Customer Security Programme Updates

Reinforcing the security of the global banking system

September 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 are required to re-attest compliance with the mandatory controls set out in Customer Security Control Framework (CSCF) v2019 between July and 31 December 2020. As previously communicated to the SWIFT community, SWIFT has re-phased originally published timelines for the CSCF to make sure upcoming reinforcements are practical for our community.

Therefore, **you must attest against the CSCF v2019 (KYC-SA baseline 2019.3)** by the end of 2020. **Tip 5023980** explains how to check the baseline of your attestation or draft in KYC-SA.

Re-attesting now has no impact on the expiry date of your attestation - whether you attest now or at year-end, your

attestation against the KYC-SA baseline 2019.3 remains valid until the end of 2021.

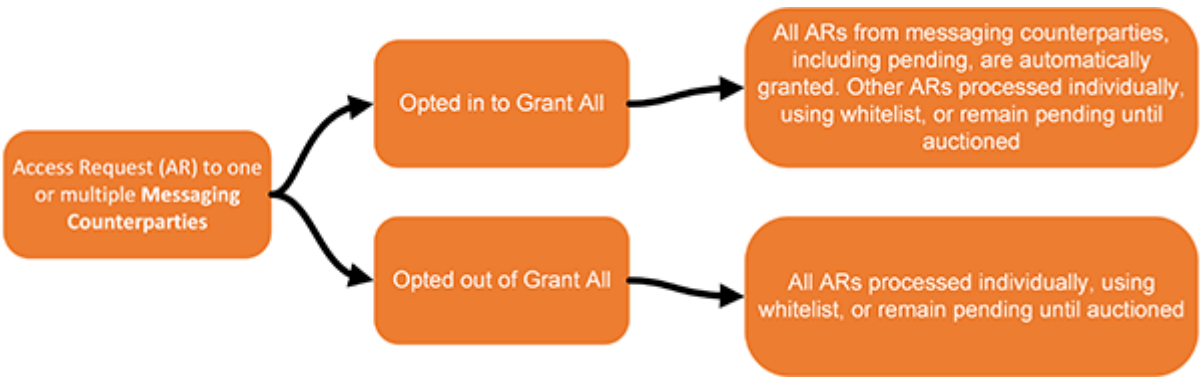
As the **published CSCF v2020 and v2021** contain *clarifications* on the controls, SWIFT recommends making use of these additional guidelines and clarifications when re-attesting against the KYC-SA baseline v2019.3.

For more dedicated CSP information and SWIFTSmart trainings, visit the refreshed **security attestation support page on mySWIFT**.

KYC-SA -- Get Ready for Grant All

In order to simplify sharing and consumption of counterparty attestation data amongst all institutions, SWIFT will activate the Grant All function in KYC-SA in November 2020. This will allow all institutions that have opted in to automatically grant attestation data access requests received from existing messaging correspondents.

Once Grant All is activated, the following workflow will apply to all access requests:



Implementation of Grant All

Grant All will be implemented in two stages, which are planned as follows:

- From 11 September, all institutions are opted in to Grant All. KYC-SA security officers may opt institutions out of the function before activation in November (and may opt in again at any point in the future should they chose to do so). To complement the Grant All functionality, an enhanced messaging counterparty view is now available in KYC-SA so that granters can review the messaging counterparty list and view which counterparties have granted access.
- In November, Grant All will be activated - details will be communicated shortly to KYC-SA Security Officers, Granters and Administrators. From then on, institutions that are opted in to Grant All will benefit from simplified processing of requests from messaging counterparties. Institutions that are opted out of Grant All will continue to process access requests in the same way as before activation, and should continue to check regularly for new access requests, to process them in a timely manner.

Tip 5024147 provides further information on how you can ensure your institution is prepared for the implementation of Grant All.

