Connectivity

SWIFTNet Link 7.0

Functional Overview

December 2010

Table of Contents

1 Introduction

SWIFTNet Link

SWIFTNet Link is SWIFT's mandatory software product for customers of SWIFTNet services. SWIFTNet Link provides the minimal functionality for technical interoperability between customers that use SWIFTNet services.

SWIFTNet Link is designed to provide the following functionality:

- the necessary minimal functionality to access and use SWIFTNet services over the SWIFT secure IP network
- the technical interoperability at the customer end between the requestor application and the network and between the secure IP network and the responder application.

Purpose of this document

The purpose of this document is to provide a description of the main functional enhancements on SWIFTNet Link 7.0 as well as the other functionalities that are removed in this release.

2 Enhancements and features

2.1 Message and File Copy

SWIFTNet 7.0 introduces additional copy functionality for InterAct messages and FileAct files exchanged in store-and-forward mode. It also adds more flexibility in terms of determining the copy destination.

When the copy feature is used, SWIFT can now automatically copy the entire message or file to a copy destination. It can be used to either simply copy a message or file for information purpose (T-copy), or to make the delivery dependent on approval of a third party that must authorise the message delivery (Y-copy).

The service administrator decides on the traffic flows that are copied, and which options are used related to this. Note that the FileAct header-only copy remains available as an option.

Copy for information purpose (T-copy)

In this mode, SWIFT delivers the message or file to the recipient (as usual), and simultaneously provides a copy of the full message or file "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 full message or file to the copy destination that must authorise, or refuse the transaction. If it is authorised, then SWIFT delivers the original message or file to the recipient. If it is refused, then SWIFT does not deliver the message or file, and informs the sender about the refusal.

Note For messages, this feature only supports full message copy.

2.2 Message and File Distribution

SWIFTNet 7.0 introduces the ability 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 have 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 (for example when non-repudiation is used), then SWIFT can only deliver it to recipients who have also installed SWIFTNet 7.0 interface software. Recipients who do not have the required interface software will not receive the signed message or file. Instead, SWIFT will send a failed delivery notification to the sender, for each such receiver in the distribution list. If the message or file distribution request is not signed, SWIFT can deliver it to both 6.x and 7.0 interfaces.

2.3 Enhanced Store-and-Forward Delivery Options

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

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, as 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" and use the SWIFTNet 7.0 interface software. 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), then 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.

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 messaging interface can specify when opening a session. It does not affect what traffic is routed to which queue, because customers define this routing upfront through their message routing rules.

Availability of delivery notifications as system messages

With SWIFTNet 7.0, the delivery notifications and 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.

2.4 Session History Report

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 putting the session history report in a queue.

When sending the request to SWIFT, it is possible to specify the time frame 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 *Interface Vendor Specifications for InterAct and FileAct* and in the SWIFTNet System Messages volume of the User Handbook.

2.5 Enhanced Traffic Segregation

With SWIFTNet 7.0, SWIFT provides additional segregation capability to channel InterAct traffic and FileAct traffic separately, over the lines of an Alliance Connect Gold connectivity product.

This allows customers to channel for example Browse and InterAct traffic over one line, and FileAct traffic over the other. Alternatively, it allows to channel Browse and FileAct over one line, and InterAct over the other.

Customers can configure this setup using a new SWIFTNet Link command. They must also update their firewall(s) as mentioned in the *Network Access Control Guide*.

Note In this context, FIN traffic follows the same path as InterAct traffic.

For more information, see the *SWIFTNet Link Operations Guide*.

2.6 Enhanced Error Text

In SWIFTNet 6.3, SWIFT has enhanced (and simplified) the error text or severity for a number of common errors generated by SWIFT's central system.

With SWIFTNet 7.0, SWIFT enhances the error text (or severity) for a number of remaining error areas, including errors generated by SWIFTNet Link of the HSMs. In particular, the description now allows to better identify the root cause of the problem (for example, if the problem is with the sender or receiver).

To ensure backward compatibility, SWIFT does not provide the new error text by default. Therefore, application developers must explicitly select the new error reporting to benefit from this enhancement. SWIFT expects that in a future release, this new capability will become the default mode.

Customers will see the new, simplified error text when they use applications that select the new error reporting mode and that show the SWIFTNet error text to customers.

2.7 Easier Reconciliation of Notifications

SWIFTNet 7.0 introduces the ability to receive the store-and-forward notifications as system messages. These system messages include the same header information that was used for the original message or file.

This enhancement will ease the reconciliation as customers can now determine the context of the original message or file directly from the notification, instead of having to find back this information through the technical reference.

Customers who want to take benefit of this enhancement must check with their application developer or interface vendor to ensure that their implementation uses the new approach of using system messages for notifications.

