SWIFT's Solution for ESMIG

Service Description

This service description provides information about the features and functions of SWIFT's Solution for ESMIG and describes the specific roles and responsibilities of SWIFT and the customers in relation to accessing the Eurosystem Single Market Infrastructure Gateway (ESMIG) through SWIFT's Solution for ESMIG. This document is for all customers who want to connect to ESMIG using SWIFT's Solution for ESMIG.

13 May 2022

Link to this document: https://www2.swift.com/go/book/book200623

Table of Contents

Preface

Purpose of this document

This service description provides information about the features and functions of SWIFT's Solution for ESMIG and describes the roles and responsibilities of SWIFT and the customers in relation to SWIFT's Solution for ESMIG. It has been reviewed by the Banca d'Italia - acting on behalf of the Eurosystem - and contains the latest available information about SWIFT's Solution for ESMIG at the time of publication. It may be updated or supplemented from time to time in accordance with the applicable terms and conditions.

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

Audience

This document is for the customers who want to connect to the Eurosystem Single Market Infrastructure Gateway (ESMIG) using SWIFT's Solution for ESMIG.

SWIFT-defined terms

In the context of SWIFT documentation, certain terms have a specific meaning. These terms are called SWIFT-defined terms (for example, user or SWIFT services and products). These terms have the specific meaning set out in the SWIFT Glossary as amended or supplemented by this service description (see Glossary on page 8).

Significant changes

The following table lists all changes since the release of February 2022.

Updated and new information	Location
Inclusion of information related to Eurosystem Collateral Management System (ECMS)	Throughout the document
Phase-out of java-based proxy solution	User-to-Application Flows on page 16 Overview of Service Names (A2A) and URLs (U2A) on page 54

Related documentation

This service description, together with the latest available version of related documentation published by SWIFT, constitutes SWIFT's catalogue of connectivity services.

Connectivity

- Alliance Cloud Service Description
- Alliance Connect Gold Service Description
- Alliance Gateway Service Description
- Alliance Gateway Instant Service Description
- Alliance Gateway Instant User Guide
- Connectivity Packs - Configurations for Multi-Vendor Secure IP Network Connectivity
- Network Access Control Guide

- Network Configuration Tables Guide
- Resilience Guide
- Resilience Test Scenarios for Alliance Connect Gold
- Shared Infrastructure Programme Policy
- SWIFTNet Naming and Addressing Guide
- SWIFTNet Instant System and Network Requirements
- SWIFTNet Link Error Codes
- *SWIFTNet Link Installation Guide* (AIX, Linux, Oracle Solaris, or Windows)
- SWIFTNet Link Service Description
- SWIFTNet Service Description
- SWIFTNet System Messages

Certificates

- HSM Box Operations Guide
- HSM Card Operations Guide
- HSM Token Operations Guide
- SWIFT Certificate Centre - Getting Started with your Personal Token
- SWIFTNet PKI Certificate Administration Guide
- SWIFTNet PKI Service Description

Ordering and support

- Price List for SWIFT's Solution for ESMIG
- Pricing and Invoicing - Ordering, Invoicing, and Payment
- SWIFT Advanced Support and Care Services Service Description
- SWIFT Community Support Service Description
- SWIFT's Solution for ESMIG Support Page

Policies and legal

- BIC Policy
- HSM Box Terms and Conditions
- HSM Tokens and Cards Terms and Conditions
- SWIFT By-laws
- SWIFT Corporate Rules
- SWIFT Customer Testing Policy
- SWIFT Data Retrieval Policy
- SWIFT General Terms and Conditions
- SWIFT Glossary
- SWIFT Personal Data Protection Policy

Note

Customers can find the latest version of most of these documents at swift.com > Ordering and Support > Knowledge Centre (User Handbook).

Customers should also refer to the European Central Bank (ECB) website for relevant ESMIG documentation (see www.ecb.europa.eu > Payments & Markets > TARGET services*) and to the Banca d'Italia website for relevant tender documentation, including the Concession Contract (see* www.bancaditalia.it *> Bandi e avvisi scaduti > G011/18 - Eurosystem Single Market Infrastructure Gateway Concessions).*

1 Introduction

Business background

The Eurosystem operates various market infrastructures, including TARGET2, TARGET2-Securities (T2S), TARGET Instant Payment Settlement (TIPS), Eurosystem Collateral Management System (ECMS), and potentially other services and applications in the future.

The solution will provide both A2A (application-to-application) as well as U2A (user-to-application) modes. The A2A mode allows participants to automate exchange of messages and files with the Eurosystem Single Market Infrastructure Gateway (ESMIG). The U2A mode allows users at the participant's side to access online portals provided by ESMIG, for example, to manage application configuration or to manually enter transactions.

Network service providers (NSPs)

ESMIG is presented as a modular solution that can accommodate access to T2, T2S, TIPS, and ECMS, and additional services/applications. For all these services, the NSP communicates with ESMIG through a proprietary communication protocol documented by the Eurosystem.

SWIFT, as an NSP, provides A2A communication through InterAct, FileAct, and SWIFTNet Instant, which enables customers to re-use what they may already have. For U2A, a custom browser-based solution has been implemented.

SWIFT's Solution for ESMIG provides access to ESMIG both for the ESMIG testing and go-live phases, and will be available as of the corresponding dates according the Eurosystem timelines. For more information, see the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TARGET consolidation).

1.1 Acronyms

In this service description, the following acronyms have the specific meaning set out in the official ESMIG documentation.

A2A	Application-to-Application
AGI	Alliance Gateway Instant
BAH	Business Application Header
DEP	Data Exchange Protocol
ECB	European Central Bank
ECMS	Eurosystem Collateral Management System
ESMIG	Eurosystem Single Market Infrastructure Gateway
NSP	Network Service Provider
OPC	(SWIFT) Operating Centre
T2S	TARGET2-Securities
TIPS	TARGET Instant Payments Settlement

U2A	User-to-Application

1.2 Glossary

4CBs	The 4 central banks (that is, Banca d'Italia, Banco de España, Banque de France, Deutsche Bundesbank) that have been appointed by the Eurosystem to make the necessary preparations to have Network Service Providers provide connectivity services to the Eurosystem Single Market Infrastructure Gateway (ESMIG). Also referred to in this service description as '**ESMIG operator**'.
Concession Contract	Contract between the Eurosystem and a Network Service Provider (NSP) regarding the right granted to the NSP by the Eurosystem to provide connectivity services to access the Eurosystem Single Market Infrastructure Gateway (ESMIG).
Customer	• a Eurosystem central bank that uses SWIFT to connect to the Eurosystem Single Market Infrastructure Gateway (ESMIG) • a Di.Co.A. that uses SWIFT to connect to ESMIG For the avoidance of doubt and in the context of TIPS, a customer may also be an instructing party or a reachable party that is authorised to access ESMIG and has selected SWIFT as its network service provider to connect to ESMIG. In this service description, the terms TIPS participant, reachable party, and instructing party have the specific meaning set out in the official Eurosystem documentation for the TIPS service.
Di.Co.A.	A SWIFT user authorised by the Eurosystem to connect to ESMIG.
End user	A physical person that accesses the ESMIG U2A web service for a customer.
ESMIG operator	Refer to the definition of 4CBs.
ESMIG requirements	In the scope of this service description, ESMIG requirements refer to the *ESMIG Connectivity - Technical Requirements and Compliance Check* as assessed by the ESMIG operator as part of the *ESMIG NSP Compliance Check Procedure*.
Hosting Terms and Conditions	The terms and conditions allowing the Network Service Providers to install and maintain equipment at the premises of the ESMIG operator and attached as attachment 1.3 to the *Concession Contract* and as may be amended from time to time.
Incident	An incident at SWIFT can either be a 'service' incident or a 'customer' incident. For more information about SWIFT's Incident Management, see the relevant *SWIFT Support Service Description*. An incident in the context of 'ESMIG is considered and handled as a service incident.

TARGET Services	A number of services developed and operated by the Eurosystem that ensure the free flow of cash, securities, and collateral across Europe.
TARGET2-Securities	The Eurosystem technical platform for settling securities transactions in central bank money.
TARGET2	Trans-european Automated Real-time Gross settlement Express Transfer system for the settlement of money transfers within the European Union. The Eurosystem has announced that TARGET2 will evolve into a new RTGS system accessible through ESMIG and referred to as T2.
TARGET Instant Payment Settlement (TIPS)	The Eurosystem settlement service for instant payments in the TARGET2 framework.

2 Solution Description

This chapter describes SWIFT's Solution for ESMIG for customers connecting through a local connectivity infrastructure or, as set out in Alternative Options to Access SWIFT's Solution for ESMIG on page 31, a SWIFT-operated connectivity infrastructure.

2.1 Scope of SWIFT's Solution for ESMIG

Components of SWIFT's Solution for ESMIG

SWIFT's Solution for ESMIG consists of the following components:

- **Security components**
  - **Security hardware (HSM or personal token)** for the use of **SWIFTNet Public Key Infrastructure** for ESMIG, and SWIFTNet PKI certificates.
  - **SWIFTNet PKI certificates** required for ESMIG A2A and U2A messaging services.
- **Network connectivity components**
  - The **lines and related equipment** necessary for customers to access SWIFT's backbone network.
  - The **Alliance Connect Packs** that allow to connect to SWIFT's backbone network.
  - The **interconnection** between SWIFT's backbone network and ESMIG, including the necessary equipment at the premises of the ESMIG operator.

  For further details, see Network Connectivity on page 28.
- **SWIFTNet Link (SNL)**

  Connectivity interface for the use of the SWIFTNet messaging services (InterAct and FileAct) and to generate/verify digital signatures based on SWIFTNet PKI, see A2A Messaging Flows on page 13, Messaging Features on page 19, Specific A2A Messaging Flows for TIPS on page 15, Specific Messaging Features for TIPS on page 26, Communication Layer on page 28, and Using SNL or SAG to Generate Signature in XML-DSIG format on page 60.
- **Alliance Gateway**

  For the sole purpose of administering the certificates through the SWIFTNet Online Operations Manager and accessing U2A with HSM-based certificates and to generate/verify digital signatures based on SWIFTNet PKI. Other features of Alliance Gateway may be used by the customer that fall outside the scope of SWIFT's Solution for ESMIG, for example, the use of Alliance Gateway as a communication interface. For further details, see Network Connectivity on page 28 and Communication Layer on page 28.
- **Alliance Gateway Instant (AGI)**

  Communication interface to support the use of the SWIFTNet Instant messaging service to exchange instant messages, see Specific A2A Messaging Flows for TIPS on page 15, Specific Messaging Features for TIPS on page 26, and Communication Layer on page 28.
- **Messaging flows**

  ESMIG messaging flows are handled using SWIFTNet messaging, for which some options are constrained by the ESMIG requirements (see A2A Messaging Flows on page 13, Messaging Features on page 19, Specific A2A Messaging Flows for TIPS on page 15, Specific Messaging Features for TIPS on page 26, and Resilience of the Solution on page 29).
- **SWIFT central infrastructure**

SWIFT operates equipment and services located in SWIFT's operating centres (OPCs) that enable the network connectivity and support the required messaging flows. This includes SWIFT's ESMIG gateway that acts as a bridge between the customer and ESMIG. For more information, see A2A Messaging Flows on page 13.

- **SWIFT infrastructure at Eurosystem premises**

  As per the *ESMIG - Technical Requirements*, SWIFT provides the necessary infrastructure at ESMIG operator sites. This infrastructure acts as the gateway between the SWIFT network and ESMIG. The boundary between the SWIFT infrastructure and ESMIG is the demarcation line (as illustrated below) and is situated at the level of the SWIFT infrastructure used to provide SWIFT's Solution for ESMIG.

- **Support Module for ESMIG**

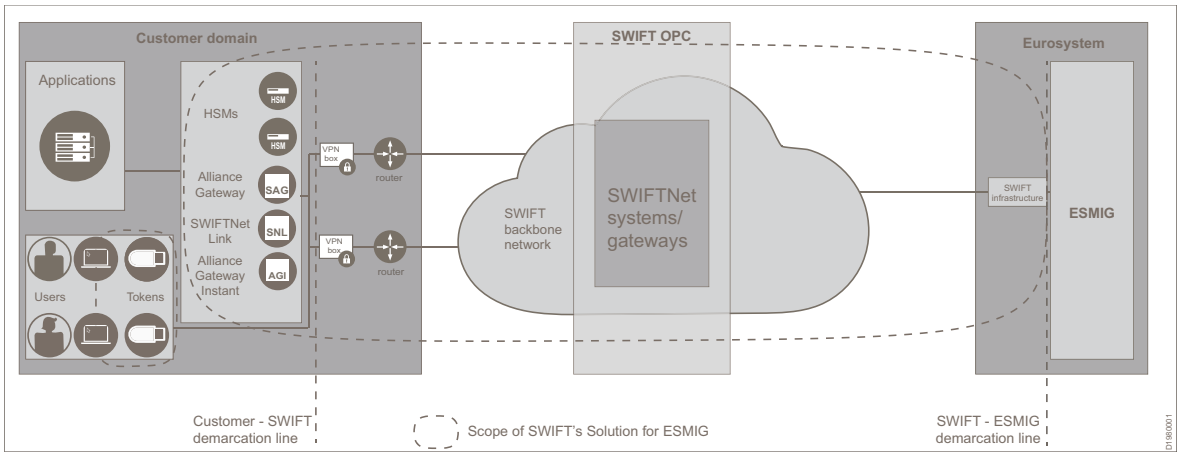
  In addition, SWIFT provides, as part of SWIFT's Solution for ESMIG, a 'SWIFT Support Module for ESMIG' (see SWIFT Support Module for ESMIG on page 35).

- **Other components**

  - 1 connected SWIFT destination (connected 8-character BIC)
  - 2 online own security officers
  - SWIFTSmart
  - Access to the SWIFT User Handbook

For high-level illustration: demarcation and main components of SWIFT's Solution for ESMIG

The following graphic provides a high-level illustration of the demarcation and main components of SWIFT's Solution for ESMIG:



The boundaries of SWIFT's responsibility for SWIFT's Solution for ESMIG are as follows:

- On the customers' side: the components of SWIFT's Solution for ESMIG to be installed and operated within the customer domain and the network connectivity components to access SWIFT's backbone network, including any components of SWIFT's Solution for ESMIG and the network connectivity components to access SWIFT's backbone network used by the Group Hub or Service Bureau selected by the customer to connect to SWIFT's backbone network.
- On the ESMIG operator side: the necessary infrastructure components to connect with ESMIG installed by SWIFT at the premises of the ESMIG operator.

Note *The ESMIG requirements under the Concession Contract have been designed for customers connecting within the European Economic Area (EEA) or Switzerland. It is also possible for customers to connect from outside the EEA or Switzerland based on specific conditions to be agreed with SWIFT (for example, certain maximum prices or KPIs might not apply). For further information, customers can contact their SWIFT Account Manager.*

The following sections describe in more detail each of the components and services that are part of SWIFT's Solution for ESMIG.

Key characteristics

SWIFT's Solution for ESMIG, which provides access to ESMIG, has the following key characteristics:

- SWIFT's Solution for ESMIG is based on existing services and products, such as SWIFTNet messaging, PKI certificates and related security management, security equipment, Alliance Connect Packs, lines and related equipment, Alliance Gateway, SWIFTNet Link, and Alliance Gateway Instant. Customers can use these services and products for their ESMIG operations or other purposes.
- Customers can subscribe to SWIFT's Solution for ESMIG for T2, T2S, ECMS, or TIPS, or any combination of those services. Also, for each service, it is possible to use A2A and U2A, or to use U2A only. For TIPS, it is possible to use the message and file channels separately.

