ATTESTATION OF THE TARGET2 SINGLE SHARED PLATFORM

Against increasing risks of cyber-attacks in the financial world, SWIFT has introduced the SWIFT Customer Security Programme (CSP) to support all SWIFT users in the fight against cyber fraud and to reinforce the security of the Global financial community. This programme comprises the SWIFT Customer Security Framework (CSF) which establishes a security baseline for the entire SWIFT community and must be implemented by all users on their local SWIFT infrastructure.

The CSF, updated by SWIFT on a yearly basis, includes a mandatory attestation process whereby SWIFT users are required to submit a self-attestation against the mandatory security controls using the Registry Security Attestation Application KYC online portal developed by SWIFT for this purpose. Access to this portal is provided to each SWIFT user, allowing the submission of own data.

Starting from mid-2021, SWIFT mandates that all attestations have to be independently assessed according to the so-called “Community-Standard Assessment”. More specifically, SWIFT mandates that all attestations will need to be independently assessed through either:

- **External assessment**, by an independent external organisation which has existing cybersecurity assessment experience, and individual assessors who have relevant security industry certification(s), or;
- **Internal assessment**, by a second or third line function (e.g. compliance, risk management, internal audit) or its functional equivalent, independent from the first line function that submitted the attestation.

For 2021, following SWIFT rules, compliance to the Customer Security Control Framework (CSCF) of TARGET2 Single Shared Platform (SSP) was also verified by the Internal Audit functions of the 4CBs.

As usual, the attestation for the SWIFT infrastructure used for the TARGET2 Single Shared Platform (SSP) is not visible in the SWIFT KYC portal being related to technical BICs. In order to comply with the transparency vis-à-vis the TARGET2 participants, the Eurosystem is using this publication to disclose the compliance of the TARGET2 SSP with all mandatory controls defined in the CSF following the same structure and providing the equivalent information that could normally be found in the SWIFT KYC portal.

General information

1. Type of evaluation: Independent Internal Assessment
2. SWIFT infrastructure

2.1 Architecture type: A1 (Full stack)

2.2 Messaging interface product name: Alliance Access

Mandatory controls compliance

1 - Restrict Internet Access & Segregate Critical Systems from General IT Environment

1.1 SWIFT Environment Protection

☐ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☒ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

1.2 Operating System Privileged Account Control

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

1.3 Virtualisation Platform Protection

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

1.4 Restriction of Internet Access

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

2 - Reduce Attack Surface and Vulnerabilities

2.1 Internal Data Flow Security

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

2.2 Security Updates

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

2.3 System Hardening

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

2.6 System Hardening

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

2.7 System Hardening

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

2.10 System Hardening

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

3 - Physically Secure the Environment

3.1 Physical Security

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

4 - Prevent Compromise of Credentials

4.1 Password Policy

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

4.2 Multi-factor Authentication

☐ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☒ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

5 - Manage Identities and Segregate Privileges

5.1 Logical Access Control

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework The
☐ SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

5.2 Token Management

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

5.4 Physical and Logical Password Storage

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

6 - Detect Anomalous Activity to Systems or Transaction Records

6.1 Malware Protection

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

6.2 Software Integrity

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

6.3 Database Integrity

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

6.4 Logging and Monitoring

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

7 - Plan for Incident Response and Information Sharing

7.1 Cyber Incident Response Planning

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

7.2 Security Training and Awareness

☒ The SWIFT infrastructure of the SSP complies as per implementation guidelines in the Customer Security Framework
☐ The SWIFT infrastructure of the SSP complies using alternative implementation while meeting the same control objective

In case of enquiries, please contact your National Central Bank.