Connectivity

3SKey

Service Description

This document describes the features and functions of the components of the 3SKey solution and the roles and responsibilities of all parties involved in the 3SKey solution.

17 September 2010
# Table of Contents

Table of Contents ............................................................................................................................... 2  
Preface ................................................................................................................................................. 3  

1 Introduction ........................................................................................................................................ 4  
1.1 Advantages of the 3SKey Solution ......................................................................................... 4  
1.2 Eligibility Criteria .................................................................................................................. 4  

2 Features and Functions ........................................................................................................... 5  
2.1 Overview ................................................................................................................................. 5  
2.2 Description of the Solution ...................................................................................................... 5  
2.3 Components of the 3SKey Solution ........................................................................................ 8  
  2.3.1 SWIFT Components ....................................................................................................... 9  
  2.3.2 3SKey Subscriber Components .................................................................................. 9  
  2.3.3 3SKey User Components .......................................................................................... 10  
2.4 Key Service Availability .........................................................................................................11  

3 Ordering and Support ............................................................................................................ 12  
3.1 Ordering ................................................................................................................................ 12  
3.2 Support .................................................................................................................................. 12  

4 Roles and Responsibilities .................................................................................................... 14  
4.1 SWIFT’s Roles and Responsibilities ..................................................................................... 14  
4.2 The 3SKey Subscriber’s Roles and Responsibilities ............................................................. 15  
4.3 The 3SKey User’s Roles and Responsibilities ...................................................................... 16  

5 Pricing and Invoicing ............................................................................................................. 17  
5.1 Charges ................................................................................................................................. 17  

6 Contractual Framework ......................................................................................................... 18  

7 Glossary of Terms .................................................................................................................. 19  

Legal Notices .................................................................................................................................... 20
Preface

Purpose of the document

This document describes the features and functions of the various components of the 3SKey (SWIFT Secure Signature Key) solution and the roles and responsibilities of all parties involved in the 3SKey solution.

Note

This service description, together with other relevant contractual service documentation, is an integral part of the contractual arrangements between SWIFT and the 3SKey subscribers, the 3SKey users or any other organisations that order the 3SKey Developer Toolkit for the provision and the use of the relevant components of the 3SKey solution.

Audience

This document is for the following audience:

• 3SKey subscribers (typically, banks) that require information about the features and functions of the components of the 3SKey solution, and about the roles and responsibilities of all parties involved in the 3SKey solution
• 3SKey users (typically, corporate clients of banks, or their representatives) that require information about the features and functions of the components of the 3SKey solution, and about the roles and responsibilities of all parties involved in the 3SKey solution
• persons that intend to subscribe to or use the 3SKey solution, and require information about the features and functions of the components of the 3SKey solution and about the roles and responsibilities of the parties involved in the 3SKey solution

First edition

This document is the first edition of the book.

SWIFT-defined terms

In the context of SWIFT documentation, certain terms have a specific meaning. These terms are called SWIFT-defined terms (for example, customer, user, or SWIFT services and products). The definition of SWIFT-defined terms appears in the SWIFT Glossary.

Related documentation

• Pricing and Invoicing – Price List
• 3SKey Developer Guide
• 3SKey Terms and Conditions
• 3SKey Tokens Terms and Conditions
• 3SKey Developer Toolkit Terms and Conditions
• 3SKey Portal Online Help
• 3SKey Best Practices Guide
• SWIFT Glossary
• 3SKey Certificate Policy
• Support Service Description
1 Introduction

When a bank interacts with their corporate customers through electronic banking channels, it may need to authenticate received data at the level of the individual(s) authorised to serve instructions to it. For example, a specific individual in the corporate treasury department must approve payment instructions.

In practice, banks and their corporate clients must often manage and use multiple and different types of personal signing mechanisms (for example, multiple tokens with different passwords). Using and maintaining different authentication methods in parallel adds to the complexity and leads to higher operational risk and cost.

To address this issue, SWIFT launches the 3SKey solution. With this solution, SWIFT supplies to 3SKey subscribers (typically, banks) PKI-based credentials for redistribution to their 3SKey users (typically, corporates). 3SKey users then use these credentials to sign messages and files exchanged with one or more 3SKey subscribers over any mutually agreed channel.

