



SWIFTNet for TARGET2

TARGET2

Getting Started

This user guide is for Credit Institutions and Ancillary Systems that intend to implement the TARGET2 service as a Direct Participant. This document provides the information to successfully plan, implement and test SWIFTNet for TARGET2 in both user-to-application mode and application-to-application mode.

March 2007



Legal Notices

Copyright

Copyright © S.W.I.F.T. SCRL (“SWIFT”), avenue Adèle 1, B-1310 La Hulpe, Belgium, or its licensors, 2006. All rights reserved.

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

Confidentiality

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

Disclaimer

SWIFT supplies this publication for information purposes only. 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 version.

Trademarks

SWIFT, S.W.I.F.T., the SWIFT logo, Sibos, SWIFTNet, SWIFTAlliance, SWIFTStandards, SWIFTReady, and Accord are trademarks of S.W.I.F.T. SCRL. Other SWIFT-derived service and product names, including SWIFTSolutions, SWIFTWatch, and SWIFTSupport are tradenames of S.W.I.F.T. SCRL.

SWIFT is the trading name of S.W.I.F.T. SCRL.

Other product or company names in this publication are tradenames, trademarks, or registered trademarks of their respective owners.

Preface

About this document

This user guide provides information to successfully plan, implement and test SWIFTNet services for TARGET2.

For the latest available version of this document, see www.swift.com > Products & Services > Initiatives > TARGET2.

Audience

SWIFT intends this document for TARGET2 project managers and individuals that want to order and establish a SWIFTNet infrastructure to access the TARGET2 service.

Related documentation

TARGET2 documents

(for the latest version, see <https://target2.ecb.int>)

Username en Password can be obtained from your NCB)

- *TARGET2 User Detailed Functional Specification (UDFS) Book 1*
- *TARGET2 User Detailed Functional Specification (UDFS) Book 2*
- *TARGET2 User Detailed Functional Specification (UDFS) Book 4*

SWIFTNet messaging documents

(for the latest version, see www.swift.com or contact your SWIFT Account Manager)

- *SWIFTNet Service Description*
- *SWIFTNet Connectivity Packs*
- *SWIFTNet Resilience Guide*
- *SWIFTNet Naming and Addressing Summary*
- *SWIFT Network Access Control Guidelines*
- *SWIFTNet Certificate Administration Guide*

Document conventions

This document uses the typographical conventions shown in the following table:

Bold	Names of files, parameters, API calls, user logon, and logon groups. References to a directory or a menu. GUI elements and command names.
<i>Italics</i>	Important information and document names.
<code>Courier</code>	User input, directory paths, parameter values, place holders, and system output examples.

Table of Contents

1	Introduction.....	7
2	TARGET2.....	8
2.1	TARGET2 Participation	8
2.2	TARGET2 Accessibility.....	8
2.3	TARGET2 Services	10
2.3.1	Information and Control Module	11
2.3.2	Payments Module.....	11
2.3.3	Ancillary System Interface	11
2.3.4	TARGET2 BIC.....	11
2.3.5	Directories for TARGET2.....	12
2.4	About User-to-Application Mode	12
2.5	About Application-to-Application Mode	12
3	TARGET2 on SWIFTNet.....	13
3.1	SWIFTNet Messaging Services for TARGET2.....	13
3.1.1	SWIFTNet FIN and FIN Copy	14
3.1.2	SWIFTNet InterAct	14
3.1.3	SWIFTNet FileAct.....	14
3.1.4	SWIFTNet Browse.....	14
3.1.5	TARGET2 SWIFTNet Services.....	15
3.1.6	SWIFTNet Features for InterAct and FileAct.....	15
3.2	XML Standards.....	17
3.3	SWIFTNet Connection.....	17
3.4	SWIFTNet Interfaces for TARGET2.....	17
3.4.1	User-to-Application Mode	17
3.4.2	Application-to-Application Mode	19
4	Migration Planning	21
5	A Guide to the Implementation Process	22
5.1	Implementation Process	22
5.2	Prerequisites.....	23
5.2.1	Configuration for User-to-Application Mode	23
5.2.2	Configuration for Application-to-Application Mode	23
5.3	How to Prepare the SWIFTNet Infrastructure	25
5.3.1	New SWIFTNet Members.....	25
5.3.2	Implementation Checklist.....	26
5.4	Service and Software Ordering.....	28

5.4.1	Register for SWIFTSupport	28
5.4.2	Ordering	28
5.4.3	Subscribe to TARGET2	28
5.5	Installation and Configuration	31
5.5.1	Software Installation	31
5.5.2	How to Install the FIN Copy Patch	31
5.5.3	Pre-Agreed MAC	31
5.6	How to Prepare for Testing.....	32
5.6.1	BKE with TARGET2 CID	32
5.6.2	How to Start TARGET2 in Test mode.....	32
5.7	How to Prepare for TARGET2 Live.....	33
5.7.1	BKE with TARGET2 CID	33
5.7.2	How to Start TARGET2 in Live Mode	33
6	Support for TARGET2	34
A	Acronyms	35

1 Introduction

This guide outlines the SWIFTNet components that are necessary to exchange messages with TARGET2 in user-to-application mode and application-to-application mode.

It explains the SWIFTNet requirements and presents information for users that want to implement the TARGET2 service as a direct participant.

There are several types of participants for TARGET2. This guide covers information for **direct** participants and multi-addressee BICs only (see section 2.1 TARGET2 participation)

Audience profile

SWIFT intends this document for the following types of users in the Credit Institutions and Ancillary Systems that participate in TARGET2:

- technical project managers
- technical security officers
- network administrators
- operators

Individuals that work on the TARGET2 project may have to perform the following tasks:

- design and install IT solutions for financial purposes
- ensure secure networks
- control data traffic flow

Summary of contents

This guide contains the following information:

- an overview of the SWIFTNet components for TARGET2
- a description of the user-to-application and application-to-application infrastructure
- prerequisites for the implementation of user-to-application mode and application-to-application mode
- a checklist for the implementation of user-to-application and application-to-application mode for TARGET2

2 TARGET2

TARGET2 is the new European Real-Time Gross Settlement (RTGS) system, which is based on the Single Shared Platform (SSP) operated by Banca d'Italia, Banque de France and Deutsche Bundesbank (3CB). The SSP is an integrated central technical platform.

