



SWIFTNet Messaging Services

SWIFTNet 7.0

Release Overview

Version 1.0 - Preliminary version

This document provides customers with an overview of the key features that SWIFT will introduce with SWIFTNet 7.0

31 December 2008

Table of Contents

1	Introduction	4
2	Executive Summary	5
3	Key Release Dates	7
4	Expected Customer Impact.....	8
4.1	Customers.....	8
4.1.1	Mandatory change(s).....	8
4.1.2	Upgrade to release 7.0 interface software.....	8
4.1.3	Testing release 7.0	8
4.2	Interface and Application Providers	9
5	Detailed Release Contents and Expected Customer Impact.....	10
5.1	Message copy	10
5.1.1	Background.....	10
5.1.2	Changes introduced with this Release	10
5.1.3	Expected Impact	10
5.2	Message and file distribution	11
5.2.1	Background.....	11
5.2.2	Changes introduced with this release.....	11
5.2.3	Expected Impact	11
5.3	Using solutions made easier.....	12
5.3.1	Background.....	12
5.3.2	Changes introduced with this release.....	12
5.3.3	Expected Impact	12
5.4	RMA for InterAct and FileAct	13
5.4.1	Background.....	13
5.4.2	Changes introduced with this release.....	13
5.4.3	Expected Impact	13
5.5	Enhanced store-and-forward delivery options	14
5.5.1	Background.....	14
5.5.2	Changes introduced with this release.....	14
5.5.3	Expected Impact	14
5.6	Session history report	15
5.6.1	Background.....	15
5.6.2	Changes introduced with this release.....	15
5.6.3	Expected Impact	15
5.7	Easier SWIFTNet Link installation framework	16
5.7.1	Background.....	16
5.7.2	Changes introduced with this release.....	16
5.7.3	Expected Impact	16
5.8	Enhanced guidelines to monitor and operate SWIFTNet Link.....	17

5.8.1	Background.....	17
5.8.2	Changes introduced with this release.....	17
5.8.3	Expected Impact.....	17
5.9	Easier routing management using shared BIC operations	18
5.9.1	Background.....	18
5.9.2	Changes introduced with this release.....	18
5.9.3	Expected Impact.....	18
5.10	Security and routing management through new Browse GUI	19
5.10.1	Background.....	19
5.10.2	Changes introduced with this release.....	19
5.10.3	Expected Impact.....	19
5.11	Enhanced capability to handle undeliverable traffic.....	20
5.11.1	Background.....	20
5.11.2	Changes introduced with this release.....	20
5.11.3	Expected Impact.....	20
5.12	Ability to delete Distinguished Names (DNs)	21
5.12.1	Background.....	21
5.12.2	Changes introduced with this release.....	21
5.12.3	Expected Impact.....	21
5.13	On-line SWIFTNet Link certificate recovery.....	22
5.13.1	Background.....	22
5.13.2	Changes introduced with this release.....	22
5.13.3	Expected Impact.....	22
5.14	Enhanced access control to services.....	23
5.14.1	Background.....	23
5.14.2	Changes introduced with this release.....	23
5.14.3	Expected Impact.....	23
5.15	Easier role delegation	24
5.15.1	Background.....	24
5.15.2	Changes introduced with this release.....	24
5.15.3	Expected Impact.....	24
5.16	Enhanced Shared Security Officer functionality	25
5.16.1	Background.....	25
5.16.2	Changes introduced with this release.....	25
5.16.3	Expected Impact.....	25
5.17	Security administration segregation.....	26
5.17.1	Background.....	26
5.17.2	Changes introduced with this release.....	26
5.17.3	Expected Impact.....	26
5.18	Human password expiry enforcement	27
5.18.1	Background.....	27
5.18.2	Changes introduced with this release.....	27
5.18.3	Expected Impact.....	27
	Legal Notices	28

1 Introduction

This document provides customers with an overview of the key features that SWIFT will introduce with SWIFTNet 7.0.

