How to meet SWIFT's operational requirements in 2018

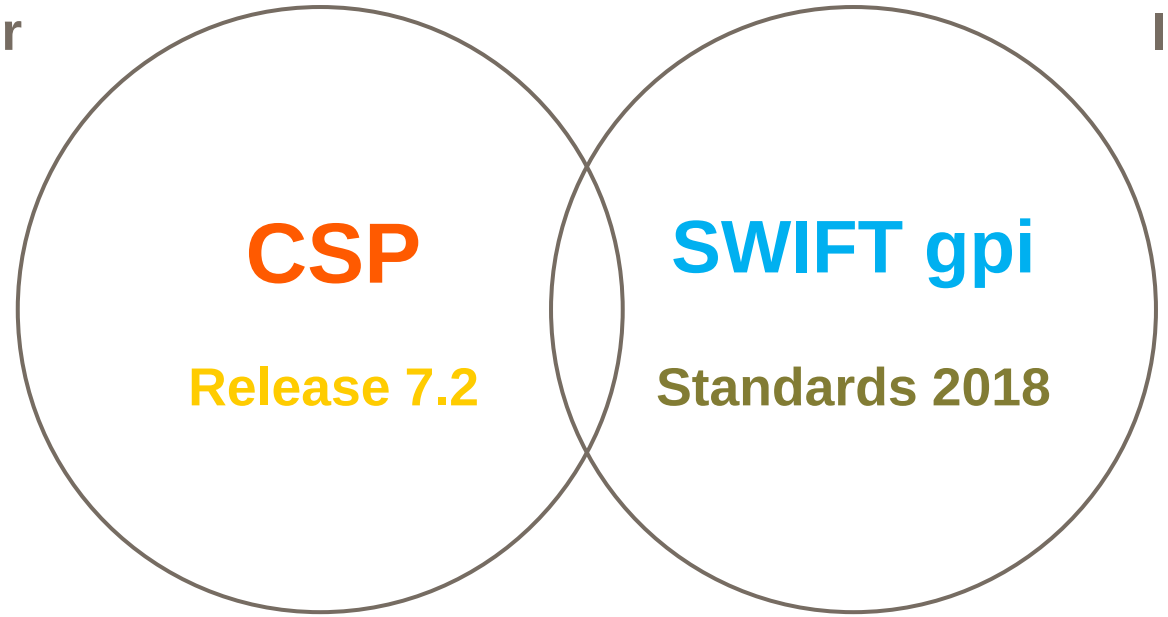
Victor Abbeloos
Sven De Kerpel
Pat Antonacci

19 September 2018

Transforming the industry together

Reinforcing security & driving payments innovation

Enhance your security



Innovate your offer

Release 7.2

Release 7.2 | A mandatory upgrade!

SWIFT Applications to be migrated

- SWIFTNet Link
- Alliance Gateway
- Alliance Access
- Alliance Entry
- Alliance Web Platform Embedded
- Remote File Handler
- Alliance Messaging Hub
- Hardware Security Module

SWIFT Applications impacted

- Alliance Lite2
- Alliance Lifeline
- Alliance Remote Gateway

Mandatory Technology Refresh	– Mandatory upgrade of embedded COTS – Introduce 64-bit support – Refresh OS Baseline
Security	– Align the community on latest security updates – Large scale deployment of latest HSM enhancements
Product Evolution	– Release alignment as a foundation for future evolutions – Ensure deployment of latest messaging evolutions to entire community
Supportability	– Renew the baseline to ensure supportability and long term stability – Introduction of updated Release Policy

Release 7.2 | Timeline and dependencies

Timeline	**November 2018**		
Warning Impact of missing November 2018 deadline	**CSP** – Customer will have to self-attest that he is not using supported software and as such not CSP compliant	**Alliance Access / Entry** – SR 2018 has a significant impact on MT103 and MT202 COV with regards to GPI (UETR mandatory) – Only a release 7.2 update will provide automatic UETR addition	**SWIFTNet Link** – Following the SWIFTNet Root Key Renewal in the second half of 2019, SNL 7.0 and HSM Software v6.0 will not be able to connect to the SWIFT network anymore
Links to other initiatives	– SR2018 & CSP: see above – SR2018/GPI: releases 7.2.50 and 7.3 support SR2018, including UETR related changes		

