAct traffic has to be processed by the Service Bureau's SWIFTAlliance Gateway. To connect to this gateway, the customer must install the SAB software and purchase a specific SAB license behind a Gateway.
.

There are three possibilities to access the browse service using a service bureau: an existing SAG, a dedicated SAG or the Service Bureau network.

> Back to questions

2.10 Q: What if the participant has no direct connectivity to SWIFTNet?

A: This is the case in a set-up between one or more branch(es) where the back-office application (in the case of application-to application mode) or the end-users (in the case of user-to-application mode) is/are located and the Head Office or hub abroad where the SWIFT connectivity is located.

The most logical way is to have a SAG/SNL in the Head-office/hub. The back-office application and/or SABs in the branches are connected to SAG over LAN/WAN (although remote connectivity to SAG is only accepted under strong restrictions of security and is not encouraged: see NACG for details).

The case in which the Head Office would not have SAG is very unlikely and not advisable (since all remote applications would need their own SNL).

> Back to questions

2.11 Q: Do participants need to change hardware?

A: Even if you require additional SWIFTNet interface software (SAB, SAG), new hosting hardware is not always required. It is possible to install SAB, SAS and/or SAG on the same host as SAA/SAE, but customers should always be careful not to overload their system.

Depending on possible traffic increase, connectivity may need upgrading.

> Back to questions

2.12 Q: Connection to SWIFTNet via leased line or dial-up?

A: Real Time access to TARGET2 requires at a minimum 64K lines. That means that all Connectivity Packs are supported except Connectivity pack 2 with the economy line.

If switching to an application-to-application mode, at least connectivity pack 2 needs to be installed. (No Dial-up)

> Back to questions

2.13 Q: How much bandwidth must a customer foresee for his TARGET2 traffic?

A: Distinction should be made between NCBs, Ancillary systems, direct participants and occasional participants.

Most critical factor may be the download of big files (16 MB) by NCBs within agreed timeframes.
The Connectivity Pack document describes the rules to estimate the necessary bandwidth TPS for TARGET2 traffic. For the NCBs only, guidance by 3CB is needed for determining individual traffic flows, after which SWIFT can help in calculating bandwidth/TPS.
The minimum connectivity requirement is a 64K line (no economy line).

> Back to questions

2.14 Q: Does 3CB impose a fallback solution to the participants?

A: No, a fallback/contingency solution is the responsibility of each institution.

> Back to questions

3 Interfaces offering for TARGET2

3.1 Q: What is the recommended SWIFT interface for manual access to ICM (user-to-application mode)?

A: The minimum requirement for accessing TARGET2 in manual mode is the SWIFTAlliance WebStation. Vendors can provide a solution for manual access to ICM, based on the application-to-application mode. For such a configuration, please contact the Vendor.

SWIFTAlliance Access/Entry users can use the SWIFTAlliance WebStation that is part of the SWIFTAlliance Starter Set.

Optionally, TARGET2 participants can purchase the SWIFTAlliance Gateway WebStation Concentrator licence, a licence that permits more than one concurrent user.

These licences do not allow application-to-application operations.

3.2 Q: Which software installation is required?

A: The SWIFTAlliance WebStation (SAB) must be installed on your PC (See *SWIFTAlliance WebStation 6.0, Installation Guide*)

In case you use a SAB behind a SWIFTAlliance Gateway, you have to configure a Proxy server on the SAG. For details, contact your SWIFTAlliance Gateway Administrator or see the *SWIFTAlliance Gateway Operations Guide*, Chapter 12 - *Configuring SWIFTNet Browse traffic*.

Configure your firewalls for the Browse service – see details in question 3.4 below.

3.3 Q: How do I configure my SAB for accessing the ICM?

A: You have to configure the browsing mode in SAB. On the SAB itself, follow the steps as described in section 2.1 *Configuring SWIFTNet Browsing Mode* in the *SWIFTAlliance WebStation 6.0, User Guide*.

