ROSSWIFT
Annual General Meeting
SWIFT updates

Ekaterina Kalinina, head of Russia & CIS, SWIFT

26 April 2021

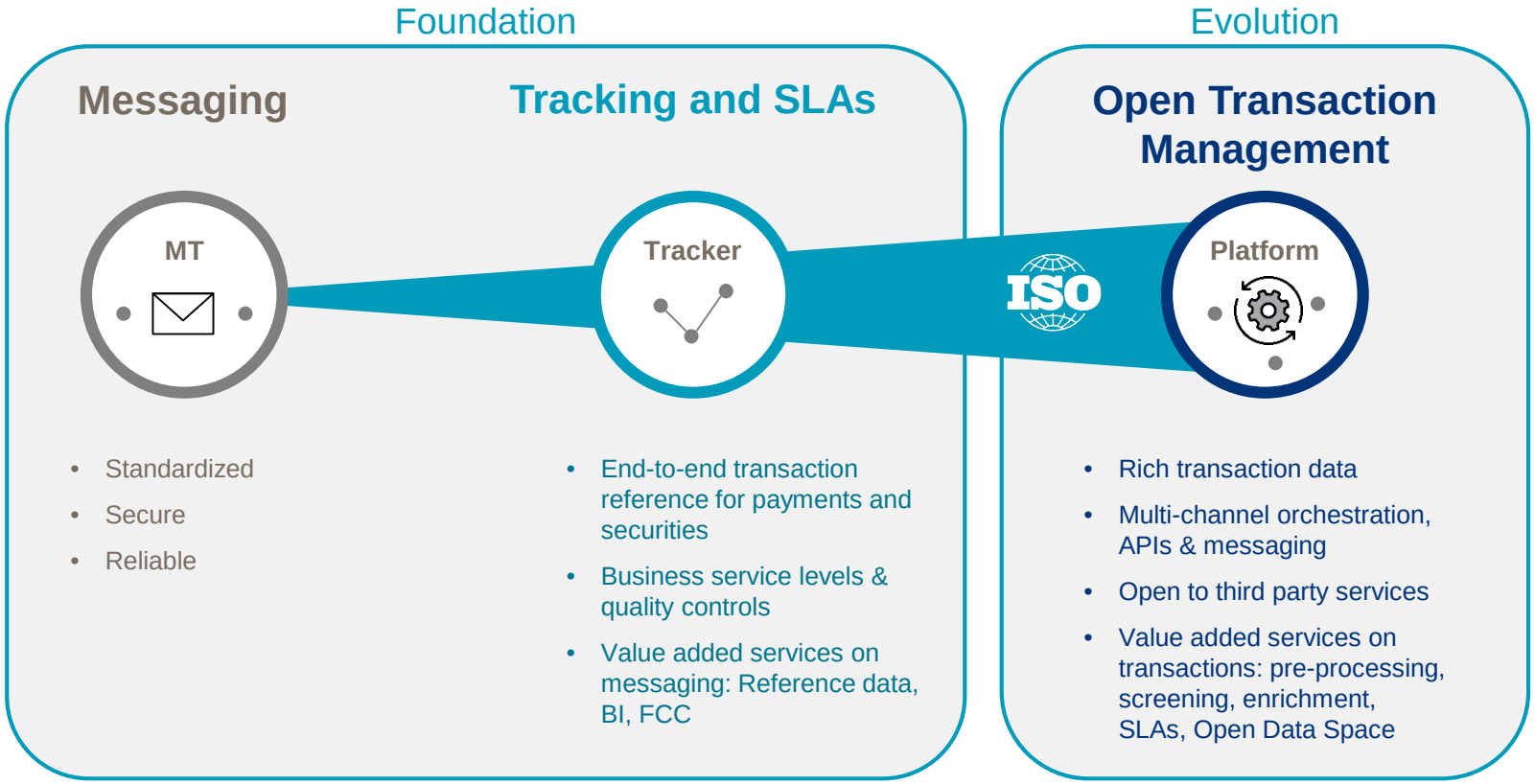
SWIFT © 2021. All rights reserved. The document is provided in confidence to the National Member/User Groups. Do not distribute this document outside the National Member/User Group without SWIFT's prior written consent.