1.1 Advantages of the 3SKey Solution

3SKey subscribers

The 3SKey solution is designed to enable 3SKey subscribers to address the needs of 3SKey users. 3SKey subscribers associate each individual 3SKey user with a specific token independently of the other 3SKey subscribers. 3SKey subscribers access the central infrastructure (operated by SWIFT) to make sure that the certificate hasn't been revoked.

This approach leaves each 3SKey subscriber free to set and apply its own Know-Your-Customer rules when it associates 3SKey users. Each 3SKey subscriber associates its 3SKey users independently and does not need to rely on the association performed by other 3SKey subscribers.

The 3SKey solution enables 3SKey subscribers to cost-effectively implement (or strengthen) authentication and non-repudiation on their existing electronic banking channels.

3SKey users

A 3SKey user must currently use many different security devices to authenticate itself towards third parties (typically, banks). The use of a single token towards multiple 3SKey subscribers will help to reduce cost and operational risk and increase convenience.

1.2 Eligibility Criteria

Eligibility to subscribe to the 3SKey service

The 3SKey service is available to all SWIFT users and service bureaux.

Eligibility to order and distribute 3SKey tokens

All 3SKey subscribers may order 3SKey tokens from SWIFT for their own use or for distribution to 3SKey users. All other SWIFT users may order 3SKey tokens from SWIFT for their own use or for distribution to affiliates within their corporate group. All SWIFT partners that order a 3SKey Developer Toolkit may also order 3SKey tokens from SWIFT for their own internal use.

Eligibility to order the 3SKey Developer Toolkit

The 3SKey users and all SWIFT partners may order the 3SKey Developer Toolkit from SWIFT.

The 3SKey subscribers receive the 3SKey Developer Toolkit automatically as an integral part of their subscription to the 3SKey service.
2 Features and Functions

2.1 Overview

SWIFT delivers the 3SKey solution through the following components:

- **SWIFT Public Key Infrastructure (PKI)**
  The underlying PKI that SWIFT manages and operates. 3SKey subscribers and their 3SKey users can access the PKI either through the 3SKey portal or through the 3SKey certificate revocation check facility, as applicable.

- **3SKey tokens**
  Secure devices that hold either the signing credentials of the 3SKey user or the authentication credential for the 3SKey subscriber to access the portal.

- **3SKey portal**
  Accessed by the 3SKey users to manage the 3SKey tokens (activation, renewal, recovery, and revocation of the tokens).
  Accessed by the 3SKey subscribers to get the Secure Socket Layer (SSL) certificates for the 3SKey certificate revocation check facility, and to get reports on the tokens that they distribute.

- **3SKey certificate revocation check facility**
  Accessed by the 3SKey subscriber to check whether a 3SKey user’s (unexpired) certificate has been revoked.

- **3SKey Developer Toolkit**
  Software libraries that 3SKey subscribers and integrators use to enable web servers and applications to work with the 3SKey service. This includes signing, signature verification, and certificate revocation check functions.

2.2 Description of the Solution

**Set-up of the solution**

The set-up of the solution consists of the following steps:

1. **Supply and distribution of 3SKey tokens**
   If an organisation has subscribed to the 3SKey service and has placed an order for the 3SKey tokens, then SWIFT provides the tokens to the 3SKey subscriber. The tokens are inactive (that is, they cannot be used to sign transactions).
   The 3SKey subscribers then distribute the tokens to their 3SKey users.
2. Activation

SWIFT supplies inactive tokens (that is, they cannot be used to sign transactions). The 3SKey user must first activate its token by using the secure access (provided by the inactive token) to the 3SKey portal over the Internet. As a result, a business credential (that is, a certificate and private key) is created and stored on the token. The activation process does not require the supply of any identification information about the 3SKey user, and the business credential is entirely anonymous. It does not contain the name of any individual but just a Unique ID that is used by 3SKey subscribers to associate the 3SKey user with the certificate.