- Registering and Setting up a SWIFTNet Browse User
- Configuring Internet Explorer (configuring the HTTP Proxy, configuring the Security Settings, Obtaining the SWIFT CA Certificate, Certifying Internet Explorer)
- Setting up SWIFTNet Browse Service Links

3.4 Q: What are the necessary firewall settings for SWIFTNet Browse?

A: To avoid maintaining a list of IP addresses, SWIFT recommends to configure the firewall for SWIFTNet Browse as described in section 5.1 *Global Approach to SWIFTNet Browse Service Access* in the *SWIFTNet 6.0, Network Configuration Tables Guide* (available on the SNL and SAB CD Rom).

> Back to questions

3.5 Q: How to integrate SABs in a Terminal Server environment?

A: There is currently no workaround from SWIFT to integrate SAB in a Terminal Server environment. This solution would be useful when more than 30 to 50 SABs must be deployed (Only large customers are using Terminal Servers).

Only one SAB instance is supported to run on the same host (no multi-user functionality). The SAB installation can be facilitated considerably by the duplication tool, as announced in the SAB release letter of version 5.0.15. However, some post-installation steps remain, such as extra software installation and network configuration.

Concrete business cases can be reported via SWIFT Support to Product Management; this will allow SWIFT to have a better view on the real field requirements.

> Back to questions

3.6 Q: What is the recommended SWIFT interface for automated access?

A: TARGET2 participants that want to automate their applications to access SSP have to purchase the SWIFTAlliance Gateway Single Window - this licence fully meets the TARGET2 requirements for automation.

If the TARGET2 participant wants to develop its own application, it also needs to purchase the SWIFTAlliance Gateway Developer toolkit.

> Back to questions

3.7 Q: Can the TARGET2 participant use SWIFTAlliance Access and SWIFTAlliance Messenger to access the ICM?

A: No, TARGET2 uses SWIFTStandards XML messages and some additional proprietary ones, which SAA 5.9/6.0 do not support.

SAA 5.9/6.0 supports MX-based SWIFTSolutions: SWIFTNet Cash Reporting, SWIFTNet Funds and SWIFTNet Exceptions and Investigations, but does not support proprietary standards.

As SWIFTAlliance Messenger is an SAA option, the rationale is the same and therefore SAM 2.0/6.0 does not support TARGET2 either.

Currently there is no plan to offer a dedicated TARGET2 adapter packaged with the SWIFTAlliance product portfolio. The TARGET2 protocol is fully specified by 3CB and can be developed in house or with a help of a third party vendor (liaise with SWIFT Partner Solutions for more information).

> Back to questions

3.8 Q: Why is SWIFTAlliance Gateway Automation licence not recommended for TARGET2 – "Application-to-Application" mode?

A: The interface solution for automated access to TARGET2 is SWIFTAlliance Gateway Single Window.

The application that handles the automated access to TARGET2 must be connected to SWIFAlliance Gateway via a host adapter. Only the SWIFTAlliance Gateway Single Window licence includes a host adapter (RAHA, MQHA). The file transfer agent (FTA) included in the SWIFTAlliance Gateway Automation and Single Window licence cannot be used to automatically fetch a file in real-time mode. This must be done via a specific TARGET2 application or a separate FileAct application that supports fetching a file in real-time mode.

Some customers will go anyhow for a SAG automation just (and only) to get the weekly TARGET2 directory updates automatically. They will then have to download the full TARGET2 file directory manually. FileAct responses as reply to InterAct requests will have to be retrieved manually via the SAB.

Some background:
In response to an InterAct request from the TARGET2 participant, TARGET2 will send an InterAct response. However, in some cases (for example a too long message), TARGET2 will put the answer within a file. It is the responsibility of the user to fetch the file in real-time mode.
Fetching the file can be done in two ways: manual (with the SWIFTAlliance WebStation) or automated (by an application connected to the SWIFTAlliance Gateway Single Window).

> Back to questions

4 TARGET2 – Security

4.1 Q: What type of security is used for TARGET2 via SWIFTNet?

A: All SWIFTNet interfaces, whether provided by SWIFT or by other parties, interoperate with the SWIFTNet Link (SNL).