Release 7.2 | Call to action for SWIFT users

1. Assess if you have SWIFT applications to migrate (if any)

2. Prepare for the migration NOW : read the Release 7.2 Migration Guide, paying special attention to:
   - the Hardware and OS prerequisites in chapter 3
   - the SWIFT applications prerequisites in chapter 5

3. Plan your migration:
   - To be in time for Standards Release 2018, GPI and CSP
   - (Service Bureaux) To give time to your clients to align
   - To be fully migrated before November 2018

4. Migrate all your SWIFT Application instances (also Test or Disaster Recovery instances)

5. Upgrade Release 7.2 to Release 7.2.50 or Release 7.3 to be able to install Standards Release 2018

LINKS:
- Release 7.2 swift.com page
- Release 7.2 Support Page
- Migration Guide

Note: It will not be possible to upgrade your current system locally to the new release.
You must perform either a new installation, or an installation from the prepared backup file.

Customer Security Programme

CSP | SWIFT's Response to the evolving cyber threat

Customer Security Programme (CSP)

Launched in May 2016, the CSP supports all customer segments in reinforcing the security of their local SWIFT-related infrastructure

You

Secure and Protect

- SWIFT Tools
- Security Controls Framework

Your Community

Share and Prepare

- Intelligence Sharing
- SWIFT ISAC Portal

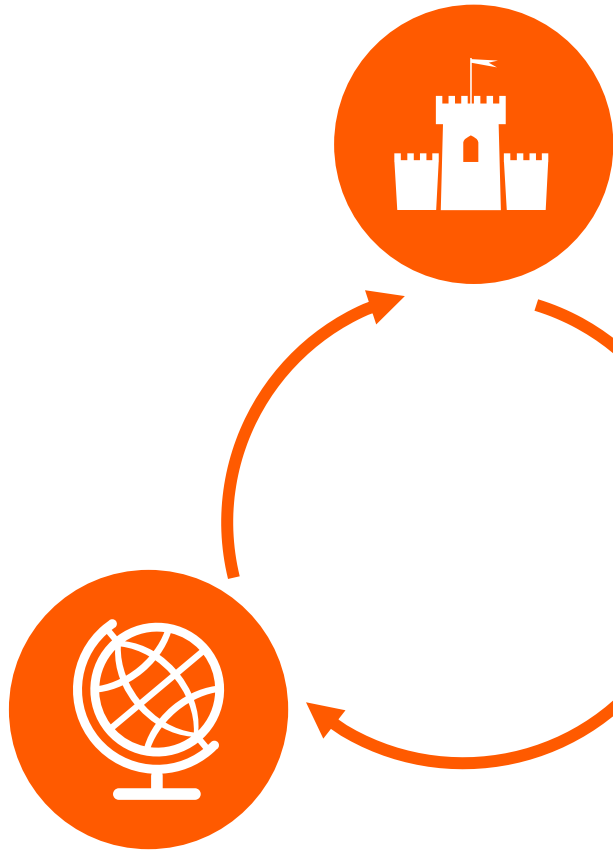
Your Counterparts

Prevent and Detect

- Transaction Pattern Detection
  - RMA, DVR and 'In Flight' Sender Payment Controls

CSP | 2018 Priorities & milestones

Compliance, Re-Attestation, Consultation, Prepare for 2019



You

- ✓ June: Change Management process – Customer Security Controls Framework (CSCF)
- ✓ June: Updated Customer Security Attestation Policy
- ✓ August: Release of CSCF v2019 (version 2)
- ✓ Ongoing: Interface Hardening – Release 7.2 implementation and 7.3 planning – sign up for webinars
- End of December: (at the latest) all users must re-attest full compliance with all mandatory controls CSCF v1

