Annex 1
Admission Criteria

to the bLink Platform Participation Contract

1. Definitions

The following definitions are used in this document:

API Service	An API service represents the smallest unit of the application offered via an API for which an application agreement is concluded.
Application	An application is a service that a Service Provider makes available to the Service User via one or more API services via the bLink Marketplace. The contractual conditions of the application are defined in the respective application specification, which becomes the application agreement if the data exchange is successful.
Application Agreement	Agreement between the Service Provider and the Service User, which is concluded when the Service Provider answers the service call on the platform in accordance with the application specification (details in the *bLink Platform Participation Contract*, section 6.2 N 44 et seq.).
bLink Marketplace	A service operated by SIX that publishes all applications and makes them available for use.
End Customer	The End Customer is a customer of the Service Provider and account/security account holder.
Participant	The participant is the contractual partner of SIX in the *bLink Platform Participation Contract*. The participant assumes the role of either Service Provider or Service User in the application agreement.
Participation Contract	With a positive decision on admission to the platform and at least one of the desired applications, the *bLink Platform Participation Contract* comes into effect with the legally valid signing of the participation conditions.
Partner API	The API of a Service Provider, about the existence and use of which the Service Provider can freely decide within the scope of Annex 2 — Partner API Application Specifications, in particular with regard to the design of the API Service and the technical specifications (ownership).
Platform	The bLink platform operated by SIX.
Service Provider	Party that provides the API service.
Service User	Party that obtains the API service.
User	The User uses the API service provided by the Service User.

The term "customer" is used in the "bLink Platform Participation Contract". For certain applications, it makes sense for there to be a differentiation and "customer" is used as a generic term covering "End Customer" or "User," i.e. "customer" can mean either "End Customer" or "User."

2. General

This Annex shall describe the admission criteria, the fulfillment of which is a prerequisite for participating in the Platform. The admission criteria shall consist of the following integral parts to be fulfilled in full:

1. General admission criteria

General admission criteria are uniformly regulated for all applications and shall be met at all times within the scope of all applications, independently of the role applied for (Service User or Service Provider) and the defined security level.

2. Criteria for fulfilling the purpose limitation

The criteria for fulfilling the purpose limitation shall define the proof of compliance to be provided with the purpose limitation as described in the respective application specifications (Annex 2). These criteria shall be defined per application. Should the participant decide to opt in for a certain application, the purpose limitation criteria of the corresponding application must be met.

3. Security criteria in the submitted role

The security criteria regulate the objectives and required mechanisms for secure data exchange as defined in the Participation Contract and are based on the protection requirements of the respective application. The scope of the security criteria thus extends to all parties and components involved in the data transmission outside the application. This also applies to the transmission path and the parties and components involved between the customer and the application, insofar as the customer is involved in the authorization and authentication of the service calls.

The security criteria are determined by the defined security level for the requested role (Service User or Service Provider) of the Participant in the respective application.

Participants who meet security criteria for a defined security level are authorized to use applications of the same or lower security levels in the same role, provided that the criteria in section 2 and section 4 of this chapter (fulfillment of purpose limitation, technical specifications) are met.

4. Technical specifications

The technical requirements are defined in the application specifications as technical specifications and are to be implemented by the Participant.

5. Regular repetition of the admission test

The Participant undertakes to repeat the test of the admission criteria no later than 12 months after the results of the last test in accordance with the Participation Contract (Chapter 3 N 8 et seq.).

3. Special regulations

1. Financial institutions supervised by FINMA or FMA

Financial institutions that can prove that they are authorized as a Swiss bank as defined in Article 1 of the Swiss Federal Act on Banks and Savings Banks ("Swiss financial institution") and meet the criteria for fulfilling the purpose limitation in accordance with chapter 2 section 2 are admitted to the bLink platform. The existence of this authorization must be confirmed in writing by the Swiss financial institution and will be checked by SIX based on the publicly available information on the website of the Swiss Financial Market Supervisory Authority ("FINMA"; www.finma.ch).