For more information about the functionalities offered by ESMIG in the different messaging channels (U2A and A2A), see the relevant *User Detailed Functional Specifications (UDFS)* and the relevant *User Handbook* available on the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TARGET consolidation > For professional use.

Note *SWIFT's Solution for ESMIG provides an extra feature to ensure balancing of T2S traffic, in case strongly unbalanced traffic volumes are to be exchanged with T2S. This feature may be proposed to customers with very high volumes, as and when appropriate.*

2.2 Message Formats

Overview

ESMIG supports messages in the ISO 20022 format. SWIFT's Solution for ESMIG supports the transport of these messages using InterAct, FileAct, and SWIFTNet Instant messaging services (see A2A Messaging Flows on page 13 and Specific A2A Messaging Flows for TIPS on page 15).

Note *In the context of SWIFT's Solution for ESMIG, SWIFT does not validate the data content of messages or files exchanged.*

ESMIG functional specifications

For information about the message formats used for ESMIG messaging flows, and other related information, customers must refer to the relevant *User Detailed Functional Specifications (UDFS)* available on the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TARGET services, and the MyStandards platform, on which the Eurosystem publishes the standards for their services.

2.3 A2A Messaging Flows

This section describes the ESMIG A2A messaging flows that are common for T2, T2S, TIPS, ECMS, and potentially other future services offered by the Eurosystem accessible through ESMIG connectivity. These exchanges use a proprietary ESMIG communication protocol (Data Exchange Protocol [DEP]). SWIFT shields customers from this communication protocol by operating a gateway at SWIFT that allows the customer to use the existing SWIFTNet messaging services.

The SWIFT-hosted gateway for the A2A ESMIG flows acts as a bridge between customers and ESMIG. This gateway accepts messages and files from customers using the existing SWIFTNet messaging services and delivers these messages and files to ESMIG using the ESMIG protocols as per the interface specifications defined by the ESMIG operator. Similarly, the gateway accepts messages and files from ESMIG and delivers these to customers using SWIFTNet messaging services.

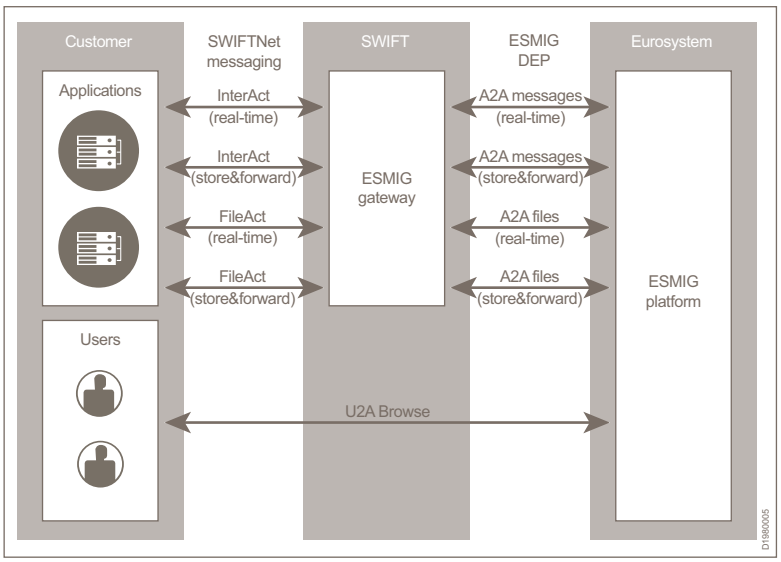
The messaging flows covered in this section are:

- A2A messaging to reach common ESMIG components (for example, to reach CRDM for common reference data management).
- A2A messaging flows to support specific business message or file flows (for example, for T2 and T2S).

The specific business messaging flows for instant payments for TIPS are covered in Specific A2A Messaging Flows for TIPS on page 15.

For information about the SWIFTNet messaging services and the specific roles and responsibilities related to SWIFTNet messaging (including SWIFT PKI and Hardware Security Modules [HSMs]), see the SWIFTNet PKI Service Description. Except where stated otherwise in this document, the principles set out in that service description apply.

SWIFT's ESMIG gateway acts as a bridge between the customer and ESMIG



Messaging channels

The supported messaging channels, and the use of these channels are defined in the documentation provided by Eurosystem in particular in the *User Detailed Functional Specifications (UDFS)* available on the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TARGET services.

SWIFT's Solution for ESMIG uses the following messaging channels for A2A flows:

- **InterAct real-time**

  Typically used to query ESMIG, or to perform specific actions, and to obtain a response. If the answer can be provided quickly and is smaller than the ESMIG message limit, then it is returned in the InterAct response. Otherwise, ESMIG returns an indication, in the InterAct response, that the proper answer will be provided separately through the store-and-forward channel.

  In case SWIFT cannot deliver a real-time InterAct message to ESMIG within 60 seconds from the moment the message was sent, the SNL of the customer will generate a timeout locally. In this case, SWIFT does not deliver the message to avoid potential duplicate responses. The customer may resend the query to ESMIG.

  For more information, see the *User Detailed Functional Specifications (UDFS)* (Timeout Management and Oversized Data Management sections).

- **FileAct real-time**

  Multiple messages can be grouped in a file and sent over the file channel.

- **InterAct store-and-forward**

  This message channel is used, for example, to send instructions to ESMIG or to receive information from ESMIG, or both.

- **FileAct store-and-forward**

  This file channel is used, for example, to send instructions to ESMIG or to receive information from ESMIG, or both.

Identification of the TARGET Service

When customers exchange traffic with ESMIG using InterAct or FileAct, specific addressing DNs are used as responder (for traffic sent by customers) or requestor (for traffic received by customers). For the list of requestor and responder DNs per TARGET Service, see Header Fields on page 23.

Error handling

Customers can receive errors on the messaging level and on the business level. Messaging level errors can be generic SWIFTNet errors or specific errors related to SWIFT's Solution for ESMIG (generated by SWIFT's gateway or by ESMIG). Business level errors are documented in the *User Detailed Functional Specifications (UDFS)*.

Error handling for messaging level errors related to A2A flows is as follows:

- **Generic SWIFTNet errors**

  SWIFT returns the standard SWIFTNet error codes in case of generic SWIFTNet errors (for example, a CUG (Closed User Group) error for a customer who is not subscribed to the service).

- **For messages exchanged in real time**

  Specific errors related to SWIFT's Solution for ESMIG can be reported. Such an error is present in the InterAct response message.

- **For files exchanged in real time**

  Errors detected by SWIFT's ESMIG gateway can be returned by using the normal FileAct reject protocol, whereby the RejectDescription and RejectInfo contain the appropriate information. Some errors can also be returned in the FileAct delivery notification (`Sw.AckFileRequest`), as is the case for errors reported by ESMIG. Note that the FileAct delivery notification is mandatory

for real-time file transfers (see Mandatory Use of Delivery Notification for FileAct Real-time on page 20).

- **For messages and files sent in store-and-forward mode**

  Error reporting is performed through the delivery notification (or the failed delivery notification) mechanism after the message or file has been delivered to SWIFT. The AckInfo contains the ESMIG error codes and the AckDescription contains the error text.

For an overview of the error codes related to SWIFT's Solution for ESMIG, see Knowledge Base article 5019756.

Specific rules

The use of SWIFTNet messaging services in the context of SWIFT's Solution for ESMIG is very similar to the use and the operation of other SWIFTNet messaging services. However, some specific rules apply when using SWIFT's Solution for ESMIG. For further information about these rules, see Messaging Features on page 19.

Certificates

For A2A traffic flows, customers must follow the existing requirements related to the use of SWIFTNet certificates. Customers can use existing certificates or decide to create specific ones for ESMIG traffic flows.

Message integrity

SWIFT's Solution for ESMIG message flow is secured. For the connection between SWIFT and ESMIG, the session layer integrity is provided by a mutual authenticated TLS session established between ESMIG and SWIFT. SWIFT validates that the messages exchanged with ESMIG conform to the proprietary ESMIG communications protocol format.

For those messages that are signed by ESMIG, message level integrity is verified by validating the PKI signature and the status of the certificate used for signing. For the connection between customers and SWIFT, the standard SWIFTNet integrity control applies.

Proof of delivery

Customers who want to keep non-repudiation evidence for A2A transactions (that is, traffic sent to ESMIG over the store-and-forward channel) must select the delivery notification option. This notification provides the signature of the delivery acknowledgement issued by ESMIG. For more information about support for delivery notifications, see Support for Enhanced Delivery Notification System Messages on page 20. For more information about signature verifications, see Verifying Signatures on page 61.

2.4 Specific A2A Messaging Flows for TIPS

In addition to the A2A messaging flows described in A2A Messaging Flows on page 13, customers who connect to the TIPS platform for the exchange of messages and files, specifically in the context of instant payment messaging flows, can use the SWIFTNet messaging services, as defined below:

- **Messages**

  SWIFTNet Instant is the messaging service that is designed to provide the required characteristics needed for instant messaging, that is, message exchanges with low latency, in a 'fire-and-forget' (at most once) delivery mode, with notification and technical acknowledgement options.

- **Files - store-and-forward**

These flows are supported by the FileAct store-and-forward messaging service (delivery of files from TIPS to the customers). The store-and-forward mode allows the TIPS application to send the files to SWIFT independent of the availability of the receiving customers, who receive the files when they connect to SWIFT using the appropriate service name. It is the same service as used for other TIPS file flows, referred to in A2A Messaging Flows on page 13.

For information about the SWIFTNet messaging services and the specific roles and responsibilities related to SWIFTNet messaging, SWIFT PKI, and Hardware Security Modules (HSMs), see the SWIFTNet Service Description and the SWIFTNet PKI Service Description. For more information about Alliance Gateway Instant, the mandatory software to access and use SWIFTNet Instant, see the Alliance Gateway Instant Service Description. Except where stated otherwise in this document, the terms and conditions set out in these service descriptions apply to the provision and use of SWIFT's Solution for ESMIG.

Messaging channels

The supported messaging channels (U2A and A2A) and the use of these channels are defined in the documentation provided by Eurosystem in particular in the relevant *User Detailed Functional Specifications (UDFS)* available on the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TIPS > For professional use.

Identification of parties on SWIFTNet

BICs serve as identifiers or as part of network addresses, or both, for the transfer of messages and files between the customers and the TIPS platform. The ESMIG operator for the TIPS application is identified by the BIC `TRGTXETP`.

Error handling

Customers can receive errors at the messaging level and at the business level. Messaging level errors can be generic SWIFTNet errors (generated locally or centrally at SWIFT OPC). Business level errors are documented in the relevant *User Detailed Functional Specifications (UDFS)*.

Examples of messaging level errors are: a Closed User Group (CUG) error for a customer who is not activated on the service, or a message size error for a message that exceeds the maximum message size. For more information on possible error codes, see the SWIFTNet Link Error Codes and the Alliance Gateway Instant User Guide.

Certificates

For A2A traffic flows, customers must follow the standard requirements related to the use of SWIFTNet certificates. Customers must also create dedicated certificates per Alliance Gateway Instant.

For FileAct, customers can re-use existing certificates or decide to create specific ones for TIPS traffic flows.

2.5 User-to-Application Flows

Overview

SWIFT provides access to the ESMIG browser-based services over SWIFTNet through a browser-based solution that is designed to support the specific ESMIG U2A flows. Customers can use the ESMIG U2A solution as part of:

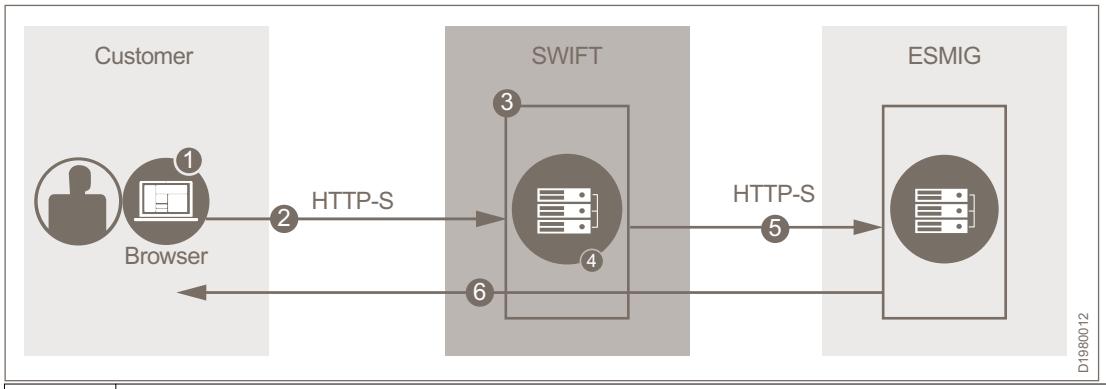
- a 'standard ESMIG access' solution in conjunction with the A2A mode
- a 'low-volume U2A access' solution.

The U2A access solution is available over MV-SIPN and over the Internet (for Alliance Cloud customers only). For setup information, see the SWIFT's Solution for ESMIG - U2A Setup Guide.

Customers can access the ESMIG U2A platform using one of the following solutions, which are described in the following sections:

- The ESMIG U2A SWIFT Login Application v2.x, a java-free solution.
- An automatically downloaded java proxy solution.

User-to-application flows based on the ESMIG U2A SWIFT Login Application v2.x



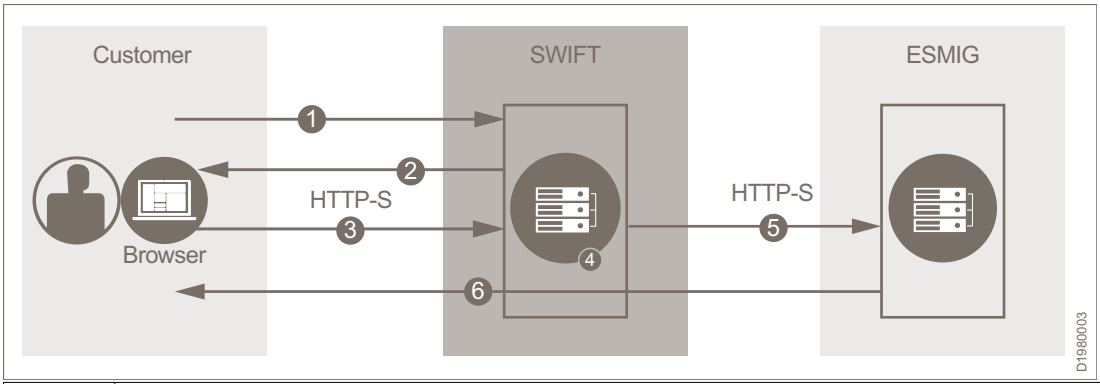
1	End user logs in to the ESMIG U2A SWIFT Login Application v2.x
2	End user enters URL and (through local .pac proxy file) reaches SWIFT (HTTP-S).
3	End user has to authenticate using its credentials (such as a token PIN).
4	SWIFT verifies that the user's certificate DN is allowed to access the relevant service (CUG).
5	SWIFT forwards connection request to ESMIG.
6	Transport Layer Security (TLS) handshake from ESMIG and end-to-end HTTP-S session is established.

