SWIFT Compatible Interface – Security Conformance Requirements

Conformance Statement

This document lists the security requirements that a messaging/communication interface must comply with. These requirements are extracted from the Customer Security Controls Framework v2021.

Revision: July 2020

Table of Contents

Significant Changes

This section lists all significant changes to the content of the Interface - Security Conformance Requirements since the July 2019 edition.

The table does not include editorial changes that SWIFT makes to improve the usability and comprehension of the document.

New and updated information since the July 2019 edition of the Interface Certification – Security Conformance Requirements	Location
Control 1.4 - 'Restriction of Internet Access' made mandatory in the CSCF v2021	Page 6

1 General Information

1.1 Supplier

Full name of the organisation that has registered this interface product and the name of the author of this Conformance Statement.

Organisation	
Author	
Date	

1.2 Product Information

The name and version numbers of the interface product to which this certification and conformance claim applies.

Product Name *		
Product Version Number		
Product Functionality	**FIN**	
	RMA	
	FileAct Store-and-Forward	
	FileAct Real-time	
	InterAct Store-and-Forward	
	InterAct Real-time	
	Communication Interface	

Note *: If your messaging/communication interface has different names for the different protocols it supports, then please provide the names accordingly.

1.3 Operational Environment

The hardware platform(s) and/or software platforms for which this product's performance is guaranteed

Hardware Platform on which product is guaranteed	
Software Platform on which product is guaranteed	

2 Conformance Requirements

The security conformance requirements list the security requirements that a messaging/communication interface must comply with. These requirements are derived from the corresponding Customer Security Controls Framework (CSCF) version.

SWIFT ensures that CSCF controls updates are typically announced mid-year, with attestation and compliance by SWIFT users against the mandatory controls outlined in this release by the end of the version year (end 2021 for v2021). In line with the CSCF change management process, the corresponding security conformance requirements is also announced mid-year.

Messaging/communication interface providers must attest their compliance to v2021 of the security conformance requirements by mid-2021 (self-attested). The customer confirmation needs to be completed by end 2021 (compatible). Customer confirmation of the vendor self-attestation can be achieved either after the installation of the product, by demo, or any other means that enables the customer to evaluate correctness of the vendor self-attestation.

The tables below identify the mandatory and optional elements that an interface product may support.

- Column **Feature** identifies the feature.
- Column **Ref** contains the reference to the relevant section in the Customer Security Framework document
- Column **Note** contains references to notes which describe the feature in more detail and where appropriate gives reference to the specification source.
- Column **M/A** describes whether the feature is Mandatory or Advisory.
- The next columns (one per interface protocol type) is marked “E”, “S” or “N” to indicate support of the feature, where “E” means that the feature is embedded in the software, “S” means that the feature is supported by the software (e.g. by 3rd-party solution), and “N” means the feature is not supported. “N/A” indicate that this interface type is not supported by the product, or the requirement is not applicable to the given protocol.
  The following protocols are listed: FIN, RMA, FileAct Store-and-forward (FA SnF), FileAct Real-time (FA RT), InterAct Store-and-forward (IA SnF), InterAct Real-time (IA RT), Communication Interface (Comm Intf).
  Note: Although there is no protocol certification for InterAct Real-time, vendors are requested to confirm their compliance if their messaging interface supports this protocol.

- *Customer Confirmation* row to be completed by the customer, after interim certification.

Important:
It is advised that the customer can easily report on the different requirements specified below. The messaging/communication interface can optionally implement a Configuration Reporting function listing its different settings in a single report.

The configuration reporting function is mandatory for messaging/communication interfaces used by SWIFT Service Bureaux.

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Configuration Reporting function	N/A	N/A	A							

2.1 Restrict Internet Access & Protect Critical Systems from General IT Environment

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
SWIFT Environment Protection	1.1	A1	M							
Customer Confirmation										
Operating System Privileged Account Control	1.2	A2	M							
Customer Confirmation										
Restriction of Internet Access	1.4	A3 & A4	M							
Customer Confirmation										

Notes

A1 The messaging/communication interface must support the deployment in a secure zone and allow customers to respond to the following requirements.
Software in the secure zone can only be used to operate, monitor and manage the secure zone and includes also the SWIFT-related components (messaging interface, communication interface, browser-based GUI, SWIFTNet Link, Hardware Security Module (HSM), jump server, and any applicable operator PCs solely dedicated to the operation or administration of the local SWIFT infrastructure).