2 Executive Summary

Lowering total-cost-of-ownership, providing new features, easier operations and more flexibility

SWIFTNet 7.0 is a major SWIFTNet release. It allows customers to benefit from new business features, provides various functional enhancements requested by several customers, and introduces changes that will simplify and ease operations. In the area of security administration, it brings new options that provide additional flexibility and ease specific time-consuming tasks.

Feature overview

Table 1 provides an overview of the new messaging features or changes that are part of this release, which SWIFT expects to make available on SWIFTNet by the end of June 2010.

Table 1: Summary of changes introduced with SWIFTNet 7.0

Area	Description of changes	Messaging service			
		FIN	InterAct	FileAct	Browse
Business features	1. Message copy		✓		
	2. Message and file distribution		✓	✓	
	3. Using solutions made easier		✓	✓	
	4. RMA for InterAct and FileAct		✓	✓	
Operational features	5. Enhanced store-and-forward delivery options		✓	✓	
	6. Session History Report		✓	✓	
	7. Easier SWIFTNet Link installation framework	✓	✓	✓	
	8. Enhanced guidelines to monitor and operate SWIFTNet Link		✓	✓	
	9. Easier routing management using shared BIC operations		✓	✓	
	10. Security and routing management through new Browse GUI	✓	✓	✓	✓
	11. Enhanced capability to handle undeliverable traffic		✓	✓	
Security features	12. Ability to delete Distinguished Names (DNs)	✓	✓	✓	
	13. On-line SWIFTNet Link certificate recovery	✓	✓	✓	
	14. Enhanced access control to services		✓	✓	
	15. Easier role delegation	✓	✓	✓	
	16. Enhanced Shared Security Officer functionality	✓	✓	✓	
	17. Security administration segregation	✓	✓	✓	
	18. Human password expiry enforcement		✓	✓	

The availability of the functionality mentioned in Table1, depends on whether the feature requires only an update on SWIFT's central systems, whether it requires the installation of the release 7.0 SWIFTNet Link/Alliance Gateway communication software, or if it requires also the release 7.0 of the messaging interface software. This is indicated per feature separately in section 5.

SWIFT customers can install and use the new SWIFTNet 7.0 interfaces at their earliest convenience, and must do so at the latest by end December 2011. As a precautionary measure, SWIFT recommends that developers and service providers conduct appropriate regression tests with SWIFTNet 7.0.

Alliance customers that want to use the new features that require an interface update, will need release 7.0 of the Alliance Portfolio. For more information about the Alliance releases, see the *Alliance Release Overview*, available on www.swift.com.

For more information about the overall SWIFTNet release policy, see the *SWIFTNet and Alliance Release Policy*, which is available on www.swift.com.

3 Key Release Dates

Table 2 provides the key target (tentative) release dates for SWIFTNet 7.0. All dates refer to end of month.

Table 2: Key target dates for SWIFTNet 7.0

Event	Target date / period	Description
Preliminary Release Overview and Vendors specifications	December 2008	Availability of the preliminary versions of the release overview and the developer's documentation
Final Release Overview Final Vendors specifications	August 2009	Availability of final release overview and the developers' documentation
Availability on integration testbed (ITB)	April 2010	Full availability of SWIFTNet 7.0 on ITB for developer testing. Availability of the final version of the SWIFTNet communication software (SWIFTNet Link and Alliance Gateway software).
Availability on production environment	June 2010	Full availability of SWIFTNet 7.0 on the Production environment for live operations.
General distribution	September 2010	Full availability of the SWIFTNet 7.0 qualified version of the Alliance interface products for live operations and general distribution.

4 Expected Customer Impact

SWIFT has designed and tested SWIFTNet 7.0 to ensure backward compatibility with customer systems working with releases 6.0, 6.1 and 6.3. Once the release is available, all users can install and use the new SWIFTNet 7.0 interface software at their earliest convenience, but must do so at the latest by end December 2011.

SWIFTNet 7.0 may impact SWIFT customers, service providers, and interfaces and application providers, as explained below.