When an end user enters a URL to connect to a web portal of an application reachable through ESMIG, SWIFT performs an access control check so that only end users of subscribed customers can access the relevant U2A service. This consists of a CUG (Closed User Group) check on the level of the end user's certificate DN. Upon successful completion of the CUG check (and other security checks, such as, a check on certificate validity), an end-to-end TLS session is established with the web portal.

End users must use the same certificate for the authentication with SWIFT and to connect to the ESMIG U2A application.

User-to-application flows using the automatically downloaded java proxy

Important The java-based proxy solution will be phased out in November 2023 and will not support the access to the ECMS U2A application. To access the ECMS applications over the U2A channel, the use of the ESMIG Login Application will be mandatory.



1	End user enters URL and (through local .pac proxy file) reaches SWIFT (HTTP-S).
2	SWIFT java code is downloaded to end user workstation for authentication process.
3	SWIFT java code asks the end user to enter credentials (such as a token PIN).
4	SWIFT verifies that the user's certificate DN is allowed to access the relevant service (CUG).
5	SWIFT forwards connection request to ESMIG.
6	Transport Layer Security (TLS) handshake from ESMIG and end-to-end HTTP-S session is established.

When an end user enters a URL to connect to a web portal of an application reachable through ESMIG, SWIFT performs an access control check so that only end users of subscribed customers can access the relevant U2A service. This consists of a CUG (Closed User Group) check on the level of the end user's certificate DN. Upon successful completion of the CUG check (and other security checks, such as, a check on certificate validity), an end-to-end TLS session is established with the web portal.

End users must use the same certificate for the authentication with SWIFT (steps 3 and 4 in the above graphic) and to connect to the ESMIG U2A application (step 6).

Personal certificates

End-user certificates for ESMIG U2A must be of type personal certificate, and stored on a personal token or on an HSM box.

The customer's security officers can manage the personal token certificates and personal HSM certificates through the SWIFTNet Online Operations Manager, both for those stored on personal tokens as well as for those stored on HSMs.

When personal tokens are used, the certificates are set up on the tokens and end users can access a number of functions to manage the token (such as, activate a token, change the password) directly through the SWIFT Certificate Centre. For more information about HSM-based certificates, see the SWIFTNet PKI Certificate Administration Guide.

Customers must ensure that their end users renew their personal certificates manually when they reach the renewal period. For tokens, this is done through the SWIFT Certificate Centre.

Note *It is important that customers correctly configure their network, browser, and other settings to ensure that U2A flows function correctly. For example, due to the use of end-to-end TLS by ESMIG, customers must not in any way interrupt the end-to-end TLS session (something that is typically done by an authenticating proxy). For the necessary configuration details, see* Related information *on page 19.*

Related information

The following documents or sections provide additional information:

- For certificate management (including setting up a certificate for use on a personal token), see the SWIFTNet Online Operations Manager User Guide available at www.swift.com > Documentation.
- For personal tokens, see the SWIFT Certificate Centre - Getting Started with your Personal Token available at www.swift.com > Documentation.
- For token drivers, URLs for U2A, browser configuration requirements, supported browsers and platforms, and when using ESMIG U2A services in a terminal services environment like Citrix, see Overview of Service Names (A2A) and URLs (U2A) on page 54.

More technical details are published on our SWIFT's Solution for ESMIG Support Page as they become available.

2.6 Messaging Features

Note *Customers should also refer to Specific Messaging Features for TIPS on page 26 for messaging features that are specific in the context of connecting to TIPS.*

2.6.1 TARGET Services Environments

For each of the different TARGET Services (for example, T2, T2S, TIPS, and ECMS) ESMIG provides a production environment and different test environments. For each of these environments, SWIFT makes available application-to-application and user-to-application flows (see A2A Messaging Flows on page 13 and User-to-Application Flows on page 16) through a set of dedicated SWIFTNet messaging services, Closed User Groups (CUGs), and URLs for U2A flows. Customers access the production environment by means of the corresponding SWIFTNet live services or URLs. Customers access each of the test environments by means of the corresponding SWIFTNet pilot services or URLs.

For the exact names of these SWIFTNet messaging services, see Overview of Service Names (A2A) and URLs (U2A) on page 54.

2.6.2 Maximum Messages and File Sizes

The ESMIG requirements impose maximum sizes for the message and file channels. Therefore, SWIFT performs checks on message and file sizes (for the message and file flows specifically in the context of instant payment flows for TIPS, see Specific Messaging Features for TIPS on page 26).

The maximum sizes supported by ESMIG are lower than what is normally supported as maximum size on SWIFTNet and are currently as follows:

- For the message channel (InterAct), the maximum size is 32 KB.
- For the file channel (FileAct), the maximum size is 32 MB (if the file is compressed, then the maximum uncompressed size is 99 MB).

Note *These maximum sizes apply to the data as provided, by the customers or their application, to SWIFTNet Link.*

Note *Customers must ensure that their applications or interfaces can process compressed data received from ESMIG. For the message channel, this is relevant if applications expect that a message after decompression cannot exceed 100 KB. To avoid the risk that decompressed messages exceed 100 KB, customers can configure the ESMIG static data to have such flows delivered through the file channel. For files, the decompressed file data can be up to 99 MB in size. Customers must ensure that their systems can handle such data sizes.*

2.6.3 Mandatory Use of Delivery Notification for FileAct Real-time

Customers must select the 'delivery notification' option when sending a file on a FileAct real-time service for TARGET Services such as T2 or T2S (`Sw:AckIndicator=TRUE`) in order for SWIFT to always be able to provide the delivery notification to the sender after the file transfer. If the file is acknowledged positively by ESMIG, then the delivery notification contains `Accepted=TRUE`.

If the file is not acknowledged positively by ESMIG, then the delivery notification contains `Accepted=FALSE` and the AckDescription and AckInfo contain the error detected.

Note *The customer should not provide any AckDescription or AckInfo in the AckFileResponse because SWIFT does not analyse these fields.*

In case a customer sends a file to ESMIG, and does not request a delivery notification for a real-time file transfer, then SWIFT will reject the files using the normal 'Reject' FileAct protocol.

Note *For FileAct store-and-forward flows, the use of delivery notification remains optional.*

2.6.4 Mandatory Use of System Messages for Store-and-forward Delivery Notifications

When using SWIFTNet store-and-forward to send traffic to TARGET Services, SWIFT will send delivery notifications to the sender in certain scenarios. For example, if the sender requests a delivery notification, then SWIFT will send this notification to the sender upon successful delivery of the message or file to the recipient. Similarly, if the message or file could ultimately not be delivered, SWIFT automatically generates a failed delivery notification addressed to the sender.

Developers of interface software have two technical means to receive these delivery notifications, either as store-and-forward primitives or as system messages. In the context of TARGET Services, customers must use a system message approach to receive store-and-forward notifications. This means that `Sw:DeliveryNotificationViaSystemMessage` must be set to `TRUE` when sending store-and-forward messages or file transfers. This is required because SWIFT needs to provide additional information in some notifications (see Support for Enhanced Delivery Notification System Messages on page 20).

If customers send traffic on a TARGET store-and-forward service and do not use this system message approach, then store-and-forward will deliver the message or file to SWIFT's gateway, which will reject it by sending a failed delivery notification.

2.6.5 Support for Enhanced Delivery Notification System Messages

The ESMIG requirements require that customers can receive the signature of the technical acknowledgement as it was issued by ESMIG using the proprietary DEP protocol. SWIFT provides

this information in a field inside the relevant store-and-forward delivery notifications. Therefore, the customer's messaging interface must support the following delivery notifications:

- `xsys.011.001.02`: new version of the delivery notification system message
- `xsys.012.001.02`: new version of the failed delivery notification system message

These new versions are automatically used by SWIFT when a (positive or negative) technical acknowledgement with a signature coming from ESMIG must be provided to the customer.

In case the store-and-forward delivery fails for reasons not related to TARGET Services (for example, message or file delivery attempts exhausted or expired), then the failed delivery notification is provided in the original format `xsys.012.001.01`

2.6.6 Support for Message and File References

Overview

For operational, support, or reconciliation purposes, SWIFT provides, in certain fields, support for the following message identifiers as known by ESMIG:

- **ActorMessageId**

  Field provided to ESMIG for traffic sent to TARGET Services. It is composed by SWIFT's ESMIG gateway based on information from the sender. The maximum length of this field is 100 characters.

- **ESMIGMessageId**

  Field composed by ESMIG and provided to the receiving customer, for traffic received from ESMIG. The maximum length of this field is 100 characters.

- **SWIFTNet reference**

  Traffic exchanged through ESMIG can also be referred to by the usual SWIFTNet references that messaging interfaces already use (that is, 'SwiftRef' for InterAct and 'TransferRef' for FileAct). Note that this information is available to ESMIG as the 'Communication Id' (see Knowledge Base article 5019348).

For support purposes, customers should ensure that their application tracks and provides access to these message identifier fields. Customers should use the **ESMIGMessageId** when communicating with the ESMIG operator and the **SWIFTNet reference** when communicating with SWIFT Support. The **ActorMessageId** is common to the ESMIG operator and SWIFT.

InterAct message sent to ESMIG

SWIFT's ESMIG gateway concatenates the value of the **SwiftRequestRef** field with the value of **MsgId** from the **Sw:E2EControl** field, using a colon as separator. The result is provided to ESMIG as the **ActorMessageId**.

For messages sent in real-time, SWIFT will add to the InterAct response the **ESMIGMessageId** generated by ESMIG. This information will be present as an XML attribute **ESMIGMessageId** on the `SwInt:ResponsePayload` XML tag.

FileAct file sent to ESMIG

SWIFT's ESMIG gateway concatenates the value of the **SwiftRequestRef** field with the value of **MsgId** from the **Sw:E2EControl** field, using a colon as separator. The result is provided to ESMIG as the **ActorMessageId**.

For files sent in real-time, SWIFT will add within the **AckInfo** of the delivery notification, the **ESMIGMessageId** (if available) generated by ESMIG. More specifically, **Sw:AckInfo** will contain

`ESMIGMessageId=<id>`, where `<id>` is the ESMIGMessageId of the associated response file sent by ESMIG.

InterAct message received from ESMIG

SWIFT will add to the InterAct request the **ESMIGMessageId** generated by ESMIG. This information will be present as an XML attribute `ESMIGMessageId` on the `SwInt:RequestPayload` XML tag.

FileAct file received from ESMIG

The **ESMIGMessageId** is placed within the **FileInfo** field. If this is a real-time FileAct file transfer that is an answer to an earlier sent file, then the **FileInfo** field will also contain the same information as the **ActorMessageId** of the corresponding original file.

2.6.7 Handling of Compression

Overview

ESMIG allows its customers to send compressed data, and similarly, ESMIG provides compressed payload content to the customer.

SWIFT supports compression as follows:

- For the file channel (FileAct), in case customers send files that are compressed, or for files received from ESMIG that are compressed, this must be indicated using the **FileInfo** keyword `SwCompression=ZIP`. The only compression supported by ESMIG is ZIP. If the file is not compressed, then the **FileInfo** keyword must be `SwCompression=NONE`. Customers send the compressed data as a file using FileAct without any additional base64 encoding.
- For the message channel (InterAct), the same compression indication (`SwCompression=NONE` or `SwCompression=ZIP`) is used as an XML attribute in the `SwInt:RequestPayload` or `SwInt:ResponsePayload` XML tag. Customers must apply base64 encoding to the compressed data and use the result as the InterAct message payload.

For details on the compression method supported by ESMIG, see the relevant *User Detailed Functional Specifications (UDFS)* available on the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TARGET consolidation > For professional use. See also the note in Maximum Messages and File Sizes on page 19.

Compression algorithm (ZIP)

When a customer sends a compressed message or file to ESMIG, the filename inside the compressed archive is ignored. If the compressed archive contains more than one file, then only the first file is processed and additional files are ignored.

When a customer receives a compressed message or file from ESMIG, the filename inside the compressed archive is always 'message', and there is always only one file in the archive.

2.6.8 Header Fields

Service Name

The SWIFTNet **Service Name** field reflects the combination of:

- the applicable ESMIG application environment (for example, UTEST, PROD - see Configuration of Access to ESMIG Test and Production Environments on page 34)
- the applicable ESMIG messaging channel (real-time messages, real-time files, store-and-forward messages, store-and-forward files)

When exchanging traffic with ESMIG, the applicable service name must be used. For an overview of all service names, see Overview of Service Names (A2A) and URLs (U2A) on page 54.

Request Type

The **Request Type** field of InterAct messages or FileAct file transfers must be used based on the following convention:

- If the payload (or file contents) contains only a ISO 20022 message, then the **Request Type** contains the ISO 20022 message identifier.
- If the payload (or file contents) contains a Business File Header (BFH), the value `admi.xxx.file` can be used for the **Request Type**. It is possible to use the ISO message identifier in the Request Type in case all messages present have the same ISO message identifier. For T2S only, for backward compatibility reasons, `admi.xxx.t2sfile` can also be used.
- Otherwise, the message or file contains a flat file. For the **Request Type** for such flat files, see Knowledge Base article 5024663.

In the unlikely case that SWIFT would receive a request type from ESMIG that does not comply with the Request Type rules, SWIFT will replace it by `admi.xxx.unknowncontent`. Customers can use this to route the message or file to an error queue for investigation purposes.

Requestor DN

For messages sent by customers to ESMIG, this **Requestor DN** field is specified by the sender. This field value must match the entry that was registered during service provisioning (the provisioning forms allow either a specific Requestor DN, or a DN wildcard in the (sub)tree of the institution).

For messages sent by ESMIG to customers, the **Requestor DN** field is fixed and contains:

- For T2

Application	Requestor DN
Billing	cn=billing,o=trgtxepm,o=swift
Business Day Management (BDM)	cn=bdm,o=trgtxepm,o=swift
CLM	cn=clm,o=trgtxepm,o=swift
CRDM	cn=crdm,o=trgtxepm,o=swift
Datawarehouse	cn=dwh,o=trgtxepm,o=swift
ECONS	cn=econs,o=trgtxepm,o=swift

Application	Requestor DN
RTGS	cn=rtgs,o=trgtxepm,o=swift

- For T2S

Application	Requestor DN
Billing	cn=billing,o=trgtxe2s,o=swift
Business Day Management (BDM)	cn=bdm,o=trgtxe2s,o=swift
CRDM	cn=crdm,o=trgtxe2s,o=swift
Datawarehouse	cn=dwh,o=trgtxe2s,o=swift
T2S	cn=t2s,o=trgtxe2s,o=swift

- For TIPS

Application	Requestor DN
Billing	cn=billing,o=trgtxetp,o=swift
CRDM	cn=crdm,o=trgtxetp,o=swift

- For ECMS

Application	Requestor DN
ECMS	cn=ecms,o=trgtxecm,o=swift
BILL	cn=billing,o=trgtxecm,o=swift

This is irrespective of the ESMIG application environment or the messaging channel.