SWIFT provides the following services for TARGET2:

SWIFTNet FIN and FIN Copy services for payments and settlement.

SWIFTNet InterAct for real-time cash management, SWIFTNet FileAct for the distribution of the TARGET2 directory and reporting, and SWIFTNet Browse for online information and control services.

2.1 TARGET2 participation

TARGET2 SSP is for credit and financial institutions that connect directly to the platform, called Direct Participants.

Direct participants have specific access features to the TARGET2 platform, which include:

- one or more RTGS accounts within the payments system (that is, Payments Module [PM])
- direct access to the PM and real-time information and control measures
- their own 8-digit or 11-digit SWIFT Bank Identifier Code (BIC) registered in the PM
- responsibility for their own liquidity management in the PM and for monitoring the settlement process
- Indirect participants access the TARGET2 platform through a direct participant.

2.2 TARGET2 technical access

There are two interfaces to connect to TARGET2 Single Shared Platform (SSP):

- the Ancillary System Interface (ASI)
- the Information and Control Module (ICM)

There are two technical modes to access ICM:

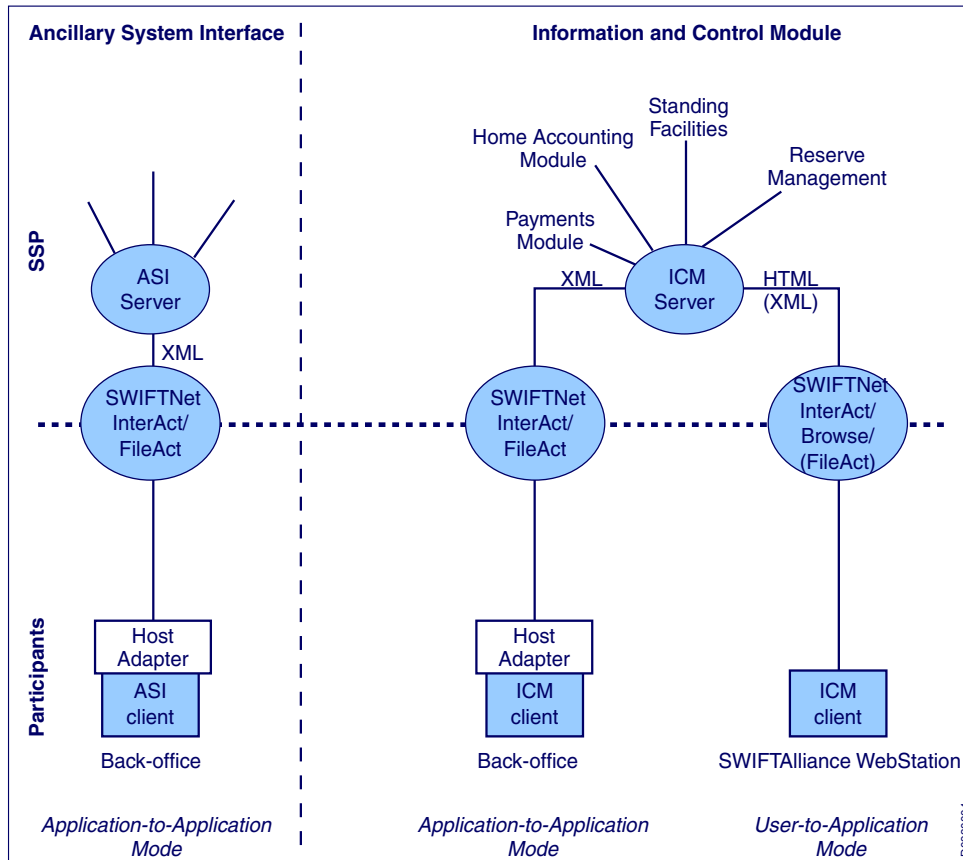
Application-to-application

The messaging is fully automated (back office).

User-to-application

The information is displayed in a web browser.

ASI users can access the SSP using application-to-application mode only.



2.2.1 TARGET2 BIC

TARGET2 has defined Bank Identifier Codes (BIC) for specific purposes in separated test and production environments. Some of the BICs are used during the migration period only. Other BICs are permanent.

Proposed BIC	Purpose	Validity period
TRGTXEPMXXX	To exchange messages directly with Payments Module (PM) participants	Permanent
TRGTXEPMASI	Liquidity transfer through the Ancillary System Interface (ASI)	Permanent
TRGTXEPMTGT	TARGET payments for delivery to the PM participants from external Central Banks (CB) that have not migrated to the Single Shared Platform (SSP)	Migration
TRGTXETGccc	To exchange payments from PM participants to external CBs. Note: ccc is the SWIFT service code for the migrated national RTGS system.	Migration

For more information, see the *User Detailed Functional Specifications (UDFS)*, Book 1, Section 9 Technical Specifications.

2.2.2 Directories for TARGET2

Two directories are used for payment addresses:

- the TARGET2 Directory
- the SWIFT BIC Directory

The TARGET2 Directory has been set up by the SSP operator in addition to the SWIFT BIC Directory to support the specific needs of the SSP and its users. The TARGET2 Directory lists the institutions that can be addressed in TARGET2. It contains direct and indirect participants' BIC addresses. The Directory provides the routing information for TARGET2 payments and is organised alphabetically by institution. It can only be downloaded through SWIFTNet FileAct from the SSP.

For more information, see the *User Detailed Functional Specifications (UDFS)*, Book 1, Section 2 User Guide for Payments Module.

2.3 User-to-Application mode

In user-to-application mode, the information is displayed in a browser that runs on a PC system (SWIFTAlliance WebStation). Participants do not need to develop any specific application.