Our vision is to deliver instant account-to-account payments across the world, available 24/7 in domestic and cross border environments

SWIFT payments travel frictionless and with transparency, while being compliant and highly secure

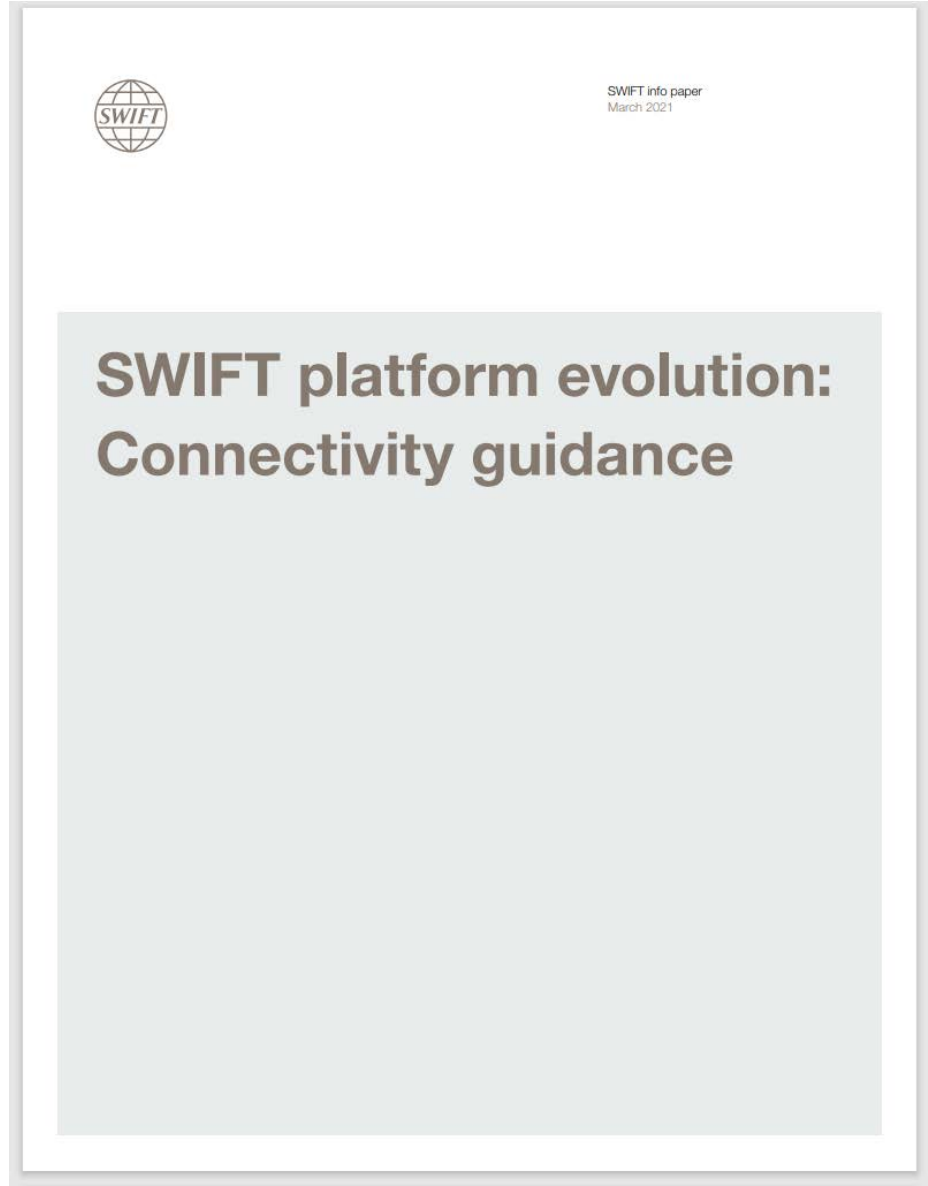
- gpi Instant
- gpi
- MI evolution and real-time payments
- CBPR+
- ISO 20022
- SLA tracking
- SWIFT FCC and CSP

Transforming our foundation into an open state-of-the art platform which leverages ISO 20022 data



Connectivity Guidance

- Our vision for customer connectivity to the SWIFT platform, as it evolves towards the transaction management concept described in SWIFT's strategy
- Provides the information required to understand the options available – and the pros and cons of each – to help plan implementations
- Download now: https://www2.swift.com/myprofile/res/documents/platform/swift-infopaper-platform-connectivity-guidance.pdf (login required)



SWIFT gpi global adoption

SWIFT gpi is seeing unparalleled growth in adoption, traffic and corridors

Very large **community**

4,228+
financial institutions signed
(3,700 end 2019)

800
banking groups
(60 of top 60 banking groups)
(536 end 2019)

208
countries covered
(200 end 2019)

88+%
SWIFT cross-border payments represented
(80% end 2019)

Millions **live** payments

1,569+
live gpi members
(750 end 2019)

2,724+
country corridors
(1,700 end 2019)