2.8 General Security Enhancements

SWIFTNet Link 7.0 introduces the following security enhancements:

Human password expiry enforcement

With SWIFTNet Link 7.0, customers can decide to block certificates that have an expired human password. Once this option is activated, it will not be possible to use these certificates for signing traffic. To be able to use their certificates again, users must first change their password. Users can still change the password of their certificates even if they have already expired.

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

Use of Policy OIDs for all certificates

In line with industry best practices, SWIFT will implement a Policy Object Identifier (Policy OID) for each SWIFTNet PKI certificate. Comprehensively using Policy OIDs ensures that non-business certificates can be easily differentiated from each other and that there is a unique and unambiguous relationship between a given certificate and its corresponding Certificate Policy.

SWIFT will assign the appropriate Policy OID to existing non-business certificates such that over time, through their normal renewal process, these certificates will acquire the assigned Policy OID. All new non-business certificates created after the deployment of SWIFTNet 7.0 will immediately acquire the appropriate Policy OID. There is no change to the Policy OID values of business certificates.

End-to-end signature

SWIFTNet 7.0 introduces new service attributes that allow to mandate the use of an end-to-end signature and to specify the format of the signature (either crypto block or signature list) for all traffic exchanged on a service. SWIFT will centrally check that traffic sent on a service is compliant with the selected service attributes.

2.9 Enhanced HSM Resilience and Security

SWIFTNet Link 7.0 introduces the following HSM box resilience and security enhancements:

Support for additional boxes per cluster

Customers will now be able to configure an HSM cluster with up to four boxes. The HSM cluster will keep certificates up-to-date between the primary box and all the replicas. It will only use two boxes for signing at any time and automatically switch traffic to a replica in case of failure.

This feature allows restoring cluster operations without manual intervention when a box becomes unavailable. It also allows to have spare boxes actively connected in the cluster, keeping their configuration up-to-date and ensuring their correct functioning before they are needed.

Note that the current network and security requirements that apply between a SWIFTNet Link and an HSM box and between HSM boxes will also apply to the additional boxes.

For details on these requirements, see the *Network Access Control Guide*.

Concurrent use of HSM certificates over multiple SNLs

Currently, customers need to set up distinct certificates for SWIFTNet Links used by an application in multi-active mode. SWIFTNet Link 7.0 removes this restriction by ensuring that only one SWIFTNet Link can update a certificate at a time.

This feature will allow customers to rationalise the number of certificates needed for applications using multi-active SWIFTNet Links.

SWIFT recommends changing these certificates or their password only outside of business hours as all systems using these certificates must be updated simultaneously.

Avoid application certificates lock-out due to invalid logins

Customers will be able to optionally configure, on their HSM boxes, a different lock-out policy based on the password length of their certificates. Therefore customers can ensure that application certificates (that is, certificates that are protected by sufficiently long passwords) are not automatically locked-out after multiple consecutive invalid login attempts.

This feature allows to protect application certificates from denial-of-service attacks within the customers’ institution, which could result in service disruption of critical applications such as FIN.

SWIFT advises to use this option when application certificate passwords are generated randomly and renewed at least every two years (as recommended in the password policy). The current lock-out policy is unchanged for human certificates whose passwords are short and might be vulnerable to brute force attacks.

Improved power management in HSM box

Currently the CPU on the HSM box is set to operate at its maximum frequency regardless of the load on the system. The result is greater power consumption than necessary. HSM software version 5.6 will load and enable CPU governors to give the operating system more control over the power management. This results in reduction in power consumption and heat generation.

2.10 Improved HSM Operability

SWIFTNet Link 7.0 introduces the following HSM box operability enhancements:

Interfaces can now integrate HSM box commands

Interfaces are now able to provide customers with certain HSM box management commands such as activating an HSM box, initialising a partition or opening a Remote PED session, thereby avoiding the need to use the SWIFTNet Link environment for such commands.

Note Excessive use of the HSM commands can result in reduced Main Message Flow throughput.

Flexible HSM box identification in a cluster

Customers can now select a unique HSM box identification for a cluster from HSM1 to HSM99, thereby avoiding ambiguous HSM cluster name and profile names. Renaming an existing cluster will require the cluster reconfiguration and re-creation of profiles.

Easier HSM registration for a SWIFTNet Link running on a cluster

Customers running a SWIFTNet Link instance on a cluster platform (with two hosts in active/standby mode sharing disks), will be able to register their HSM boxes by updating the SWIFTNet Link on the active host only. They will no longer have to repeat the HSM registration after switching the SWIFTNet Link instance over to the standby host.