Interactions with systems outside the secure zone must be limited to:
- Bi-directional communication with back-office applications
- Outbound logging data

This interaction must be controlled by transport layer statefull firewalls possibly in combination with ACLs and application firewalls.
Operators can access the secure zone systems:
- From dedicated operator PCs within the secure zone on which internet access is highly restricted and ideally blocked.
- From a general purpose operator PC to the secure zone via a jump server located within the secure zone (using e.g. a Citrix-type solution or Microsoft Terminal Server) that does not have internet access.
- From a general purpose operator PC, if they only access the messaging or communication interface by means of a browser-based GUI that is located in the secure zone and is logically separated from the messaging and communication interface. See the point A4 below for specific security controls under this set-up that cannot be used for operating system administration activities

A2 The messaging/communication interface must restrict to the maximum extent possible the use of administrator-level operating system accounts, unless needed to install, configure, maintain, operate and support emergency activities.

A3 The messaging/communication interface must restrict to the maximum extent possible the access to the internet. If internet access is needed from the secure zone, access should be granted only to whitelisted URL destinations via a proxy with content inspection and adequate blocking/filtering controls. Connections are only permitted if initiated in the outbound direction.

A4 Control internet access provided on the general purpose operator PCs used to access a messaging or communication interface through a browser-based GUI, through one of the following options:
1. Internet access through a remote desktop or virtual machine solution
2. Internet access from the general purpose operator PC to only whitelisted URL destinations via a proxy with content inspection, in combination with adequate blocking/filtering controls and permitting only outbound initiated connections.
3. Internet access from the general purpose operator PC through a Web Gateway (with content inspection, in combination with blocking/filtering controls) using maintained blacklisted URL destinations

2.2 Reduce Attack Surface and Vulnerabilities

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Internal Data Flow security	2.1	B1	M							
Alliance Gateway, LAU for relaxed MP		B1A	M							
Customer Confirmation										
Security Updates	2.2	B2	M							
Customer Confirmation										
System Hardening	2.3	B3	M							
Customer Confirmation										
Back Office Data Flow Security	2.4A	B4	M							
Customer Confirmation										
External Transmission Data Protection	2.5A	B7	M							
Customer Confirmation										
User Session Confidentiality and Integrity	2.6	B1 & B5	M							
Customer Confirmation										
Transaction business controls	2.9A	B6	A							
Customer Confirmation										
Application Hardening	2.10	B8	M							
Customer Confirmation										
RMA Business Controls	2.11A	B9	M							
Customer Confirmation										

Notes

B1 The messaging/communication interface must use confidentiality, integrity, and mutual authentication mechanisms (such as 2-way TLS, or LAU in combination with a confidentiality protection) to protect data flows with other systems in the secure zone. This includes following data flows:

- GUI to messaging interface
- RMA application to messaging interface
- GUI to communication interface
- Messaging interface to communication interface

Secure protocols use current, commonly accepted cryptographic algorithms (for example, AES, ECDHE), with key lengths in accordance with current best practices. More guidelines on cryptographic algorithms can be found in SWIFT Knowledge Base TIP 5021566.

The communication between the Operator PC and the messaging/communication interface is protected using a secure mechanism (for example, one-way TLS) to support the confidentiality, integrity and authentication of the connection.

This applies to user sessions (GUI activity by normal user) and must be applied to sessions running within the secure zone as well as sessions from outside the secure zone.

The messaging/communication interface must offer or support protection of interactive user sessions through a secure protocol (for example https or TLS in line with the above guidelines).

B1A LAU is a mandatory requirement for relaxed Message Partners. This functionality must already have been implemented since Q2 2018.