2.4 Application-to-Application mode

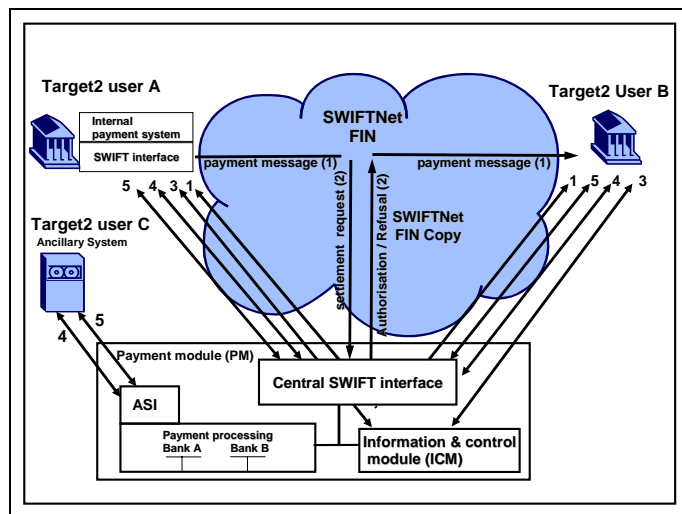
In application-to-application mode, information and messages are transferred automatically between the Single Shared Platform (SSP) and the individual participant's internal back-office application via the SWIFTAlliance Gateway. SWIFTNet InterAct is used to exchange messages in real time and SWIFTNet FileAct for file transfer.

See section 5.2.2 for the options to implement TARGET2 in application-to-application mode.

3 TARGET2 on SWIFTNet

3.1 SWIFTNet messaging services for TARGET2

The following diagram provides an overview of the SWIFTNet messaging services that TARGET2 uses:



The arrows in the diagram indicate the following services:

1. SWIFTNet FIN
2. SWIFTNet FIN Copy
3. SWIFTNet InterAct
4. SWIFTNet Browse
5. SWIFTNet FileAct

For a description of the SWIFTNet messaging services, see the *SWIFTNet Service Description* and the *FIN Service Description*.

The following SWIFTNet messaging services are used for the different ICM access modes.

application-to-application mode	user-to-application mode
SWIFTNet InterAct	SWIFTNet InterAct
SWIFTNet FileAct	SWIFTNet FileAct
	SWIFTNet Browse

3.1.1 SWIFTNet FIN and FIN Copy

A TARGET2 participant uses MT 103 and MT 103+, MT 202 (bank transfer) and (optionally) MT 204 (direct debit) for payments initiation.

Following FIN messages can also be exchanged between direct participants for reporting and control purposes (MT999, 191,192,195,196,199, 291, 292, 295, 296, 299).

The FIN Copy mechanism is used to copy a Euro payment to the TARGET2 Payments Module for settlement purposes. TARGET2 receives a complete copy of the FIN message and can then authorise or prevent delivery of the message to the addressee. SWIFT stores the FIN message until TARGET2 either authorises or rejects it.

Specific FIN Closed User Groups have been created:

TARGET2 FIN Services	Usage in the SSP
TGT	FIN Y-Copy PM
TGH	FIN V-Shape HAM

3.1.2 SWIFTNet InterAct

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

In the Payments module, TARGET2 uses SWIFTNet InterAct in real-time query-and-response mode.

3.1.3 SWIFTNet FileAct

SWIFTNet FileAct supports the exchange of large volumes of data. TARGET2 uses SWIFTNet FileAct to send reports and to distribute the TARGET2 Directory.

TARGET2 uses SWIFTNet FileAct in the following modes:

- real-time, file-download mode, in which TARGET2 participants pull information (for example, to download the TARGET2 Directory, or to get long reports)
- store-and-forward mode, in which TARGET2 will push information in a file (for example, the TARGET2 Directory updates) to the TARGET2 participants.

3.1.4 SWIFTNet Browse

SWIFTNet Browse enables secure, browser-based access to the web servers that are available on SWIFTNet. SWIFTNet Browse provides TARGET2 direct participants with secure browse capabilities through the SWIFT Internet Protocol Network (SIPN).

For example, by accessing the Information and Control Module (ICM) by means of a SWIFTAlliance WebStation and a browser, participants can view the current liquidity position, the payments queue, or the system status.

The SWIFTAlliance Webstation also allows to combine the manual exchange of SWIFTNet InterAct and SWIFTNet FileAct messages.

3.1.5 TARGET2 SWIFTNet services

A SWIFTNet service is a combination of one or more core SWIFTNet messaging services (that is, SWIFTNet InterAct, SWIFTNet FileAct, SWIFTNet Browse, and SWIFTNet FIN), that are configured in a specific manner and used in the context of a SWIFTNet messaging solution.

Each SWIFTNet service has a service profile and a service name and is associated with a Closed User Group (CUG).

Payment and accounting processing services

The Payment and Accounting Processing Services (PAPSS) is the underlying SWIFTNet service for SWIFTNet InterAct and SWIFTNet FileAct. The PAPSS service allows access to the Information and Control Module (ICM) and the Ancillary System Interface (ASI).

Different services are defined for live and pilot operations, and for real-time and store-and-forward, as shown in the following table:

	PAPSS live service name	PAPSS test service name
real-time	trgt.papss	trgt.papss!p
store-and-forward	trgt.sfpapss	trgt.sfpapss!p

3.1.6 SWIFTNet Features for InterAct and FileAct

Role-based access control (RBAC)

The Role-Based Access Control parameter is used to control end-user access to specific functions. These roles are communicated to the community by the Single Shared Platform (SSP) operator.

In user-to-application mode, each participant must manage his users (that is, each participant must assign specific roles to each user).

Because no manual intervention is required in application-to-application mode, there is only one RBAC role which must be assigned to the application.

The activities related to RBAC must be executed by security officers.

RBAC is mandatory for TARGET2.

For more information, see the *Certification Administration Guide and UDFS*.

Non-repudiation support (NRS)

The SWIFTNet non-repudiation support feature enables SWIFT, in case of dispute, to confirm that a message exchange has taken place.

For TARGET2, non-repudiation is defined as optional at service level. This means that the sender application can decide which messages are sent with the non-repudiation support option selected.

However note that TARGET2 has decided that a certain number of InterAct messages have NRS as mandatory feature.

More information on these messages can be found in the *TARGET2 UDFS*.

Message routing and message reception registry (MRR)

Based on central routing rules, SWIFT delivers each message either to a store-and-forward queue or to a specified SNL. The central routing rules are stored in the SWIFT Message Reception Registry (MRR) and are managed by the receiving customer.

No MRR rules are necessary for real-time messages in pull mode. The response to a real-time message is routed back to the SNL that originated the request.