4.1 Customers

4.1.1 Mandatory change(s)

RMA for InterAct and FileAct

Relationship Management Application (RMA) is a means to manage business relationships and is currently used for FIN traffic. SWIFT plans to provide similar RMA capabilities for InterAct and FileAct traffic. This means that customers' interfaces will have to be upgraded to support the required traffic filtering.

See section 5.4 for more information.

Human password expiry enforcement

With SWIFTNet 7.0, it will no longer be possible to use expired human passwords to exchange traffic using certificates that are protected with these passwords.

See section 5.18 for more information.

4.1.2 Upgrade to release 7.0 interface software

SWIFTNet 7.0 is accompanied by the following releases of SWIFT interface products:

- SWIFTNet Link 7.0
- Alliance Gateway 7.0
- Alliance Web Platform 7.0
- Alliance WebStation 7.0
- Alliance Starter Set 7.0
- Alliance Access/Entry/Workstation 7.0

SWIFT customers should upgrade their interfaces to the new releases mentioned above at their earliest convenience, but at the latest by end December 2011, after which date SWIFT will no longer support release 6.x interfaces.

Note that a number of the new messaging features associated with SWIFTNet 7.0 are only available when the customer uses an application or interface that was upgraded for SWIFTNet 7.0.

For more information about the SWIFT interface releases, see the *Alliance Release Overview*, available on www.swift.com.

4.1.3 Testing release 7.0

As a precautionary measure, SWIFT recommends that service administrators, vendors, and developers of in-house systems that support such customers conduct appropriate regression tests with release 7.0 of SWIFTNet on the developers' test environment, known as the Integration Testbed (ITB). SWIFT recommends that these tests involve representative traffic volumes and that they are performed as early as possible after the introduction of SWIFTNet release 7.0. This allows for increased reaction time in the unlikely event that problems are encountered.

In addition to the precautionary measures above, service administrators, vendors, and developers of in-house systems that support such customers may need to adapt their existing systems to the new functionality and, where appropriate, conduct the appropriate integration testing.

4.2 Interface and Application Providers

SWIFT also encourages interface and application providers to support the new features that SWIFT is introducing with SWIFTNet 7.0.

As of SWIFTNet 7.0, qualification of messaging interfaces is mandatory. SWIFT provides an overview of the mandatory and optional items for messaging interfaces in the document *SWIFTNet Messaging Services - Interfaces Vendor Specifications for InterAct and FileAct*. SWIFT plans to provide more information on the qualification programme separately.

5 Detailed Release Contents and Expected Customer Impact

This section outlines the changes that SWIFT will introduce with SWIFTNet 7.0.

5.1 Message copy

5.1.1 Background

With SWIFTNet 6.1, SWIFT had introduced copy capabilities on SWIFT, for SWIFTNet FileAct used in store-and-forward mode. This allows a service provider to set up a service where the FileAct header information is copied to a central place. It is available in T-copy (for information) or Y-copy mode (requiring authorisation to trigger delivery).

5.1.2 Changes introduced with this Release

SWIFTNet 7.0 introduces copy functionality for InterAct messages exchanged in store-and-forward mode. When used, SWIFT automatically copies the message to a copy destination. It can be used to either simply copy a message for information purpose (T-copy), or to make delivery dependent on approval of a third party that must authorise the message delivery (Y-copy).

The service administrator decides on the message flows that are copied, and which options are used related to this.

Copy for information purpose (T-copy)

In this mode, SWIFT delivers the message to the recipient (as usual), and simultaneously provides a copy of the message "for information" to one or more copy destination(s). This can be for example an accounting centre, a head office, a netting system or a regulatory body.

Copy for authorisation purpose (Y-copy)

In this case, SWIFT does not deliver the sender's message immediately to the recipient, but keeps it on hold at SWIFT. SWIFT copies the messages to the copy destination that must authorise, or refuse the transaction. If the message is authorised, then SWIFT delivers the original message to the recipient. If it is refused, then SWIFT does not deliver the message and informs the sender about the refusal.

Note This feature only supports full message copy, it currently does not support partial message copy.

