# Annex 1
# Admission Criteria

for Consent as a Service for the bLink Platform

The following table includes a list of security criteria for application specifications of the **"high" security level** and the **service user (SU) role** from the **bLink Platform Participation Conditions, Annex 1**, and shows which criteria are covered by CaaS and which must still be provided by the service user.

| SG ID | Security goal/requirement | SF ID | Security function/process | AG ID | Assessment goal/security mechanism | Scope technical examination (TE) or process | Covered by | Comments |
|---|---|---|---|---|---|---|---|---|
| C01 | **Confidentiality**<br>The user and their authorization must be clearly identified for access to the application that uses the service, and confidentiality must be guaranteed. | F01 | The user must be clearly identified from the first time they access the service. | M01 | Session authentication on the part of the SU is **clearly linked** with the securely authenticated login in online banking (approval by the user in the online banking application) and service access – Token-User ID link in the SU application | TE | CaaS | User data in the sense of customer data |
| | | F02 | Strong authentication mechanisms to the SU application by the user | M02 | Either two-factor authentication is used or a strong technical password policy with the following features must be implemented in the SU application:<br>- Minimum length: 8 characters<br>- Complexity: combination of upper and lower case, figures, special characters required<br>- Change interval: at least every six months | TE | SU | |
| | | F03a | Session timeout in the SU application | M03a | If the session has been inactive for a longer period (max. 1 hour), the user must be logged out of the SU application. | TE | SU | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | F03b | Session timeout of the SU administrators | M03b | If the administrators' sessions are inactive, they must be limited in terms of time (to a few minutes) to limit the risk of the session being hijacked and consequently to minimize rogue changes to the configuration. | TE | CaaS<br><br>SU | CaaS administrators on the side of SIX are limited to a session timeout of 15 minutes.<br><br>For SU administrators managing criteria M02, M03a, M05 and M13 as well as M07 and M10 in the described special cases. Also applies to SU administrators who have access to unencrypted data in the context of M08. |
| | | F04 | The authentication information must be securely stored and must not be visible in plain text | M04 | The storage of authentication information (tokens) must be encrypted (using encryption processes approved by SIX).<br>Cryptographic keys used have a defined owner, who is responsible for protecting them. If the key user is not a person, a person must be assigned to it. | TE | CaaS | |
| | | F05 | Identification and authentication must be handled via a secure path. | M05 | The user's access to the application or the SU web service must take place on an encrypted basis via https (TLS encryption). No outdated protocols (e.g. TLS 1.0) or algorithms are used here | TE | SU | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| C02 | Authorization for data access must be given only to users who have agreed to the Service User's data access to the Service Provider and are authorized by the Service Provider | F06 | The user's consent to use of the service must be maintained | M01 | Session authentication on the part of the SU is **clearly linked** with the securely authenticated login in online banking (approval by the user in the online banking application) and service access – Token-User ID link in the SU application | TE | CaaS | |
| | | | | M06 | If an user cancels the SU service, the associated token must be deleted by the SU in its application within 24 hours.<br>The SU must also advise the user to withdraw consent in the online banking application at the bank | Process + contract between SU and users | SU | The SU must inform the user to revoke their consent.<br>In addition, the SU must inform SIX to delete the associated provider token. |
| C03 | Access to the data transferred from the SP must be adequately protected (at rest, in transit, at processing). | F07 | Data at rest (including backups) must be securely stored and protected against access by outsiders. | M07 | The user's data transferred from the SP is encrypted if it is stored **outside** the application. Only authorized persons (need-to-know) have access to this data (within and outside the application) or the key that is used for encryption. | TE | SU | If the SU application does not use a clipboard, CaaS fully meets this criterion |
| | | | | M08 | There are additional security measures (e.g. firewalls, antivirus software, IDS, etc.), to protect the tokens and user data. | TE | CaaS | The user data including consumer token must be protected with customary care. CaaS fully meets this criterion for provider tokens. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | F08 | Access to data must be restricted and logged. | M09 | Roles must be defined that separate technical access, application access and user access (data). Logs must be monitored for suspicious activities (by users or administrators at the SU). | Process & TE | CaaS | CaaS fully meets this criterion for provider tokens. |
| | | F09 | The issue of access rights must be regulated | M10 | An access management process must be defined and implemented that regulates the granting, maintenance and withdrawal of rights (incl. administrator rights). The existing user rights must also be subjected to recertification periodically (at least annually). | Process | CaaS<br>SU* | Access management for access to provider tokens is provided by CaaS.<br>*If the SU integrates the management of CaaS via an API, the security criteria (M10) must be ensured by the SU. |
