

A quick and easy way to your SWIFT-CSCF assessment

Consileon supports the SWIFT assessment for you and works with you to implement the necessary measures.

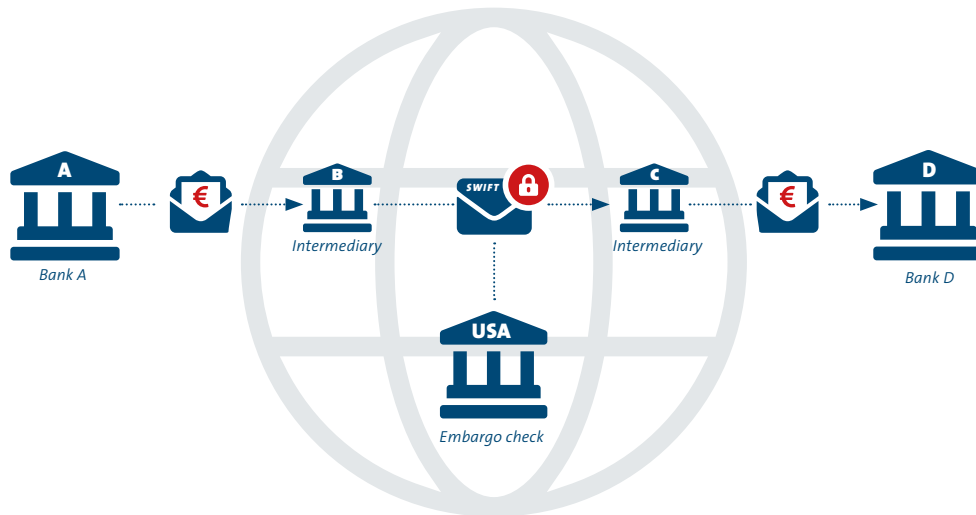
www.consileon.de



Why everything has changed at SWIFT

No international payment transactions without SWIFT

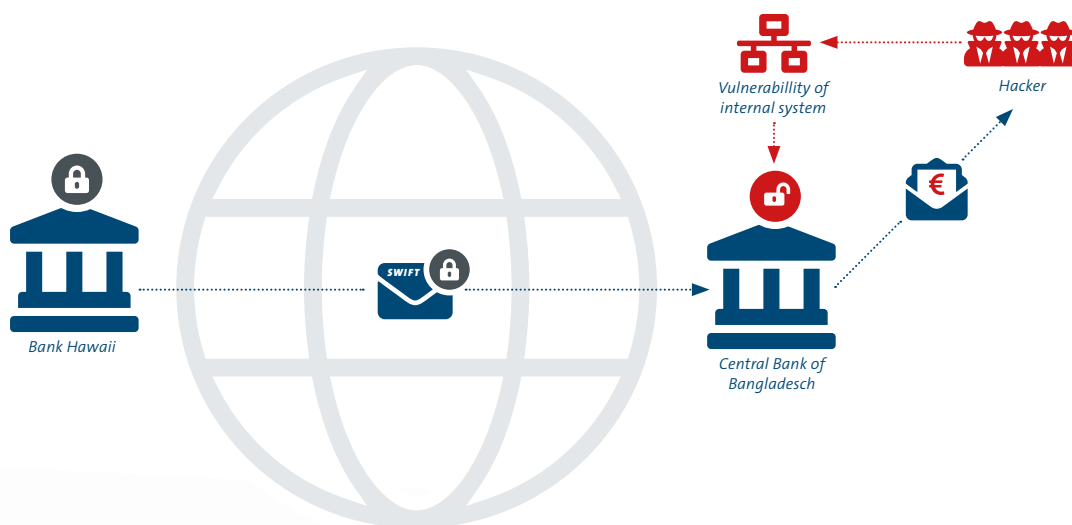
For a long time, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) mainly operated a secure communication channel for the international payment transactions of banks. This is still the case today. It is practically impossible to move money internationally without SWIFT. About 11,000 banks and financial institutions are currently connected to SWIFT and, in total, move around six trillion US Dollars per day.



Simplified representation of a transfer process using the SWIFT network.

The weak point is systematically attacked

But one event changed everything. Three hackers attacked a Japanese bank and the criminals managed to break into the bank's internal system. They used a fictitious application for this attack. Because there were no other internal security mechanisms that separated the personnel department from the payment systems, the cybercriminals were able to make fictitious transfers using the secure SWIFT network.