Financial institutions that can prove that they are authorized as a Liechtenstein bank by the Liechtenstein Financial Market Authority ("FMA") and meet the criteria for fulfilling the purpose limitation in accordance with chapter 2 section 2 are admitted to the Platform. The existence of this authorization must be confirmed in writing by the Liechtenstein financial institution and will be checked by SIX based on the publicly available information on the website of FMA (www.fma-li.li).

SIX reserves the right to separately verify the fulfillment of additional criteria introduced as part of an application by the banks regulated by FINMA or FMA.

2. Swiss authorities

The term "Swiss public authority" refers to a public body in Switzerland that performs public administration functions entrusted to it by public law. Within the framework of the Participation Contract, the authority acts as a Participant in the role of Service Provider or Service User.

Participants who qualify as a Swiss authority and meet the criteria for fulfilling the purpose limitation according to Chapter 2 section 2 and the security criteria in the submitted role according to Chapter 2 section 3 are admitted to the Platform.

The qualification as an authority must be confirmed in writing by the Participant and presented accordingly on request (e.g. appearance of the website, the administrative structure) and will be reviewed by SIX on the basis of the publicly available information on the relevant website.

SIX reserves the right to separately verify the fulfillment of additional criteria introduced as part of an application by the Swiss authorities.

3. SIX as Participant

SIX is admitted to the Platform as a Participant if the components of the admission criteria according to Chapter 2 are met. The verification of the fulfillment of the requirements is carried out in accordance with the procedure defined in Chapter 9 of the Participation Contract.

4. General Admission Criteria

ID	Category	Criterion	What is the goal?	Covered information/topics	Data to be provided by the Participant
1	Identification	Is entered in the commercial register as a legal entity	- Confirmation that the company is entered into the commercial register as a legal entity and is active - Identification of the company address and registered management	Company name and legal form Address Identification number Identification of the management / authorized signatories	- Incorporation documentation
2	Business model	Has a documented business model with the intended services	- Identification of the applicant's business activities - Comparison and reconciliation of the business model with the intended services	Identification and summary of the company's business and services	- Business model/business plan
3	Liquidity	Has a resilient business plan and a budget plan for 1–3 years	- Analysis of annual financial statements and budget planning to summarize the applicant's financial situation	Overview of financial data and calculation of key ratios	- Annual financial statements
4	Organizational structure	Provides an organization chart showing key functions and branches	- Overview of the applicant's structure with key functions and responsible persons - Overview of countries and locations where the applicant operates	The management cannot be identified in more detail through the commercial register Summaries of additional sites and services	- Organizational chart
5	Auditing	Accounting standards List of auditors	- Ensuring that the applicant has adequate accounting processes and appropriate internal controls	Names of the auditors	- List of auditors/along with annual financial statements
6	Compliance with sanctions and measures to combat money laundering and the financing of terrorism	Is not included on sanctions lists and alert lists issued by the regulatory authorities as a company or because of its members of the management/owners	- Preparation of profiles of the applicant's management, e.g. managing directors, finance directors, employees responsible for the application - Identification of negative incidents concerning financial crimes in which members of the management were/are involved. - Identification of whether the company and its management are politically exposed	Bribery, corruption, fraud Links to public officials (PEP status) Illegal and criminal actions Financial non-compliance Regulatory non-compliance Legal disputes Harmful reporting Entry on sanctions list	n/a
7	Compliance with laws	- Has no members of the management/owners that have a criminal record, are listed in registers of bankruptcies and debt collections that **preclude exemplary management** - Lists pending admission and criminal procedures	- Identification of negative incidents such as criminal proceedings or insolvency proceedings in which members of the management are involved	Criminal records/register of bankruptcies and debt collections covered by criterion 6	- Extracts of criminal records of the management - Confirmation that the provider is not involved in any legal proceedings

8	Rejected admissions for other banks, regulators	Details of whether a relevant assessment for admission has already been rejected by another authority with details of the reason	- Confirmation of whether the company has been admitted/licensed by relevant authorities	Active and valid licenses and permits are held No licenses or permit; this is covered under criterion 6: "Regulatory non-compliance"	- Licenses/confirmations of relevant authorities
9	Reliability, honesty, integrity of the management	Evidence of knowledge/skills/experience from their CVs	- Preparation of profiles, such as the CVs of the applicant's management, e.g. managing directors, finance directors, employees responsible for the application - Identification of negative incidents regarding employment, such as loss of employment or dismissal by the employer	Background information (e.g. nationality, place of residence, degree program) Past activities Compliance with laws and personal integrity (covered under criterion 6 and 7)	- CVs of the key members of the management