Your Community

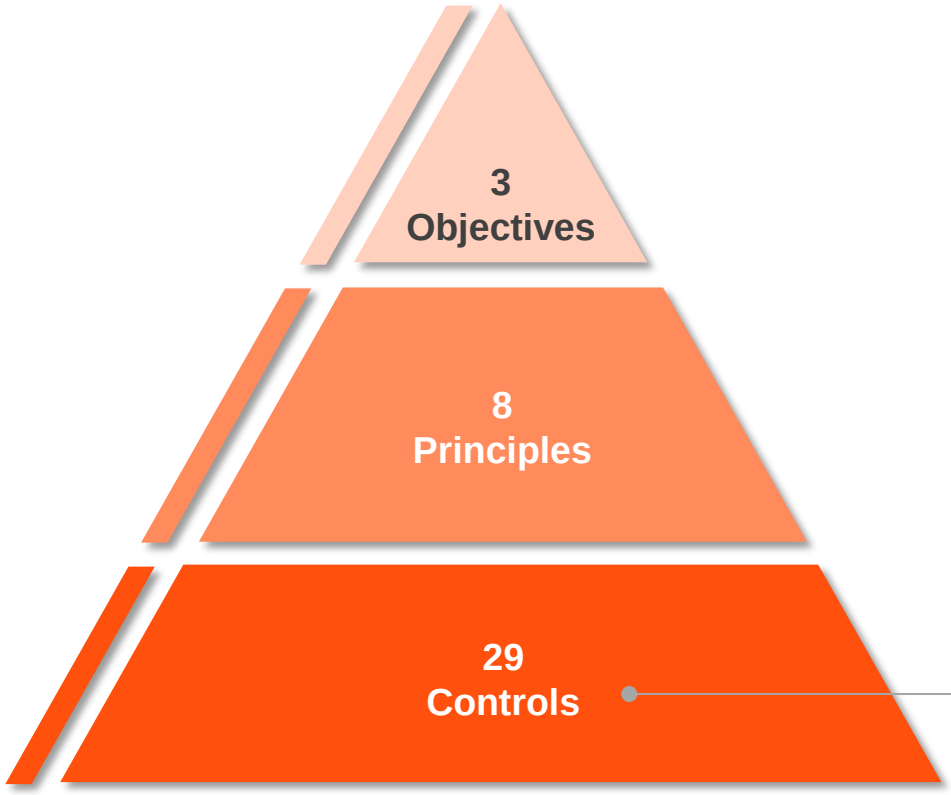
- ✓ February: SWIFT–ISAC: STIX/TAXII available
- ✓ Ongoing: Directory of Cyber Security Providers
- ✓ Ongoing: Industry engagement – look for local events and sign up for webinars

Your Counterparts

- ✓ Quarterly: Quality Assurance review
- ✓ July: KYC-SA v3 – Request/Grant and reporting enhancements
- ▪ October: Sender Payment Controls Service goes live

CSP | Customer Security Controls Framework v2019

Security Controls



CSP Security Controls Framework

Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

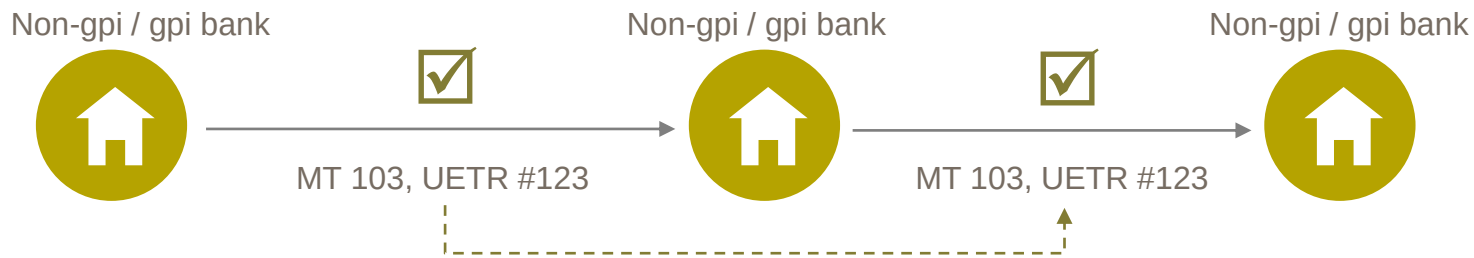
- 19 controls are mandatory – 3 advisory promoted:
  - 2.6 Secure Operator sessions
  - 2.7 Yearly vulnerability scanning
  - 5.4 Physical and Logical Password Storage
- 10 controls are advisory - 2 new advisory controls:
  - 1.3A Virtualization Platform Protection
  - 2.10A Application Hardening
- Full compliance against mandatory controls by end 2019

CSP | Call to action for SWIFT users

1. Ensure that you fully comply with all the mandatory security controls and re-attest by 31 December 2018 latest.
2. Engage in SWIFT ISAC, sign up for notifications – and contact us immediately if you suspect a breach of your SWIFT related-infrastructure
3. Ensure mandatory security updates of SWIFT software are installed.
4. Request access to your counterparties attestation and grant access to your institution's attestation (where appropriate). Consider your institution's counterparty risk frameworks to utilise counterparty attestation data.
5. Consider SWIFT's anti-fraud tools (Payment Controls, Daily Validation Reports, RMA clean-ups, etc.)