5.1.3 Expected Impact

Type of impact	SWIFT does not expect impact for users or services that do not take advantage of this feature. Customers that want to take advantage of this feature will need to adapt or configure their business applications or interfaces.
Customers impacted	Customers that use SWIFTNet InterAct in store-and-forward mode and use services that use this new feature.
Start of impact	When the service administrator has defined the service to use this feature, when the customer has installed the SWIFTNet 7.0 compatible messaging interface software, and after SWIFT has deployed SWIFTNet 7.0.

5.2 Message and file distribution

5.2.1 Background

In some business contexts, the same message or file needs to be sent to several recipients. For example, in the context of message flows for loans, an agent bank may need to send the same message to a lender, to a custodian and possibly a central securities depository. Similarly, in the context of market data distribution, a provider may need to distribute the same market data file to dozens of recipients.

Today this is possible on SWIFTNet but requires the sender to send each message or file individually to each recipient.

5.2.2 Changes introduced with this release

SWIFT now introduces the possibility to send a message or file to a distribution list. In this case, the customer sends the message or file only once, together with a distribution list that contains the recipients that need to receive it. Because the sender provides the recipient list, the sender has full control over the list and can change it over time or even use a different one for every exchange.

This feature is available only for services that work in store-and-forward mode. The ability to distribute messages or files to recipients who are subscribed to the service, also depends on the traffic flows that the service administrator allows for the service.

Note If the message or file to be distributed is signed, then SWIFT can only deliver it to recipients who have also installed SWIFTNet 7.0 interface software. If it is not signed, SWIFT can deliver it to both 6.x and 7.0 interfaces.

5.2.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature. Customers that want to take advantage of this feature may need to adapt or configure their business applications or interfaces.
Customers impacted	Customers that use SWIFTNet InterAct or FileAct in store-and-forward mode and want to use this new feature.
Start of impact	When the customer has installed the SWIFTNet 7.0 compatible messaging interface software, and after SWIFT has deployed SWIFTNet 7.0.

5.3 Using solutions made easier

5.3.1 Background

Customers can use a number of solutions that SWIFT organises, for example Funds or Cash reporting. Customers currently need to first complete an order form to subscribe to such a solution. As part of the ordering process, customers also provide information related to routing and other operational parameters. Customers who want to use an additional solution need to subscribe specifically to that solution as well, even if they are operationally ready for the additional solution.

5.3.2 Changes introduced with this release

SWIFT will allow customers to subscribe to a many-to-many messaging environment that provides access to all solutions at once. This is similar to FIN where a subscriber to FIN can use all messages, in the context of various business solutions, (usually) without the need for explicit subscription or operational configuration per solution.

This will remove the need for ad-hoc subscriptions and repetitive and dedicated configuration setups, because most customers are happy to use default message routing and queue setup.

SWIFT plans to introduce this new approach once RMA for SWIFTNet services is available. This will offer full control on managing "who can exchange with who" in this many-to-many messaging environment.

SWIFT will publish the list of solutions that are eligible for this environment at a later date.

5.3.3 Expected Impact

Type of impact	Joining once provides access to all solutions that fall within the scope of this many-to-many environment.
Customers impacted	All users that use one or more solutions that SWIFT provides and that are in scope
Start of impact	When SWIFT has published that this new approach is available.

5.4 RMA for InterAct and FileAct

5.4.1 Background

With SWIFTNet Phase2 for FIN, SWIFT has introduced Relationship Management Application (RMA) as the new means to manage business relationships. The solution consists of two parts: customers exchange authorisations (indicating "who can send traffic to who") and their messaging interfaces apply these rules to control what traffic they can exchange with which correspondent.

5.4.2 Changes introduced with this release

SWIFT plans to provide similar RMA capabilities for InterAct and FileAct traffic.

SWIFT is currently finalising customer consultation, in order to collect feedback on aspects such as granularity of authorisations. The final version of this SWIFTNet 7.0 Release Overview will contain the details on this item.