Table 1: General admission criteria

5. Security Criteria in the Submitted Role

The following table includes a list of security criteria for application specifications of the **"basic" security level and the Service User (SU) role**:

SG ID	Security goal/requirement	SF ID	Security function/process	AG ID	Assessment goal/security mechanism	Scope: technical examination (TE) or processes
C01	**Confidentiality** The User and their authorization must be clearly identified for access to the application that uses the service and confidentiality must be guaranteed.	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
		F04	The authentication information must be securely stored and must not be readable in plain text.	M04	The storage of authentication information (tokens) must be encrypted (using encryption processes approved by SIX). 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
C03	Access to the data transferred from the SP must be adequately protected (at rest, in transit, at processing).	F09	The granting 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
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, data must not be stored abroad and the User's data must not be accessed from abroad (e.g. system administrators, support personnel, etc.). Technical/organizational measures are used to ensure this does not happen. The User themselves may access their data from anywhere.	TE
I01	**Integrity** Access to the SP service must be traceable.	F13	All events needed to ensure traceability (audit trail) must be logged.	M12	An audit trail regarding service authentication (use of User token) must be maintained.	TE
T01	**Technology** 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

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. - 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). - There is 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 have been announced.	Process
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 management, guarantees prompt, qualitatively appropriate introduction or updating of the APIs.	Process
P04	The SU has a management process for its own subcontractors, who process relevant data	F22	Subcontractors processing data must meet the same data retention requirements as the SU.	M19	There is a contract and management process for subcontractors with equivalent security requirements.	Process

Table 2: Security criteria for the Service User at “basic” security level

The following table includes a list of security criteria for application specifications of the **"high" security level and the Service User (SU) role**. The listed security criteria apply **in addition** to those of the "basic" security level:

SG ID	Security goal/requirement	SF ID	Security function/process	AG ID	Assessment goal/security mechanism	Scope: technical examination (TE) or processes
C01	**Confidentiality** 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 **uniquely 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
		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 to be implemented in the SU application: - Minimum length: 8 characters - Complexity: combination of upper and lower case, figures, special characters required - Change interval: at least every six months	TE
		F03a	Session timeout in the SU application	M03a	If the session has been inactive for a longer period (max. 1h), the User must be logged out of the SU application.	TE
		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
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 customer's consent to the use of the service must be maintained.	M01	Session authentication on the part of the SU is **uniquely 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
				M06	If a User cancels the SU service, the associated token must be deleted by the SU in its application within 24 hours. The SU must also advise the User to withdraw consent in the online banking application at the bank.	Process + contract between SU and Users
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
				M08	There are additional security measures (e.g. firewalls, anti-virus software, IDS, etc.), to protect the tokens and User data.	TE
		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 administrators at the SU).	Process & TE

C04	Authorization to access data may 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 administrators at the SU).	Process & TE
		F11	If an administrator changes their 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
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
A01	**Availability, BCP, DR** 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
P01	**Processes** Security policy	F19	There is a security policy in place.	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
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
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 data center is regulated and monitored).	TE

Table 3: Security criteria for the Service User at "high" security level

The following table includes a list of security criteria for application specifications of the **"very high" security level and the Service User (SU) role**. The listed security criteria apply **in addition** to those of the "high" security level:

SG ID	Security goal/requirement	SF ID	Security function/process	AG ID	Assessment goal/security mechanism	Scope: technical examination (TE) or processes
I03	**Integrity** The non-repudiation of a transaction must be guaranteed. Transactions are all API request/response calls that form a logical unit.	F25	The transaction must be complete.	M22	The Service User must provide the same information to the Service Provider as if the User were executing the transaction themselves.	TE
		F26	The transaction must be uniquely referenced.	M23	The transaction must have a unique transaction ID	TE
		F27	Verification of the transaction response.	M24a	The SU is obliged to check that the order sent and the confirmation received from the Service Provider match, to inform the User immediately of any discrepancies and to enable any corrective measures to be taken.	Process
		F28	Designation of automated orders.	M25	Rule-based or automated transactions must be recognizable by the Service Provider.	TE
		F29	Non-repudiation of User orders.	M26	When a User issues automated (rule-based) orders, the Service User must ensure the traceability and non-repudiation of those orders.	TE
		F30	Storage of the transaction response (recommendation).	M27	The Service Provider's transaction response should be stored in such a way that it can be used at a later date for any claims.	n/a

