Anhang 1
Zulassungskriterien

zum Teilnahmevertrag bLink Plattform

1. Definitionen

In diesem Dokument werden folgende Definitionen verwendet:

Anwendung	Eine Anwendung ist eine Dienstleistung, die ein Service-Provider über ein oder mehrere API Services dem Service User via bLink Marketplace zur Verfügung stellt. Die vertraglichen Bedingungen der Anwendung werden in der jeweiligen Anwendungsspezifikation definiert, die bei erfolgreichem Datenaustausch zum Anwendungsvertrag wird.
Anwendungsvertrag	Vereinbarung zwischen dem Service Provider und dem Service User, die mit Beantwortung des Service Calls durch den Service Provider auf der Plattform gemäss Anwendungsspezifikation zustande kommt (Details im Teilnahmevertrag Ziff. 6.2 N 44 ff).
API Service	Ein API Service repräsentiert die kleinste Einheit der über ein API angebotenen Anwendung, für die ein Anwendungsvertrag zustande kommt.
bLink Marketplace	Ein durch SIX betriebener Service, der alle Anwendungen publiziert und zur Nutzung bereitstellt.
Endkunde	Kunde des Service Providers und Konto-/Depotinhaber
Nutzer	Der Nutzer nutzt den vom Service User bereitgestellten API Service.
Partner API	Die API eines Service Providers, über deren Bestand und Verwendung dieser im Rahmen von Anhang 2 - Partner API Anwendungsspezifikationen - frei entscheiden kann, dies insbesondere im Hinblick auf die Ausgestaltung des API Service und die Technischen Spezifikationen (Ownership).
Plattform	Die durch SIX betriebene bLink Plattform
Service Provider	Erbringt den API Service.
Service User	Bezieht den API Service.
Teilnahmevertrag	Mit positivem Zulassungsentscheid zur Plattform und zu mindestens einer der gewünschten Anwendungen kommt mit rechtsgültiger Unterzeichnung der Teilnahmebedingungen der Teilnahmevertrag zustande.
Teilnehmer	Der Teilnehmer ist der Vertragspartner von SIX im Teilnahmevertrag bLink Plattform. Der Teilnehmer nimmt im Anwendungsvertrag entweder die Rolle als Service Provider oder als Service User ein.

Im Teilnahmevertrag wird die Bezeichnung «Kunde» verwendet. Für gewisse Anwendungen ist eine Differenzierung sinnvoll und «Kunde» dient dort als Oberbegriff zu «Endkunde» oder «Nutzer», d.h. «Kunde» kann sowohl «Endkunde» oder «Nutzer» sein.

2. Allgemeines

Dieser Anhang beschreibt die Zulassungskriterien, deren Erfüllung eine Voraussetzung für die Teilnahme an der Plattform ist. Die Zulassungskriterien bestehen aus nachfolgenden Bestandteilen die vollumfänglich zu erfüllen sind:

1. Generelle Zulassungskriterien

Generelle Zulassungskriterien sind für alle Anwendungen einheitlich geregelt und sind unabhängig von der beantragten Rolle (Service User oder Service Provider) sowie des definierten Sicherheitslevels im Rahmen aller Anwendungen zu erfüllen.

2. Kriterien für die Erfüllung der Zweckbindung

Die Kriterien für die Erfüllung der Zweckbindung definieren den zu erbringenden Nachweis zur Einhaltung der Zweckbindung wie sie in den jeweiligen Anwendungsspezifikationen (Anhang 2) beschrieben sind. Diese Kriterien sind pro Anwendung definiert. Entscheidet sich der Teilnehmer einer Anwendung beizutreten, sind die Zweckbindungskriterien der entsprechenden Anwendung zu erfüllen.