SWIFTNet Public Key Infrastructure (PKI) is a mandatory component of SNL that provides security and trust across all SWIFTNet Services.
SWIFTNet PKI can be used for:
• Authentication
• Non-repudiation
• Integrity.

With SWIFTNet Phase2, RMA will replace BKE. Between the participants in the TARGET2 FIN Copy Closed User Group, the RMA is not mandatory, it can be by-passed. However, for communication between the participants and SSP, RMA is necessary. MT900/910/940/950 do not require MAC authentication, so RMA is only relevant to MT103 and MT202 messages that are not part of the FIN Copy process (i.e. that do not contain a 103 field). Note that security set-up between internal applications and SNL is the responsibility of the customer.

> Back to questions

4.2 Q: How many certificates will be needed to operate TARGET2?

A: First step is to add TARGET2 certificates to the existing PKI/DN tree. Institutions with a large PKI tree probably want to group these certificates under an organizational unit and have dedicated SO. In this DN-tree, human-based and application-based certificates will appear. From the 'human' side, Security Officers will take at least two certificates. The number of other end-user certificates depends on the level of accountability the institution wants to apply. If the institution wants to have segregation of functions amongst operators (recommended),

then every operator will need a certificate. An advantage of using personal certificates rather that institutional is the granularity of Role Based Access Control. If RBAC is used, roles are granted per certified entity, i.e. per person. Since TARGET2 plans to use up to 50 different roles, institutions need to check with their NCBs which roles are relevant in their case.
Large institutions may need to have several operators with the same role profile.
SAG offers the functionality to have all these operators share the same PKI certificate (but different virtual SAG profiles); other institutions want to track users' accountability through PKI (e.g. when the application does not allow to track who sent which message) and therefore require each operator to use its own specific certificate.
From the application side, since all direct participants will need all three SWIFTNet services (InterAct/FileAct/Browse), there is a need for at least one InterAct/FileAct and one Browse certificate.
All of these certificates may be multiplied if there is a test and/or backup site. For test purposes, lite certificates are strongly recommended.

> Back to questions

4.3 Q: What are the dependencies between SWIFTNet Phase 2 and TARGET2?

A: There is no dependency between SWIFTNet Phase 2 and TARGET2. SWIFTNet Phase 2 establishes the security mechanisms and the relationship management tools of the single messaging platform of the future. It introduces a single security model to access all SWIFTNet services (including FIN) based on standard Public Key Infrastructure (PKI) and provides new and better control mechanisms against unwanted traffic.

The SWIFTNet Phase 2 will be introduced gradually starting in January 2007 and ending in December 2008.

To ensure that the users can participate in TARGET2 regardless of their migration status in SWIFTNet phase 2, and without the need to exchange bilateral keys with all of their possible counterparties, changes need to be introduced in all FIN interfaces, under the form of a pre-agreed MAC mechanism.

The Pre-Agreed MAC mechanism removes the obligation to perform BKE between all TARGET2 participants.

Each TARGET2 participant must ensure that their FIN interface has been upgraded to support the pre-agreed MAC. The SWIFT interface users on SAA/SAE release 5.5 will need to install SAA patch 5540 or cumulative patch 5560. These features are included in SAA release 5.9 and release 6.0.

> Back to questions

5 Ordering and Support

5.1 Q: What is the role of a service partner in the context of TARGET2?

A: A new partner certification cycle has been established specifically for TARGET2 implementations. Pre-requisite to this new certification will be the qualification of service partners engineers in SAA, SAS, SAG or connectivity (check swift.com); they can advise and install the SWIFT components necessary for TARGET2.

> Back to questions

5.2 Q: How to get support from SWIFT ?

A: SWIFT Customer Support have been closely involved with the SSP design and have been thoroughly trained on the features and e-ordering for TARGET2. The on-line support at www.swift.com can be reached by all registered users.