3. Association

The 3SKey user associates with its 3SKey subscriber (or 3SKey subscribers). As a result, the 3SKey subscriber application links the 3SKey user with the Unique ID. Such association is achieved as agreed by the 3SKey subscriber and the 3SKey user (typically, through a physical presence or through the use of secure, pre-existing, remote identification technology). During the association process, the 3SKey subscriber verifies that the certificate is valid and accesses the 3SKey certificate revocation check facility to verify that the certificate has not been revoked.

When the association process is complete, any message that is signed with the credential is linked to that 3SKey user representative.
Use of the solution

1. Use of the token

When the activation and association steps are complete, the 3SKey user can use the token to sign messages and files towards the 3SKey subscriber. The 3SKey user application software or 3SKey user browser interacting with a 3SKey subscriber web application (for example, e-banking) signs the messages with the user’s token. The 3SKey subscriber’s application verifies the signature and can access the 3SKey certificate revocation check facility to verify that the certificate has not been revoked.

2. Using the business credential with multiple 3SKey subscribers

A 3SKey user can use the same business credential to sign messages for transactions with other 3SKey subscribers. The 3SKey user must associate with each 3SKey subscriber separately. This is the same process as described in step 3 of “Set-up of the solution”.
1. **Revocation**
   If the 3SKey token has been stolen, or its security or reliance is otherwise compromised (typically, the individual using the token leaves the company) the 3SKey user, or a 3SKey user group administrator, can request the revocation of its certificate through the 3SKey portal. Consequently, SWIFT updates the certificate revocation list with the certificate information. In turn, when the 3SKey subscribers' application checks the certificate revocation list, the certificate will appear as revoked and, consequently, the application of the 3SKey subscriber can stop to trust it.

   Certain 3SKey subscribers may also require their 3SKey users to de-associate the certificate with them directly.

   For more information, 3SKey users should check the conditions governing the use of the certificate with their 3SKey subscribers.

2. **Renewal**
   The 3SKey user’s token will expire after 3 years. Before its token expires, the 3SKey user must renew its certificate on a new token through the portal. The new token will inherit the original Unique ID.

3. **Recovery**
   It may be necessary to recover a certificate, if the certificate has been revoked, if the certificate has expired, or if the 3SKey user has lost its password. In this case, the 3SKey user asks a 3SKey user group administrator to set up the certificate for recovery. Through the 3SKey portal, the 3SKey user can recover its certificate onto a new token that has been set up for recovery by the administrator. The new token will hold a new business certificate with the original Unique ID and will be valid for 3 years. The old certificate cannot be used anymore.

### 2.3 Components of the 3SKey Solution

**Deployment of the components**

The components of the 3SKey solution are deployed by the different parties, as follows:

- **SWIFT**: SWIFT PKI, 3SKey portal, and 3SKey certificate revocation check facility
- **3SKey subscriber**: 3SKey subscriber application, 3SKey subscriber tokens, and 3SKey Developer Toolkit
• 3SKey user: 3SKey user application, 3SKey user tokens, 3SKey Developer Toolkit, and web browser

2.3.1 SWIFT Components

SWIFT PKI
The SWIFT PKI supports the following PKI operations:
• new certificate issuance
• certificate renewal
• certificate revocation
• certificate recovery

3SKey portal
SWIFT provides a web portal.
• An authenticated 3SKey user can access the portal to perform the following functions:
  − activation of the 3SKey token
  − certificate renewal
  − certificate revocation
  − certificate recovery
  − password and security code management
  − user group management functions
• An authenticated 3SKey subscriber can access the portal to perform the following functions:
  − retrieve the SSL certificates (used to securely access the 3SKey certificate revocation check facility)
  − retrieve a report on the 3SKey subscriber’s distributed tokens and their status

3SKey certificate revocation check facility
The 3SKey subscriber application obtains the Certificate Revocation List (CRL) using a secure access to the 3SKey certificate revocation check facility through the Internet. This requires an SSL certificate which the 3SKey subscriber obtains from the portal.

The 3SKey certificate revocation check facility is only available to the 3SKey subscribers.

For more information, see the 3SKey Developer Guide.