5.4.3 Expected Impact

Type of impact	Customers will need to adapt or configure their business applications or interfaces.
Customers impacted	Customers exchanging InterAct or FileAct traffic.
Start of impact	When the customer has installed the SWIFTNet 7.0 compatible messaging interface software, after SWIFT has deployed SWIFTNet 7.0; and in line with the schedule for using RMA that SWIFT will make available.

5.5 Enhanced store-and-forward delivery options

5.5.1 Background

SWIFT already provides a number of advanced delivery features for store-and-forward delivery. These include, amongst others, the notions of delivery session with sequence numbering and possible duplicate indication, and the ability to specify the delivery order.

Currently, only one session can exist on a queue at the same time. If another system attempts to open a queue that is already open, SWIFT generates an error message. If the user decides to forcibly open the queue, then this action aborts the session that was open at that time.

5.5.2 Changes introduced with this release

With SWIFTNet 7.0, the following new delivery options become available:

1. The option to receive traffic from one queue on several systems in parallel

This is useful for customers who have several systems that receive traffic and are operational at the same time, because such a setup provides enhanced resilience as well as increased throughput (load balancing).

To use this option, customers must configure their queue(s) as "shareable". As of that moment, several concurrent sessions on the same queue will be allowed. When SWIFT delivers traffic from a queue and more than one session is open, SWIFT will distribute the traffic in a (roughly) equal manner over the different sessions. If a session is interrupted (for example because one of the receiving systems is not available), SWIFT will automatically adjust the traffic distribution to the remaining systems. When the system logs in again, it can participate in the traffic distribution again.

This option is equivalent to the "shared delivery subsets" feature on FIN.

2. The ability to specify a traffic subset

When opening a delivery session, it is possible to restrict delivered traffic to "messages only" or "files only". Similarly there is an option to deliver "urgent only" (or "normal only") traffic.

Note that these are "filters" that a message interface can specify when opening a session. It does not affect what traffic is routed to which queue, because that is defined upfront by the message routing rules that are centrally defined.

3. The availability of delivery notifications as system messages

With SWIFTNet 7.0, the (failed) delivery notifications become available also in the form of normal system messages. Before this release, they were only available as store-and-forward primitives to developers, and could not be processed in the same way as system messages.

5.5.3 Expected Impact

Type of impact	SWIFT does not expect any impact for users or services that do not take advantage of this feature. Customers that want to take advantage of this feature will need to adapt or configure their business applications or interfaces, for example to group the traffic together again towards backoffice application(s).
Customers impacted	Customers that use SWIFTNet InterAct or FileAct and want to use this new feature.
Start of impact	When the customer has installed the SWIFTNet 7.0 compatible messaging interface software, and after SWIFT has deployed SWIFTNet 7.0.

5.6 Session history report

5.6.1 Background

SWIFTNet uses the concept of "sessions" for traffic sent or received in store-and-forward mode. For traffic sent, this is the case when "input channels" are used. For traffic received, sessions are always used. During a session, traffic is marked with sequence numbers to support First-In-First-Out (FIFO) type of traffic exchanges.

5.6.2 Changes introduced with this release

This new feature allows a user to send a request to SWIFT to get a report with an overview of past sessions, with related session details. SWIFT will process this request, retrieve the necessary information and respond by sending the session history report.

When sending the request to SWIFT, it is possible to specify the timeframe and the input or output channels as parameters for generating the report. The report lists the session information, including open and close time, number of messages, sequence number range, and other related information.

These exchanges are in the form of system messages. SWIFT describes the technical details in the SWIFTNet Messaging Services - Interfaces Vendor Specifications for InterAct and FileAct and in the SWIFTNet system messages volume of the User Handbook.

5.6.3 Expected Impact

Type of impact	SWIFT does not expect any impact for users or services that do not take advantage of this feature. Customers that want to take advantage of this feature will need to adapt or configure their business applications or interfaces.
Customers impacted	Customers that use SWIFTNet InterAct or FileAct and want to use this new feature.
Start of impact	When the customer has installed the messaging interface software that can handle these system messages, and after SWIFT has deployed SWIFTNet 7.0.