Responder DN

For messages sent by customers to ESMIG, the **Responder DN** field is fixed and always contains:

- For T2

Application	Responder DN
Billing	cn=billing,o=trgtxepm,o=swift
Business Day Management (BDM)	cn=bdm,o=trgtxepm,o=swift
CLM	cn=clm,o=trgtxepm,o=swift
CRDM	cn=crdm,o=trgtxepm,o=swift
Datawarehouse	cn=dwh,o=trgtxepm,o=swift

Application	Responder DN
ECONS	cn=econs,o=trgtxepm,o=swift
RTGS	cn=rtgs,o=trgtxepm,o=swift

- For T2S

Application	Responder DN
Billing	cn=billing,o=trgtxe2s,o=swift
Business Day Management (BDM)	cn=bdm,o=trgtxe2s,o=swift
CRDM	cn=crdm,o=trgtxe2s,o=swift
Datawarehouse	cn=dwh,o=trgtxe2s,o=swift
T2S	cn=t2s,o=trgtxe2s,o=swift

- For TIPS

Application	Responder DN
Billing	cn=billing,o=trgtxetp,o=swift
CRDM	cn=crdm,o=trgtxetp,o=swift

- For ECMS

Application	Responder DN
ECMS	cn=ecms,o=trgtxecm,o=swift
BILL	cn=billing,o=trgtxecm,o=swift

This is irrespective of the ESMIG application environment or the messaging channel.

For messages sent by ESMIG to customers, the **Responder DN** is the DN that the customer has configured in the ESMIG static data to be used as network address for the related traffic flow.

Note *The provisioning forms contain a section that allows customers to specify the routing rules for store-and-forward traffic received from ESMIG. The DN information in the SWIFTNet routing rule(s) needs to be defined in such a way that it matches (literally or through wildcards) the **Responder DN** defined in the ESMIG static data.*

2.6.9 Use of SWIFTNet Messaging Options for ESMIG

The SWIFTNet messaging services used for ESMIG do not support the SWIFTNet non-repudiation option. Customers can obtain proof of delivery for non-repudiation purpose by using delivery notifications for transactions sent over the store-and-forward channel to ESMIG (see A2A Messaging Flows on page 13 and Support for Enhanced Delivery Notification System Messages on page 20). Also, the SWIFTNet end-to-end signing option is not used for the flows between

customers and SWIFT's ESMIG gateway as there is already an end-to-end signature in the payload for business messages (that is, signature in the Business Application Header or Business File Header inside the message or file payload). Apart from the specific rules explained in the previous sections, the other options for SWIFTNet messaging remain available also for the traffic exchanged on the ESMIG SWIFTNet services. This includes, for example, the option to ask for non-delivery warnings, or to use the priority field, or to ask for an undelivered traffic report.

Note *Using the priority field will not imply any effect towards the ESMIG application as ESMIG does not support this notion from a network perspective.*

2.6.10 Unsuccessful Traffic Delivery (Store-and-Forward Flow)

For messages and files that customers send to ESMIG, information related to any delivery failure is provided through notifications as described in Mandatory Use of System Messages for Store-and-forward Delivery Notifications on page 20. Please note that a failed delivery notification indicates that SWIFT did not get an acknowledgement of delivery from the receiver and considers the delivery unsuccessful. The receiver may or may not have received the message or file. If the message or file did reach the receiver, then the receiver could possibly act on it, for example, by sending a business answer to the sender. Senders need to be aware (and prepared) that this could happen, even if a failed delivery notification was received from SWIFT.

For messages and files that customers receive from ESMIG, the normal store-and-forward delivery processing applies (see SWIFTNet Service Description).

If a customer has any doubt as to a possible failed delivery, then the customer can check if there were any alerts logged by their interface software, or check for any output sequence gap when opening the next session. To identify any undelivered message or file, customers can look for any missing entries by comparing their list of successfully received messages or files with the list of messages or files that ESMIG has sent (for example, by using the GUI provided by ESMIG through the U2A channel).

If necessary, customers can also contact SWIFT to obtain the reference (or references) of non-delivered messages or files and, based on this information, can contact the ESMIG operator or download any such message or file through the GUI provided by ESMIG.

2.7 Specific Messaging Features for TIPS

Note *Unless otherwise specified, the information in this section applies to application-to-application (A2A) flows only related to instant payments messaging flows, as described in Specific A2A Messaging Flows for TIPS on page 15.*

2.7.1 TIPS Environments

Customers can access the relevant production and test environments. For each of these environments, SWIFT makes available A2A and U2A flows (see Specific A2A Messaging Flows for TIPS on page 15 and User-to-Application Flows on page 16) through a set of dedicated SWIFTNet messaging services, Closed User Groups (CUGs), and URLs for U2A flows. Customers access the production and the test environments by means of the corresponding SWIFTNet services names or URLs.

For the exact names of these services, see Overview of Service Names (A2A) and URLs (U2A) on page 54.

2.7.2 Maximum Messages and File Sizes

The ESMIG requirements impose maximum sizes for the message and file channels. Therefore, SWIFT's Solution for ESMIG checks on message and file sizes. The maximum sizes for TIPS are:

- For the message channel (SWIFTNet Instant), the maximum size is 10 KB.
- For the file channel (FileAct), the maximum size is 1GB.

2.7.3 Support for Message and File References

For operational, support, or reconciliation purposes, SWIFT provides, in certain fields, support for the following message identifiers:

- **MsgRef header field**

  Business unique identifier assigned by the sender. For business messages it is a copy of the message identifier transported in the payload. For notifications generated by AGI it refers to the original message sent.

- **MsgNetworkRef**

  The reference assigned by SWIFT at the time of sending. The MsgNetworkRef is unique for each message send attempt. In case the same message is resent with a PossibleDuplicate equal to true, a new MsgNetworkRef is assigned.

For support purposes, customers must ensure that they can provide at least one of these identifiers.

2.7.4 Header Fields

Service

The **Service** field reflects the combination of:

- the applicable ESMIG environment (for example, CERT, PROD, see Configuration of Access to ESMIG Test and Production Environments on page 34)
- the applicable messaging channel (SWIFTNet Instant or FileAct store-and-forward)

When exchanging traffic with ESMIG, the applicable service name must be used. For an overview of all service names, see Overview of Service Names (A2A) and URLs (U2A) on page 54.

Message Type

The **Message Type** field of SWIFTNet Instant must contain the ISO 20022 message identifier.

For files received from ESMIG, the RequestType field will contain the indication of the type of data.

Sender

For messages sent by customers to ESMIG, this **Sender** field is specified by the sender and contains the sender's DN. This field value must match the entry that was registered during service subscription (the subscription to SWIFT's Solution for ESMIG allows either a specific Requestor DN, or a DN wildcard in the (sub)tree of the institution).

For messages sent by ESMIG to customers, the Sender field is fixed and contains `cn=tips,o=trgtxetp,o=swift`, irrespective of the environment or the messaging channel.

Receiver

For messages sent by customers to ESMIG, the **Receiver** field is fixed and contains `cn=tips,o=trgtxetp,o=swift`, irrespective of the ESMIG environment or the ESMIG messaging channel.

For messages sent by ESMIG to customers, the **Receiver** is the DN that the customer has configured in the ESMIG static data to be used as network address for the related traffic flow

Note *The subscription form to SWIFT's Solution for ESMIG contains a section that allows customers to specify the store-and-forward traffic queue(s) to be used for the traffic received from ESMIG. Also the Alliance Gateway Instant (AGI) configuration contains routing rules for traffic received. The DN information specified in the **Receiver** field in the routing rule(s) needs to be defined in such a way that it matches (literally or through wildcards) the corresponding information defined in the ESMIG static data.*

2.8 Network Connectivity

SWIFT's Solution for ESMIG allows for various backup/alternative network access solutions and procedures to support business continuity planning. For further details, see the Connectivity Packs - Configurations for Multi-Vendor Secure IP Network Connectivity.

Also, the *Alliance Connect - Resiliency Testing Scenarios* can help customers develop their connectivity resilience (continuity of business) scenarios as well as the Resilience Guide, which provides general practical recommendations for building an appropriate level of resilience (that is, availability and reliability) for their applications.

For an overview of the Alliance Connect offerings, see www.swift.com > Alliance Connect.

Network requirements

Customers must set up their communication infrastructure (network software or devices such as firewalls, proxies) so that the required ESMIG flows are enabled. For details about the network requirements, see Network Configuration Requirements on page 58.

2.9 Communication Layer

SWIFTNet Link

Customers who connect to ESMIG must have or have access to SWIFTNet Link to exchange messages and files using InterAct or FileAct.

The ESMIG U2A flows and the TIPS instant messaging (SWIFTNet Instant) do not use the SNL software.

For the specific roles and responsibilities related to SWIFTNet Link, see the SWIFTNet Link Service Description. Except where stated otherwise in this document, the principles set out in these service descriptions apply.

Communication interface

Alliance Gateway is part of SWIFT's Solution for ESMIG, for the sole purpose of administering the certificates through the SWIFTNet Online Operations Manager and accessing U2A with HSM-based certificates. Optionally, Alliance Gateway can also be used for the messaging flows to and from ESMIG (InterAct, FileAct).

There are no changes to the communication software (such as, Alliance Gateway) required for exchanging messages and files using InterAct or FileAct.

For the specific roles and responsibilities related to Alliance Gateway, see the Alliance Gateway Service Description. Except where stated otherwise in this document, the principles set out in that service description apply.

Alliance Gateway Instant

Customers who connect to ESMIG to access TIPS and need to exchange messages with SWIFTNet Instant must use the communication software Alliance Gateway Instant (AGI). AGI acts as a local gateway between a customer's business application and the SWIFT network.

For more information and for the specific roles and responsibilities related to Alliance Gateway Instant, see the Alliance Gateway Instant Service Description. Except where stated otherwise in this document, the principles set out in this service description apply.

2.10 Resilience of the Solution

Overview

SWIFT's Solution for ESMIG benefits from the resilience of the overall SWIFTNet infrastructure.

Disaster recovery

In the case of a failure of all of the primary operating centres, and without prejudice to applicable service levels (if any), SWIFT will initiate the appropriate recovery procedures with a view to restore access to ESMIG as soon as possible. SWIFT provides a disaster recovery solution that allows to restart from an empty state ('cold' start) in the unlikely event of the loss of the primary sites. In such an event, SWIFT cannot guarantee that the data that was stored at SWIFT operating centres will still be available at the time of service restoration. Therefore, customers must follow the normal recommendations related to recovering from a disaster scenario, such as resending messages or files with possible duplicate indication, as set out in more detail in the SWIFTNet Service Description or otherwise notified by SWIFT.

2.11 Data Retention

SWIFT supports customers who need to resend traffic, by allowing to retrieve traffic that was exchanged in store-and-forward mode. For live traffic, SWIFT allows customers to retrieve InterAct messages during a period of 124 days, and FileAct files during a period of 5 days. For pilot services, traffic can be retrieved during 4 days.

As per ESMIG requirements, SWIFT retains a copy of all messages and files exchanged between customers and ESMIG for retrieval by the Eurosystem during a period of 6 months. SWIFT deletes such data thereafter as per a regular housekeeping process.

2.12 Security

2.12.1 SWIFTNet Public Key Infrastructure

For an overview of the SWIFTNet Public Key Infrastructure, see the SWIFTNet PKI Service Description. Except where stated otherwise in this document, the principles set out in that service description and section references apply.

2.12.1.1 Certificates Used by ESMIG

Business certificate for payload signing by ESMIG

In addition to the detailed description of the SWIFTNet PKI certificates in the SWIFTNet PKI Service Description, an additional certificate class has been introduced, that is, business certificate for payload signing by ESMIG. Payload signing is used by ESMIG, in the context of T2 and T2S, for the signature in the Business Application Header (BAH) and Business File Header (BFH). The signature must be built according to the rules defined in the relevant *User Detailed Functional Specifications (UDFS)* available on the European Central Bank (ECB) website at www.ecb.europa.eu > Payments & Markets > TARGET consolidation > For professional use.

This business certificate for payload signing by ESMIG is identified by Policy ID 1.3.21.6.3.10.100.2. This class of digital certificates is used by ESMIG to sign message (and file) payloads and is also used for the signature of technical acknowledgements (as and when provided by ESMIG) present inside the enhanced delivery notifications (see Support for Enhanced Delivery Notification System Messages on page 20).

The validity period of digital certificates in this class is 24 months. For more information about how to use SNL or SAG to generate or verify a signature, see Using SNL or SAG to Generate Signature in XML-DSIG format on page 60.

Customers can check certificate revocation status information by using the appropriate functions.

Strong level of authentication

This class of digital certificates provides customers with a strong level of authentication and non-repudiation. Customers who receive InterAct or FileAct messages in which the payload contains a signature with a certificate of this class can process this payload as described in the arrangements between the customer and by the ESMIG operator directly.

2.12.1.2 Certificates Used by the Customer

The certificate usage in SWIFTNet InterAct, FileAct, and SWIFTNet Instant traffic is described in the SWIFTNet PKI Service Description, and is applicable without modification. That document also describes the personal certificates that are used in the context of SWIFT's Solution for ESMIG (stored either on a personal token or an HSM box).

In order to support non-repudiation of origin (NRO) for some U2A flows, and until June 2022, the personal tokens used for T2S need to have two certificates, one used for authentication purpose and one used for non-repudiation of origin purpose.

Security officers can select the 'dual' option for the certificate class when administering the certificates for use with personal tokens. Personal tokens that were created with a single certificate can be converted to contain two certificates.

In all other cases (for example, customers only accessing T2 U2A or TIPS U2A) do not need tokens with two certificates.

Customers or business senders must use their regular SWIFTNet PKI certificates for payload signing in the Business Application Header (BAH) and the Business File Header (BFH).

Certificates used to sign the BAH and the BFH for live traffic must be stored on a SWIFT-provided HSM.

For the certificate usage in the context of BAH and BFH, see the SWIFTNet PKI Service Description, except for the revocation status check performed by ESMIG on the certificates used by the customers to sign the BAH and BFH, where the customer must refer to the documentation provided by the ESMIG operator.

Note *The Eurosystem has defined the concept of 'business sender' and 'technical sender', which the customer may have to agree upon and implement in coordination with another ESMIG actor, which could either be a party running the customer's operations, or a party for which the customer is running operations. For more information, contact the ESMIG operator or refer to the relevant documentation (see www.ecb.europa.eu > Payments & Markets > T2S > TARGET services).*

2.12.2 Security Monitoring

Use of data for security monitoring and investigation purposes

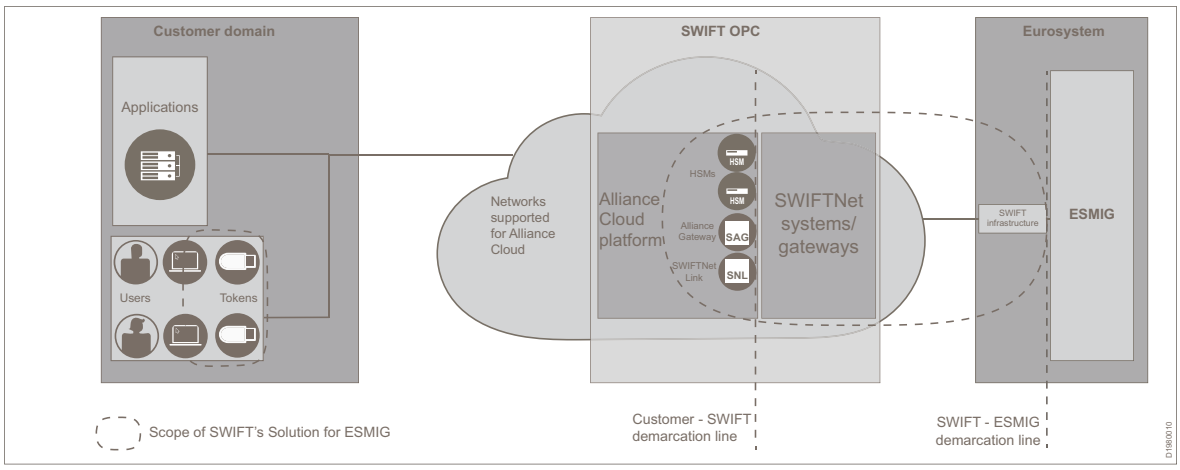
In accordance with the SWIFT Data Retrieval Policy and the Distributed Architecture principles, SWIFT may process and store traffic and message data in order to support SWIFT's protection measures and forensic capabilities against cybersecurity threats. SWIFT processes and stores such data on dedicated security systems and in strict accordance with its security policies and procedures and may analyse such data in the context of a specific security investigation as part of its security monitoring and investigation processes.