In store-and-forward mode, each direct participant must configure an MRR rule to identify the store-and-forward queue to which the files sent by TARGET2 in store-and-forward mode must be delivered. This configuration is part of the subscription process.

When participants subscribe for the first time to the store-and-forward service, SWIFT provides a default generic queue where all the store-and-forward messages are delivered to.

Participants can optionally request SWIFT to create additional store-and-forward queues.

Participants that already use SWIFTNet FileAct store-and-forward services may choose to use a generic queue or define additional queues. The choice depends upon operational requirements.

Distinguished names

Distinguished Names (DN) are identifiers used in the headers of messages. The requestor and responder DN identify the sender and receiver of the message.

There are no specific rules for the DN tree structure but it is strongly recommended that participants adapt the DN name to the new SWIFTNet phase 2 rules.

The basic DN structure is as follows:

<o=yourbic, o=swift>

In this structure, <yourbic> is the BIC8 of the participant's institution. The TARGET2 Directory uses the beneficiary's BIC, name, or national sort code, to deliver the related BIC for use in the SWIFT message header.

For more information see the *SWIFTNet Naming and Addressing Guide*.

SWIFTNet public key infrastructure

The Public Key Infrastructure (PKI) is a mandatory component that, together with the SWIFTNet Link (SNL), provides security and trust across all SWIFTNet services.

For more information, see the *SWIFTNet Certificate Administration Guide* and the *SWIFTNet Service Description*.

3.2 XML Standards

Two XML standards are used in TARGET2:

- SWIFTStandards XML (MX)
- TARGET2 XML standards

For more information, see the *User Detailed Functional Specifications (UDFS)*, Book 4.

3.3 SWIFTNet connection

The SWIFT Secure IP Network (SIPN) is the underlying technical communication network that provides SWIFTNet connectivity to exchange information and run control measures. The SIPN uses multiple Network Partners to connect users to the SIPN backbone access points.

Connectivity packs are available for specific traffic requirements, throughput speed, and resiliency. To select the appropriate connectivity pack, a participant must calculate its expected traffic measured in Transactions Per Second (TPS). Depending on the evolution of traffic that relates to TARGET2, participants may need to upgrade connectivity. TARGET2 participants cannot use economy lines (that is, lines that have a bandwidth of less than 64 Kbps).

Bandwidth requirements

For more information, see the *SWIFTNet Connectivity Packs*.

3.4 SWIFTNet interfaces for TARGET2

3.4.1 User-to-Application Mode

SAB is a browser-based interface that provides access to SWIFTNet FileAct-based and SWIFTNet Browse-based SWIFTSolutions as well as market infrastructures. SAB runs on a standard PC, under Windows, with a standard browser.

SWIFTAlliance WebStation (SAB) is mandatory for participants that want to access the Information and Control Module (ICM) in manual mode. It is also highly recommended as a backup solution for those participants opting for the Application-to-Application mode.

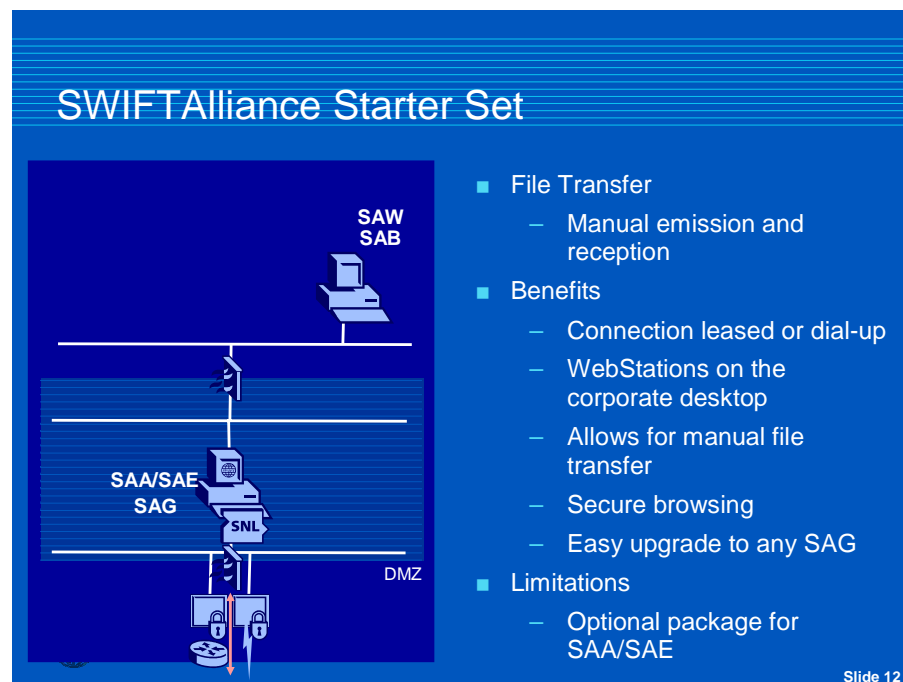
SAB can be connected directly to SWIFTNet or, indirectly through a SWIFTAlliance Starter Set (SAS) or SWIFTAlliance Gateway (SAG).

As part of the SWIFTNet phase 2 migration, all SWIFTAlliance Access or SWIFTAlliance Entry (SAA/SAE) users have a SAS or SAG.

SAS increases the capabilities of the SAA/SAE interface because it enables operators to perform manual file transfer and to browse securely. SAS allows one operator at a time to access ICM and to initiate and receive files manually. SAS includes the SAB software license with the file-transfer Graphical User Interface (GUI).

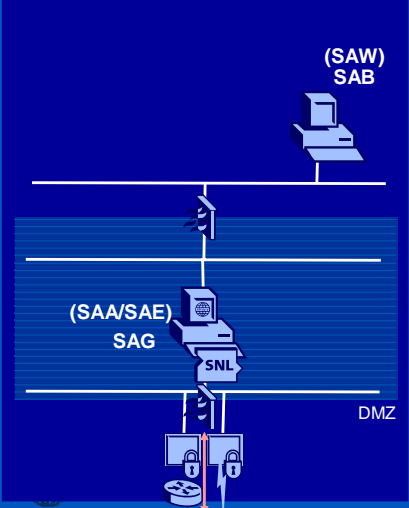
For SAA/SAE users, SAS may be a more appropriate configuration than a SAB directly connected to SWIFTNet.