2.3.2 3SKey Subscriber Components

3SKey subscriber application
During the association phase, the 3SKey subscriber application performs the following activities:
• establishes the correspondence between the Unique ID and an identity (for example, the name of a person or a function)
• verifies the signature
• verifies that the certificate is a 3SKey business certificate by checking that it has the Policy ID 1.3.21.6.3.20.200.1
• verifies that the certificate has not expired
• ensures that the certificate has not been revoked

When processing business transactions, the 3SKey subscriber application performs the following activities:
• verifies the signature of messages or files that have been signed with a 3SKey token
ensures that the signing certificate is a 3SKey business certificate by checking that it has the Policy ID 1.3.21.6.3.20.200.1
• verifies that the signing certificate has not expired
• ensures that the signing certificate has not been revoked
• keeps non-repudiation logs of the signed transactions

Note The 3SKey subscriber is responsible for the integration of the 3SKey service with its application(s) using the 3SKey Developer Toolkit or with assistance of a vendor of its choice.

3SKey subscriber tokens
The 3SKey subscribers receive specific tokens to access the portal to retrieve an SSL certificate and access a token report. The SSL certificate enables the subscribers to securely access the 3SKey certificate revocation check facility. The token report lists the tokens that the 3SKey subscriber has ordered and distributed with their status.

3SKey Developer Toolkit
To facilitate the implementation of the 3SKey subscriber application functions, SWIFT automatically provides the 3SKey Developer Toolkit to all 3SKey subscribers.

For more information about the 3SKey Developer Toolkit, see the 3SKey Developer Guide.

Web browser
The 3SKey subscriber browser accesses the 3SKey portal to retrieve the SSL certificates and to retrieve a report on its distributed tokens and their status. The 3SKey subscriber must ensure that its web browser meets the applicable specifications set out in the 3SKey Developer Guide.

2.3.3 3SKey User Components

3SKey user application
The application enables users to sign files and messages with the 3SKey token and to send them to the 3SKey subscriber’s application.

Note The 3SKey user is responsible for the integration of the 3SKey service with its application(s) using the 3SKey Developer Toolkit or with assistance of a vendor of its choice.

3SKey user tokens
The users install the software for the 3SKey tokens. They activate their token through the 3SKey portal and associate them with their 3SKey subscriber. Users can then use their tokens with their 3SKey subscriber either through the 3SKey user browser or through the 3SKey user application.

3SKey Developer Toolkit
To facilitate the implementation of the 3SKey user application functions, SWIFT provides an optional 3SKey Developer Toolkit.

For more information about the 3SKey Developer Toolkit, see the 3SKey Developer Guide.

Web browser
The 3SKey user accesses the 3SKey portal using a web browser. The portal is used for token management purposes (activation, revocation, recovery, and renewal). The web browser enables access to Web-based bank services (for example, cash management). The 3SKey user must ensure that its web browser meets the applicable specifications set out in the 3SKey Developer Guide.
2.4 Key Service Availability

3SKey certificate revocation check facility availability

The 3SKey certificate revocation check facility is designed to be available 24 hours a day, 7 days a week, through LDAPS and HTTPS channels, subject to any unavailability as set out hereafter.

SWIFT is not responsible if the 3SKey certificate revocation check facility cannot be reached due to problems with the internet channels used by the 3SKey subscriber.

Planned unavailability

SWIFT plans for specific dates and times when the 3SKey service, typically access to the 3SKey portal, will be unavailable. SWIFT notifies its customers in advance on www.swift.com of planned unavailability.

Planned unavailability can be for the following events:

- downtime due to scheduled equipment maintenance
- scheduled system changes (for example, changes to software or hardware configurations or business continuity testing)

SWIFT performs system changes and maintenance during allowable downtime windows. These windows occur during weekends (Saturday and Sunday).

During an allowable downtime window, the 3SKey portal may be unavailable either for the whole duration of the downtime, or only intermittently.

For more information about scheduled downtime, see www.swift.com > Support > Operational status.