3. Sicherheitskriterien in der beantragten Rolle

Die Sicherheitskriterien regeln die Ziele und benötigten Mechanismen für einen sicheren Datenaustausch im Sinne des Teilnahmevertrages und basieren auf dem Schutzbedarf der jeweiligen Anwendung. Der Scope der Sicherheitskriterien erstreckt sich somit auf alle an der Datenübertragung beteiligten Parteien und Komponenten ausserhalb der Applikation. Dies betrifft auch die Übertragungsstrecke und die beteiligten Parteien und Komponenten zwischen Kunde und der Applikation, insofern der Kunde an der Autorisierung und Authentifizierung der Service-Calls beteiligt ist.

Die Sicherheitskriterien bestimmen sich nach dem definierten Sicherheitslevel für die beantragte Rolle (Service User oder Service Provider) des Teilnehmers in der jeweiligen Anwendung.

Teilnehmer, die Sicherheitskriterien für ein definiertes Sicherheitslevel erfüllen, sind für die Nutzung von Anwendungen derselben oder tieferen Sicherheitslevels in der selben Rolle berechtigt, sofern die Kriterien von Ziffer 2 und Ziffer 4 dieses Kapitels (Erfüllung der Zweckbindung, Technische Spezifikation) eingehalten sind.

4. Technische Spezifikationen

Die technischen Anforderungen sind in den Anwendungsspezifikationen als Technische Spezifikationen definiert und sind vom Teilnehmer umzusetzen.

5. Regelmässige Wiederholung der Zulassungsprüfung

Der Teilnehmer verpflichtet sich, die Prüfung der Zulassungskriterien spätestens 12 Monate nach dem letzten Prüfergebnis gemäss Teilnahmevertrag (Kapitel 3 N 8 ff.) zu wiederholen.

3. Sonderregelungen

1. FINMA-regulierte Banken

Teilnehmer, die über eine Bewilligung als schweizerische Bank im Sinne von Art. 1 des schweizerischen Bundesgesetzes über die Banken und Sparkassen verfügen, und die Kriterien zur Erfüllung der Zweckbindung gemäss Kapitel 2 Ziffer 2 erfüllen, sind zur Plattform zugelassen.

Das Vorliegen einer solchen Bewilligung ist vom Teilnehmer schriftlich zu bestätigen und wird durch SIX aufgrund der öffentlich verfügbaren Informationen auf der Webpage der Eidgenössische Finanzmarktaufsicht FINMA (www.finma.ch) überprüft.

SIX behält sich vor, die Erfüllung von im Rahmen einer Anwendung zusätzlich eingeführten Kriterien bei FINMA-regulierten Banken gesondert zu prüfen.

2. Schweizerische Behörde

Als «Schweizerische Behörde» wird eine öffentliche Stelle in der Schweiz bezeichnet, welche Aufgaben der öffentlichen Verwaltung wahrnimmt, die ihr aufgrund öffentlichen Rechts auferlegt sind. Im Rahmen des Teilnahmevertrags tritt die Behörde als Teilnehmer in der der Rolle als Service Provider oder als Service User auf.

Teilnehmer, die als schweizerische Behörde qualifizieren und die Kriterien zur Erfüllung der Zweckbindung gemäss Kapitel 2 Ziffer 2 sowie die Sicherheitskriterien in der beantragten Rolle gemäss Kapitel 2 Ziffer 3 erfüllen, sind zur Plattform zugelassen.

Die Qualifikation als Behörde ist vom Teilnehmer schriftlich zu bestätigen und auf Verlangen entsprechend darzulegen (z.B. Auftritt Webseite, Aufbau Verwaltungsstruktur) und wird durch SIX aufgrund der öffentlich verfügbaren Informationen auf der entsprechenden Webpage überprüft.

SIX behält sich vor, die Erfüllung von im Rahmen einer Anwendung zusätzlich eingeführten Kriterien bei Schweizerischen Behörden gesondert zu prüfen.