B2 The messaging/communication interface must be updated to remain in sync with the latest versions of security updates (such as security patch to remedy Java vulnerabilities).
The messaging/communication interface must be updated if a security problem is found in the software or its configuration.The legitimate source and integrity of the

messaging/communication interface (security) updates/patches are ensured by the provider for the user to be able to validate them when applying them.

B3 To maintain a proper operational state for messaging/communication interfaces in a hardening environment, vendors have to provide its customers guidance on how to configure its system in a hardening environment or provide any overruling application-specific configuration settings.

B4 The messaging/communication interface must offer or support the means to ensure confidentiality, integrity, and mutual authentication of the data flows between the back office or middleware and itself. This protection must cover man-in-the-middle risks, unintended disclosure, modification, and access to the data while in transit.

For example, this can be implemented using mechanisms such as “LAU or another message based authentication solution such as XML-DSig in combination with a confidentiality protection”, 2-way TLS, or AES GCM Authentication Encryption.

B5 This requirement relates to the operator scope documented under B1 above.
In addition, operator sessions must have a configurable inactivity lock-out feature that limits the session to the minimal timeframe necessary to perform business-as-usual duties.

B6 The messaging/communication interface must offer parameterised restrictions that allow control of business transactions. This can consist e.g. (but is not limited to) of 4-eyes implementation for SWIFT messaging, allowed business transaction hours, session number control. It should also offer reporting facilities (such as summary of transactions sent/received facilitating end of day or period reconciliation).

B7 The messaging/communication interface must offer or support the means to ensure confidentiality of the data extracted or replicated for back-up, recovery of further off-line processing.

When functionalities or tools to extract messaging data are provided, mechanism allowing encryption of the data at rest should be provided using commonly accepted cryptographic algorithms (for example, AES, ECDHE), with key lengths in accordance with current best practices based on passphrase provided by the end-user. More guidelines on cryptographic algorithms can be found in SWIFT Knowledge Base TIP 5021566
Mechanism to decrypt the data could be provided or at least the procedure explained.

If data encryption cannot be ensured, at a minimum:
- the transmission of the data is protected by implementing secure flows including between messaging interfaces or underlying databases
- the users responsibilities must be clearly identified in the documentation and basic steps highlighted to protect such replicated or extracted data.

B8 To maintain a proper operational state for messaging/communication interfaces in a hardening environment, vendors have to provide its customers guidance with application-specific configuration settings on how to configure its interface in a hardening environment while maintaining the CSP compliance.

B9 The messaging/communication interface must offer parameterised restrictions that allow control of RMA exchange. This can consist e.g. (but is not limited to) of 4-eyes implementation for RMA exchanges. It should also offer reporting facilities on RMA/counterparties identification or listing allowing periodic reviews.

2.3 Physically Secure the Environment

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Physical Security	3.1	C1	M							
Customer Confirmation										

Notes

C1 The messaging/communication interface must not rely on the presence of external ports (for example, USB serial bus) on user PCs and server systems, except for software maintenance purposes or to allow normal messaging operations such as signing of messages or user authentication via PKI USB tokens.

2.4 Prevent Compromise of Credentials

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Password Policy	4.1	D1	M							
Customer Confirmation										
Multi-factor Authentication	4.2	D2	M							
Customer Confirmation										

Notes

D1 The messaging/communication interface must allow the definition - and enforce following password policy parameters:
- Password expiration
- Password length, composition, complexity, and other restrictions
- Password reuse
- Lockout after failed authentication attempts, and remedy
- Password requirements may be modified to accommodate specific use cases:
  - In combination with a second factor (for example, one-time password)
  - Authentication target (for example, operating system, application, mobile device, token)
  - Type of account (general operator, privileged operator, application-to-application account or logical authentication keys).

More good practice guidelines on password parameter and when relevant Personal Identification Number (PIN) settings can be found in SWIFT Knowledge Base TIP 5021567 and 5022038.

D2 The messaging/communication interface must support (either embedded or by external software) multi-factor authentication for its end-user login. The authentication factors presented are individually assigned and support individual accountability of access to the messaging interface.