| C04 | Authorization to access data must be given only to SU administrators if this is needed for the service to be supplied | F08 | Access to data must be restricted and logged | M09 | Roles must be defined that separate technical access, application access and user access (data). Logs must be monitored for suspicious activities (by users or administrators at the SU). | Process & TE | CaaS | CaaS fully meets this criterion for provider tokens. |
| | | F11 | If an administrator changes position or role, access rights must be withdrawn or amended within an appropriate period | M10 | An access management process must be defined and implemented that regulates the granting, maintenance and withdrawal of rights (incl. administrator rights). The existing user rights must also be subjected to recertification periodically (at least annually). | Process | CaaS<br>SU* | Access management for access to provider tokens is provided by CaaS.<br>*If the SU integrates the management of CaaS via an API, the security criteria (M10) must be ensured by the SU. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| C05 | If data is stored or accessed outside Switzerland, the user must be informed clearly and comprehensively and appropriate consent must be obtained | F12 | It must be possible to restrict data storage and access (not user access) to Switzerland. | M11 | If the user's explicit consent has not been obtained, the data must not be stored abroad or accessed from abroad (by system administrators, support personnel, etc.). Technical/organizational measures are used to ensure this does not happen. The users themselves may access their data from anywhere. | TE | SU | For the provider tokens, storage is carried out by SIX in Switzerland. |
| I01 | **Integrity**<br>Access to the SP service must be traceable | F13 | All events needed to ensure traceability (audit trail) must be logged. | M12 | An audit trail re service authentication (use of user token) must be maintained. | TE | CaaS | |
| I02 | Anomalous use of the service must be detected | F14 | Mechanisms that detect deviations from planned behavior must be defined. | M13 | Users' access must be monitored for security-relevant events (such as the use of incorrect passwords) | TE | SU | Incorrect logins must be monitored. |
| A01 | **Availability, BCP, DR**<br>Access data must not be lost | F16 | The SU must be able to restore the tokens and link. | M14a | Backup or data mirroring must be available for the tokens and link or there is a data recovery concept. Any backups should have the same protection measures as the primary server. | TE | CaaS | |
| T01 | **Technology**<br>Identification of the IT systems involved | F18 | The SU can demonstrate the systems on which the relevant data is processed and stored. | M15 | The SU maintains an inventory of the systems that contains the access data and the transferred data. | Process | CaaS | SIX maintains an inventory of the CaaS environment |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| P01 | **Processes**<br>Security policy | F19 | There is a security policy | M16 | Existence of a documented and current security policy that records the company's basic security objectives and security requirements and the security organization in the company. | Process | CaaS | |
| P02 | There is an incident management process for dealing with disruptions and security incidents. | F20 | The SU can manage incidents and communicates security incidents | M17 | - The SU has an incident management process to ensure that incidents and security incidents can be managed over the entire life cycle<br>- The SU has a documented and implemented SIEM process that also allows incidents to be reported to SIX. Generally, there is a process for notifying the parties involved (i.e. SIX, customers, relevant authorities) immediately that the confidentiality of account information has been breached in their area of responsibility (pursuant to article 92 of PSD2)<br>- There is a contact point (incl. name and e-mail) for customers in cases of fraud, technical problems and receivables management and details of the contact point have been announced | Process | CaaS | The service user must provide a contact point (including name and e-mail) for customers in cases of fraud, technical problems and receivables management and details of the contact point must be announced. |
| P03 | The SU has a change management process | F21 | Change management process exists and has been implemented | M18 | The SU has a current, adequate change management process that, taking account of the separation of functions, approval and test process as part of change | Process | SU | CaaS has a change management process |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | management, guarantees prompt, qualitatively appropriate introduction or updating of the APIs | | | |
| P04 | The SU has a management process for its own subcontractors that process relevant data | F22 | Subcontractors that process data must fulfill the same data storage terms as the SU. | M19 | There is a contract and management process for subcontractors with equivalent security requirements | Process | SU | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| P05 | Administrator's security check | F23 | Criminal record | M20 | The following documents must have been obtained for all the SU's administrators: criminal record and extract from the debt collection register | Process | CaaS<br>SU | For SU administrators managing criteria M02, M03a, M05 and M13 as well as M07 and M10 in the described special cases. Also applies to SU administrators who have access to unencrypted data in the context of M08. |
| P06 | Physical access | F24 | Servers for token storage must be adequately protected in physical terms | M21 | Servers for token storage are adequately protected in physical terms (e.g. access to computer center is regulated and monitored) | TE | CaaS | |