Unplanned unavailability

If SWIFT becomes aware of a problem with the 3SKey service, then it initiates any recovery or fallback operation for which it is responsible and that is necessary to restore the service.

The levels of service that this document specifies assume normal operating conditions. These include resilient operations during most single-component failure scenarios within the active and standby SWIFT operating centres where SWIFT runs the 3SKey service. The 3SKey service design is resilient, and can handle many anomalous events without impact to the activities of the 3SKey subscribers and users. However, under certain, very unlikely, disaster scenarios (for example, the destruction of a SWIFT operating centre, dual failures of similar components, or component failures during SWIFT operating centre switchovers), SWIFT may be unable to meet these levels of service, in whole or in part. The potential for data loss also exists in a few of these rare circumstances.

Note In case a disaster strikes a SWIFT operating centre where SWIFT runs the 3SKey service, this may prevent SWIFT to process fully all revocation requests received in the 15 minutes preceding the disaster. In such case, the 3SKey users can contact SWIFT for assistance to trace the affected requests.
3 Ordering and Support

3.1 Ordering

Subscribe to the 3SKey service

Subject to the eligibility criteria in section 1.2, an organisation can subscribe to the 3SKey service using the 3SKey subscription form. It is mandatory to subscribe first to the 3SKey service in order to rely on a 3SKey certificate for live business transactions.

As an integral part of its subscription, the 3SKey subscriber is entitled to the following:

- access to the 3SKey portal
- access to the 3SKey certificate revocation check facility (maximum 10)
- 3SKey tokens as specified in the subscription form
- the 3SKey Developer Toolkit

Note

The subscription to the 3SKey service by a SWIFT user permits the 3SKey subscriber to extend, under its sole responsibility, the benefit of the subscription to affiliates within its corporate group. Otherwise, the subscription to the 3SKey service is personal. Consequently, the 3SKey subscriber may not share the certificate revocation list with a third party (or, in the case of a SWIFT user, a non-affiliated entity), or may not verify the status of a 3SKey certificate on behalf of a third party (or, in the case of a SWIFT user, a non-affiliated entity).

For more information about the right for 3SKey subscribers to use the 3SKey service, see the 3SKey Terms and Conditions.

Order 3SKey tokens

Subject to the eligibility criteria in section 1.2, an organisation can order the 3SKey tokens for its own use or distribution to 3SKey users using the 3SKey tokens order form.

The provision and use of 3SKey tokens are subject to U.S. export restrictions and other sanction programmes. Persons located in or from Cuba, North Korea, Iran, Sudan or Syria and persons identified on U.S. government or EU “denied party” or specifically designated nationals lists are not permitted to possess or use 3SKey tokens.

Order the 3SKey Developer Toolkit

Subject to the eligibility criteria in section 1.2, an organisation can order the 3SKey Developer Toolkit using the 3SKey Developer Toolkit order form.

3.2 Support

Support for 3SKey subscribers and the 3SKey Developer Toolkit

SWIFT is the single point of contact to report all problems and queries that relate to the 3SKey service and the 3SKey Developer Toolkit. Support is available to all 3SKey subscribers and other organisations that have ordered the 3SKey Developer Toolkit. Individual users within their respective organisation must register to use the Support service.

For more information about how to register for Support, see the Customer login section on the www.swift.com home page.
Related information

For more information about Support services, see the Support Service Description.

Support for 3SKey users

Online support for the token management functions is available for 3SKey users through the 3SKey portal.
4 Roles and Responsibilities

The following three parties are involved in the 3SKey solution:

- **SWIFT**: provides the 3SKey service and supplies the 3SKey tokens and the 3SKey Developer Toolkit
- **The 3SKey subscriber**: subscribes and integrates the 3SKey service and distributes 3SKey tokens to 3SKey users
- **The 3SKey user**: integrates and uses the 3SKey service with their 3SKey subscriber (or 3SKey subscribers). The 3SKey users will normally obtain the 3SKey tokens from their initial 3SKey subscriber.