SAS runs on the same system as SAA/SAE and SWIFTNet Link (SNL). It is available on Windows, AIX, and Solaris.



Participants that require more than one concurrent user must purchase the SWIFTAlliance Gateway (for example, the WebStation Concentrator licence). In this case, the participant must purchase SAB separately as it is not included in the SAG licence.

SAG licence profile 'SAB Concentration'



- SAG licence allowing for SAB concentration
- Benefits
 - SAB on the corporate desktop
- Limitations
 - Requires Connectivity Pack 2 to 5

Slide 13

3.4.2 Application-to-Application mode

SWIFTAlliance Gateway (SAG) is mandatory to access the Information and Control Module (ICM) in application-to-application mode.

SAG acts as a concentrator for SWIFTNet message flows. SAG extends the SWIFTNet connection to multiple applications and multiple SWIFTAlliance interfaces (for example, SWIFTAlliance WebStation and SWIFTAlliance Access). The traffic from multiple applications and SWIFTAlliance WebStations is concentrated onto a single window.

SAG licence profile 'Single Window'

- The 'typical' SAG Licence
- Benefits
 - Full SWIFTNet concentrator
 - SAG in the DMZ
 - Scalability, resource optimisation
 - Resilience
- Limitations
 - Requires Connectivity Pack 2 to 5

Slide 15

Back-office applications exchange messages with SAG by means of a host adapter as follows:

MQ-Series Host Adapter (MQHA).

The MQHA adapter enables applications to use the WebSphere MQ API and queuing mechanism to exchange messages with SAG.

Remote API Host Adapter (RAHA).

The RAHA adapter offers a set of API to local and remote applications.

The SAG **Single Window** licence is the only licence that includes a host adapter. The SAG **Automation** licence does not meet all the requirements for TARGET2 in application-to-application mode

Participants must purchase SWIFTAlliance WebStation (SAB) separately because it is not included in the SAG licence.

4 Migration planning

The customer implementation process consists of a development phase and a test phase, before going live.

TARGET2 will go live based on different waves:

- Each wave consists of a group of central banks and the respective, national banking communities.
- There will be 3 implementation groups (plus one contingency) that migrate during scheduled specific weekends.

TARGET2 migrates the groups over a period of six months, during which both TARGET1 and TARGET2 components will co-exist.

Countries that are not part of the current TARGET do not participate in the migration groups. They will join according to a specific timetable and procedure.

Registration details for T2 participants to Pilot services.

GROUP 1:	
26.02.2007 – 13.04.2007	SSP forms submission to CBs
26.02.2007 – 11.04.2007	e-mssf submission to SWIFT Implementation date: Sat 28 April 2007 e-mssf approvals by the CBs e-mssf approvals by SSP Service Desk
02.04.2007 – 27.04.2007	key exchange
16.04.2007 – 27.04.2007	Static data loading
12.04.2007 – 29.04.2007	SWIFT Provisioning and Implementation
1 May 2007	Start of user testing phase

GROUPS 2 & 3:	
26.03.2007 – 18.05.2007	SSP forms submission to CBs
26.03.2007 – 09.05.2007	e-mssf submission to SWIFT Implementation date Group 2: Saturday 16 June 07. Implementation date Group 3: Saturday 30 June 07. e-mssf approvals by the CBs e-mssf approvals by SSP Service Desk
30.04.2007 – 01.06.2007	key exchange
21.05.2007 – 01.06.2007	Static data loading
09.05.2007 – 03.06.2007	SWIFT Provisioning and Implementation
19 June 07 Group 2 2nd of July 07 Group 3 (except Italy)	Start of user testing phase

5 A guide to the Implementation Process

5.1 Implementation

The following table gives an overview of the activities for direct participants involved in the implementation of the SWIFTNet components for TARGET2 .

Activity
Identify the technical requirements for TARGET2 implementation: - line capacity - access mode - interfaces
Upgrade connectivity.
Line provisioning and installation.
Order required interfaces.
Software delivery.
Subscribe to TARGET2 (test services).
Install SWIFT software.
Install patch for pre-agreed Mac.
Install FIN Copy patch.
Configure the SWIFTNet interface.
Exchange keys with test TARGET CID (TRGTXEP0).
Activate TARGET 2 in test mode.
Perform testing.
Subscribe to TARGET2 (live services).
Exchange keys with live TARGET CID (TRGTXEPM).
Activate the TARGET 2 service in live mode.
Go live.

The number of implementation steps that participants must follow to enable TARGET2 on SWIFTNet depends on the existing SWIFTNet infrastructure.

New SWIFTNet users must build the necessary SWIFTNet infrastructure before implementing TARGET2 on SWIFTNet. See section 5.3.1.

5.2 Configuration prerequisites

This section outlines the conditions and requirements for participants that want to establish and implement SWIFTNet infrastructure components for TARGET2.

In the configuration plan, participants must define the appropriate resilience for local and remote disaster systems, and the operational procedures in case of failure.

5.2.1 Configuration for User-to-Application mode

The minimum configuration for participants that want to access TARGET2 in user-to-application mode is as follows:

Managed Customer Premises Equipment (M-CPE) VPN boxes connected with a minimum of 64 Kbps bandwidth to the SWIFT Secure IP Network through a Network Partner.

A SWIFTAlliance WebStation connected directly to the M-CPE, or indirectly through a SWIFTAlliance Starter Set (SAS) or a SWIFTAlliance Gateway (SAG).

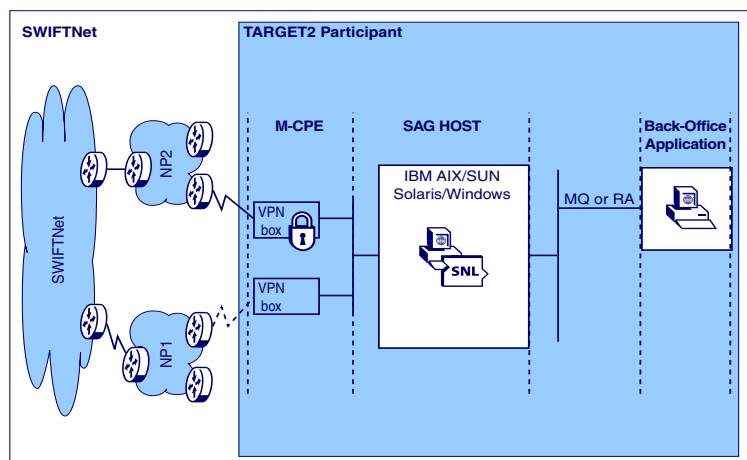
5.2.2 Configuration for Application-to-Application mode

The minimum configuration for participants that want to access TARGET2 in application-to-application mode is as follows:

Managed Customer Premises Equipment (M-CPE) VPN boxes connected with a minimum of 64 Kbps bandwidth to SWIFT Secure IP Network through a Network Partner.