5.7 Easier SWIFTNet Link installation framework

5.7.1 Background

Currently, SWIFTNet Link installation (or upgrade) uses an interactive, GUI-based installation procedure. On some environments, this involves the use of an X-terminal.

5.7.2 Changes introduced with this release

SWIFTNet Link 7.0 introduces a new installation framework to ease the installation (or upgrade) of SWIFTNet Link. This can provide significant time savings as well as reduce operational risk, particularly for customers with a large number of SWIFTNet Link instances.

Next to the existing GUI-based installation framework, SWIFT provides the ability to use a command-line installation based on an input parameter file prepared in advance for easy execution by operators. This approach can reduce the installation time, allows unattended installations of multiple instances, avoids manual errors and increase auditability of the actions performed in production environments.

The use of an input parameter file will also avoid user interaction during the installation process: Operation managers can prepare the parameter files for the different SWIFTNet Links in advance, so that the actual software installation can be scripted or carried out potentially by other parts of the organisation. This provides further segregation of duties if required.

In addition, this new installation method will no longer require the use of an X-terminal. This is because this represented for some customers a security concern, and for others implied some performance issues when executed remotely.

The interactive, GUI-based installation remains available as an alternative.

5.7.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that decide to use this new feature for SWIFTNet Link installations.
Start of impact	When the customer installs the SWIFTNet 7.0 compatible SWIFTNet Link software, and after SWIFT has deployed SWIFTNet 7.0.

5.8 Enhanced guidelines to monitor and operate SWIFTNet Link

5.8.1 Background

SWIFT provides documentation related to SWIFTNet Link in the SWIFTNet Link service description and the SWIFTNet Link release letters. For developers, SWIFT also provides technical documentation.

5.8.2 Changes introduced with this release

With SWIFTNet 7.0, SWIFT provides in the SWIFTNet Link documentation more guidelines on how to monitor/operate SNL. This will help customers to operate more efficiently and will support more pro-active management.

5.8.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers.
Customers impacted	There is no impact. Customers that use FIN, InterAct or FileAct can benefit from the enhanced documentation.
Start of impact	After SWIFT has deployed SWIFTNet 7.0 and made the related documentation available.

5.9 Easier routing management using shared BIC operations

5.9.1 Background

Today, SWIFTNet provides the ability to reroute real-time traffic between two or more SWIFTNet Links for all traffic, or for a specific traffic flow (for example, the traffic of one service). This allows a customer to switch traffic delivery from one system to another without the need to contact SWIFT. Similarly, SWIFT provides a function to query the routing rules and to display for each routing rule to which SWIFTNet Link SWIFT will deliver real-time traffic.

Currently, customers need to execute the reroute (or the getroutingrules) command separately for each BIC that occurs as responder in the relevant routing rules.

5.9.2 Changes introduced with this release

With SWIFTNet 7.0, customers have the option to execute the routing functions to cover more than one BIC at once. To do this, customers can define several BICs in the scope of the *SiteManager* role, by adding them to the *Includes* qualifier for that RBAC role. When customers execute a routing command, SWIFT will check the *SiteManager* role and the BICs that are defined as part of its scope. This will determine for which group of responder BICs the routing command will have effect.

5.9.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use SWIFTNet InterAct or FileAct and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.10 Security and routing management through new Browse GUI

5.10.1 Background

SWIFT provides the ability for customers to manage their SWIFTNet security and routing online. Customers currently require an application such as the Alliance WebStation to administer their certificates, roles and routing rules.

5.10.2 Changes introduced with this release

SWIFTNet 7.0 introduces the ability for customers to administer their security and routing through a new SWIFT-managed service available over Browse. This service offers access to the same functionality as the GUI on the Alliance WebStation. Also, new functionality will be available through this Browse service. Note that this new functionality will not be implemented on the Alliance WebStation.

This approach has the advantage that SWIFT can introduce enhancements to these functions without the need for customers to install a new version of a local application.

This new service will also enable various new security features described under sections 5.12 through 5.16.

5.10.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that decide to use this new feature for security, role or routing management.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.11 Enhanced capability to handle undeliverable traffic

5.11.1 Background

When customers exchange traffic in store-and-forward mode, currently SWIFT has no functionality to prevent messages or files being delivered.