3. SIX als Teilnehmer

SIX ist als Teilnehmer zur Plattform zugelassen, sofern die Bestandteile der Zulassungskriterien gemäss Kapitel 2 erfüllt sind. Die Prüfung der Erfüllung der Voraussetzungen erfolgt gemäss dem im Teilnahmevertrag, Kapitel 9 definierten Verfahren.

4. Generelle Zulassungskriterien

ID	Kategorie	Kriterium	Was ist das Ziel?	Abgedeckte Information / Themen	Vom Teilnehmer zu liefernde Daten
1	Identifikation	hat einen Handelsregistereintrag als juristische Person	- Bestätigung, dass das Unternehmen als juristische Person im Handelsregister eingetragen ist und aktiv ist - Identifikation von der Unternehmensadresse und eingetragene Geschäftsleitung	Unternehmensname & Rechtsform Anschrift Identifikationsnummer Identifizierung der Geschäftsleitung / Unterschriftsberechtigten	- Gründungsunterlagen
2	Businessmodell	besitzt ein dokumentiertes Businessmodell mit den beabsichtigten Diensten	- Identifikation von den Geschäftstätigkeiten des Antragstellers - Vergleich und Abstimmung des Businessmodells mit den beabsichtigten Dienste	Identifikation und Zusammenfassung der Geschäfte und Dienstleistungen von dem Unternehmen	- Geschäftsmodell / Business Plan
3	Liquidität	besitzt einen belastbaren Businessplan und einen Budgetplan für 1-3 Jahre	- Analyse von Jahresabschlüssen und Budgetplanung um die finanzielle Situation des Antragsstellers zusammen zu fassen	Übersicht von Finanz-Kennzahlen und Ausrechnung von Schlüssel-Ratios	- Jahresabschlüsse
4	Organisatorischer Aufbau	legt Organigramm mit Schlüsselfunktionen und Niederlassungen vor	- Übersicht über die Struktur des Antragstellers mit den Schlüssel-Funktionen und verantwortlichen Personen gewinnen - Übersicht in welchen Ländern und Orten der Antragsteller tätig ist	Weitere Identifikation der Geschäftsleitung wenn durch Handelsregister nicht möglich Zusammenfassungen der weiteren Standorte und Dienstleistungen	- Organigramm
5	Rechnungsprüfung	Rechnungslegungsstandards Liste der Revisoren	- Sicherstellung, dass der Antragstellende ein angemessenes Rechnungslegungsverfahren und entsprechende interne Kontrollen hat	Namen der Revisoren	- Revisorenliste / zusammen mit Jahresabschlüsse
6	Einhaltung von Sanktionen, Anti- Geldwäscherei und Anti-Terrorismusfinanzierung	ist als Firma oder mit seinen Mitglieder des Geschäftsleitung / Besitzer nicht auf Sanktionslisten und Warnlisten der Aufsichtsbehörden aufgeführt	- Erstellung von Profilen von der Geschäftsleitung des Antragstellers z.B. Geschäftsführer, Finanzleiter, für den Antrag verantwortlichen Mitarbeiter. - Identifikation von negativen Vorfällen zu dem Thema Finanzstraftaten, in denen Geschäftsleitungsmitglieder involviert waren / sind - Identifikation, ob die Fima und deren Geschäftsleitung politisch exponiert sind	Bestechung, Korruption, Betrug Beziehungen zu offiziellen Amtsträgern (PEP Status) Rechtswidrige und kriminelle Handlungen Finanzielle nicht-Konformität Regulatorische nicht-Konformität Rechtsstreitigkeiten Schädliche Berichterstattung Eintrag auf Sanktionsliste	n/a