The following graphic provides an overview of the interactions between the different parties:

![Diagram of interactions between SWIFT, 3SKey subscriber, and 3SKey user]

4.1 SWIFT’s Roles and Responsibilities

**Description**

SWIFT’s primary responsibilities are as follows:

- provision the service as described in this service description
- qualify the tokens
- personalise tokens with a Unique ID
- provide and implement the Certificate Policy
- ensure the uniqueness of the ID of a certificate from activation and through its complete lifecycle
- supply the inactive tokens
- provide a portal for 3SKey users for token management functions
- provide the 3SKey certificate revocation check facility to the 3SKey subscribers
- provide the 3SKey Developer Toolkit, including the technical specifications and the relevant libraries to integrate the 3SKey service in the applications of the 3SKey user and subscriber
Roles and Responsibilities

- provide support to 3SKey subscribers, 3SKey users and partners that have ordered a 3SKey developer toolkit
- provide 3SKey documentation that is available on www.swift.com
- report on the status (activated, not activated, revoked, or used for recovery) of the business certificates that are stored on the tokens ordered by a 3SKey subscriber
- revoke business certificates through an exception procedure
- provide, on request of the 3SKey user or subscriber, non-repudiable evidence of the activation, renewal, revocation, or recovery of a certificate performed on the 3SKey portal for up to 6 months after the expiry date of the certificate used
- provide, on request of the 3SKey user or subscriber, evidence of the revocation status of a specific certificate for up to 10 years

For more information about SWIFT's roles and responsibilities with regard to the 3SKey solution, see the 3SKey Terms and Conditions, the 3SKey Tokens Terms and Conditions or the 3SKey Developer Toolkit Terms and Conditions, as applicable.

4.2 The 3SKey Subscriber’s Roles and Responsibilities

Description

The 3SKey subscriber's primary responsibilities are as follows:

1. For the distribution of 3SKey tokens to the 3SKey users
   - order the necessary 3SKey tokens from SWIFT
   - subject to all applicable export restrictions and other sanctions programmes, distribute the 3SKey tokens and the associated password to the 3SKey users, and if not included on the tokens, link the 3SKey users to or supply the 3SKey users with the relevant installation instructions and software
   - manage the token renewal process with the 3SKey users

2. For the use of the 3SKey service
   - subscribe to the 3SKey service with SWIFT
   - integrate the 3SKey service with the 3SKey subscriber's application
   - provide 3SKey users with the relevant documentation for using the 3SKey service and tokens
   - provide 3SKey users with best-practice guidelines
   - associate and record the association of the tokens with 3SKey users that subscribe to the service
   - obtain and manage a valid SSL client certificate to secure the 3SKey certificate revocation check facility
   - obtain and manage a working internet connection to the 3SKey portal and the 3SKey certificate revocation check facility
   - define the internal rules for revocation check
   - apply a Know-Your-Customer policy for 3SKey users that use the 3SKey service
   - un-associate a 3SKey user upon his request
   - inform SWIFT of security threats that relate to the 3SKey service
   - verify the signatures of messages received from 3SKey users and check that the signing certificates are valid 3SKey business certificates

To the extent reasonably necessary for its use of the 3SKey solution, the 3SKey subscriber has the right, at its own cost and under its sole responsibility, to translate information provided by SWIFT and to include this information in its end-user documentation. Any such translations shall
however confirm that, towards SWIFT, the English version of SWIFT documentation is the only official and binding version.

More information

For more information about the 3SKey subscriber’s roles and responsibilities with regard to the 3SKey solution, 3SKey subscribers can refer to the 3SKey Terms and Conditions, the 3SKey Tokens Terms and Conditions, or the 3SKey Developer Toolkit Terms and Conditions.