5.11.2 Changes introduced with this release

With SWIFTNet 7.0, SWIFT implements central functionality that allows SWIFT to suspend delivery of a message or file sent in store-and-forward mode. Typically this will be used in the rare case where a receiver has problems receiving a specific message or file, and asks SWIFT to put this message or file on hold. This allows SWIFT to continue to deliver other traffic.

If the receiver can resolve the issue, they may request to SWIFT Customer Support Centre to release the message or file for delivery. Alternatively, they can ask to SWIFT to terminate further delivery attempts, in which case the sender will receive, as usual, a failed delivery notification.

5.11.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use SWIFTNet InterAct or FileAct in store-and-forward mode, and need to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.12 Ability to delete Distinguished Names (DNs)

5.12.1 Background

SWIFT provides the ability for customers to manage their SWIFTNet security online. Security Officers are responsible to administer the SWIFTNet PKI tree for their institution. They can create new users and can issue a certificate to these. Security Officers can also revoke certificates and disable users, after these have become obsolete. However, the disabled users stay visible to the Security Officers.

5.12.2 Changes introduced with this release

SWIFTNet 7.0 introduces the ability for Security Officers to delete obsolete users. If the user held a certificate, Security Officers will first need to revoke the certificate, remove the roles and disable the user for at least 124 days before they can delete it. This period ensures that pending operations, involving the user that needs to be deleted, complete gracefully (such as if the user had signed traffic with the non-repudiation option). If the user never held any certificate, Security Officers can immediately delete it.

Note

This new feature is only available through the new Browse GUI, see section 5.10 for more information.

5.12.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use the new Browse GUI for their security management (see section 5.10) and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.13 On-line SWIFTNet Link certificate recovery

5.13.1 Background

Each SWIFTNet Link instance owns a certificate used for communication with SWIFT. When issuing new SWIFTNet Link instances to customers, SWIFT prepares the SWIFTNet Link instances for certification and provides customers with initial secrets. Customers then use these secrets to generate the SWIFTNet Link certificates at installation time. Later on, if customers would ever need to recover their certificates, they would need to request SWIFT to prepare the SWIFTNet Link instances for recovery and to issue new initial secrets off-line.

5.13.2 Changes introduced with this release

SWIFTNet 7.0 introduces the ability for customers to recover their SWIFTNet Link certificates on-line. Customers will be able to prepare their SWIFTNet Link instance for recovery without SWIFT involvement, similarly to how they manage other certificates. A new role will allow customers to control who in their institution can manage their SWIFTNet Link certificates.

Note

This new feature is only available through the new Browse GUI, see section 5.10 for more information.

5.13.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use the new Browse GUI for their security management (see section 5.10) and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.14 Enhanced access control to services

5.14.1 Background

SWIFTNet provides the optional ability for services to use Role-Based Access Control (RBAC). The service administrators decide if this feature is used for their service. When it is used, customers must assign the relevant RBAC roles to the users who need to send traffic on such services. In such a case, SWIFT will reject traffic that users send on a service for which they do not have any RBAC role. This allows customers to control who can access which services within their institution.

Currently, such access control is only possible for services that use RBAC.

5.14.2 Changes introduced with this release

SWIFTNet 7.0 introduces the ability for customers to control user access to services not using RBAC. Customers will be able to subscribe to this new optional feature. SWIFT will then provision a new role for each non-RBAC service to which the customer has subscribed. After that, customers will be able to assign these roles to all users involved in these services within their institution. When customers are ready with the changes, they will be able to activate on-line the central enforcement for each service individually. Once activated for a service, SWIFT will reject traffic that users send on that service if they don't have the corresponding RBAC role.

Note

This new feature is only available through the new Browse GUI, see section 5.10 for more information.

5.14.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use the new Browse GUI for their security management (see section 5.10) and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0 and after customers have activated this feature.