2.13 Alternative Options to Access SWIFT's Solution for ESMIG

Instead of connecting through their own local SWIFT connectivity infrastructure, customers may also decide to connect to SWIFT's Solution for ESMIG through a SWIFT connectivity infrastructure operated by a third party (typically, a Group Hub or Service Bureau), or through a SWIFT-operated connectivity infrastructure such as SWIFT's Alliance Cloud.

When connecting through a SWIFT-operated connectivity infrastructure, SWIFT operates all necessary connectivity infrastructure components in the SWIFT OPCs (operating centres) and, consequently, SWIFT's Solution for ESMIG does not include the provision of lines and related equipment.

Alliance Cloud is one example of a SWIFT-operated connectivity infrastructure. The following graphic provides a high-level illustration of the scope, demarcation line, and main components of SWIFT's Solution for ESMIG when connecting through Alliance Cloud. When connecting through Alliance Cloud, customers can access both A2A and U2A flows with the exception of the A2A Instant Messaging flows, which are only supported through the customer's own local SWIFT connectivity infrastructure as described in Scope of SWIFT's Solution for ESMIG on page 10 or through a SWIFT connectivity infrastructure operated by a third party.



3 Pricing and Invoicing

The Price List for SWIFT's Solution for ESMIG and the Pricing and Invoicing - Ordering, Invoicing, and Payment describe and set out the prices applicable to customers for SWIFT's offering and applicable invoicing and payment conditions.

4 Ordering and Subscription

4.1 Ordering

Order SWIFT services and products

To use SWIFT services and products, a customer must subscribe to, or order, the relevant services and products. In all cases, customers must subscribe to SWIFT's Solution for ESMIG to access all relevant ESMIG environments.

In addition to the service subscription, customers can order all necessary components of SWIFT's Solution for ESMIG. The list of necessary components may vary depending on whether customers decide to connect directly or indirectly, or through a SWIFT-operated connectivity infrastructure, to deploy a dedicated or non-dedicated connectivity infrastructure.

Customers must, before ordering any SWIFT services and products for their use of SWIFT's Solution for ESMIG, always contact their SWIFT Account Manager to discuss their specific requirements and obtain a specific quotation. Where applicable, this quotation must be referenced in the subscription to SWIFT's Solution for ESMIG and when ordering the other necessary components.

Related information

For information about:

- SWIFT's online ordering facility and how to order, see www.swift.com > Ordering.
- Pricing and invoicing, see Pricing and Invoicing on page 32 and the Price List for SWIFT's Solution for ESMIG.

4.2 Subscription and Configuration

This section describes the two independent steps related to the subscription to, and configuration of the customer access to, SWIFT's Solution for ESMIG.

4.2.1 Subscription

The subscription to SWIFT's Solution for ESMIG is performed through the use of the relevant subscription e-form, available at www.swift.com > Ordering A-Z > SWIFT's Solution for ESMIG.

Certain conditions must be met for the customer to be activated on SWIFT's Solution for ESMIG, including:

- to have entered into all relevant agreements, with the Eurosystem or other parties concerned, to be permitted to access ESMIG and, for the Di.Co.A.s, to use all relevant TARGET services or applications.
- to provide all necessary configuration data for their configuration (see Configuration of Access to ESMIG Test and Production Environments on page 34).

Customers who indirectly connect to the TIPS platform (typically a TIPS participant connecting through an instructing party and/or serving a reachable party that connects through an instructing party) must use a paper-based subscription form available upon request from their SWIFT Account Manager.

4.2.2 Configuration of Access to ESMIG Test and Production Environments

Customers who need to access the ESMIG test or production environments must provide the configuration details of their technical infrastructure set-up (for example, SWIFTNet address and routing rules).

The participation of the customer to the relevant Closed User Group (CUG) is subject to the approval of, as applicable, the relevant central bank or another Di.Co.A. (typically a CSD) and of the ESMIG operator.

The desired technical implementation date of the customer to access the test and production environments is selected by the customer during the activation process.

The actual implementation date of the customer data in the relevant Closed User Group (CUG) is subject to the approval, as applicable, of the relevant central bank or another Di.Co.A. (typically a CSD) and of the ESMIG operator.

The business implementation date of the customer on each of the relevant environments is not under the direct control of SWIFT and must be agreed upon between the customer and the ESMIG operator.

Changes to the technical infrastructure details of each environment can be performed at a later stage through the change configuration option available at www.swift.com > Ordering and Support > Change, replace & upgrade.

5 Support

SWIFT Support services

Except where stated otherwise in this document or other relevant service descriptions, the principles set out in the SWIFT Support documentation apply (typically, the SWIFT Community Support Service Description and, as the case may be, the SWIFT Advanced Support and Care Services Service Description).

Overview

By default, SWIFT is the single point of contact to report all problems and queries that relate to SWIFT services and products. Support is available to all customers. Individuals within a customer organisation must be registered users of the customer on swift.com. For more information about how to register for Support, see the Customer login section on www.swift.com.

SWIFT provides global Support services to all its customers, 24 hours per day, 7 days a week, for all SWIFT services and products in accordance with the support level to which the customer subscribes and subject to the other terms of this Support section.

Additional support features

SWIFT displays the operational status of the SWIFT services at www.swift.com > Support > SWIFT Operational Status.

Registered users can subscribe to receive e-mail notifications specifically about changes to the operational status for SWIFT's Solution for ESMIG.

Customers can subscribe to this notification service, on the SWIFT Operational Status page or on the myProfile notifications.

5.1 SWIFT Support Module for ESMIG

Overview

Subject to the other terms of this service description, customers subscribing to SWIFT's Solution for ESMIG will continue to benefit from all the existing Support features of their SWIFT Support package. On top of this, customers will automatically benefit from additional Support features for their use of SWIFT's Solution for ESMIG (as listed under Additional Support features on page 35).

Optionally, customers can at any time upgrade to a higher payable Advanced Support service.

For more information about SWIFT's Support offering, see Support and Care Services.

Additional Support features

The SWIFT Support Module for ESMIG comes with specific Support features designed to assist customers in using SWIFT's Solution for ESMIG.

The SWIFT Support Module for ESMIG is automatically provided to all customers subscribing to SWIFT's Solution for ESMIG without the need for a separate order or subscription and complements the customer's existing Support package as follows:

- **Coordination of 3-way problem resolution**

In the case of an incident with impact 'blocking' or 'severe' and with urgency 'critical' (as defined in Fault Clearance (Failure Resolution Times) on page 40), the customer may contact SWIFT Support to initiate the *coordination of 3-way problem resolution* with the ESMIG operator.

SWIFT Support will then contact the ESMIG operator helpdesk without any undue delay, if this would help resolving the incident. SWIFT Support continues to coordinate the incident resolution until resolved or until handover to the ESMIG operator helpdesk for further handling with the customer.

- **Proactive Monitoring and Alerting** to notify upon lost SNL and/or AGI connectivity events, for any SNL and/or AGI interfaces used for one or multiple ESMIG services in the production environment (for those customers connecting through a local SNL or AGI connectivity infrastructure). In order for alerts to be routed to the correct operational contacts, it is the customer's responsibility to assign them the 'SWIFT Operational Helpdesk (Level 1)' and backup roles through MySWIFT > My tools > My profile and account > Contact Roles > Operations and Support Customer Escalation.
- **Remote Access** to SWIFTNet Link (SNL) and/or Alliance Gateway Instant (AGI) (for those customers connecting through a local SNL or AGI connectivity infrastructure). In agreement with the customer, and if conditions and circumstances allow for it, SWIFT can remotely access the customer's computer in order to troubleshoot and diagnose critical problems efficiently. For more information about the Remote Access service, see the SWIFT Advanced Support and Care Services Service Description.

6 Service Levels

This section contains the customer and SWIFT responsibilities in relation to the service levels offered to customers subscribed to SWIFT's Solution for ESMIG. It also defines the Key Performance Indicators (KPIs) used to measure the service levels related to the provision and the use of SWIFT's Solution for ESMIG.

These service levels apply to the provision and the use of SWIFT's Solution for ESMIG to access the ESMIG production environment only. They become effective as of the first calendar month following the technical activation of the customer in that environment.

6.1 SWIFT's Responsibilities

As a general principle, SWIFT is responsible for:

- managing the availability of SWIFT's Solution for ESMIG and the SWIFT-operated components of SWIFT's Solution for ESMIG, including informing customers of SWIFT messaging maintenance periods through www.swift.com > Ordering and Support > Operational status.
- supporting the ESMIG operator, including but not limited to providing access to information related to the creation, progress, and resolution of cases reported by a customer to SWIFT Support, as per the Failure Resolution Times KPIs specified in Fault Clearance (Failure Resolution Times) on page 40.
- providing information about the related KPIs available to the ESMIG operator, as specified in Reporting on page 44.

6.2 Customer's Responsibilities

The service levels related to the provision and the use of SWIFT's Solution for ESMIG apply if and to the extent each customer abides by all responsibilities and other mandatory instructions applicable to it in connection with the provision and the use of SWIFT's Solution for ESMIG.

Without prejudice to the generality of the foregoing:

- The customer must only use the releases or updates of SWIFT services and products that SWIFT currently supports, as specified in the SWIFT Release Timeline or as otherwise notified by SWIFT (for example, in a release letter, or elsewhere in this service description). Consequently, the customer must subscribe to applicable maintenance services and, when using software, install all new releases or updates and remove preceding releases or updates, by no later than the date specified in the SWIFT Release Timeline or otherwise notified by SWIFT (for example, in a release letter, or elsewhere in this service description). Failure to do so may lead to termination of the affected SWIFT services and products.
- The customer must regularly check the latest information made available by SWIFT (typically, through SWIFT's standard documentation or SWIFT Operational Status) regarding the conditions applicable to its use of SWIFT's Solution for ESMIG or its operational status, including but not limited to the published Support Knowledge Base tips.
- In case of problems, the customer must:
  - notify SWIFT Support by telephone of the problem as soon as practicable
  - assist SWIFT in identifying, investigating, and resolving the problem
  - progress a case, during its resolution period, through SWIFT's call and problem management process, as described in the relevant SWIFT Support documentation (typically, the SWIFT Community Support Service Description and, as the case may be, SWIFT

Advanced Support and Care Services Service Description). All cases reported to SWIFT Support must be processed through SWIFT's call and problem management process. For more information, see the 'Call and Problem Management Process' section of the relevant *SWIFT Support Service Description* (see www.swift.com > Support > Support and Care Services).

  - promptly correct the problem if it is the customer's responsibility to do so, and notify SWIFT when it has been resolved
  - respond correctly and promptly to any actions requested, recovery or fallback procedures initiated, or directions given by SWIFT to mitigate or resolve the problem, and revert to normal operation conditions when the problem is resolved.

- The customer must ensure qualified and suitably trained personnel is available at all times.
- The customer must provide timely information on any changes under its control that may affect the provision or use of SWIFT's Solution for ESMIG (for example, customers must inform SWIFT through the Configuration Browser or case management system about a planned maintenance, failover test, or an upgrade to Alliance Connect. For more information, see Knowledge Base article 1798719.
- The customer must inform SWIFT reasonably in advance when material traffic increase or decrease is planned so as to allow SWIFT to make an adequate long-term capacity planning.
- The customer must ensure to keep up-to-date with the obligations for any other subscribed product or services as set out in the relevant SWIFT service description.
- The customer is responsible for taking good care of its VPN boxes and for storing the spare VPN box in a safe place, easily reachable in case of replacement.

6.3 Key Performance Indicators (KPIs)

This section describes Service Availability Key Performance Indicator (KPI), the Connection Availability KPI, the Failure Resolution Times KPIs, and performance-related KPIs related to the provision and the use of SWIFT's Solution for ESMIG to access the ESMIG production environment during normal operations.

6.3.1 Service Availability

Overview

SWIFT's Solution for ESMIG is designed to offer a service 24 hours per day, 7 days per week as follows:

- SWIFTNet Instant and U2A access are operated to allow uninterrupted round-the-clock operations, every day of the year, with zero downtime.
- InterAct, FileAct, and the other components of SWIFT's Solution for ESMIG are operated to offer a service 24 hours per day, 7 days per week subject to SWIFT’s maintenance schedule described in the SWIFTNet Service Description. SWIFT’s maintenance schedule is consistent with the maintenance windows of the TARGET Services (for example, the T2/T2S weekend service downtime) and other official downtime windows scheduled by or for the ESMIG operator.

A2A service availability KPI

The A2A service availability Key Performance Indicator (KPI) is the percentage of time that the A2A services are available for all customers to send and to receive traffic (with no impact on performance). It measures the availability of the A2A-related components of SWIFT's Solution for

ESMIG in the SWIFT OPCs (operating centres), the SWIFT core network and the SWIFT infrastructure hosted at ESMIG operator sites, excluding:

- the components that fall within the scope of the Connection Availability KPI
- all connectivity infrastructure components operated by SWIFT (as described in Alternative Options to Access SWIFT's Solution for ESMIG on page 31)
- and, more generally, any component in the customer's and Eurosystem's domains.

The A2A service availability KPI is calculated, for each A2A service (such as T2, T2S, TIPS, and ECMS), using the following formula:

$$ServiceAvailability = \left(\frac{ServiceTime - OutageTime}{ServiceTime}\right) . 100$$

where:

- **Outage Time** is the sum of the outage time of each connected customer (in minutes) in the reporting period (excluding ESMIG service downtime if any) whereby outage means that such customer cannot send or receive messages to or from ESMIG. The outage time is computed per customer by adding the outage time for (1) the components of SWIFT's Solution for ESMIG in the SWIFT European OPCs (operating centres), (2) the SWIFT core network and (3) the SWIFT infrastructure hosted at ESMIG operator sites, and removing any overlaps to avoid double-counting.
- **Service Time** is the sum of the expected availability time of each customer (in minutes) in the reporting period (excluding any ESMIG service downtime windows).

The A2A service availability KPI shall not be less than 99,98 calculated on a monthly basis.

U2A Service Availability KPI

The U2A Service Availability Key Performance Indicator (KPI) is the percentage of time that the U2A services are available to the customers to access ESMIG web resources. It measures the availability of the U2A-related components of SWIFT's Solution for ESMIG in the SWIFT OPCs (operating centres) excluding the availability of those components that fall within the scope of the Connection Availability KPI and, more generally, any component in the customer's and Eurosystem's domains. It is calculated for each U2A service (such as T2, T2S, TIPS, and ECMS).