> Back to questions

5.3 Q: Do we have TARGET2 services defined on the ITB?

A: No, the TARGET2 services are defined only in production and test and training (pilot). Vendors can test on the ITB the basic functionalities of SWIFT. They can also simulate sending and receiving party as per TARGET2 requirements. If specific TARGET2 tests are needed, vendors will need to approach customers for testing purposes in pilot service.

> Back to questions

5.4 Q: When to register to SWIFTNet services for TARGET2?

A: TARGET2 is going to live operation in November 2007. The testing for TARGET2 users is foreseen as of May 2007. SWIFT registration is available through the e-ordering section of www.swift.com.

E-MSSF to SWIFT	Subscription to Test	Start of test date	Live Date
Group 1	26 Feb until 11 Apr 2007	01 May 2007	19 Nov 2007
Group 2	26 Mar until 09 May 2007	19 Jun 2007	18 Feb 2008
Group 3	26 Mar until 09 May 2007	02 Jul 2007	19 May 2008

Country Migration Groups

Group 1	Group 2	Group 3	Group4
Austria	Belgium	Denmark	Contingency
Cyprus	Finland	Estonia	
Germany	France	ECB	
Latvia	Ireland	Greece	
Lithuania	The Netherlands	Italy	
Luxembourg	Portugal	Poland	
Malta	Spain		
Slovenia			

> Back to questions

5.5 Q: How can a synonym destination register to TARGET2 for test?

A synonym destination is not allowed to have a FIN test destination (ending in 0) and can only use a DN for SWIFTNet services.

As the e-ordering for TARGET2 is consolidating the subscription to SWIFTNet FIN and SWIFTNet services, the following solution is proposed:

Customers who want to subscribe to the Payments Module (PM) & Information and Control Module (ICM) for testing can do this as follows:

1. The Master destination should subscribe a test BIC to the respective FIN CUG TGT/TGH/TGC (scenario 1, 2, 3 or 4)
2. The synonym destination should subscribe to “ICM only” (scenario 5)

The synonym can subscribe to all live services independently from their master destination.

5.6 Q: Can a non-connected BIC (BIC1) be registered for TARGET2?

Yes, for example Ancillary Systems who want to subscribe to SWIFT and register for TARGET2 SWIFTNet Services only and not using FIN, will only receive a non-connected BIC (ending with 1 in the 8th character position).
A BIC1 cannot send or receive any FIN messages but can be used in the text of a payment message. This BIC1 can be used for the Account allocation in the SSP and the publication in the TARGET2 directory.

The e-ordering form of scenario 5 is suitable for such a case: the assigned SWIFT BIC8 must uniquely be used as a component of the DN structure.

5.7 Q: How to register additional BICs for TARGET2 FIN services only?

In case you want to register additional BICs for the Payments Module or the HAM module, a TARGET2 change form is available in the e-ordering section on www.swift.com.

5.8 Q: Where can I find the browse URL of the TARGET2 webserver?

The URL to access the ICM can be found in the ICM User Handbook, section 2.1.

Live URL: https://trgt-papss.ssp.swiftnet.sipn.swift.com

Test URL: https://trgt-papss-cust.ssp.swiftnet.sipn.swift.com

5.9 Q: What pricing structure is applicable for TARGET2 traffic?

The pricing scheme for TARGET2 is based on standard SWIFT pricing, covering all messaging flows in TARGET2.
Specific test and training prices are applicable during the migration period from May 2007 until May 2008. Please contact your SWIFT account Manager for more details.

Note:
User = Direct Participant and/or Ancillary System

FIN
Standard pricing as defined in SWIFT Price List (section 3.1)

- From User to User
Standard pricing depending on tier, domestic or international, as appropriate

- From SSP to User and from User to SSP
Standard fixed price for all users (from and to market infrastructure), always paid by the user

FIN Copy
Standard FIN Copy price of 5,42 eurocents/copy + 0,3 eurocents/copy to cover the feature "mass retrieval" selected by the Service Administrator)
(assumption daily avg > 300,000 copies – see SWIFT Price List, section 4.1). Always paid by the user.

SWIFTNet InterAct

- From SSP to User and from User to SSP

International traffic price for all users, tier dependent, real-time or store-and-forward as appropriate (see SWIFT Price List, section 5.1). Always paid by the user.