Standards Release 2018

Standards Release 2018 | Mandating ALL SWIFT users to add, pass on and receive UETR on ALL key payments

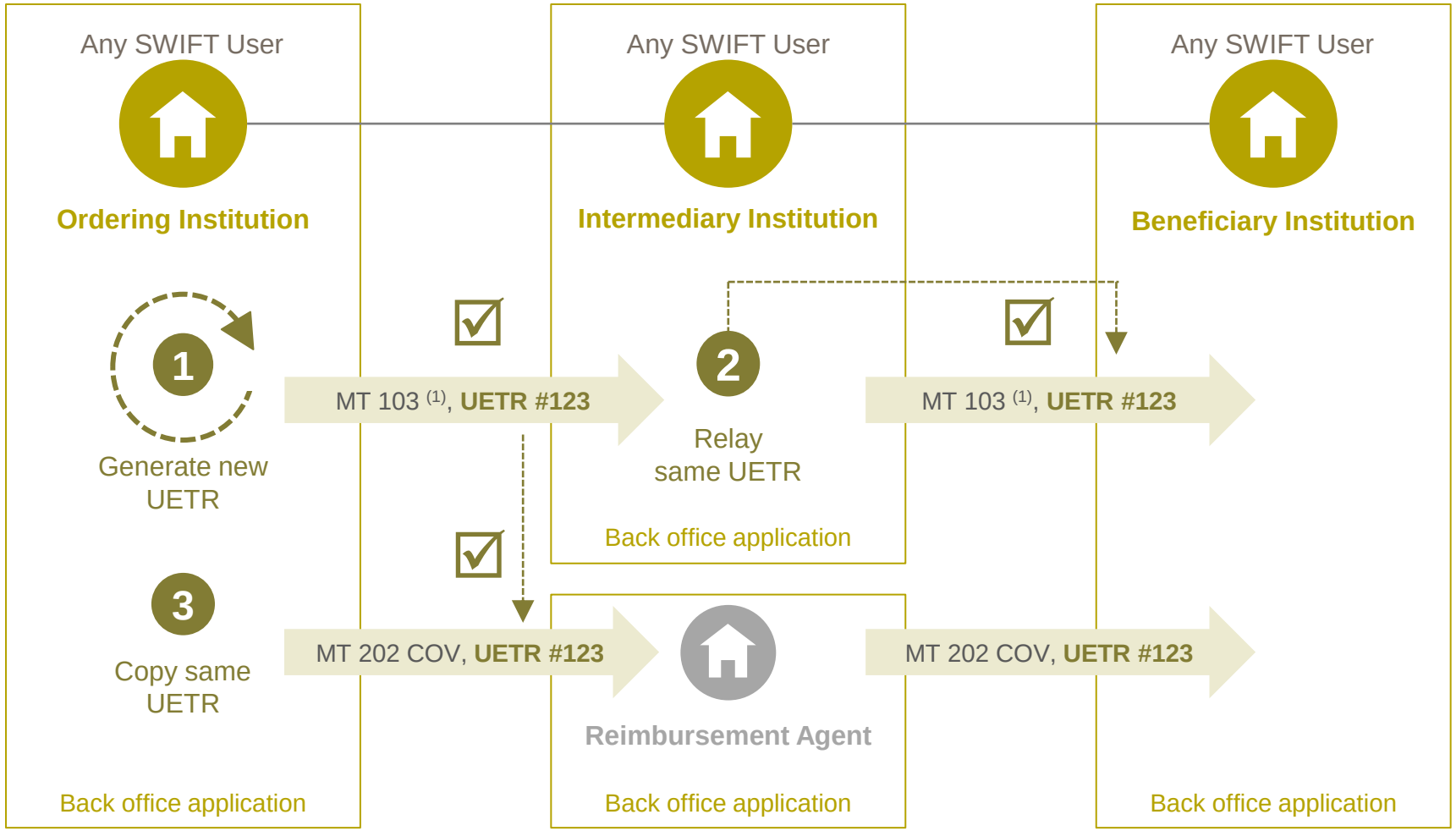


All SWIFT Users, including non-gpi members, must **add and pass on a UETR** (Unique End to End Transaction Reference) in all MT 103, MT 103 STP, MT 103 REMIT, MT 202, MT 205, MT 202 COV and MT 205 COV messages