SWIFT publishes new version of the CSP Policy

SWIFT published a revised version of the **CSP Policy** on 28 August. The most significant updates in this version incorporate:

- the re-introduction of the ‘self-assessment’ type of assurance in KYC-SA, in addition to the Independent Internal/External Assessment,
- SWIFT’s reporting to jurisdictional overseers (i.e. a supervisory authority that has responsibility to oversee a market sector for an entire jurisdiction, e.g. market infrastructures, banking, national financial stability, stability of a currency zone. The role of jurisdictional overseer can be played by the Central Bank or by a dedicated institution),

- the reporting of the failure to conduct a SWIFT mandated external assessment to supervisors and,
- the introduction of the Grant All functionality

Coming soon: CSP Update 2021 webinars

SWIFT will run CSP Update 2021 webinars in the course of Q4 2020, which will focus on the changes to the CSCF v2021 and the Independent Assessment Framework (IAF). It will also remind SWIFT's customer (i) of their obligations in 2020, to attest in the KYC-SA application against the CSCF v2019 as soon as possible and no later than 31 December 2020 and (ii) of the possibility to select the self-assessment option in 2020 onwards. The Independent External/Internal Assessment will become mandatory as of 2021

Note that the **SWIFTSmart Modules** have recently been updated to reflect the changes related to the CSCF v2021 and revised IAF. Keep an eye out for updates to the **webinar page on swift.com** for more details.

Digital Sibos 2020 - Cybersecurity sessions

Sibos 2020 will bring the financial community together online from 5 to 8 October and the conference programme will centre around a core theme of 'Driving the Evolution of Smart Finance'.

For cybersecurity, we have a number of sessions scheduled:

- Covid-19: Open-Season for Cyber Hackers? Wednesday 7 October
- The Cyber Resource Problem – is it Totally Unsolvable? Tuesday 6 October

- CSP Evolution and Effectiveness. Monday 5 October

Please visit **https://www.sibos.com/conference-at-glance** to learn more. Registration is now open and online participation will be free of charge.

CSP swift.com pages revamp: refreshed content with a brand new layout!

SWIFT has undergone a full review and refresh of its CSP content on swift.com.

Check out the **CSP main page**, from which you can access any CSP-related information: Controls, attestation, independent assessment, risk management, …

The search function has been improved and every CSP page benefits from a new layout, which makes it more user-friendly and easy to read while providing links to relevant information.

Fighting Institutional Payments Fraud e-book

We recently published an e-book entitled ‘Fighting Institutional Payments Fraud’, which aims to provide the best practices, policies and tools to protect institutions from cyber criminals and hackers.
When the world goes through a period of instability or rapid change, as it is today, cybercriminals are ready and waiting to exploit uncertainty and find gaps in normally hard-edged security frameworks. One major type of fraud that is especially challenging is institutional payments fraud, where cybercriminals try to gain illicit access to an institution’s systems and steal large sums undetected.
Our new e-book provides insight into understanding the attackers - tactics, techniques and processes, how to continue to build a

cyber-aware culture across your organisation, why collaboration is key, how to review your processes in light of evolving threats and how to automatically identify and stop uncharacteristic payments by implementing payment security controls **Download your copy of the e-book**.

Follow the Money: SWIFT & BAE publish new report

View the reportSWIFT and BAE Systems Applied Intelligence have published ‘Follow the Money’, a new report that describes the complex web of money mules, front companies and cryptocurrencies that criminals use to siphon funds from the financial system after a cyber-attack.

Although there has been much research into the methods that cybercriminals use to conduct attacks, there has been less investigation into what happens to funds once they have been stolen. The aim of this report is to illuminate the techniques used by cyber criminals to ‘cash out’ so that SWIFT’s global community of over 11,000 financial institutions, market infrastructures and corporates can better protect themselves.

The report highlights the ingenuity of money laundering tactics to obtain liquid financial assets and avoid any subsequent tracing of the funds. For instance, cyber criminals often recruit unsuspecting job seekers to serve as money mules that extract funds by placing legitimate sounding job advertisements, complete with references to the organisation’s diversity and inclusion commitments. They use insiders at financial institutions to evade or undermine the scrutiny of compliance teams carrying out know-your-customer (KYC) and due diligence checks on new account openings. And they convert stolen funds into assets such as property and jewellery which are likely to hold their value and less likely to attract the attention of law enforcement.

View the report

Stay connected    

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.