5.15 Easier role delegation

5.15.1 Background

SWIFT provides the ability for customers to manage their SWIFTNet security online. Security Officers are responsible to administer the SWIFTNet PKI tree for their institution. They can create new users and assign them roles. For each relevant service, Security Officers need to assign roles to each user one-by-one.

5.15.2 Changes introduced with this release

SWIFTNet 7.0 will allow the simplification of role delegation for customers managing a large number of users, especially for services that use multiple roles. The following enhancements become available:

- The possibility for customers to assign roles to a group of users in one action. This avoids having to assign the roles to each user individually.
- The ability to use the profile of a user as a template for assigning roles to other users. This allows the Security Officer to assign in one action roles to other users who need to share the same set of roles.

Note

This new feature is only available through the new Browse GUI, see section 5.10 for more information.

5.15.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use the new Browse GUI for their security management (see section 5.10) and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.16 Enhanced Shared Security Officer functionality

5.16.1 Background

SWIFT allows customers to manage their SWIFTNet security online. Security Officers are responsible to administer the SWIFTNet PKI tree for their institution. Customers can also decide to delegate this to the Security Officers of another institution; this is the Shared Security Officers option. Currently only Security Officers that are at the top level within an institution can become Shared Security Officers and their scope of authority includes the entire tree of the other institution(s).

5.16.2 Changes introduced with this release

SWIFTNet 7.0 allows customers to use the Shared Security Officer functionality with more flexibility. Customers will be able to appoint Security Officers that are at a lower level within their institution as Shared Security Officers and to limit their scope of authority to a subset of the other institutions' tree. To do this, top-level Security Officers will be able to delegate the Shared Security Officer role to lower-level Security Officers within their institution. They will also be able to specify the branches that the new Shared Security Officers should be able to administer within the other institution(s).

Note

This new feature is only available through the new Browse GUI, see section 5.10 for more information.

5.16.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that use the new Browse GUI for their security management (see section 5.10) and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.17 Security administration segregation

5.17.1 Background

SWIFT allows customers to manage their SWIFTNet security online. Security Officers are responsible to administer the SWIFTNet PKI tree for their institution. Customers can limit the scope of authority of their Security Officers to specific branches within their institution tree.

5.17.2 Changes introduced with this release

With SWIFTNet 7.0, it will become possible for customers to segregate security administration in their institution. Customers will be able to appoint Security Officers for managing certificates and roles for test environments only.

To do this, customers should dedicate a branch in their institution tree for test environments and limit the scope of authority of “test” Security Officers to this branch. New roles will allow customers to ensure that “test” Security Officers can only manage lite certificates and that they can only delegate roles for pilot services.

5.17.3 Expected Impact

Type of impact	SWIFT does not expect impact for customers that do not use this new feature.
Customers impacted	Customers that perform their security management and want to use this new feature.
Start of impact	After SWIFT has deployed SWIFTNet 7.0.

5.18 Human password expiry enforcement

5.18.1 Background

SWIFT provides a mechanism for customers to protect the access to their SWIFTNet PKI private keys using passwords. SWIFTNet 6.0 has introduced uniform password practices that depend on whether a certificate is owned by a human or by an application. Customers can specify the type of password policy to use when creating new users or when recovering existing users.

Each password policy enforces a specific set of rules, including the renewal frequency. With SWIFTNet 6.0, if an expired password is used, SWIFTNet Link only generates warnings.

Note that SWIFTNet interfaces may already enforce password renewal.

5.18.2 Changes introduced with this release

With SWIFTNet 7.0, it will no longer be possible to use expired human passwords.

For application passwords, however, there is no change. If an expired application password is used, SWIFTNet Link will continue to only generate warnings.

5.18.3 Expected Impact

Type of impact	Customers can no longer use human passwords that have expired to exchange traffic using certificates that are protected with these passwords .
Customers impacted	Customers that use InterAct or FileAct with SWIFTNet PKI certificates with human passwords.
Start of impact	When the customer has installed SWIFTNet Link 7.0 .

Legal Notices

Copyright

SWIFT © 2008. All rights reserved.

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

Confidentiality

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

Disclaimer

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