The U2A service availability KPI is calculated using the following formula:

$$ServiceAvailability = \left(\frac{ServiceTime - OutageTime}{ServiceTime}\right) . 100$$

where:

- **Outage Time** is the sum of the outage time of each connected customer (in minutes) in the reporting period whereby outage means that such customer cannot access ESMIG web resources (excluding any ESMIG service downtime windows). This could, for example, be caused by the complete loss of the then active SWIFT OPC.
- **Service Time** is the sum of the expected availability time of each customer (in minutes) in the reporting period (excluding any ESMIG service downtime).

The U2A Service Availability KPI shall not be less than 99,98 calculated on a monthly basis.

6.3.2 Connection Availability

Overview

SWIFT's Solution for ESMIG is designed to permit customers to connect 24 hours per day, 7 days per week, excluding ESMIG service downtime windows (for example, the T2/T2S weekend service downtime) and other official downtime windows scheduled by the ESMIG operator.

Connection Availability KPI

The Connection Availability Key Performance Indicator (KPI) is the percentage of time that the connection of customers is considered to be operational so that customers can access the A2A or U2A services. It measures the availability of the network connectivity components that are in the scope of SWIFT's Solution for ESMIG, excluding all components in the SWIFT OPCs (operating centres) and the non-network connectivity components in the customer's domain and ESMIG domain.

The KPI is calculated for each TARGET service or application (such as T2, T2S, TIPS, and ECMS).

The Connection Availability KPI is calculated using the following formula:

$$ConnectionAvailability = 100 - \frac{TotalOutageTime}{TotalServiceTime} . 100$$

where:

Total Outage Time is

$$TotalOutageTime = \sum_{i=1}^{n} d\_outage_i * nr\_DiCoAs\_affected_i$$

where:

- `i` identifies the outage
- `n` is the number of outages during the period
- `d_outagei` is the duration of the outage `i`
- `nr_DiCoAs_affectedi` is the number of customers affected by the outage `i` for a duration `d_outagei` (that is, if an outage has a different effect on different customers, it will be split and considered with different durations as per customer affected)

  Note *In case of an outage affecting the link between ESMIG and the SWIFT network, then the outage affects all the customers.*

Total Service Time is the product of (i) the total number of customers who are actively using SWIFT's Solution for ESMIG (within the limitation as defined in the Overview section in Key Performance Indicators (KPIs) on page 38) and (ii) the Service Time in minutes in the reporting period (excluding any ESMIG service downtime windows).

The Connection Availability KPI shall not be less than 99,999% calculated on a monthly basis.

6.3.3 Fault Clearance (Failure Resolution Times)

Overview

SWIFT provides global, follow-the-sun support to all its customers, 24 hours per day, 7 days a week, for all SWIFT services and products (including the lines and related equipment (if any) necessary for customers to access SWIFT's backbone network), as described in the relevant

SWIFT Support documentation (typically, the SWIFT Community Support Service Description or as the case may be, the SWIFT Advanced Support and Care Services Service Description).

All issues or incidents reported to SWIFT Support are tracked in the online case management system. The failure resolution times are calculated based upon these case interaction time stamps.

Failure resolution times

SWIFT measures failure resolution times by the use of the following two Key Performance Indicators (KPIs):

- Maximum Time To Intervene (see Maximum Time To Intervene (MxTTI) KPI on page 42)
- Maximum Time To Repair (see Maximum Time To Repair (MxTTR) KPI on page 43)
- Status Notification Interval (Maximum Status Notification Interval (SNI) KPI on page 43)

Scope of the Failure Resolution Time KPIs

The MxTTI and MxTTR and SNI KPIs apply to cases related to operational connectivity issues, as defined below, on the ESMIG production environment which result from a failure within SWIFT's Solution for ESMIG.

- Cases raised by telephone (not e-mail or the SWIFT online case management system) by the customer and related to its then active connection to ESMIG. More specifically, this covers the then active network connectivity components, messaging, SWIFTNet Public Key Infrastructure, and SWIFT central infrastructure gateways as defined in the scope of SWIFT's Solution for ESMIG (see the section Solution Description on page 10), excluding the security components SWIFTNet Link, Alliance Gateway, Alliance Gateway Instant, and other components of SWIFT's Solution for ESMIG not expressly listed above.
- For Premium Plus customers, cases raised by SWIFT on behalf of the customer as part of SWIFT proactive monitoring duties and regarding their use of the operational connectivity to SWIFT's Solution for ESMIG (as defined here above), and cases that the customer and its SWIFT Service Manager would agree to include in the scope of the failure resolution process during the monthly Service Meetings.

  The following are examples of cases that would not be considered as operational connectivity issues:

  - Cases related to implementations, which are typically cases where the customer or SWIFT informs of the event of an implementation or maintenance change. Such cases stay in general open for a longer period without interaction, and will not be taken into account for the service levels.
  - Duplicate cases
  - Cases as a follow-up of a survey

Priority, impact, and urgency levels

Priority levels

The following table lists the priority levels applicable to cases raised by the customer and related to operational connectivity issues. The priority levels in this table are classified based on the impact and the urgency assigned to the case (see tables Impact levels on page 42 and Urgency levels on page 42):

Priority level	Description
High	**Blocking and Severe** impact, with **Critical** urgency

Priority level	Description
Medium	**Major** impact, with **Critical** urgency
Low	All other combinations of Impact and Urgency levels

Impact levels

Impact level	Description
Blocking	A problem that prevents the use of SWIFT's Solution for ESMIG to access the ESMIG production environment.
Severe	A problem that causes serious disruption to the use of SWIFT's Solution for ESMIG to access the ESMIG production environment, or that potentially leads to a security issue.
Major	A problem that causes reduced functionality or degraded performance of SWIFT's Solution for ESMIG to access the ESMIG production environment, but still allows its use.
Minor	A problem whereby a non-critical feature of SWIFT's Solution for ESMIG to access the ESMIG production environment becomes unusable, but for which a workaround is possible.

Urgency levels

Urgency level	Description
Critical	Significant business/operational impact now or expected within 24 hours.
High	Significant business/operational impact expected between 2-4 calendar days.
Normal	Significant business/operational impact expected between 5-7 calendar days.
Low	Significant business/operational impact expected in more than 7 calendar days.

For further information about the classification levels, see the relevant *SWIFT Support Service Description*.

Maximum Time To Intervene (MxTTI) KPI

Definition: This Key Performance Indicator (KPI) defines the maximum time elapsed between the acceptance of a telephone initiated case by SWIFT and the start of the incident/problem clearing process, whereby the start of the clearing process is the first update made to case status or a primary analyst is assigned to the case.

Measurement: Based on the case logs and related time stamps as recorded in SWIFT's case management system.

Key Performance Indicators:

- For high priority issues: 0.5 hour
- For medium priority issues: 4 hours
- For low priority issues: 8 hours

Maximum Time To Repair (MxTTR) KPI

Definition: This KPI defines the maximum time between the acceptance of a telephone initiated case by SWIFT and service restoration. Service restoration means that either the service has been restored or SWIFT has notified the customer that a fix or workaround that permits the restoration of the service is available. This KPI covers the time spent by SWIFT only. It excludes, for example, any time necessary for the customer to provide information, the time it takes to obtain data requested by SWIFT, and the time to follow up on SWIFT instructions.

MxTTR is temporarily suspended by the following events: (1) the ESMIG operator is not available to support or provision access to the faulty components, or (2) the ESMIG operator refuses to allow contractor personnel to enter the relevant ESMIG operator site(s), or force majeure (a circumstance due to an external, unpredictable event unrelated to computer operations and when that circumstance could not have been either foreseen or prevented with all due reasonable care).

Measurement: Based on the case logs and related time stamps as recorded in SWIFT's case management system.

Key Performance Indicators:

- For high priority issues: 4 hours
- For medium priority issues: 8 hours
- For low priority issues: 16 hours

Maximum Status Notification Interval (SNI) KPI

Definition: This 'time to notify' KPI defines the maximum time elapsed between the acceptance of a telephone initiated case by SWIFT and the start of the incident/problem resolution process, whereby the start of the resolution process is the first update received by the ESMIG operator from SWIFT.

Measurement: Based on the case logs and related time stamps as recorded in SWIFT's case management system.

Key Performance Indicators:

- For high priority issues: 1 hour
- For medium priority issues: 2 hours
- For low priority issues: 4 hours

6.3.4 A2A Real-Time Message Delivery Time

SWIFT's Solution for ESMIG is designed to offer message transfer using the InterAct messaging service (in real-time mode) in accordance with the A2A real-time message delivery time KPI.

A2A real-time message delivery time KPI

The A2A real-time message delivery time of a message is the measure of time taken to deliver a message from the sender to the receiver. More specifically, it is the time from the moment a message is provided to the sending SNL, including the time the message spends on the SWIFT network and in the SWIFT Operating Centre (OPC), up to the moment the message is ready for delivery to ESMIG. It excludes any time spent in the customer's or the ESMIG infrastructure. It is applicable to real-time InterAct messages only (excluding any delivery notification).

The A2A real-time message delivery time must be less than 2 seconds for 95% of the messages and less than 40 seconds for 100% of the messages, covering all traffic sent by all customers, within a given service and calculated on a monthly basis.

6.3.5 A2A Store-and-Forward Message Delivery Time

SWIFT's Solution for ESMIG is designed to offer message transfer using the InterAct messaging service (in store-and-forward mode) in accordance with the A2A store-and-forward message delivery time KPI.

A2A store-and-forward message delivery time KPI

The A2A store-and-forward message delivery time of a message is the measure of time taken to deliver a message from the sender to ESMIG. More specifically, it is the time from the moment a message is provided to the sending SNL, including the time the message spends on the SWIFT network and in the SWIFT Operating Centre (OPC), up to the moment the message has been made available for delivery to ESMIG. It excludes any time spent in the customer's or the ESMIG infrastructure. It is applicable to store-and-forward InterAct messages only that are sent to ESMIG (excluding any delivery notification). The A2A store-and-forward message delivery time must be less than 10 seconds for 95% of the messages and less than 60 seconds for 100% of the messages, covering all traffic sent by all customers, within a given service and calculated on a monthly basis.

6.3.6 A2A Instant Message Delivery Time

SWIFT's Solution for ESMIG is designed to offer message transfer using SWIFTNet Instant messaging service in accordance with the A2A instant message delivery time KPI.

A2A instant message delivery time KPI

The A2A instant message delivery time (sometimes also referred to as 'transit-time') of an instant message is the measure of time taken to deliver an instant message from the sender to the receiver. More specifically, it is the time from the moment a message is provided to the sending AGI including the time the message spends on the SWIFT network and in the SWIFT Operating Centre (OPC), up to the moment the message has been received by the receiver's AGI and is ready for delivery to the consuming middleware/application. It excludes any time spent in the customer's MQ infrastructure. It is applicable to instant messages only (excluding any of the optional 'Notify' or 'TechAck' notifications). The A2A instant message delivery time must be less than 250 milliseconds for 95% of the messages and less than 1 second for 100% of the messages, covering all traffic sent and received to and from all customers, within a given service and calculated on a monthly basis.

6.4 Reporting

Service availability

SWIFT will report the actual monthly KPI figures to the ESMIG operator.

Connection availability

SWIFT will report the actual monthly KPI figures to the ESMIG operator.

A2A real-time message delivery time KPI

SWIFT will report the actual monthly KPI figures to the ESMIG operator.

A2A store-and-forward message delivery time KPI

SWIFT will report the actual monthly KPI figures to the ESMIG operator.

A2A instant message delivery time KPI

SWIFT will report the actual monthly KPI figures to the ESMIG operator.

Failure resolution times

SWIFT will record time stamps based upon the different customer interactions in the case management system, allowing to measure Failure Resolution Times KPIs (MxTTI, MxTTR, SNI) for the reported cases.

SWIFT will report the actual monthly KPI figures to the ESMIG operator.

ESMIG incident reports

SWIFT provides a report to the ESMIG operator after an ESMIG service incident. SWIFT may publish the final incident report after consultation with the ESMIG operator. The final incident report summarises the event, the investigation results, and the action plan agreed with the ESMIG operator to prevent recurrence.

Operational quarterly meetings

The Support team will, for those customers who have subscribed to the Premium package, submit any outstanding issues for inclusion in the case reviews held during the quarterly planned meetings.

Service management meetings

For customers who have subscribed to the Premium Plus or Premium Plus Custom service, service management meetings will cover, including but not limited to, a review of any outstanding issues as well as a case review, both of which will also include issues related to SWIFT's Solution for ESMIG.

6.5 Customer Rights and Remedies

In case of a material breach or repeated minor breaches of the KPIs set out in Key Performance Indicators (KPIs) on page 38, SWIFT will use all commercially reasonable efforts to:

- investigate the underlying cause of the breach
- take necessary measures to prevent the breach(es) from recurring or report on the cause, the status and the remedies necessary to prevent recurrence of the breach(es)
- inform the ESMIG operator accordingly.

7 Contractual Framework

Concession Contract

The *Concession Contract* provides that SWIFT shall offer to customers to enter into agreements regarding the provision and the use of SWIFT's Solution for ESMIG.

7.1 Scope of the Agreement

ESMIG-dedicated connectivity infrastructure

Customers who subscribe to SWIFT's Solution for ESMIG can opt for a new local or SWIFT-operated connectivity infrastructure fully dedicated to their access to ESMIG entirely provided by SWIFT.

These customers will enter into a new ESMIG Connectivity Services Agreement with SWIFT for the provision and the use of all components of SWIFT's Solution for ESMIG (see Elements of the ESMIG Connectivity Services Agreement on page 48).

Non-dedicated connectivity infrastructure

Customers who subscribe to SWIFT's Solution for ESMIG can also opt for a non-dedicated local or SWIFT-operated connectivity infrastructure, which they can then use for both their access to ESMIG and other purposes at the customers' discretion.

These customers will enter into an ESMIG Connectivity Services Agreement with SWIFT for their subscription to the relevant messaging services to access ESMIG in all relevant testing and production environments.

The provision and use of the non-dedicated connectivity infrastructure components (other than lines and related equipment) used by customers for both their access to ESMIG and other purposes shall continue to be governed by (existing) applicable terms and conditions save that these shall automatically be amended or supplemented as expressly provided in this service description, including the Specific Provisions on page 48, to meet the minimum requirements described in and be otherwise consistent with the *Concession Contract*. These amendments and supplements apply if and to the extent these non-dedicated local or SWIFT-operated connectivity infrastructure components are used by customers to access ESMIG.

As regards the lines and related equipment to connect to SWIFT's backbone network provided by the SWIFT Network Partners that customers may decide to re-use as part of their non-dedicated connectivity infrastructure to access ESMIG, the ESMIG Connectivity Services Agreement will govern the provision and use of such lines and related equipment on the following conditions:

- save to the extent expressly provided otherwise in this section, the provision and use of the re-used lines and related equipment will be governed by the same terms and conditions as those set out in the agreement(s) executed by the customer with its selected Network Partner(s) which, for the avoidance of any doubt, will be acting as SWIFT’s subcontractor(s)
- the provision and use of the re-used lines and related equipment will conform to the obligations and requirements applicable to SWIFT for the provision of such lines and related equipment under the *Concession Contract*
- any recourse regarding the re-used line(s) and related equipment shall be towards SWIFT exclusively; SWIFT has the right to appoint the Network Partner(s) concerned as its agent or representative to handle any dispute relating to the provision of the lines or related equipment

For the avoidance of any doubt, the foregoing applies if and to the extent the lines and related equipment are re-used to access ESMIG. Any other use of the lines and related equipment to

access other services over SWIFT shall continue to be governed by the agreement(s) executed by the customer with its selected Network Partner(s) exclusively.

