SCHWEIZERISCHE NATIONALBANK
BANQUE NATIONALE SUISSE
BANCA NAZIONALE SVIZZERA
BANCA NAZIUNALA SVIZRA
SWISS NATIONAL BANK

Banking Operations

Zurich, 19 April 2024

Requirements for service bureaus with communication interfaces to the SIC system, attestation process and withdrawal of approval

One of the Swiss National Bank's statutory tasks is to facilitate and secure the operation of cashless payment systems (art. 5 para. 2 (c) of the National Bank Act, NBA). To this end, it acts as commissioning party and system manager of the SIC system. The SNB acts according to the principle that the core payments infrastructure must meet the highest security standards as well as banks' specific requirements regarding efficiency. The SNB, together with SIC participants, aims to continuously develop the SIC system to ensure security and efficiency on a long-term basis.[1]

SIC system security depends not only on the level of protection of the system itself, but also of the local infrastructure used by SIC participants to exchange payment messages. This includes infrastructure of third parties, known as service bureaus (SBs), which some SIC participants use to submit payment messages to the SIC system. SBs usually have their own communication interface to the SIC system and offer various services in the area of payment message exchanges.

To ensure the security of the gateways and thereby the entire SIC system, the SNB has decided to only approve SBs for access to and exchange of payment messages with the SIC system if they meet the minimum requirements defined by the SNB. The minimum requirements apply to all already approved SBs and all new SBs seeking to offer their services to SIC participants in the future. The minimum requirements, a description of the certification process (attestation) and an overview of all approved SBs can be accessed on the SIC Ltd website.[2]

[1] SNB, 'The Swiss Interbank Clearing (SIC) payment system – Report on the SIC system and Disclosure Report', 2022.
[2] https://www.six-group.com/en/products-services/banking-services/interbank-clearing/info-center.html

1. Requirements for service bureaus

According to the SIC Handbook,[3] SBs are service providers who transmit transactions on behalf of SIC participants or their service providers (e.g. in instances of business process outsourcing, BPO) and submit them to the SIC system via their own communication interface. Transactions delivered by the SIC system are forwarded by the SB to the SIC participant or its service provider.

1.1. Minimum requirements for all service bureaus

All SBs approved by the SNB must meet the following requirements at all times:

Organisational requirements

- **SB is Swiss-domiciled company with own legal personality (legal entity)** => *The SB must be a company entered in the Swiss commercial register and have an independent auditor.*
- **Data security** => *The SB must have implemented documented technical and organisational measures that meet the minimum requirements for data security in accordance with art. 6 of the Federal Act on Data Protection and the associated Ordinance to the Federal Act on Data Protection, as well as the requirements and provisions in regulations on ensuring data security issued by the SNB and SIC Ltd.*
- **Contractual agreement between SB and customer (SIC participant)** => *The SB must conclude a contract with each of its customers specifying at least the parties' rights and obligations in relation to the services being provided in connection with the SIC system.*
- **Risk management** => *The SB must have a framework for the integrated identification, measurement, management and monitoring of key risks.*
- **Changes in company purpose** => *The SB must promptly inform the SNB of significant changes in corporate structure or purpose.*
- **Discontinuation of service** => *The SB must ensure (e.g. contractually) that its customers, for which it provides the technical connection to the SIC system as a service, receive sufficient notice (at least six months) if that service is being discontinued. This is to ensure that the customers can switch seamlessly to a different SB.*

[3] The SIC Handbook is provided to all service bureaus (including new applicants) in a suitable form.