4.3 The 3SKey User’s Roles and Responsibilities

Description

The 3SKey user’s primary responsibilities are as follows:

• perform integration work that relates to the functioning of the 3SKey service with the 3SKey subscriber (or 3SKey subscribers)
• activate the token through the 3SKey portal
• for authentication purposes towards SWIFT, safe keep the unique ID and related security code
• associate one or more tokens with the 3SKey subscriber (or 3SKey subscribers)
• perform token management according to the guidelines provided in the 3SKey documentation
• safe keep the acknowledgement of all management functions performed on the 3SKey portal
• order new tokens prior to token expiration
• revoke tokens in case of security threat, if the token is no longer used or as may be otherwise necessary or desirable.
• inform the 3SKey subscriber(s) of any security threat that may affect the use of the 3SKey service
• follow the best-practice guidelines provided by the 3SKey subscriber

More information

For more information about the 3SKey user’s roles and responsibilities with regard to the 3SKey solution, 3SKey subscribers can refer to the 3SKey Terms and Conditions, the 3SKey Tokens Terms and Conditions, or the 3SKey Developer Toolkit Terms and Conditions.
5 Pricing and Invoicing

5.1 Charges

The 3SKey subscriber must pay to SWIFT all charges and fees for the various components of the 3SKey solution.

The charges for the subscription to the 3SKey solution are as follows:

- a one-time service fee for the subscription by 3SKey subscribers to the 3SKey service
- a yearly recurring fee for subscription by 3SKey subscribers to the 3SKey service
- a one-time fee for the supply of the 3SKey tokens

For more information about the pricing scheme, see the Price List at [www.swift.com > Ordering > Pricing](http://www.swift.com > Ordering > Pricing).
6 Contractual Framework

Terms and conditions

The 3SKey Terms and Conditions govern the provision and use of the 3SKey service.

The 3SKey Tokens Terms and Conditions govern the supply, distribution and use of the 3SKey tokens.

The 3SKey Developer Toolkit Terms and Conditions govern the provision and use of the 3SKey Developer Toolkit.

Always consult swift.com

The latest available version of the 3SKey Terms and Conditions, the 3SKey Tokens Terms and Conditions, and the 3SKey Developer Toolkit Terms and Conditions is available at www.swift.com > About SWIFT > Legal

Other contractual arrangements between 3SKey subscribers and 3SKey users

It is for the 3SKey subscribers and their 3SKey users directly to consider any other contractual arrangements that are necessary or desirable amongst themselves in connection with their use of the 3SKey service.
## Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>3SKey</td>
<td>Stands for SWIFT Secure Signature Key.</td>
</tr>
<tr>
<td>3SKey portal</td>
<td>A web application server for 3SKey token and certificate management operations: activation, renewal, recovery, user group administration, security code change, and revocation.</td>
</tr>
<tr>
<td>3SKey subscriber</td>
<td>Organisation participating in the 3SKey service, SWIFT customer, with the intent of offering secure application to its customers. Typically, a bank.</td>
</tr>
<tr>
<td>3SKey user</td>
<td>Organisation, or an individual user in such organisation, that is customer of a 3SKey subscriber, with the intent of using the secure application provided by the 3SKey subscriber. Typically, a corporate.</td>
</tr>
<tr>
<td>Active token</td>
<td>A 3SKey token that holds a valid business certificate.</td>
</tr>
<tr>
<td>Administrator</td>
<td>A designated person in the 3SKey user's organisation, responsible for assigning tokens to a user group, distributing tokens to the users, revoking certificates and setting them up for recovery. The administrators can also view the status of the certificates for all tokens in their user group. The administrators can also perform all 3SKey user functions with their own tokens.</td>
</tr>
<tr>
<td>Business certificate</td>
<td>A certificate valid for signing a business transaction. Such a 3SKey certificate is identified with Policy ID 1.3.21.6.3.20.200.1.</td>
</tr>
<tr>
<td>Security code</td>
<td>Personal authentication string that is generated by the portal at activation time and that the 3SKey user can use to revoke its certificate and must provide to recover its certificate.</td>
</tr>
</tbody>
</table>
Legal Notices

Copyright
SWIFT © 2010. All rights reserved.
You may copy this publication within your organisation. Any such copy must include these legal notices.

Disclaimer
The information in this publication may change from time to time. You must always refer to the latest available version on www.swift.com.

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

Trademarks
SWIFT is the trade name of S.W.I.F.T. SCRL. The following are registered trademarks of SWIFT: SWIFT, the SWIFT logo, 3SKey, Innotribe, Sibos, SWIFTNet, SWIFTReady, and Accord. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.