



Customer Security Programme Updates

Reinforcing the security of the global banking system



November 2020

Welcome to the SWIFT Customer Security Programme (CSP) update – designed to provide you with the latest important information relating to the CSP.

Submit your security attestation now!

All SWIFT customers must re-attest against the Customer Security Controls Framework (CSCF) v2019 ([baseline 2019.3](#)) by 31 Dec 2020.

Baseline 2019.3 has been available in the KYC-Security Attestation application (KYC-SA) since July. This means that if you attested before July, you must re-attest.

[Tip 5023980](#) explains you how to check the baseline of your attestation or draft in KYC-SA.

Re-attesting now or at year-end has no impact on the expiry date of your attestation - either way, your attestation against baseline

2019.3 remains valid until the end of 2021 and we recommend you do it sooner rather than later.

As the [published CSCF v2020 and v2021](#) contain clarifications on the controls, SWIFT recommends making use of these additional guidelines and clarifications when re-attesting against the baseline v2019.3.

For more dedicated CSP information, visit the [security attestation support page on mySWIFT](#).

KYC-SA – Grant All has been activated

We have now activated the new KYC-SA Grant All function, which simplifies the sharing and consumption of counterparty attestation data amongst all institutions. For institutions that remain opted in to Grant All, all pending and new attestation data access requests received from existing [messaging counterparties](#) will be automatically granted. Any data access requests from other counterparties will remain pending until they are processed manually, or via the AllowList.

To support the Grant All function, KYC-SA security officers, granters, viewers and requesters can now access the 'My Messaging Counterparties' overview. This new view provides a list of your institution's messaging counterparties, information on when you last exchanged live messages, and whether you have access to their attestation data.

[Tip 5024147](#) provides further information on how your institution can use the Grant All function to handle access requests from messaging counterparties more efficiently.

New CSP documentation available

SWIFT has published some additional CSP documentation to

support customers and their independent assessors for their attestation and assessments on the [Knowledge Centre](#). These additions comprise:

- Two Excel workbooks titled 'Controls Matrix' to assist customers in determining relevant elements in each CSP Security Control as per their architecture type,
- The CSP decision tree 2021 to assist customers in determining their CSP architecture type in the light of the CSCF v2021, and
- The [CSP SWIFT Smart Modules](#) related to the Customer Security Control Framework (CSCF), Independent Assessment Framework (IAF), and Policy have been updated in line with the latest documentation.

Migration from STIX/TAXII to MISP

SWIFT plans to migrate the mechanism we use to share of Indicators of Compromise from the current STIX format over TAXII protocol to MISP in Q1 2021. This is part of our continuous effort to improve our offering and will enable you to connect to MISP and setup MISP integration or API access for your institution, provided you have access to the SWIFT ISAC. Once this is possible, we will not accept additional on-boarding requests on the current STIX/TAXII solution. However, we will continue to support the STIX/TAXII solution during the first half of 2021 in order to facilitate a smooth migration of our impacted customers.

A more detailed timeline and FAQ's will be published in the coming weeks on the SWIFT ISAC portal. Stay tuned for further updates.



Digital SIBOS 2020 continues Cybersecurity session on 9th March 2021

The Cybersecurity sessions during the Sibos 2020 week (5-8 Oct) had record-breaking viewership and we're not stopping there. The Sibos digital monthly series kicks off from Tuesday, 10th November featuring a one-day program every second Tuesday of the month until March 2021.

For cybersecurity, we have planned a panel session for early March 2021

- Bringing Cybersecurity to the Masses – Does the answer lie in New Tech?
- Tuesday, 9 March 2021

Please visit our site to learn more >



Find an event in your region

Upcoming SWIFT Community Updates

We are running a number of SWIFT Community Updates, digital events exclusively for SWIFT customers, in November and December. These will bring together market leaders, and subject matter experts. We will discuss the key trends and latest developments impacting you and your community: from our ambitious new strategy to enable instant and frictionless transactions, to managing risk in these unprecedented times, adopting new technologies, the SWIFT services available to you, and much more.

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.