2.5 Manage Identities and Segregate Privileges

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Logical Access Control	5.1	E1	M							
Customer Confirmation										

Notes

E1 The messaging/communication interface must support the design that related accounts are defined according to the security principles of need-to-know access, least privilege, segregation of duties and 4 eyes principles:
- Need-to-know (for example, an account allowing for system installation and update should have access to the information, files and system resources needed for this specific task, but should not have access to the business data).
- Least-privilege: the messaging/communication interface should allow setting up the accounts in a way that all privileges can be tailored to individual needs. Accounts should then be granted only the privileges needed for normal routine operations. Additional privileges can be granted on a temporary basis.

Segregation of duties and 4-eyes principles must be enforced for sensitive operations such as user management, security configuration, transaction submission and approval etc.

Items that need to be protected by segregation of duties (please note the list may not be comprehensive):
- Creation/modification of flows towards other applications, such as but not limited to back office, middleware, other messaging/communication interface, SNL
- Operators creation/modification, operator profiles creation / modification
- Security configuration, such as but not limited to application passwords, certificates, LAU keys, LT configuration, authentication server
- Messaging (FIN/RMA) operations, such as but not limited to message creation, modification, verification, approval

2.6 Detect Anomalous Activity to Systems or Transaction Records

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Malware protection	6.1	F1	M							
Customer Confirmation										
Software integrity	6.2	F2	M							
Customer Confirmation										
Database integrity	6.3	F3	M							
Customer Confirmation										
Logging and Monitoring	6.4	F4	M							
Customer Confirmation										

Notes

F1 The messaging/communication interface must support anti-malware software to be running on its server. Normal operations of the messaging interface software should not result in malware alerts.

F2 The messaging/communication interface must support software integrity validation (either embedded or by external software of all of its software components. Such software integrity checks should be conducted upon start-up, and additionally at least once per day. Software integrity checks provide a detective control against unexpected modification to operational software.

In addition, integrity check of downloaded software is conducted via verification of the checksum at the time of its deployment.

F3 Applies to messaging interfaces only. The messaging interface must embed database integrity validation when the database is embedded or support this validation in case of hosted database components.
The integrity check must ensure record-level integrity and must confirm that there are no gaps in sequential transaction numbering.

F4 The messaging/communication interface must be able to log any detailed abnormal system behaviour (such as messages outside normal business hours, multiple failed login attempts, and authentication errors).
- Events must be logged
- It must be possible to keep at least 12 months of log files (can be stored on a separate system).
- It must be possible to monitor these log files online (i.e. they are kept in the system) or to consult them offline (i.e. they are kept in an archive system).
- Automated monitoring with alerting can be implemented.
- Integration of logs into a centralised logging system may be provided.

Logs must provide traceability of account usage to the appropriate individual.

Log files must be sufficiently protected so that only a need-to-know account profile has access.

2.7 Plan for Incident Response and Information Sharing

Feature	Ref	Note	Mandatory/ Advisory	FIN	RMA	FA SnF	FA RT	IA SnF	IA RT	Comm Intf
Cyber Incident Response Planning	7.1	G1	M							
Customer Confirmation										

Notes

G1 The messaging/communication interface vendor must inform all its customers in case of a cyber-incident with its software about the threat, and about the remedying measures that can be taken by its customers (such as temporarily disable specific functionalities, install a patch, …).
In addition, the messaging interface vendor must inform the SWIFT Customer Support Centre.
Only “S” (Supported) is applicable to this requirement.

A Appendix A: Test Report

For each of the supported interface protocol types, the interface vendor should complete this report after completion of a customer Confirmation. The report should be returned to the certification interface test authority (swiftnet.cbt.qualification@swift.com)

Company Name	
PIC-8	
Company Contact (e-mail)	
Product Name and version number	
Interface Protocol Type	
Reference Bank name	
BIC-8	
Bank Contact (e-mail)	
Dates the reference tests were run	
Brief overview of test configuration (platform, OS, middleware, etc.)	
Comments on the Confirmation	

Legal Notices