7	Einhaltung von Gesetzen	- hat keine Mitglieder des Managements / Besitzer, die Einträge in Straf-, Konkurs-, und Betreibungsregistern haben, die einer **einwandfreien Geschäftsführung** entgegenstehen '- listet anhängige Zulassungs- und Strafverfahren	- Identifikation von negativen Vorfällen z.B. Strafverfahren oder Insolvenzverfahren in denen Geschäftsleitungsmitglieder involviert sind	Straf-/ Konkurs-/ Betreibungsregister Abgedeckt mit Kriterium 6	- Strafregisterauszüge von der Geschäftsleitung - Bestätigung dass Provider nicht in Rechtsverfahren involviert ist
8	Abgelehnte Zulassungen bei anderen Banken, Regulatoren	Angaben, ob eine relevante Beurteilung der Zulassung durch eine andere Behörde bereits abgelehnt wurde mit Angabe des Grundes.	- Bestätigung, ob das Unternehmen von relevanten Behörden zugelassen / lizenziert ist	Aktive und gültige Lizenzen und Genehmigungen vorhanden Keine Lizenzen oder Genehmigung wird dies unter Kriterium 6, regulatorische Nicht-Konformität abgedeckt	- Lizenzen / Bestätigungen von den relevanten Behörden
9	Zuverlässigkeit, Redlichkeit, Integrität von Geschäftsleitung	Nachweise über Kenntnisse / Fähigkeiten / Erfahrung gem. Lebenslauf	- Erstellung von Profilen z.B. Lebenslauf von der Geschäftsleitung des Antragstellers z.B. Geschäftsführer, Finanzleiter, für den Antrag verantwortlichen Mitarbeiter - Identifikation von negativen Vorfällen bzgl. Arbeitsplatz wie z.B. Verlust des Arbeitsplatzes oder Kündigung des Arbeitgebers	Hintergrund Information (z.B.. Nationalität, Wohnort, Studiengang) Vergangene Tätigkeiten Einhaltung von Gesetzen und Integrität der Person (unter Kriterium 6 und 7 abgedeckt)	- Lebenslauf von wichtigsten Geschäftsleitungsmitglieder

Tabelle 1: Generelle Zulassungskriterien

5. Sicherheitskriterien in der beantragten Rolle

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels Basic und der Rolle Service User (SU)** auf:

SZ-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse
C01	**Vertraulichkeit** Der Nutzer und seine Berechtigung müssen für den Zugriff auf die Applikation, die den Service nutzt, eindeutig identifiziert werden und die Vertraulichkeit muss gewährt sein.	F03b	Session-Timeout der SU Administratoren.	M03b	Die Sessions der Administratoren sind bei Inaktivität zeitlich (auf wenige Minuten) zu begrenzen, um das Risiko eines Session-Hijackings und somit u.a. böswillige Konfigurationsänderungen zu minimieren.	TE
		F04	Die Authentifizierungsinformation muss sicher gespeichert werden und darf nicht im Klartext ersichtlich sein.	M04	Die Speicherung der Authentifizierungsinformationen (Token) muss verschlüsselt sein (mit SIX bewilligten Verschlüsselungsverfahren erfolgen). Verwendete kryptographische Schlüssel haben einen definierten Owner, der für dessen Schutz verantwortlich ist. Wenn der Schlüsselnutzer keine Person ist, dann muss ihm eine Person zugewiesen werden.	TE
C03	Der Zugriff auf die vom SP transferierten Daten muss adäquat geschützt werden (at rest, in transit, at processing).	F09	Die Erteilung der Zugriffsrechte muss geregelt sein.	M10	Es muss ein Access Management Prozess definiert und implementiert sein, der Rechtevergabe, -unterhalt und -entzug regelt (inkl. Administratorenrechte). Ausserdem müssen die bestehenden Benutzerrechte periodisch (mindestens jährlich) einer Rezertifizierung unterzogen werden.	Prozess
C05	Bei Datenhaltung oder Zugriff ausserhalb der Schweiz muss der Nutzer klar und verständlich informiert werden und die entsprechende Zustimmung vorhanden sein.	F12	Datenhaltung und Zugriffe (nicht Nutzerzugriff)) müssen auf Schweiz einschränkbar sein.	M11	Wenn keine explizite Zustimmung des Nutzer vorhanden ist, darf die Datenhaltung nicht im Ausland sein oder der Zugriff nicht aus dem Ausland erfolgen (z.B. Systemadministratoren, Supportpersonal usw.). Dies wird mit technischen/organisatorischen Massnahmen sichergestellt. Der Nutzer selber darf von überall her auf seine Daten zugreifen.	TE
I01	**Integrität** Zugriff auf den Service des SP muss nachvollziehbar sein.	F13	Alle Ereignisse, welche für die Nachvollziehbarkeit (Audit-Trail) benötigt werden, müssen protokolliert werden.	M12	Ein Audit-Trail betreffs Service-Authentifizierung (Nutzung des Nutzer-Tokens) muss geführt werden.	TE
T01	**Technologie** Identifikation der involvierten IT-Systeme.	F18	Der SU kann nachweisen, auf welchen Systemen die bezogenen Daten verarbeitet und gespeichert werden.	M15	Der SU führt eine Inventar der Systeme, die die Zugriffsdaten und übertragenen Daten beinhaltet.	Prozess