$415 bn
payments sent as gpi every day
(300 bn end 2019)

75+%
cross-border MT103 sent as gpi
(60% end 2019)

Delivering real **value**

On average, **38% of SWIFT gpi payments are credited to end beneficiaries within 5 minutes**, Over 53% within 30 minutes, 77% within 6 hours, almost 100% within 24 hours

Banks have seen **significant reduction in number of payment enquiries** and quicker investigations handling

Positive reactions from corporates

Customer Security Programme update

Customer Security Programme | Performance for YE 2020

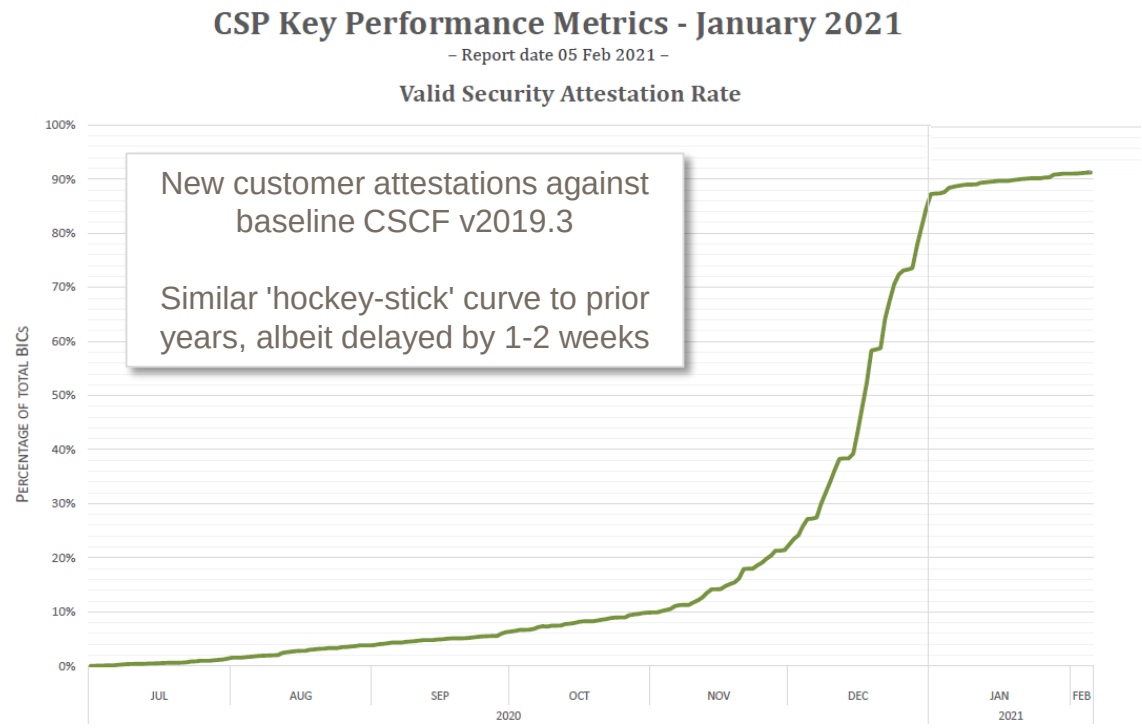
Attestation and Compliance Rates

92%

Customers having a valid CSP attestation against CSCF v2019.3

97% Average
93%-99% Range

For attested BICs, the individual compliance rate for each mandatory CSCF Control