SWIFTAlliance Gateway (SAG) that has a Single Window licence.

A host for back-office applications.



Back-office application

Participants that want to implement TARGET2 in application-to-application mode have the following options:

- to use the SWIFTAlliance Gateway Developers Toolkit to develop a proprietary application or to adapt an existing application
- to purchase an appropriate application and integration solution through a Solution Partner

For both options, participants require the SAG Single Window licence. The application exchanges messages with SAG by means of a host adapter (MQ-Series Host Adapter [MQHA] or Remote Adapter Host Adapter [RAHA]). The SAG Single Window licence is the only licence that includes a host adapter.

Solution Partners

A Solution Partner is a registered third party that has the expertise to develop and integrate applications for SWIFTNet solutions.

You can find information about using a Solution Partner to develop a SWIFTNet solution at www.swift.com/partners/solutionpartners.

SWIFTAlliance Gateway Developers Toolkit

The SWIFTAlliance Gateway Developers Toolkit provides the Application Programming Interface (API) for development and integration of applications using SWIFTNet FileAct or SWIFTNet InterAct (or both) in real-time or store-and-forward mode.

The contents of the SAG Developers Toolkit is as follows:

- a SWIFTAlliance Gateway Developer Toolkit licence for all supported operating systems
- a SWIFTAlliance Gateway run-time version for all available platforms (that is, AIX, Solaris, and Windows)
- SWIFTAlliance Gateway developer documentation and sample source code

The SAG Developers Toolkit also includes training and SWIFTSupport, and has documentation that describes each aspect of SAG, SWIFTNet, and the Toolkit.

5.3 How to prepare the SWIFTNet infrastructure

The number of implementation steps that participants must follow to enable TARGET2 on SWIFTNet depends on the existing SWIFTNet infrastructure.

In addition to the information in the previous sections of this document, participants must consider the items and decisions that are specified in sections 5.3.1 and 5.3.2.

5.3.1 New SWIFTNet members

New SWIFTNets user must build the necessary SWIFTNet infrastructure before it can implement TARGET2 in user-to-application mode or application-to-application mode on SWIFTNet.

1. Preparation	
Architecture	<p>Design the architecture to be to put in place to access TARGET2 on SWIFTNet, for the live, test, and contingency environments.</p> <p>Plan the necessary IP addresses, firewalls, routers. It is recommended that the architects make a network drawing of the required infrastructure and an inventory of components or services to be ordered.</p>
Hardware	Check the capacity of the hardware and if it can handle the traffic expectations for TARGET2.
2. Ordering	
Licences	<p>Order the required SWIFTNet Infrastructure at www.swift.com > Ordering and Support > Ordering.</p> <p>Order the number of base licences required for each of the following items:</p> <p>SWIFTNet Link (SNL) base licences</p> <p>One base licence allows to install one prime, one test, and one contingency machine.</p> <p>SWIFTAlliance WebStation</p> <p>At least one WebStation is required to administer the SWIFTNet PKI certificates.</p> <p>Note: new software must be ordered minimum four weeks before the testing start date.</p> <p>SWIFT validates the order and sends an order acknowledgement by e-mail. At a later stage in the ordering process, SWIFT will also send an e-mail confirmation that contains the technical details (for example, the SNL IDs).</p>

5.3.2 Implementation checklist

Below is a list of questions participants should ask themselves when preparing the infrastructure for TARGET2.

SWIFTNet connectivity	
Does your institution own the SWIFTNet infrastructure?	yes <input type="checkbox"/> no <input type="checkbox"/>
If yes, is your current bandwidth sufficient to include TARGET2 traffic?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you require upgrade connectivity? If you require connectivity line upgrades, then plan a typical 16-week implementation timeline (contact your network provider and inform SWIFT).	yes <input type="checkbox"/> no <input type="checkbox"/>
Additional connectivity?	yes <input type="checkbox"/> no <input type="checkbox"/>
Shared by multiple BIC: The BIC owner of the SWIFTNet Infrastructure is:	yes <input type="checkbox"/> no <input type="checkbox"/>
Are you connected to SWIFTNet through a service bureau? If yes, the service bureau is:	yes <input type="checkbox"/> no <input type="checkbox"/>

SWIFTNet components for user-to-application mode	
Do you plan to implement a separate test system?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you plan to have a local failover mechanism?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you plan to have a disaster recovery solution?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you need a new SWIFTAlliance WebStation (SAB) licence or an additional SAB licence?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you use the SAB that is part of SWIFTAlliance Starter Set (SAS)?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you need more than one concurrent user?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you have to upgrade your current SWIFTAlliance Gateway (SAG) licence (for example to run additional concurrent SABs)?	yes <input type="checkbox"/> no <input type="checkbox"/>

SWIFTNet components for application-to-application mode	
Do you plan to implement a separate test system?	yes <input type="checkbox"/> no <input type="checkbox"/>

Do you plan to have a local failover mechanism?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you plan to have a disaster recovery solution?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you need a new SWIFTNet Link (SNL) licence or an SNL licence extension (an additional test or contingency SNL instance)? Specify your or your service bureau's existing SNL ID, if you want to reuse the SNLs: Test SNL: Prime SNL: Disaster SNL:	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you need a new SAG licence?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you need an extension or upgrade of your current SAG licence (for example, an additional BIC, or from Automation to Single Window)?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you need a new SAB licence for SWIFTNet PKI certificate administration, SAG administration?	yes <input type="checkbox"/> no <input type="checkbox"/>
Does your existing hardware have the capacity to handle the traffic expectations for TARGET2?	yes <input type="checkbox"/> no <input type="checkbox"/>
Integration of your back-office application	
Do you want to integrate your back-office application through a Solution Partner?	yes <input type="checkbox"/> no <input type="checkbox"/>
Will you perform your own development for integration?	yes <input type="checkbox"/> no <input type="checkbox"/>
Do you require the SAG Developers Toolkit?	yes <input type="checkbox"/> no <input type="checkbox"/>

