BANQUE DE FRANCE
EUROSYSTÈME

**Destinataires :**
- **Détenteurs de comptes CLM hors MCA co-managés**
- **Systèmes exogènes**

# *Info-SERI n°337*

***03/10/2024***

## *Collecte des attestations SWIFT et NEXI par la Banque de France*

**Le *Customer Security Programme* (CSP) SWIFT** a été introduit afin d'aider l'ensemble des utilisateurs de SWIFT à lutter contre la cyber-fraude et renforcer la sécurité de la communauté financière mondiale. Ce programme comprend le SWIFT *Customer Security Framework* (CSF), qui sert de référentiel en matière de sécurité pour la communauté SWIFT toute entière et doit être mis en œuvre sur l'infrastructure SWIFT locale de chacun des utilisateurs.

Le CSF prévoit un processus de **certification obligatoire** : les utilisateurs de SWIFT sont tenus de soumettre une attestation de conformité aux contrôles de sécurité obligatoires *via* le portail en ligne *KYC Registry Security Attestation Application* développé par SWIFT. Chaque utilisateur de SWIFT possède un accès à ce portail, lui permettant d'entrer ses propres données.

Pour rappel, l'évaluation par un organisme **d'audit externe** est obligatoire. Les membres de l'équipe d'évaluation doivent posséder l'expertise, les compétences d'évaluation et les références appropriées. Les organismes externes peuvent être sélectionnés dans la liste des fournisseurs d'évaluation CSP sur www.swift.com ou choisis parmi les fournisseurs de service de l'établissement.

**Les participants utilisant NEXI (ex SIA-COLT)** pour se connecter aux Services TARGET doivent également se conformer au programme de sécurité NEXI. Les rapports de certification sont à déposer sur le portail NEXI.

Afin de vérifier la résilience des participants aux Services TARGET, l'Eurosystème a décidé de collecter les attestations de l'ensemble des participants directs T2 SWIFT et T2 NEXI (systèmes exogènes,détenteurs d'un ,MCA dans CLM).

**Dans ce cadre, la Banque de France – en tant qu'opérateur de T2 Banque de France – récupère pour son périmètre les rapports remis sur les portails développés par SWIFT et NEXI.**

Pour fluidifier les échanges liés à cette campagne de collecte, nous remercions les correspondants habituels des équipes support T2-BF **d'aviser leur *Security Officer* de cette**

**démarche.** Toute demande de renseignement complémentaire peut être adressée à l'adresse T2BF@banque-france.fr

**Les attestations sont à déposer en ligne avant le 31 décembre 2024**. Pour les établissements conformes « *compliant* », la certification sera valide jusqu'au 31 décembre 2025. Pour les autres, il faudra fournir un plan d'action afin de se mettre en conformité dans les meilleurs délais. Toute attestation établie sans la validation par un organisme d'audit externe entrainera automatiquement le statut « *non-compliant* ».

## *Banque de France collection of SWIFT and NEXI attestations*

The SWIFT Customer Security Programme (CSP) was introduced to help all SWIFT users to combat cyber fraud and strengthen the security of the global financial community. The SWIFT Customer Security Framework (CSF) acts as a security baseline for the entire SWIFT community and must be implemented by all users on their local SWIFT infrastructure.

The CSF includes a mandatory certification process whereby SWIFT users are required to submit online a certificate of compliance with the mandatory security controls using the KYC Registry Security Attestation Application portal developed by SWIFT for this purpose. Every SWIFT user has access to this portal, allowing them to submit their own data.

An external auditor must assess the attestation prior to its submission. Audit firms can be selected in a list of providers on www.swift.com or among the usual providers of your institution.

Participants using NEXI (formerly SIA-COLT) to connect to TARGET Services are also required to compel to NEXI Security Programme. Evaluation reports must be provided on the NEXI gateway.

The Eurosystem has decided to collects attestations from all T2 SWIFT and T2 NEXI direct participants (ancillary systems, MCA holders directly connected to the system) in order to assess their resilience.

Within this framework, the Banque de France – as the T2-Banque de France operator – will request the reports within its scope uploaded on the portal developed by SWIFT and NEXI .