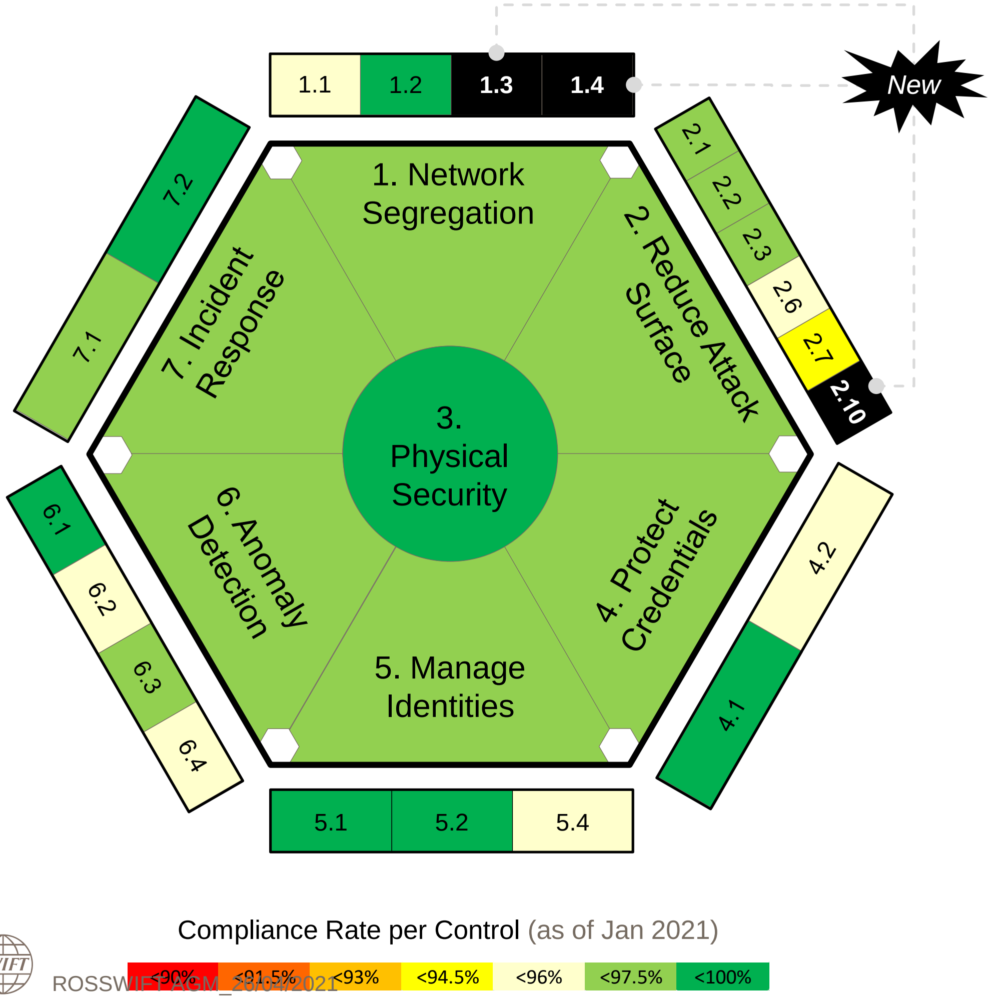


Note: Total BICs consist of BICs who are marked as active on the KYC Directory, live on FIN or SWIFTNet, and are not part of Go Local India. A valid security attestation refers to a security attestation that has been validated by SWIFT and that has not passed its expiration date.

Note: The data on these charts has different starting dates because some metrics were introduced at a later stage of the programme.

Customer Security Programme | Priorities for 2021

Introduction of CSCF v2021



In Jul 21, CSCF v2021 will come into effect

CSCF v2021 includes controls from CSCF v2020 previously delayed due to the pandemic

Compared to CSCF v2019, three controls are newly promoted from 'advisory':

- 1.3 Virtualization (details published Jul 19)
- 1.4 Internet Restrictions (details published Jul 20)
- 2.10 Application Hardening (details published Jul 19)

Deadline for CSCF v2021 is end Dec 21

Introduction of 'Independent Assurance Framework' (IAF)

Per IR 806, the *'Independent Assurance Framework'* (IAF), comes into effect in Jul 21 (previously delayed due to the pandemic)

IAF mandates that all CSP attestations must be backed up by independent assurance for the year-end deadline of Dec 21

Assessors can be internal second or third line of defence (e.g. risk office, compliance office or internal audit) or an external third party provider

Customer Considerations for IAF Implementation

Plan early, budget costs / resources and select an assessor in the first half of the year

To manage costs, consider limiting the assurance to an assessment (rather an audit) and consider internal resources (rather an external provider) with the appropriate credentials

To avoid being reported to the local supervisory authority, if applicable, submit the attestation with assurance details in the KYC-SA tool by end Dec 21

Available resources: Lists of CSP Assessment Providers and Cyber Security Service Providers; IAF, FAQ and TIP 5022902; Excel-Based Assessment Templates, SWIFTSmart Training Modules; pre-recorded videos / webinars …

Call to action for SWIFT customers

1. Stay up to date with SWIFT software releases
2. Sign up for Security Notifications and SWIFT ISAC information sharing portal
3. Agree with your counterparties to 'consume' and utilise attestation data for counterparty risk management. New 'Grant All' function will reduce operational burden and was activated in November
4. Consider SWIFT's anti-fraud tools – Payments Control Service (PCS) and RMA Relationship clean-ups
5. Inform SWIFT if you suspect a cyber-attack on your SWIFT-related infrastructure and have a response plan that has been tested
6. Ensure that you comply with CSCF v2021 mandatory controls and re-attest with independent assurance by 31 December 2021

www.swift.com