Table 4: Security criteria for the Service User at "very high" security level

The following table includes a list of security criteria for application specifications of the **"basic" security level and the Service Provider (SP) role**[1]:

SR ID	Security goal/requirement	SF ID	Security function/process	AG ID	Assessment goal/security mechanism	Scope: technical examination (TE) or processes
C01	**Confidentiality** The User and their authorization must be clearly identified for access to the application that uses the service and confidentiality must be guaranteed.	F02	The authentication information must be securely stored and must not be readable in plain text.	M52	The token issued by the SP must not contain sensitive information (CID). The token must not be saved without being encrypted either.	TE
C03	Access to keys for the service (token) and the data transferred to the SU must be adequately protected (at rest, in transit, at processing).	F26	Access to the authentication service must be protected.	M56	Access from the Internet to the service (e.g. online banking) must be secured by means of perimeter protection (proxy, WAF).	TE
		F28	The granting 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
C05	If data is stored or accessed outside Switzerland, the User must be informed clearly and comprehensively and appropriate consent must be obtained.	F11	It must be possible to restrict data storage or access (not User access) to Switzerland.	M11	If the User's explicit consent has not been obtained, data must not be stored abroad and the User's data must not be accessed from abroad (e.g. system administrators, support personnel, etc.). Technical/organizational measures are used to ensure this does not happen. The User themselves may access their data from anywhere.	TE
I01	**Integrity** Access to the SP service must be traceable.	F13	All events needed to ensure traceability (audit trail) must be logged.	M12	An audit trail regarding service authentication (use of User token) must be maintained.	TE
T01	**Technology** Identification of the IT systems involved.	F21	The SP can demonstrate the systems on which the relevant data is processed and stored.	M15	The SP maintains an inventory of the systems that contains the access data and the transferred data.	Process

[1] The "basic" security level does not cover the requirements for the exchange of "Client Identifying Data" (CID) on the bLink platform.
CID includes information about customers that makes it possible to draw direct or indirect conclusions about the existence of a customer relationship with the bank.
Also not covered by the "basic" security level are value-changing, i.e. asset-changing, transactions.

P02	There is an incident management process for dealing with disruptions and security incidents.	F22	The SP can manage incidents and communicates security incidents.	M17	- The SP has an incident management process to ensure that incidents and security incidents can be managed over the entire life cycle. - The SP 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). - There is 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 have been announced.	Process
P03	The SP has a change management process.	F21	Change management process exists and has been implemented.	M18	The SP has a current, adequate change management process that, taking account of the separation of functions, approval and test process as part of change management, guarantees prompt, qualitatively appropriate introduction or updating of the APIs.	Process
P04	The SP has a management process in place for their subcontractors processing relevant data.	F23	Subcontractors processing data must meet the same data retention requirements as the SP.	M19	There is a contract and management process for subcontractors with equivalent security requirements.	Process
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 data center is regulated and monitored).	TE

Table 5: Security criteria for the Service Provider at “basic” security level

The following table includes a list of security criteria for application specifications of the **"high" security level and the Service Provider (SP) role**. The listed security criteria apply **in addition** to those of the "basic" security level:

SR ID	Security goal/requirement	SF ID	Security function/process	AG ID	Assessment goal/security mechanism	Scope: technical examination (TE) or processes
C01	**Confidentiality** 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.	M51	The SP verifies the User with strong authentication.	TE
		F03a	Session timeout in the SP application.	M03a	If the session has been inactive for a longer period (max. 1h), the User must be logged out of the SP application.	TE
		F03b	Session timeout of the SP 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
		F25	The User must be unambiguously identified periodically.	M53	The token for User access (refresh token) must be revoked after a defined period or expire and another strong authentication process must be carried out to create the token.	TE
		F05	Identification and authentication must be handled via a secure path.	M05	The User's access to the application or the SP 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
C02	Authorization for data access must be given only to Users who have agreed to the data access and are authorized by the Service Provider.	F04	The User's consent must be checked.	M54	Non-repudiable evidence of consent for the release of data to the SU has been obtained.	TE
				M55	Access to the service obtained from the SU must be restricted to the scope (e.g. account information and payment submission) of the User consent provided.	TE
C03	Access to keys for the service (token) and the data transferred to the SU must be adequately protected (at rest, in transit, at processing).	F27	Access to the service and data must be restricted and logged.	M57	Roles must be defined that allow technical access and application access to be separated. Logs must be monitored for unusual use of the service.	TE
C04	Authorization to access data may be given only to SP administrators if this is needed for the service to be supplied.	F31	If an administrator changes their 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
I02	**Integrity** 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

A01	**Availability, BCP, DR** Access data must not be lost.	F19	The SP must be able to restore service access and consent.	M14b	Backup or data mirroring must be available for service access and consent, or there is a data recovery concept. Any backups should have the same protection measures as the primary server.	TE
P01	**Processes** Security policy	F19	There is a security policy in place.	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
P05	Administrator's security check	F23	Criminal record	M20	The following documents must have been obtained for all the SP's administrators: criminal record and extract from the debt collection register.	Process

Table 6: Security criteria for the Service Provider at "high" security level

The following table includes a list of security criteria for application specifications of the **"very high" security level and the Service Provider (SP) role**. The listed security criteria apply **in addition** to those of the "high" security level:

SG ID	Security goal/requirement	SF ID	Security function/process	AG ID	Assessment goal/security mechanism	Scope: technical examination (TE) or processes
I03	**Integrity** The non-repudiation of a transaction must be guaranteed. Transactions are all API request/response calls that form a logical unit.	F31	Receipt of the transaction must be fully acknowledged.	M58	Immediately after receiving the transaction, the Service Provider must confirm receipt to the Service User with at least the transaction information received and the status of the transaction.	TE
		F26	The transaction must be uniquely referenced.	M23	The transaction must have a unique transaction ID.	TE
TM01	**Transaction monitoring**	F32	Transaction parameters must be monitored and logged to assess risk, fraud or security incidents.	M59	Service Providers have transaction monitoring that enables them to detect fraudulent transactions in the best possible manner.	Process
D01	**Unique linking of transaction authorization to transaction**	F33	Dynamic linking of transactions.	M59	The Service Provider must authorize the transaction (if there is no exemption) using MFA by the User. The MFA has the following properties: - the User (e.g. initiator) receives information about the transaction made (e.g. amount) and the transaction recipient - the generated authentication code is specific to the transaction, which the transaction initiator agreed to when initiating the transaction and this is transparently verifiable for the initiator - the authentication code is uniquely linked to the transaction, i.e. the transaction may only be accepted if an identifier and confirmed transaction information match.	TE
		F34	Dynamic linking of batch transactions.	M60	In the case of authorizing multiple transactions as a batch (unless an exemption exists), the MFA's authentication code must be specific to the batch and display verifiable information about the batch order to the User.	TE
		F35	Designation of failed transaction authorization.	M61	In the event of a failed transaction authorization, the Service User must be notified.	TE

P07	**Processes** **Handling of exceptions**	F35	The security measures of the transactions must be reviewed regularly	M62	Security measures must be documented and periodically tested, evaluated and audited by an independent expert: Transactions are authorized using the User's multi-factor authentication (MFA), which is linked one-to-one to the transaction, unless there is a documented exemption based on a documented fraud management process.	Process
		F36	Exemptions are governed by the application specifications and are only possible for those cases that are subject to risk monitoring.	M63	The MFA for transaction authorization must only be waived in specific cases if, for example: - specific and limiting conditions regarding risks are defined - amount, recurring transactions or transaction channels are defined. In the event of anomalies or fraud, the MFA must be activated immediately or the transaction must be blocked or suspended and checked separately.	Process

Table 7: Security criteria for the Service Provider at "very high" security level