Technical requirements

- **Meeting technical requirements for own communication interface to SIC system** => *The SB must meet all the technical requirements that are necessary for its own connection to the SIC system. These are defined and formally approved by SIC Ltd as system operator (cf. 'Technical Requirements (Gateways)' in the current version of the SIC Handbook).*
- **Secure message exchange between the SB and its customers** => *The SB must ensure that message exchanges (payment messages/instructions) between itself and its customer meet high security standards (cf. 'Connection Through a Service Bureau' in the current version of the SIC Handbook and on the SIC Ltd website).*
- **Backups and miniSIC ready** => *The SB must be able to produce backup data carriers for its customers in contingency arrangements and to successfully participate in miniSIC (cf. current version of the SIC Handbook).*
- **Compliance with endpoint security requirements** => *The SB must meet the requirements of the relevant 'Endpoint security in SIC system' framework[4] and submit its attestation of this to the SNB.*
- **Recovery time** => *In cases of disruptions in its own infrastructure, the SB must be able at all times to restore the communication interface to the SIC system that it offers as a service to SIC participants back to normal operations within 24 hours. In a departure from this requirement, the SB's customers (SIC participants) can also agree shorter recovery times with the SB, i.e. for instant payments.*
- **Reporting obligation for technical disruptions** => *The SB must report to the SNB and SIC Ltd in a timely manner and in suitable form (by phone or email) any larger disruptions that cannot be resolved quickly (<1h) and have a direct impact on the communication interface to the SIC system it offers to SIC participants as a service.*
- **Compliance with further requirements in accordance with the SIC Handbook** => *The SB must be aware of the SIC Handbook and meet the applicable obligations and requirements laid out in that document.*

1.2. Extended requirements for system-critical SBs

The SIC Handbook chapter 'Extended Obligations for System-Critical SIC Participants' contains a definition of what constitutes a system-critical SIC participant. The same definition applies to an SB as soon as it meets certain qualitative or quantitative criteria set by the SNB or as soon as it has at least one customer defined as a system-critical SIC participant using its communication interface to the SIC system. The SNB appraises system-critical SBs once a

[4] The 'Endpoint security in SIC system' framework is provided to all service bureaus (including new applicants) in a suitable form.

year and informs them of their status. In this case, the following extended requirements have to be met:

- **Recovery time** => *In cases of disruptions in its own infrastructure, the SB must be able at all times to restore the communication interface to the SIC system that it offers as a service to its customers (SIC participants) back to normal operations within 4 hours. In a departure from this requirement, the SB's customers (SIC participants) can also agree shorter recovery times with the SB, i.e. for instant payments.*
- **SIC Emergency Task Force** => *The SNB decides on a case-by-case basis whether an SB is to be included in the Emergency Task Force according to the SIC Handbook. If it is to be a member, the SNB will inform the SB ad hoc on its role in the Emergency Task Force.*

1.3. Additional requirements for new entries

- **Appropriate documentation of organisational structure and purpose of the SB** => *Corporate purpose, governance, structure, participations (abroad), organisational chart including the Board of Directors, and further important information on the company (e.g. balance sheet/income statement) are to be disclosed to the SNB.*
- **Contact person** => *The SB must give the SNB and SIC Ltd one or more contact persons (name, job title, phone number, email address), who they can reach out to with questions or in exceptional situations (e.g. contingency arrangements).*

2. Attestation

Compliance with the minimum/extended requirements are to be confirmed and demonstrated regularly to the SNB in the form it requires according to the list below. The SNB will prompt the SB to do so in good time. An independent external auditor must review the SB's compliance with the requirements and provide confirmation of such compliance to the SNB in form of a written audit report. The auditor's report must confirm that all requirements specified for the SB (minimal or extended) have been reviewed and found to have been met. In such a case, a detailed audit report is not required. If the auditor finds that one or more requirements have not been met, or have only partially been met, the audit report must contain detailed information.

The attestation is to take place as follows:

- For non-system-critical SBs: every two years
- For system-critical SBs: annually
- If the SNB changes the SB's designation from non-system-critical to system-critical: Attestation of the extended requirements in chapter 1.2 must occur within 12 months after the change. Attestation must thereafter occur annually.

- For new entries: With the submission of the application
- In case of suspicion of non-compliance with the requirements: Ad hoc at the SNB's request

All costs and expenses related to the attestation are to be borne by the SB itself.

3. Withdrawal of approval

The SNB can withdraw the approval of an SB with immediate effect in the following cases:

- No attestation submitted after repeated written requests from the SNB.
- Non-compliance with requirements after expiry of the extension period granted by the SNB.
- Risks endangering the overall stability, soundness or security of the SIC system or the fulfilment of the SNB's statutory tasks.

4. Contact

Swiss National Bank, SIC Operations, Börsenstrasse 15, CH-8022 Zurich, or by email to snbsic.ops@snb.ch.