Naming and addressing	
Your institution will participate with BIC (level 2 of the requestor Distinguished Name (DN) and authoriser DN):	
For testing (pilot service), use the following DN:	
For production (live service), use the following DN:	

Resources for implementation work	
Your institution will use a Service Partner.	yes <input type="checkbox"/> no <input type="checkbox"/>
Your institution has its own teams.	yes <input type="checkbox"/> no <input type="checkbox"/>

5.4 TARGET2 service and software ordering

5.4.1 Register for SWIFTSupport

To access the online support services on swift.com, participants must be registered to SWIFTSupport. If not yet done, register to SWIFTSupport as follows:

Access www.swift.com.

Click the Ordering & Support tab and select Ordering from the drop-down menu.

Click Register and select the Register link for SWIFTSupport.

Complete the registration form.

Note: Registration to SWIFTSupport is free of charge.

5.4.2 Order

Participants should order as follows:

Line upgrades, from a Network Partner at www.swift.com > Partners > Network partners.

Hardware from a local supplier.

SWIFT software and services from SWIFT at www.swift.com > Ordering & Support > Ordering.

5.4.3 Subscribe

Before subscribing to TARGET2, participants must consult their National Central Bank (NCB) to determine the specific national requirements.

Participants must subscribe once to join the pilot services for testing operations, and once to join the live services

Go to www.swift.com > Ordering & Support > Ordering > Existing customers > Member Administered Services > Subscribe to > TARGET2.

5 different scenarios are available for direct participants and multi-addressees to select as shown below in the picture:

Scenario 1	I subscribe to the Payments and ICM Module
Scenario 2	I subscribe to the Payments, HAM and ICM Module
Scenario 3	I subscribe to HAM and ICM Module
Scenario 4	I subscribe to CB customers and ICM Module
Scenario 5	I subscribe to ICM Module Only

Depending on the choice of scenario, a specific form is available.

To complete the form on-line on www.swift.com, direct participants (**BANKCCLL**) need to prepare the following information in advance:

- **Customer Info Section:** The system will display the Customer info, complete where needed.
- **Preferred implementation date:** Please specify the activation date of your service. Check with your National Central Bank for the Service Activation date you need to mention in this field.
- **FIN Service Configuration for the Service:** The system will display by default the FIN Service code(s) related to the selected scenario (e.g. TGT for Payment Module)
- **National Central Bank:** please select the BIC Code of your National Central Bank from the drop down menu (e.g. CENTCCLL)
- **SWIFTNet Service (Real-Time):** The SWIFTNet Distinguished Name (DN) is shown **o=bankccll,o=swift**. TARGET2 does not apply specific rules

By default the screen will display the DN level 2.

By clicking on the advance button, you will see that also DN level 3 wildcard will be provisioned, meaning the DN level 2 and all lower levels can use the selected service. Should you wish to use only specific DNs you can mention these.

- **SWIFTNet Browse Information:** please specify the SNL IDs or SNJ IDs of your SWIFTAlliance WebStation that your institution will use to access the service
- **SWIFTNet Service (Store & Forward):** The SWIFTNet Distinguished Name (DN) is shown **o=bankccll,o=swift**. TARGET2 does not apply specific rules By default the screen will display the DN level 2.

By clicking on the advance button, you will see that also DN level 3 wildcard will be provisioned; meaning the DN level 2 and all lower levels can use the selected service. Should you wish to use only specific DNs you can mention these.

Traffic Routing for store and forward Service:

A default Queue Name is proposed that participants will use for all store-and-forward traffic.

e.g: BANKCCLL_generic!p.

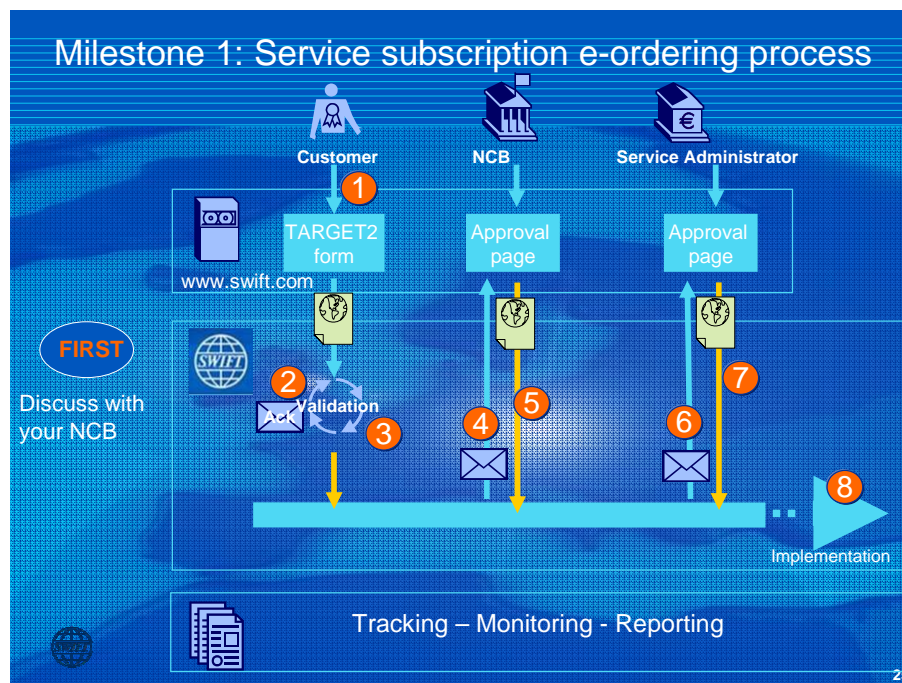
Should you want to define another queue, please click on the advance button. Whether participants can use the default queue or not depends on the operational setup (interface/application) and traffic used.