Connection through a Group Hub or Service Bureau

Customers who subscribe to SWIFT's Solution for ESMIG can decide to connect through a Group Hub or Service Bureau, which will have and operate all necessary local connectivity infrastructure components to support the customer's access to SWIFT's Solution for ESMIG.

The ESMIG Connectivity Services Agreement concluded by these customers will cover the provision and use of the messaging services to access ESMIG in all relevant testing and production environments.

The ESMIG Connectivity Services Agreement will also apply to new connectivity infrastructure components (if any) of SWIFT's Solution for ESMIG ordered by these customers which are dedicated to their access to ESMIG.

If these customers decide to also use some non-dedicated connectivity infrastructure components, the principles applicable to non-dedicated connectivity infrastructure will apply.

Note *Customers who wish to connect through a Group Hub or Service Bureau - can do so at their own risk and under their sole responsibility in accordance with the principles and conditions set out in this service description or, more generally, the Shared Infrastructure Programme Policy. Without prejudice to the generality of the foregoing:*

- *The Group Hub or Service Bureau will be considered as an agent of the customer fully authorised to act for, and on behalf of, the customer, and to provide or to receive confidential information of, or for, the customer. For example, the Group Hub or Service Bureau can log cases with SWIFT Support in its own name but also for, and on behalf of, the customer.*
- *Performance by SWIFT of its obligations towards the Group Hub or Service Bureau will discharge SWIFT as if it had performed towards the customer directly. For example, SWIFT's responsibility for those connectivity infrastructure components of SWIFT's Solution for ESMIG operated by the Group Hub or Service Bureau will end at the premises where the Group Hub or Service Bureau has installed those components. Also, Key Performance Indicators (KPIs) will apply to those components of SWIFT's Solution for ESMIG operated by the Group Hub or Service Bureau or problems logged by the Group Hub or Service Bureau relating to the customer's use of SWIFT's Solution for ESMIG.*
- *The customer acknowledges and accepts that it must ensure that SWIFT shall be permitted to disclose confidential information of the Group Hub or Service Bureau if and to the extent it is necessary or desirable for the provision or use of SWIFT's Solution for ESMIG or, more generally, the performance of SWIFT's obligations or the exercise of SWIFT's rights or remedies under the Concession Contract pursuant to the Concession Contract. For more information, see the confidentiality clause in Specific Provisions on page 48.*
- *For the avoidance of any doubt, customers - as identified through their BIC - remain fully responsible for all messages or files sent or received through a Group Hub or Service Bureau. In particular, customers acknowledge and agree that the delivery of a message or a file from ESMIG to the connectivity interface operated by their Group Hub or Service Bureau is considered to be a delivery of that message to them. Customers further acknowledge and agree that a message or a file sent through a Group Hub or Service Bureau to ESMIG remains under their responsibility.*

Other SWIFT products and services

The ESMIG Connectivity Services Agreement applies if and to the extent to the components of SWIFT's Solution for ESMIG are used to access ESMIG. This means that the ESMIG Connectivity Services Agreement does not apply to (without limitation):

- The non-dedicated local or SWIFT-operated connectivity infrastructure components if and to the extent used by customers for other purposes than to access ESMIG.
- The supplemental SWIFT services and products that customers may order and use in connection with their subscription to SWIFT's Solution for ESMIG, such as, but not limited to, Alliance Access or Alliance Gateway for the messaging flows, or value-added or other additional services or products such as the Connector for ESMIG.

7.2 Elements of the ESMIG Connectivity Services Agreement

The ESMIG Connectivity Services Agreement typically consists of the following elements:

- The relevant subscription or order forms for the different components of SWIFT's Solution for ESMIG.
- This service description and any other relevant service description(s) or other documentation applicable to the various components of SWIFT's Solution for ESMIG referred to in this service description and to the extent part of SWIFT's Solution for ESMIG. In the event of a conflict or inconsistency between this service description and any other document referenced or referred to in it, this service description shall prevail.
- The applicable standard terms and conditions below, as amended or supplemented by the Specific Provisions on page 48:
  - for all components of SWIFT's Solution for ESMIG other than those listed below: the SWIFT General Terms and Conditions
  - for the HSM boxes and tokens: the HSM Box Terms and Conditions and the HSM Tokens and Cards Terms and Conditions respectively
  - for the VPN boxes: the VPN Box Terms and Conditions
  - for the provision of an ESMIG-dedicated line, the *ESMIG-specific Terms and Conditions*

  Note *Customers can find the latest available version of the relevant terms and conditions at swift.com > About Us > Legal >* Terms and Conditions.
- The Price List for SWIFT's Solution for ESMIG and, as applicable, a quotation.

7.3 Specific Provisions

Specific provisions amending or supplementing the applicable terms and conditions

Considering the specific conditions governing the provision and the use of connectivity services for ESMIG set out in the *Concession Contract*, the provision and the use of the components of SWIFT's Solution for ESMIG shall be governed by the specific provisions set out in this section.

In the case of conflict or inconsistency between these specific provisions and the terms and conditions otherwise governing the provision and the use of the components of SWIFT's Solution for ESMIG, these specific provisions shall prevail.

The specific provisions set out in this section and, more generally, this service description, apply between SWIFT and the relevant customers of SWIFT's Solution for ESMIG if and to the extent the

components of SWIFT's Solution for ESMIG are used to access ESMIG. Nothing contained in these specific provisions, or, more generally, the ESMIG Connectivity Services Agreement shall, or shall be construed to, confer any rights or remedies on any third party (including a Group Hub or Service Bureau) supporting or otherwise involved in the connectivity of the customer to access SWIFT's Solution for ESMIG. Also, these specific provisions and, more generally, this service description, cover the provision and the use of SWIFT's Solution for ESMIG only, excluding without limitation the provision of any other SWIFT services or products in connection therewith, such as, but not limited to, value-added or other additional services or products.

Eligibility

It is a condition for the use of SWIFT's Solution for ESMIG that the customer is a SWIFT user authorised by the Eurosystem to connect to ESMIG.

Note *Those connectivity infrastructure components of SWIFT's Solution for ESMIG that are necessary to support the connection of customers to SWIFT's backbone network are also available to SWIFT users and service bureaux.*

Customers that decide to use SWIFT to connect to ESMIG only will automatically be eligible to join SWIFT in the category 'Payment Systems Participants' (PSPA) or 'Securities Systems Participants' (SSPA).

If the customer ceases to be authorised by the Eurosystem to access ESMIG or becomes aware of any change affecting its right to access ESMIG at any time, it shall notify SWIFT thereof without undue delay. If deemed appropriate, SWIFT may reassess the then current eligibility status of the customer. The customer agrees that SWIFT has the right to request at any time confirmation and evidence from either the customer or the Eurosystem of the then current eligibility status of the customer.

Nothing in SWIFT's co-operative governance shall oblige customers who decide to use SWIFT to connect to ESMIG only, to pay fees or charges exceeding the maximum prices set out in the Price List for SWIFT's Solution for ESMIG, or to accept obligations that are not necessary for their use of SWIFT to access ESMIG only. For example, the SWIFT joining process will support the registration process necessary to issue PKI certificates identifying customers towards the Eurosystem but any obligation to become a shareholding member of SWIFT for the sole use of SWIFT's Solution for ESMIG will be waived.

If the customer ceases to be authorised by the Eurosystem to access ESMIG, and if and to the extent permitted to do so under the *Concession Contract*, SWIFT shall immediately and automatically be entitled to suspend or, as the case may be, terminate the provision and the use of SWIFT's Solution for ESMIG, in whole or in part, to the customer.

ESMIG and Eurosystem

As further detailed elsewhere in this service description, and as required under the *Concession Contract*, the customer acknowledges and agrees that, when interacting with ESMIG, it is not interacting with another SWIFT user and it may not rely on any assumption that the ESMIG operator or the Eurosystem are bound by the terms and conditions normally governing the provision and the use of the SWIFT services and products by SWIFT users.

More generally, SWIFT is unable to accept and expressly disclaims any obligation to perform or shall have no liability to the extent resulting from any act, fault or omission of the ESMIG operator or the Eurosystem (including the use of any SWIFT certificate by the ESMIG operator or the Eurosystem). The customer should refer to its own arrangements with the Eurosystem in connection with its access to ESMIG and/or the TARGET services or applications to assess its rights and obligations towards the ESMIG operator or the Eurosystem in connection with its access to ESMIG or its use of any TARGET services or applications.

Each customer shall remain exclusively responsible for its business and contractual relations with its own customers, including other customers, in relation to the products and services it offers to its

own customers, including other customers, even if enabled by SWIFT's Solution for ESMIG or other SWIFT services and products.

Hosting

As per the *Concession Contract*, SWIFT's Solution for ESMIG includes certain infrastructure components hosted at the premises of the ESMIG operator (for more information, see Solution Description on page 10). Considering that the proper operation of this infrastructure is critical to the provision of SWIFT's Solution for ESMIG, SWIFT is unable to accept and expressly disclaims any obligation to perform or shall have no liability to the extent resulting from any act, fault or omission of the ESMIG operator in the context of such hosting arrangements.

Security audit report

As per the relevant provisions of the *Concession Contract*, SWIFT shall make available a yearly ISAE 3402 Type II report - or another report based on at least equivalent standards - covering SWIFT's Solution for ESMIG, including a statement from an internal or external auditor that the report presents a fair overview of the risk situation at SWIFT. Unless the customer notifies SWIFT in writing reasonably in advance of another contact person, SWIFT shall send such report to the primary security officers designated by the customer for the BIC used for subscription purposes. Such report may then be further shared within the customer's organisation on a need-to-know basis. The first report will be shared after one year of live SWIFT's Solution for ESMIG operations.

Service levels

As per article 7.8 of the *Concession Contract*, section Key Performance Indicators (KPIs) on page 38 of this service description sets out applicable Key Performance Indicators (KPIs) regarding the service and connection availability and the failure resolution times.

The KPIs apply to both ESMIG-dedicated and, to the extent used as part of SWIFT's Solution for ESMIG, non-dedicated components of SWIFT's Solution for ESMIG.

For customers connecting through a Group Hub or Service Bureau, the Connection Availability KPI apply to those connectivity infrastructure components operated by that Group Hub or Service Bureau, and the Failure Resolution Times KPIs apply to cases reported by that Group Hub or Service Bureau regarding the customers' use of SWIFT's Solution for ESMIG. SWIFT's obligations in respect of the KPIs set out in Service Levels on page 37 and, more generally, SWIFT's Solution for ESMIG are only owed to customers and not (without limitation) the Group Hub or Service Bureau through which they decide to connect.

Section Customer Rights and Remedies on page 45 states the sole and exclusive rights and remedies of customers if SWIFT ever fails to meet applicable KPIs. Also, SWIFT shall have no liability whatsoever for any failure to meet KPI if and to the extent caused by a force majeure event, a breach by customers of their obligations under applicable documentation, or any other act, omission or default of the customers or any other third party for which SWIFT is not responsible.

Liability

The ESMIG Connectivity Services Agreement governs the provision and use of SWIFT's Solution for ESMIG. The customer waives any contractual and non-contractual claim against any Central Bank part of the Eurosystem based on any act, fault or omission by SWIFT in relation to SWIFT's Solution for ESMIG. Notwithstanding anything to the contrary set out in the ESMIG Connectivity Services Agreement, each customer will hold SWIFT harmless and will indemnify and keep SWIFT indemnified from and against any and all actions, liabilities, claims, fines, demands, losses, damages, proceedings, costs, or expenses (including reasonable legal fees, costs, and expenses) suffered or incurred by, or indemnification duties to be performed by SWIFT in connection with any third-party claim or indemnification request (including any claim or request made by a Central Bank part of the Eurosystem) related to or in connection with the customer’s claim against that third party regarding the provision or use of SWIFT's Solution for ESMIG.

Subject to the general principles below, SWIFT's liability in connection with the provision and the use of SWIFT's Solution for ESMIG is to customers only and is as follows:

- **ESMIG-dedicated components**

  For ESMIG-dedicated components of SWIFT's Solution for ESMIG, SWIFT's liability (if any) will be assessed according to the applicable terms and conditions referred to in Elements of the ESMIG Connectivity Services Agreement on page 48 except that SWIFT's aggregate liability for Losses (as defined in the *Concession Contract*) will in no event be less than the applicable minimum liability caps set out in the *Concession Contract*.

- **Non-dedicated connectivity infrastructure components**

  For non-dedicated local or SWIFT-operated connectivity infrastructure components of SWIFT's Solution for ESMIG, the minimum liability caps set out in the *Concession Contract* will apply. Where (existing) terms and conditions apply between the customer and SWIFT, including the terms and conditions set out in Scope of the Agreement on page 46 governing the re-use of lines and related equipment, SWIFT's liability (if any) will be assessed according to such (existing) applicable terms and conditions it being understood that, in the event of inconsistency with the minimum liability caps set out in the *Concession Contract*, the minimum liability caps set out in the *Concession Contract* will prevail.

- **Connection to SWIFT's Solution for ESMIG through a Group Hub or Service Bureau**

  If customers connect through a Group Hub or Service Bureau, SWIFT will indemnify customers if and to the extent Losses (as defined in the *Concession Contract*) incurred as part of their use of SWIFT's Solution for ESMIG cannot be recovered up to the applicable minimum liability caps set out in the *Concession Contract* due to less favorable financial caps applicable to SWIFT's liability to the Group Hub or Service Bureaux for the provision of the faulty component(s) of SWIFT's Solution for ESMIG. Customers are solely and exclusively responsible for including in their arrangements with their Group Hub or Service Bureau appropriate provisions regarding the recovery of Losses (as defined in the *Concession Contract*).

- **Calculation of the minimum liability caps**

  If and to the extent SWIFT's liability relates to customers' use of non-dedicated components as part of SWIFT's Solution for ESMIG, then SWIFT will calculate the applicable minimum liability cap based on the portion of the charges payable by the customer for these non-dedicated components that covers the re-use of the non-dedicated component(s) to access ESMIG as specified in the Price List for SWIFT's Solution for ESMIG. The customer can only claim compensation for his own loss or damage. The customer shall not accept any liability or duty to indemnify, whether in contract, tort or otherwise, towards other customers for any action, fault or omission by SWIFT in the context of SWIFT's Solution for ESMIG, and such liability or duty to indemnify shall not be considered as own loss or damage by that customer.

  Any liability or duty to indemnify, whether in contract, tort or otherwise, to be paid by a customer to a third party shall only be considered as the customer's own loss or damage, provided that:

  - the third party does not claim compensation or indemnification from SWIFT on the basis of the same event or series of connected events; and
  - the compensation or indemnification claimed from SWIFT does not relate to loss or damage that is excluded elsewhere in the applicable standard terms and conditions part of the ESMIG Connectivity Services Agreement. Subject to minimum liability caps applicable to customers, the exclusions and limitations of liability in the applicable standard terms and conditions part of the ESMIG Connectivity Services Agreement shall always apply.