All SWIFT Users must be able to **receive the gpi fields 111** (Service Type Identifier) **and 121** (UETR) in block 3 of any Category 1 and Category 2 FIN message

➔ **Non-compliance will generate a NAK**

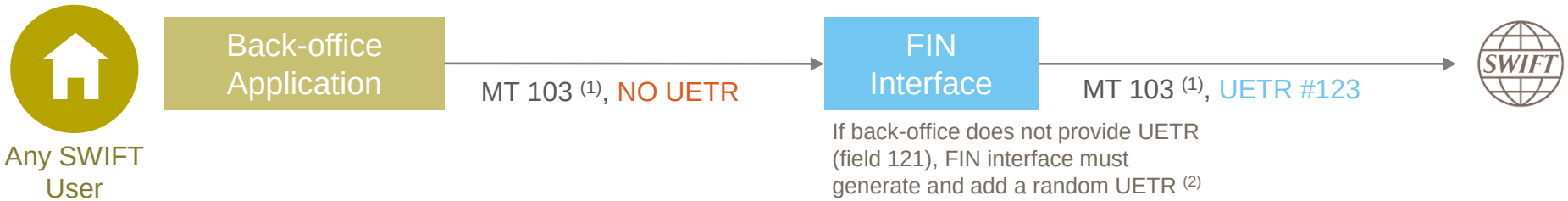
Standards Release 2018 | impact on back-office applications



(1) Mandatory UETR applies to MT 103, MT 103 STP, MT 103 REMIT, MT 202, MT 205, MT 202 COV and MT 205 COV

Example of a valid UETR #123:
77e8367b-d3e7-4dfc-8100-7f041c4058d3

Standards Release 2018 | Temporary solution if back-office application cannot be ready in time for SR 2018



(1) Mandatory UETR applies to MT 103, MT 103 STP, MT 103 REMIT, MT 202, MT 205 , MT 202 COV and MT 205 COV

(2) Document : Mandatory SR 2018 requirements for FIN messaging interface providers
Use of the FIN interface to generate UETR requires installation of new SR 2018 version of FIN interface and configuration
For Alliance Access & Entry users, migration to 7.2 .50 is pre-requisite to use FIN interface for UETR generation

Standards Release 2018 | Temporary solution if back-office application cannot be ready in time for SR 2018

	Scenario	SR 2018 Change	Back-office implementation	FIN Interface (Temporary Solution)
1	Payment Initiation	**Generate new UETR**	✓	✓ (1)
2	Intermediary traffic	**Relay same UETR**	✓	✗ (2)
3	Cover Initiation	**Copy same UETR (MT 103)**	✓	✗ (2)

(1) If customer not ready to implement UETR generation in back-office in time for SR 2018, FIN interface can provide a temporary solution.

(2) FIN Interfaces not mandated to copy or pass on UETR from incoming message into outgoing message, correct standards usage requires change in back office.

Standards Release 2018 | Call to action for SWIFT users

1. Understand the impact of Standards Release 2018 on your payments application(s) and SWIFT interfaces. Plan upgrades of these systems.
2. Upgrade payments application(s) to create, store and process UETRs.
3. Upgrade interface systems to SR2018 compliant version.
4. Test the full transaction chain (in FIN Test & Training future mode) to process payments with UETR.
5. On November 18th: Activate upgraded system for live operations.

Payment messages without UETR will be NAK'ed

SWIFT gpi & SR 2018 | Adopt gpi to maximise the benefits of your 2018 standards investment

Further information

CSP

www.swift.com/myswift/customer-security-programme-csp

Release 7.2

www.swift.com/our-solutions/a-to-z/release-7_2

Standards Release 2018

www.swift.com/sr2018

SWIFT gpi

www.swift.com/gpi