P02	Es besteht ein Incident Management Prozess, um Störungen und Sicherheitsvorfälle zu bearbeiten.	F20	Der SU kann Störfälle verwalten und kommuniziert Sicherheitsvorfälle.	M17	- Der SU verfügt über einen Incident Management Prozess, damit Incidents und Sicherheitsvorfälle über den gesamten Lifecycle verwaltet werden können - Der SU besitzt einen dokumentierten und implementierten SIEM Prozess, der auch ein entsprechendes Meldeverfahren an die SIX zulässt. Es gibt generell ein Verfahren, um die beteiligten Parteien (d.h. SIX, Kunden, relevante Behörden) unverzüglich über den Verlust der Vertraulichkeit von Kontoinformationen in ihrem Zuständigkeitsbereich zu informieren (gem. Artikel 92 der PSD2) - Kontaktstelle (inkl. Name und E-Mail) für Kunden in Fällen von Betrug, techn. Problemen und Forderungsmanagement vorhanden und kommuniziert sein	Prozess
P03	Der SU besitzt einen Change Management Prozess.	F21	Change Management Prozess ist vorhanden und umgesetzt.	M18	Der SU verfügt über einen aktuellen und angemessenen Change Management Prozess, der unter Berücksichtigung von Funktionentrennung, Genehmigung und Testprozess im Rahmen des Change Managements eine zeitnahe, qualitativ angemessene Einführung oder Aktualisierung der APIs garantiert.	Prozess
P04	Der SU besitzt einen Managementprozess für eigene Subunternehmer, die relevante Daten verarbeiten.	F22	Subunternehmen, die Daten verarbeiten muss dieselben Datenhaltungsbedingungen erfüllen, wie der SU.	M19	Es besteht ein Vertrag und Managementprozess für Subunternehmen mit äquivalenten Sicherheitsauflagen.	Prozess

Tabelle 2: Sicherheitskriterien für den Service User im Sicherheitslevel Basic

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels High und der Rolle Service User (SU)** auf. Die gelisteten Sicherheitskriterien gelten **zusätzlich** zu denen des Security Levels Basic:

SZ-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse
C01	**Vertraulichkeit** Der Nutzer und seine Berechtigung müssen für den Zugriff auf die Applikation, die den Service nutzt, eindeutig identifiziert werden und die Vertraulichkeit muss gewährt sein.	F01	Der Nutzer muss vor dem ersten Servicezugriff eineindeutig identifiziert werden.	M01	Session-Authentifizierung seitens SU wird mit dem stark authentifizierten Login im Online Banking (Freigabe durch den Nutzer in der Online Banking Applikation) und dem Servicezugriff **eindeutig verlinkt** - Token-UserId-Verlinkung in der Applikation des SU.	TE
		F02	Starke Zugriffsmechanismen auf die SU Applikation durch den Nutzer.	M02	Entweder wird eine Zwei-Faktor-Authentifizierung eingesetzt oder es muss zumindest eine starke technische Passwort Policy in der SU Applikation mit folgenden Merkmalen implementiert sein: - Mindestlänge: 8 Zeichen - Komplexität: Kombination aus Gross-/Kleinschreibung, Zahlen, Sonderzeichen erforderlich - Wechselintervall: mindestens halbjährlich	TE
		F03a	Session-Timeout in der SU Applikation.	M03a	Der Nutzer muss nach längerer Inaktivität der Sitzung (max. 1h) von der SU-Applikation abgemeldet werden.	TE
		F05	Identifikation und Authentifizierung müssen über einen gesicherten Pfad abgewickelt werden.	M05	Der Zugriff vom Nutzer auf die Applikation oder den Webservice des SU muss verschlüsselt über https (TLS Verschlüsselung) erfolgen. Dabei werden keine veralteten Protokolle (z.B. TLS 1.0) respektive Algorithmen eingesetzt.	TE
C02	Die Berechtigung für den Datenzugriff darf nur an Nutzer vergeben werden, die dem Datenzugriff des Service Users auf den Service Provider zugestimmt haben und vom Service Provider ermächtigt sind.	F06	Der Consent des Nutzers zur Nutzung des Services muss unterhalten werden.	M01	Session-Authentifizierung seitens SU wird mit dem stark authentifizierten Login im Online Banking (Freigabe durch den Nutzer in der Online Banking Applikation) und dem Servicezugriff **eindeutig verlinkt** - Token-UserId-Verlinkung in der Applikation des SU.	TE
				M06	Wenn ein Nutzer den SU-Dienst kündigt, muss der zugehörige Token durch den SU in seiner Applikation innerhalb von 24 Stunden gelöscht werden. Ausserdem muss der SU den Nutzer informieren, dass dieser bei der Bank den Consent in der Online Banking Applikation entzieht.	Prozess + Vertrag zwischen SU und Nutzer
C03	Der Zugriff auf die vom SP transferierten Daten muss adäquat geschützt werden (at rest, in transit, at processing).	F07	Daten at rest (inklusive Datensicherungen) müssen sicher abgelegt werden und vor fremdem Zugriff geschützt werden.	M07	Es besteht eine Ablageverschlüsselung für die vom SP transferierten Daten des Nutzers, falls diese ausserhalb der Applikation abgespeichert werden. Nur berechtigte Personen (Need-to-know) haben Zugriff auf diese Daten (innerhalb und ausserhalb der Applikation) resp. den Schlüssel, der zur Verschlüsselung verwendet wurde.	TE
				M08	Weitere Sicherheitsmassnahmen bestehen (e.g. Firewalls, Antivirus, IDS, usw.), um die Token und Nutzerdaten zu schützen.	TE
		F08	Zugriff auf Daten muss eingeschränkt und protokolliert sein.	M09	Es müssen Rollen definiert sein, die den technischen Zugriff, Applikationszugriff und Nutzerzugriff (Daten) trennen. Logs müssen auf verdächtige Aktivitäten der Administratoren beim SU überwacht werden.	Prozess & TE

