



EUROPEAN CENTRAL BANK  
EUROSYSTEM

<Company>  
<Street>  
<City>  
<Country>

25 July 2018

David De Vleeschouwer:  
E-mail: sss@nbb.be

## **SWIFT Customer Security Programme: self-attestation of your organisation**

Dear NBB-SSS participant,

As you are aware, the Customer Security Programme (CSP) has been introduced by SWIFT after cyber-attacks affected some institutions in the world with the objective to reinforce the security of the payment flows exchanged over the SWIFT network. As a part of the SWIFT CSP all SWIFT users had to submit a self-attestation to the SWIFT KYC-SA portal by 31<sup>st</sup> of December 2017.

In accordance with the NBB-SSS Guideline (Annex II, Article 28), the National Bank of Belgium in its capacity as operator of the participant has the responsibility to ensure the secure and reliable operations of NBB-SSS. This includes, inter alia, the adaption of measures to ensure the security of the end-points, i.e. the NBB-SSS participants. The importance of endpoint security is also corroborated by the (consultative) report on "Reducing the risk of wholesale payments fraud related to endpoint security" recently published by the Committee on Payments and Market Infrastructures. In this respect, the Eurosystem appreciates the initiative taken by SWIFT and fully supports the CSP as it provides an additional tool to seek assurance that participants connected to NBB-SSS via the SWIFT network meet certain security standards.

Against this background, the National Bank of Belgium requested access to the SWIFT CSP self-attestation of your institution earlier this year. Unfortunately, it was observed that your institution has not granted the National Bank of Belgium with access yet/not submitted the self-attestation yet.



EUROPEAN CENTRAL BANK

EUROSYSTEM

With this letter we would like to:

- **reiterate our request to grant the National Bank of Belgium with access to the self-attestation/submit the self-attestation. Access should be granted/the self-attestation should be submitted at the latest by 31 August 2018.**
- **Request your full compliance with the mandatory SWIFT CSP security controls by 31 December 2018**

Please rest assure that the collected data will be treated in strict confidence.

Operating a CSD on T2S means bearing a great responsibility not only for the smooth operations of the technical platform but also for the whole user community. In this respect you will certainly understand that the National Bank of Belgium could be considered negligent if it does not make use of all tools available to strengthen the operational resilience of the system. This comprises obtaining access to self-attestation of NBB-SSS participants. In case your institution will not grant the National Bank of Belgium with access to the self-attestation by the aforementioned deadline (**31 August 2018**) we will need to consider which restrictive measures could possibly be taken and we will reserve the rights to inform the relevant supervisory authority.

We trust you share our view that ensuring the security of the NBB-SSS participants and wider is a common objective and vitally important for the smooth operations of NBB-SSS and T2S and their user communities.

Thank you for your co-operation,

David De Vleeschouwer  
Account officer

Koen Geenen  
Co-head NBB-SSS