  SWIFT shall never be liable to more than one party for the same or similar loss or damage resulting from the same event or series of connected events.

General principles

SWIFT accepts liability (if any) to the customer for or in connection with the provision or use of SWIFT's Solution for ESMIG always subject to the following principles:

1. The customer must use all commercially reasonable efforts to limit any loss or damage, including (without limitation) to recover any loss or damage from any third party concerned.
2. Neither party may recover more than once for the same loss (including under insurance coverage).
3. No undue enrichment will ever accrue to any party.
4. SWIFT is not obliged to perform or will have no liability for any act, fault or omission to the extent exclusively resulting from any act, fault or omission of the customer, or of a third party for which SWIFT is not responsible.
5. Customers shall ensure SWIFT may exercise any right or remedies they may have towards any third party for the same event or fact, or the same series of events or facts that are (even indirectly) connected or contribute to the same loss or (even indirectly) related losses for which SWIFT is liable in accordance with this service description.
6. Except as otherwise provided in this service description or other applicable terms and conditions (if any), SWIFT's liability is subject to the following exclusions:
   a. even if SWIFT has been advised of their possibility, SWIFT excludes any liability for:
      - (i) any loss or damage the occurrence or extent of which is unforeseeable
      - (ii) any loss of business or profit, revenue, anticipated savings, contracts, loss or corruption of data, loss of use, loss of goodwill, loss of reputation, interruption of business, or other similar pecuniary loss howsoever arising (whether direct or indirect)
      - (iii) any indirect, special, or consequential loss or damage of any kind
      - (iv) any (financial) sanctions, fines and penalties of any kind imposed by any competent authority
   b. SWIFT is not obliged to perform or has no liability to the extent resulting from the provision or use of services or products not supplied by SWIFT, or in case of a Force Majeure event (as defined in the SWIFT General Terms and Conditions).
7. The provisions governing SWIFT’s liability (typically, the limitation and exclusions of SWIFT’s liability) apply whether the customer claims in contract, tort, or otherwise. The limitation and exclusions of SWIFT’s liability do not apply in case of fraud, wilful default or, more generally, to the extent not permitted under applicable law.

Confidentiality

SWIFT shall protect the customer's Confidential Information according to the applicable terms and conditions except that, as per the relevant provisions of the *Concession Contract*:

- the customer acknowledges and accepts that SWIFT shall be permitted to disclose confidential information provided by or for the customer to the Eurosystem if and to the extent it is necessary or desirable to do so pursuant to the *Concession Contract*. To the extent such information belongs to third parties (including another customer), the customer shall ensure that it is entitled to and has obtained all necessary consents to allow such disclosure.
- nothing shall prevent the customer to disclose to the Eurosystem those fees and charges paid to SWIFT for the provision or the use of the relevant components of SWIFT's Solution for ESMIG.

Maximum prices

As per the relevant provisions of the *Concession Contract*, SWIFT shall (if and to the extent the maximum prices indicated in the Price List for SWIFT's Solution for ESMIG apply) not charge customers higher fees or charges for the provision or use of SWIFT's Solution for ESMIG.

If SWIFT ever fails to comply with its obligation not to charge more than the maximum prices indicated in the Price List for SWIFT's Solution for ESMIG, SWIFT shall (if and to the extent required under the *Concession Contract*) indemnify customers.

Concession Contract

The *Concession Contract* governs the provision and, to some extent, the use of SWIFT's Solution for ESMIG. Consequently and, as a general principle, the applicable terms and conditions referred to in Elements of the ESMIG Connectivity Services Agreement on page 48, the Specific Terms and Conditions, and these Specific Provisions apply subject to the terms and conditions of the *Concession Contract* which, in the case of conflict or inconsistency, shall always prevail. For example, this means that (without limitation):

- it is a condition precedent for the provision of SWIFT's Solution for ESMIG that SWIFT has and maintains a concession for the provision of SWIFT's Solution for ESMIG
- if and to the extent reasonably required to do so under the *Concession Contract*, SWIFT shall be entitled to change, suspend or terminate the provision or the use of SWIFT's Solution for ESMIG and related conditions at any time
- the provision and the use of SWIFT's Solution for ESMIG shall immediately and automatically terminate, in whole or in part, if and to the extent SWIFT is no longer entitled to provide the services and products part of SWIFT's Solution for ESMIG under the *Concession Contract*.

Appendix A Overview of Service Names (A2A) and URLs (U2A)

The tables below contain the latest available information at the time of publication of this document.

A2A

T2

Type	T2 environment	Channel	Service name
Live usage	Production (PROD)	Files store-and-forward	esmig.t2.fast
		Messages store-and-forward	esmig.t2.iast
		Files real-time(1)	esmig.t2.fa
		Messages real-time	esmig.t2.ia
User testing	User testing (UTEST)	Files store-and-forward	esmig.t2.fast!pu
		Messages store-and-forward	esmig.t2.iast!pu
		Files real-time(1)	esmig.t2.fa!pu
		Messages real-time	esmig.t2.ia!pu
Acceptance testing	External Acceptance Testing (EAC)	Files store-and-forward	esmig.t2.fast!pe
		Messages store-and-forward	esmig.t2.iast!pe
		Files real-time(1)	esmig.t2.fa!pe
		Messages real-time	esmig.t2.ia!pe

(1) For the time being, usage of the real-time mode is limited to messages from the customer to the ESMIG platform only. Therefore, SWIFT does not provision customers on the real-time FileAct service.

T2S

Type	T2S environment	Channel	Service name
Live usage	Production (PROD)	Files store-and-forward	t2s.fast
		Messages store-and-forward	t2s.iast
		Files real-time	t2s.fa
		Messages real-time	t2s.ia
User testing	User testing (UTEST)	Files store-and-forward	t2s.fast!pu

Type	T2S environment	Channel	Service name
		Messages store-and-forward	t2s.iast!pu
		Files real-time	t2s.fa!pu
		Messages real-time	t2s.ia!pu
Acceptance testing	Interoperability testing (EAC)	Files store-and-forward	t2s.fast!pe
		Messages store-and-forward	t2s.iast!pe
		Files real-time	t2s.fa!pe
		Messages real-time	t2s.ia!pe

TIPS

Type	TIPS environment	Channel	Service name
Live usage	Production (PROD)	Instant Messages	tips.msg.ins
		Files store-and-forward	tips.fast
		Messages store-and-forward	tips.iast
		Files real-time	tips.fa
		Messages real-time	tips.ia
User testing	Certification testing (CERT)	Instant Messages	tips.msg.ins!pt
		Files store-and-forward	tips.fast!pt
		Messages store-and-forward	tips.iast!pt
		Files real-time	tips.fa!pt
		Messages real-time	tips.ia!pt
Acceptance testing	External Acceptance Testing (EAT)	Instant Messages	tips.msg.ins!pe
		Files store-and-forward	tips.fast!pe
		Messages store-and-forward	tips.iast!pe
		Files real-time	tips.fa!pe
		Messages real-time	tips.ia!pe

ECMS

Type	ECMS environment	Channel	Service name
Live usage	Production (PROD)	Files store-and-forward	esmig.ecms.fast
		Messages store-and-forward	esmig.ecms.iast
		Files real-time(1)	esmig.ecms.fa
		Messages real-time(1)	esmig.ecms.ia
User testing	User testing (UTEST)	Files store-and-forward	esmig.ecms.fast!pu
		Messages store-and-forward	esmig.ecms.iast!pu
		Files real-time(1)	esmig.ecms.fa!pu
		Messages real-time(1)	esmig.ecms.ia!pu
Acceptance testing	Interoperability testing (EAC)	Files store-and-forward	esmig.ecms.fast!pe
		Messages store-and-forward	esmig.ecms.iast!pe
		Files real-time(1)	esmig.ecms.fa!pe
		Messages real-time(1)	esmig.ecms.ia!pe

(1) For the time being, usage of the real-time mode is not available for the ECMS service. Therefore, SWIFT does not provision customers on the real-time services.

U2A

Note *The below URLs will only be applicable after the respective services have migrated to ESMIG. For **current URLs for T2S**, see SWIFT's VAN Solution for T2S - Service Description.*

The java-based proxy solution will be phased out in November 2023 and will not support the access to the ECMS U2A application.

T2/T2S/TIPS - for the java-based proxy access solution

Type	Application	Environment	URL
Live usage	ESMIG portal	Production (PROD)	https://esmigu2a.common.sipn.swift.com/esmig/goto/esmig-portal
User testing	ESMIG portal	User testing (UTEST)	https://esmigu2a.common.sipn.swift.com/esmig/goto/esmig-cert-portal

Type	Application	Environment	URL
Acceptance testing	ESMIG portal	External Acceptance Testing (EAC)	https://esmigu2a.common.sipn.swift.com/esmig/goto/esmig-eac-portal

T2/T2S/TIPS/ECMS - for the ESMIG U2A SWIFT Login Application v2.x access solution

Type	Application	Environment	URL
Live usage	ESMIG portal	Production (PROD)	https://esmig-portal.emip.swiftnet.sipn.swift.com
User testing	ESMIG portal	User testing (UTEST)	https://esmig-cert-portal.emip.swiftnet.sipn.swift.com
Acceptance testing	ESMIG portal	External Acceptance Testing (EAC)	https://esmig-eac-portal.emip.swiftnet.sipn.swift.com

Appendix B Network Configuration Requirements

IP addresses in the subnet range 149.134.0.0/16

Customers must allow outgoing TCP sessions on port 443/tcp from browse clients to the following IP address range through their firewall: 149.134.0.0/16. This is a range of IP addresses in CIDR notation. This range may be limited to the specific IP addresses used for ESMIG. The list of these specific IP addresses is available in Knowledge Base article 5018711.

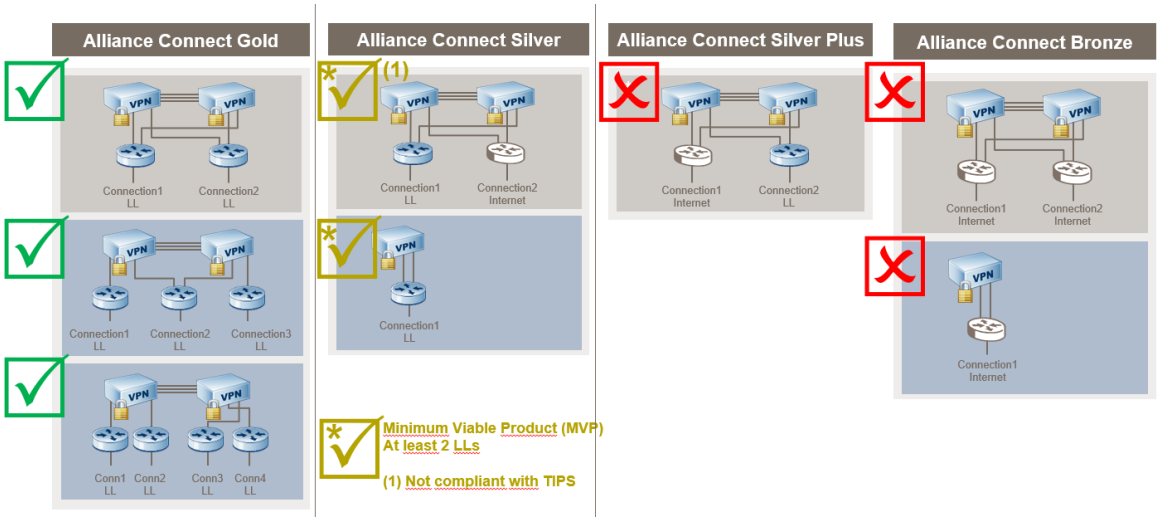
Compliant connectivity options

Considering the ESMIG requirements, customers must connect to ESMIG either:

- through (at least) two leased lines (see below for the possible combinations of Alliance Connect connectivity packages)
- using SWIFT's Alliance Cloud solution

Compliant connectivity packages for on-premises infrastructure

Only Alliance Connect Packs with a primary leased line (LL) option and at least 2 leased lines in total:



Appendix C Enhanced Delivery Notifications for ESMIG

Overview

As mentioned in A2A Messaging Flows on page 13, SWIFT operates a gateway that acts as a bridge between the ESMIG customer (using regular SWIFTNet messaging) and T2S (that use a proprietary DEP protocol). In this way, customers do not need to worry about the specifics of the ESMIG proprietary DEP protocol both for sending and for receiving.

Delivery notification system messages

The ESMIG specifications require that, for non-repudiation purposes, customers can themselves receive a signature from ESMIG acknowledging the receipt of store-and-forward traffic that customers have sent to ESMIG. To achieve this, SWIFT uses the enhanced delivery notification system messages (`xsys.011.001.02` : version of the delivery notification and `xsys.012.001.02` : version of the failed delivery notification).

These delivery notification versions have a field that makes it possible to transport the signature as provided by ESMIG. Customers can check in the **Signature** one **Reference** element containing a digest related to the message or file sent by the customer. Customers can use the SNL or SAG to verify the **SignatureValue**.

For more information, see Using SNL or SAG to Generate Signature in XML-DSIG format on page 60 and Verifying Signatures on page 61.

Time of receipt

The time of receipt of the message or file is the time as registered by ESMIG. This time is forwarded by SWIFT in the **AckSwiftTime** of the delivery notification `xsys.011.001.02`

Appendix D Using SNL or SAG to Generate Signature in XML-DSIG format

SNL provides an API to generate or verify a signature in the XML-DSIG format. This is required by customers who need to generate or verify the signature as used in the payload of messages or files (in the Business Application Header (BAH) or the Business File Header (BFH), respectively).

Customers can also use SAG to generate or verify a signature in XML-DSIG format because SAG exposes the same SNL APIs.

For more information about the use of SNL or SAG for the generation or verification of these signatures, see the *Digital Signatures using SWIFT Certificates - Implementation Guide for SWIFTNet Link and Alliance Gateway* (document available upon request from a SWIFT sales representative).

For more clarifications about the use of the Business Application Header, and the use of 'digital signature on business layer', see the ESMIG-related documentation at www.ecb.europa.eu > Payments & Markets > TARGET services.

Appendix E Verifying Signatures

Apart from the normal use of SWIFT PKI signatures when exchanging traffic, SWIFT's Solution for ESMIG supports the use of SWIFTNet PKI signatures in the following cases:

- **ESMIG signature present in delivery notifications**

  This is the case when a customer sends store-and-forward traffic towards ESMIG. The customer can receive a failed delivery notification in case of a delivery problem. The customer can also (optionally) select to receive a delivery notification for (each or some) message or file sent, in which case SWIFT will provide the delivery notification. SWIFT will provide inside these notifications a signature that ESMIG has generated (if available). This signature covers the acknowledgement by ESMIG for traffic that was sent to ESMIG over the store-and-forward channel.

- **Signature present in the Business Application Header or Business File Header**

  This is a signature used inside the Business Application Header (BAH) or Business File Header (BFH) that is inside the payload exchanged between customers and ESMIG. For more information on how to generate such a signature using SNL or SAG, and where to find more information about the usage in the ESMIG context, see Using SNL or SAG to Generate Signature in XML-DSIG format on page 60.

Customers can decide to store these signatures locally for archival purpose. If there is a need to verify such a signature, then customers can reverify the signature information themselves. If necessary, customers can request SWIFT to check if the certificate was valid at a certain date.

For more information about the offline signature reverification process, see Knowledge Base article 5019321.

Legal Notices