Simplified representation of the hacker attack on Central Bank of Bangladesh

Time is the critical factor

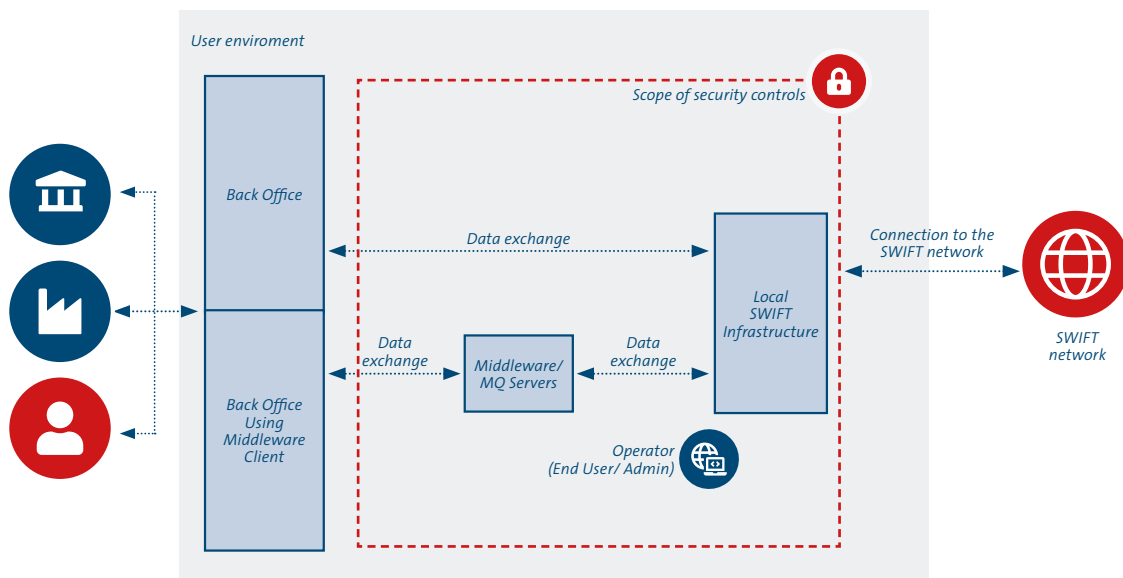
Criminals have to spend a lot of time to find the right counterpart for their fictitious bank transfers. In this case, it took the attackers more than a year until they could find a local bank that was ideal for their purposes.

Time was a critical factor for the bank as well. Detecting the loss of money alone took two days and the target bank was only informed five days later. At that point, the hackers had already withdrawn the amount of 81 million dollars and gambled it away at a casino. A faster reaction could have prevented this.

Rizal Commercial Banking Corporation (RCBC) in Manila, its manager and the branch managers responsible for the approval were subject to severe penalties. Although the hackers could be identified, they were not caught.

The lesson: Security starts with the stakeholders

Because of this event, SWIFT has come to the realisation that it must also ensure sufficient security within the affiliated banks to prevent thefts like this in the future. For that reason, SWIFT commits all participating institutions to a strict security programme, which ensures that all areas that are relevant for payment transactions and communicate with SWIFT are strictly shielded from the other IT systems of the financial institution and the Internet.



Schematic representation of the security measures of SWIFT.

Strict requirements will pose a challenge

Although the mandatory requirements of SWIFT are strict and detailed, they are certainly technically feasible. At the same time, additional provisions have already been defined, some of which will become mandatory each year.

These security measures can best be shown with a few examples:

- Extremely strict requirements when using passwords.
- Encryption of the entire internal data traffic.
- Video surveillance and motion sensors in the server environment.
- An IT check for manipulations at least once a day
- Secure external storage of logs for twelve months.
- Regular drills of reactions to a cyberattack.


A customer speaks

“To improve the security of global payments, SWIFT has established the Customer Security Program (CSP), which obligates SWIFT users to attest to the degree to which they have implemented the requirements of the SWIFT CSP. SWIFT updates this regularly and periodically changes recommended controls into mandatory controls. As the operator of a SWIFT A1 full stack architecture, the Independent Assessment Framework was already imposed on us in 2019. As part of this challenge, it’s important to highlight the strengths of Consileon Business Consultancy – not just the methodical and technical expertise but also the partnership approach and flexibility. Working with us to develop customised solutions was just as much a part of Consileon’s competence and objective as was their ongoing support until we obtained a certificate.”

Patrick Werner – Senior Vice President, Swiss Euro Clearing Bank

What we can do for you

Consileon is listed by SWIFT. You will get the following services from us:

- 
- ✓ We are your partner for the external assessment and CSCF certification
 - ✓ We will help you increase your operational cyber security to the necessary standard for SWIFT.
 - ✓ We will design the IT architecture of your Swift Secure Zone with you.
 - ✓ We will establish a robust Cyber Incident Response Process with you that can withstand the current threats.

SWIFT does not certify, warrant, endorse or recommend any service provider listed in its directory and SWIFT customers are not required to use providers listed in the directory