SWIFTNet FileAct

- From SSP to User and from User to SSP

International traffic price for all users, tier dependent, real-time or store-and-forward as appropriate (see SWIFT Price List, section 5.1). Always paid by the user.

SWIFTNet Browse

SWIFTNet Browse is charged only when the service is live (November 07). Standard price applies based on the total number of end-user platforms (live or test) accessing the webserver (for an assumption of more than 200 registered end-user platforms, a monthly fee per end-user platform is charged)

5.10 Q: Where can users find more information on TARGET2?

A: The General User Specifications and the User Detailed functional specifications (book 1 and 2) as well as the 4th book containing the XML messages specifications provide the information needed by the future TARGET2 participants and vendors. Those documents are available on the ECB website, which is user name and password protected.
URL: https://target2.ecb.int

www.swift.com contains updated information and presentations on TARGET2.

SWIFT Support can be contacted, online or by phone, to provide assistance in SWIFT related matters. For all non-SWIFT product related business questions, the national central bank is the first point of contact for all participants.

> Back to questions

5.11 Q: Do we have SWIFT training for TARGET2?

A: To make the migration to TARGET2 as smoothly as possible, SWIFT Training offers a one-day training module about the technical implications of the TARGET2 migration in relation to SWIFT. This course can be complemented by the SWIFTAlliance interface courses in the SWIFT Training portfolio.

More information is available on www.swift.com/training

➢ Back to questions

Glossary

3CB	Association of 3 Central Banks (Banca d'Italia, Deutsche Bundesbank and Banque de France) operating the SSP on behalf of the Eurosystem
3CBIAC	3CB Internal Acceptance Test
ADK	Application Development Kit
ASI	SSP Ancillary Systems Interface
BBK	Deutsche Bundesbank
BdI	Banca d'Italia
BDF	Banque de France
BKE	Bilateral Key Exchange
CBC	Central Bank Customers
CBT	Computer Based Terminal
CDR	Committed Data Rate
CLS	Continuous Linked Settlement
CM	Contingency Module
CONT	SSP Contingency system
CRSS	SSP Customer Related Services System
CUGM	Closed User Group Module
DMZ	DeMilitarised Zone
DN	Distinguished Name
EBA	European Banking Association
ECB	European Central Bank
Eurosystem	System composed of the ECB and the National Central Banks of the countries which form the euro area
FA	FileAct
FW	FireWall
HAM	Home Accounting Module
HSM	Hardware Security Module
IA	InterAct
ICM	SSP Information and Control system
Kbps / Mbps	Kilo / Megabits per second
LT	Logical Terminal
MAC	Message Authentication Code
M-CPE	Managed Customer Premises Equipment
MRR	Message Reception Registry
MQSA	SWIFTAlliance Access WebSphere MQ Interface
MSSF	Message Service Subscription Form
NACG	Network Access Control Guide
NCBs	National Central Banks
NCH	Network Computer House
PAPPS	SSP Payments System
PASO	Partner Solutions

PKI	Public Key Infrastructure
PM	SSP Payments Module
PMC	(3CB) Program Management Committee
POP	Point of Presence
RA(HA)	Remote Adaptor
RBAC	Role Based Access Control
RP	SWIFT Regional Processor
RT	Real-Time
RTGS	Real Time Gross Settlement
SAA	SWIFTAlliance Access
SAB	SWIFTAlliance WebStation
SAE	SWIFTAlliance Entry
SAG	SWIFTAlliance Gateway
SAM	SWIFTAlliance Messenger
SAW	SWIFTAlliance WorkStation
SIPN	Secure IP Network
SnF	Store-and-Forward
SNL	SWIFTNet Link
SO	Security Officer
SSP	Single Shared Platform
T&T	Test & Training
TGT	Service Code published in the BIC Directory products for Direct Participants
TG+	Service Code published in the BIC Directory products for Indirect Participants
TPS	Transactions per Second
UDFS	User Defined Functional Specifications
VPN	Virtual Private Network