Once you have completed the form and read to terms & conditions and approve your order



Check this box to confirm acceptance of your order details above, then click **Accept**

The e-ordering and validation process is described in the picture below:



Process:

1. The customer completes and submits the subscription on www.swift.com.
2. SWIFT validates the subscription.
3. SWIFT sends an acknowledgement to the participant.
4. The National Central Bank (NCB) receives a request to approve the service subscription.
5. The NCB approves the service subscription and submits the approved subscription.
6. The TARGET2 service administrator receives a request to approve the subscription that has been approved by the NCB.
7. TARGET2 approves and submits the approval page.
8. Service(s) provisioning is executed. SWIFT commits to perform the subscription and provisioning process within 3 weeks after receipt of a valid authorised form.

5.5 Installation and configuration

5.5.1 Software installation

Participants must prepare the system according to the system requirements in the release letters.

Participants must ensure that all authorisation codes and licensing sheets are available before the start of an installation or upgrade procedure.

The installation guides that accompany the SWIFTAlliance WebStation, SWIFTAlliance Starter Set and SWIFTAlliance Gateway software provide instructions to guide participants through installation and configuration.

Participants with a Service Partner that has established the SWIFT network and FIN service may prefer that the Service Partner also establishes the SWIFTNet infrastructure for TARGET2 compliance.

5.5.2 How to install the FIN Copy patch

If a participant runs SWIFTAlliance Entry or Access, then its FIN interface must be upgraded with the latest version of the FIN Copy patch. The FIN Copy patch is available at www.swift.com > Ordering & Support > Support > Download centre. The naming convention is FCP_Year_month (for example, FCP_2005_09).

Non-SWIFT interface customers must contact their interface vendor and confirm that the FIN interface supports FIN Copy. SWIFT has distributed a TARGET2-specific vendor specification document to all recognized interface and application vendors. The vendor specification document explains how to implement the TARGET2 authentication functionality.

5.5.3 How to install the pre-agreed MAC patch

The pre-agreed MAC mechanism is a non-mandatory solution that removes the obligation on participants to perform Bilateral Key Exchange (BKE) with all other TARGET2 participants for all payments messages that will be copied to the SSP.

Each TARGET2 participant must ensure that it has upgraded its FIN interface to support the pre-agreed MAC. The SWIFTAlliance Access (SAA) or SWIFTAlliance Entry (SAE) release 5.5 users must install SAA patch 5560. Patch 5560 is available online at www.swift.com > Ordering & Support > Support > Download centre.

Non-SWIFT interface customers must contact their interface vendor.

5.6 How to prepare for testing

5.6.1 BKE with TARGET2 CID

Bilateral Key Exchange (BKE) with the central institution destination is still mandatory until the users are RMA (Relationship Manager Application (RMA) enabled.

TARGET2 must initiate the key exchange.

Participants must exchange keys with the test TARGET2 CID (TRGTXEP0)

SWIFT requires that participants exchange test keys before the testing phase begins. Participants can confirm the dates with the central institution.

5.6.2 How to start TARGET2 in test mode

TARGET2 must perform some tests in co-ordination with the migration waves. As of May 2007, the migration groups have several months to complete the tests. Participants can find a detailed description of the planning and organisational aspects of user testing activities on the TARGET2 and local National Central Banks (NCB) websites.

During the testing phase, participants can access the TARGET2 Test Related Information System (T2TRIS).

This web-based application will be available to users on the TARGET2 website. T2TRIS will serve as the primary channel to exchange test-related information with the National Central Bank (NCB). It will support users' testing activities by providing updated calendar information on the TARGET2 testing activities.

NCBs remain responsible for coordinating the testing activities of local national banking communities. Participants that have any further questions about testing-related issues must direct queries to the local national contact point. Information about national contact points is available on the TARGET2 web site.

5.7 How to prepare for TARGET2 live

5.7.1 BKE with TARGET2 CID

In preparation of live bilateral operations, keys must be exchanged with the live TARGET2 CID (TRGTXEPM).

5.7.2 How to start TARGET2 in live mode

TARGET2 live mode operates on the same principle as TARGET2 test mode. Migration is performed by country groups, which enables TARGET participants to

migrate to TARGET2 in different waves, and on different, predefined dates. Each wave consists of a group of central banks and the respective national banking communities.

Participants can contact the local national central bank, or check the European Central Bank web site (TARGET2 section) to confirm dates and obtain more detailed information.

6 Support for TARGET2

Primary contact

The primary contact is the local National Central Bank (NCB).

TARGET2 support

The TARGET2 e-mail address for support is: target.hotline@ecb.int

Participants can contact the NCB for help with TARGET2 integration and testing.

SWIFTSupport

SWIFT is the single point of contact to report all problems and queries that relate to SWIFT services and products. SWIFTSupport is SWIFT's customer support service. It is available to all SWIFT customers.

Users within a customer institution must register to use the SWIFTSupport service. For more information about how to register for SWIFTSupport, see <http://www.swift.com> > Ordering & Support.

For more information about SWIFTSupport services, see the *SWIFTSupport Service Description*.

A Acronyms

ASI	Ancillary System Interface
3CB	Three Central Banks (Banca d'Italia, Bundesbank, and Banque de France)
BIC	Bank Identifier Code
BKE	Bilateral Key Exchange
CUG	Closed User Group
DN	Distinguished Name
ECB	European Central Bank
HAM	Home Accounting Module
ICM	Information and Control Module
IP	Internet Protocol
MAC	Message Authentication Code
M-CPE	Managed Customer Premises Equipment
MRR	Message Reception Registry
MT	Message Type
MQHA	MQ-Series Host Adapter
MX syntax	A type of SWIFTStandards message that is expressed in XML
NCB	National Central Bank
PAPPS	Payment and Accounting Processing Services
PKI	Public Key Infrastructure
RAHA	Remote API Host Adapter
RBAC	Role-Based Access Control
RTGS	Real Time Gross Settlement
SAB	SWIFTAlliance WebStation
SAG	SWIFTAlliance Gateway

SAS	SWIFTAlliance Starter Set
SIPN	Secure IP Network
SNL	SWIFTNet Link
SSP	Single Shared Platform
TARGET	Trans-European Automated Real-Time Gross Settlement Express Transfer
TPS	Transactions Per Second
TSSP	TARGET2 Single Shared Platform
VPN	Virtual Private Network