2.11 Enhanced HSM Supportability

SWIFT introduces the following HSM box supportability enhancements as of SWIFTNet 7.0:

Ability to monitor SSL certificate validity

A new option has been introduced to the existing SWIFTNet Link command (`perl SwHSMCertRenewal.pl`) which allows customers to query their SSL certificate creation dates. This allows customers to monitor and plan timely renewals of these certificates.

Ability to synchronise the HSM box clock with the SNL clock

Currently, customers can use a SWIFTNet Link command to change the date and time of their HSM box to a new specified value. Currently, customers can use a SWIFTNet Link command (`perl SwHSMManageServices.pl)` to change the date and time of their HSM box to a new specified value. This command has been enhanced to allow customers to use the SWIFTNet Link host date and time to set the HSM box date and time. This will simplify problem investigation as events can be more easily correlated between logs.

Improved HSM box logs

The HSM logs contain more concise log entries for `SwHSM` commands.

Ability to enable regular backup of HSM box database

A new SWIFTNet Link command (`perl SwHSMDBBackupRestore.pl`) allows customers to enable backup of the HSM box database, list the existing backup files of an HSM box, and restore a backup file to the HSM box. Backups of up to 15 days will be stored on the HSM. Any changes performed after the backup will be lost as a result of this restore.

Improved HSM box IP address change procedure

SWIFTNet Link 7.0 introduces a new SWIFTNet Link command (`perl SwHSMIPUtil.pl`) to ease the procedure for changing the IP address of an HSM box.

For more information, see the *Hardware Security Module Operations Guide.*

2.12 Operational Enhancements

Silent installation framework

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

In addition 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 increases the auditability of the actions performed in production environments.

The use of an input parameter file also avoids user interaction during the installation process. Operations 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 no longer requires the use of an X-terminal. For some customers, this represented a security concern, and for others implied some performance issues when executed remotely.

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

Self-managed SNL certificate

Each SWIFTNet Link system has its own instance certificate, which is used to secure the messaging layer and allows SWIFT to authenticate the customer's SWIFTNet Link system. This certificate is created during the SWIFTNet Link installation.

In previous releases, the user assigned a password which needed to be kept for later use (for example, in case of re-installation).

With SWIFTNet Link 7.0, this certificate is fully managed by SWIFTNet Link at installation and during future upgrades. The user no longer needs to manage the password of this certificate.

Avoid timeout due to multiple security profile renewals

When multiple security profiles in their renewal period are opened at the same time (e.g. by the communication interface, such as Alliance Gateway), the renewal operation can take more than one minute per profile. The serialisation of these operations may take time and subsequently generate time-outs at the level of the messaging interface.

SWIFTNet Link 7.0 controls the number of profiles that can be renewed at the same time. If a dedicated threshold is reached, remaining renewals will be postponed for later login.

Manual renewal of a certificate can still be triggered using the `CertInfo` command.

Ability to identify outdated HSM certificates

A new option has been introduced to the existing SWIFTNet Link `Certlist` command which allows customers to identify outdated certificates stored on their HSM. It will retrieve the details of the certificate stored on the HSM and compare them with the details of the latest certificate available in the SWIFTNet Directory.

3 Obsolete Functionality

The following functionality is suppressed or replaced in this release of Alliance Gateway.

3.1 End of Dial-up Support

As of SWIFTNet Link 7.0, SWIFT discontinues the dial-up technology and has therefore not qualified SWIFTNet Link 7.0 with the dial-up connectivity product. Consequently, dial-up technology is no longer supported on release 7.0.

What is the impact for Prime Dial customers?

In order to benefit from the new features and enhancements introduced with SWIFTNet 7.0, customers using dial-up as their prime connectivity must first upgrade their network connectivity to one of the Alliance Connect products before upgrading their SWIFTNet software to release 7.0.

Customers using Dual-I with a dial-up back-up line are however not impacted and can safely implement SWIFTNet 7.0 as soon as it becomes available.

What is the standard upgrade scenario for Prime Dial customers?

SWIFT recommends that Prime Dial customers choose Alliance Connect Bronze as a replacement option for their network connection. For more information about Alliance Connect, see the connectivity pages on www.swift.com.

3.2 End of Support for previous HSM card reader model

SWIFTNet Link 7.0 does not support the HSM card reader model (Reflex USB from Gemalto) that was supported on SWIFTNet Link 6.x versions. A new hardware model (PC USB-SW Reader from Gemalto) is introduced with SWIFTNet Link 7.0 replacing the old one.

Customers using the HSM card reader need to switch to the new model when installing SWIFTNet Link release 7.0. The HSM cards used with the previous HSM card reader model can be used transparently with the new HSM card reader model.

Legal Notices

Copyright

Confidentiality

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

Disclaimer

SWIFT supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version on www.swift.com.

Translations

The English version of SWIFT documentation is the only official 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.