Interface Certification – Security Conformance Requirements

Conformance Statement

This document lists the security requirements that a messaging interface must comply with. These requirements are extracted from the Customer Security Controls Framework Version 1.

Revision: April 2017

Table of Contents

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 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 interface must comply with. These requirements are extracted from the Customer Security Controls Framework.

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 customer, after interim certification.

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

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										

Notes

A1 The messaging 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
- 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).
- From a general purpose operator PC, if they only access the messaging or communication interface by means of a browser-based GUI. Specific security controls for this set-up:
  - o Restricted internet access on the operator PC using one of the following options:
    1. No internet access
    2. Internet access using a remote desktop or virtual machine solution
    3. Internet access from the 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.
  - o The browser-based GUI is located in the secure zone and is logically separated from the messaging and communication interface,
  - o Multi-factor authentication is implemented where appropriate (on the browser-based GUI, on the messaging interface, or on the communication interface),
  - o This set-up cannot be used for operating system administration activities.

A2 The messaging 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.

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	E	E	n/A				
Customer Confirmation				E	E					
Security Updates	2.2	B2	M							
Customer Confirmation										
System Hardening	2.3	B3	M							
Customer Confirmation										
Back Office Data Flow Security	2.4A	B4	A							
Customer Confirmation										
User Session Confidentiality and Integrity	2.6A	B5	A							
Customer Confirmation										
Transaction business controls	2.9A	B6	A							
Customer Confirmation										

Notes

B1 The messaging 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 interface must offer or support protection of interactive user sessions by a cryptographic protocol (for example https).

B1A LAU is a mandatory requirement for relaxed Message Partners. This functionality must be implemented by Q2 2018.

B2 The messaging 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 interface must be updated if a security problem is found in the software or its configuration.

B3 To maintain a proper operational state for messaging 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 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 2-way TLS, one-way TLS in combination with either LAU or XML-DSig.

B5 This requirement relates to the operator scope documented in B1.
Operator sessions must have an inactivity lock-out feature that limits the session to the minimal timeframe necessary to perform business-as-usual duties. For example, a 15-minute lock-out is recommended for end user sessions.

B6 The messaging 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 or RMA exchanges, allowed business transaction hours, session number control.

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 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 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 interface must allow the 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 settings can be found in SWIFT Knowledge Base TIP 5021567.

D2 The messaging 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 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 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.

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 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 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 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 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 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

Copyright

Restricted Distribution

Do not distribute this publication outside your organisation unless your subscription or order expressly grants you that right, in which case ensure you comply with any other applicable conditions.

Disclaimer

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

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: the SWIFT logo, SWIFT, SWIFTNet, Accord, Sibos, 3SKey, Innotribe, the Standards Forum logo, MyStandards, and SWIFT Institute. Other product, service, or company names in this publication are trade names, trademarks, or registered trademarks of their respective owners.