C04	Die Berechtigung für den Datenzugriff darf nur an SU-Administratoren vergeben werden, wenn diese für die Erbringung der Dienstleistung notwendig ist.	F08	Zugriff auf Daten muss eingeschränkt und protokolliert sein.	M09	Es müssen Rollen definiert sein, die den technischen Zugriff, Applikationszugriff und Nutzerzugriff (Daten) trennen. Logs müssen auf verdächtige Aktivitäten der Administratoren beim SU überwacht werden.	Prozess & TE
		F11	Falls ein Administrator seine Stelle oder Rolle wechselt, müssen die Zugriffsrechte innerhalb angemessener Zeit entzogen oder geändert werden.	M10	Es muss ein Access Management Prozess definiert und implementiert sein, der Rechtevergabe, -unterhalt und -entzug regelt (inkl. Administratorenrechte). Ausserdem müssen die bestehenden Benutzerrechte periodisch (mindestens jährlich) einer Rezertifizierung unterzogen werden.	Prozess
I02	Anomale Nutzung des Service muss detektiert werden.	F14	Es müssen Mechanismen definiert werden, die Abweichungen von vorgesehenem Verhalten detektieren.	M13	Die Zugriffe der Nutzer müssen auf sicherheitsrelevante Vorkommnisse (bspw. Verwendung von falschen Passwörtern) überwacht werden.	TE
A01	**Verfügbarkeit, BCP, DR** Es dürfen keine Zugriffsdaten verloren gehen.	F16	Der SU muss die Tokens und Verlinkung wiederherstellen können.	M14a	Backup oder Datenspiegelung muss für die Tokens und Verlinkung vorhanden sein oder es besteht ein Data Recovery Konzept. Allfällige Backups sollten die gleichen Schutzmassnahmen wie der Primary Server aufweisen.	TE
P01	**Prozesse** Sicherheits-Policy	F19	Sicherheits-Policy ist vorhanden.	M16	Existenz einer dokumentierten und aktuellen Sicherheits-Policy, welche die grundsätzlichen Sicherheitsziele und Sicherheitsvorgaben des Unternehmens und die Sicherheitsorganisation im Unternehmen festhält.	Prozess
P05	Sicherheitsüberprüfung des Administrators	F23	Strafregisterauszug	M20	Für alle Administratoren des SU müssen die folgenden Dokumente vorhanden sein: Strafregister- und Betreibungsregisterauszug.	Prozess
P06	Physischer Zutritt	F24	Server für Tokenspeicherung müssen physisch angemessen geschützt sein.	M21	Server für Tokenspeicherung sind angemessen physisch geschützt (z.B. Rechenzentrum mit geregeltem und kontrolliertem Zutritt).	TE

Tabelle 3: Sicherheitskriterien für den Service User im Sicherheitslevel High

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels Very High und der Rolle Service User (SU)** auf. Die gelisteten Sicherheitskriterien gelten **zusätzlich** zu denen des Security Levels High:

SZ-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse
I03	**Integrität** Die Nichtabstreitbarkeit einer Transaktion muss gewährleistet sein. Als Transaktionen gelten alle API-Request-/Response-Calls, die eine logische Einheit bilden.	F25	Die Transaktion muss vollständig sein.	M22	Service User muss dem Service Provider dieselben Informationen übermitteln als wenn der Nutzer die Transaktion selber ausführen würde.	TE
		F26	Die Transaktion muss eindeutig referenzierbar sein.	M23	Die Transaktion muss eine eineindeutige Transaktions-ID besitzen.	TE
		F27	Überprüfung der Transaktions-Antwort.	M24a	Der SU ist in der Pflicht, zu prüfen, dass gesendeter Auftrag und erhaltene Bestätigung des Service Providers übereinstimmen, respektive Nichtübereinstimmungen dem Nutzer unmittelbar mitgeteilt und allfällige Korrekturmassnahmen ermöglicht werden.	Prozess
		F28	Kennzeichnung von automatisierten Aufträgen.	M25	Regelbasierte oder automatisierte Transaktionen müssen für den Service Provider erkennbar sein.	TE
		F29	Nichtabstreitbarkeit von Nutzeraufträgen.	M26	Wenn ein Nutzer automatisierte (regelbasierte) Aufträge erteilt, muss der Service User die Nachvollziehbarkeit und Nichtabstreitbarkeit dieser Aufträge sicherstellen.	TE
		F30	Aufbewahrung der Transaktions-Antwort (Empfehlung).	M27	Die Transaktions-Antwort des Service Providers soll so aufbewahrt werden, dass sie zu einem späteren Zeitpunkt für allfällige Schadensfälle verwendet werden können.	n/a

Tabelle 4: Sicherheitskriterien für den Service User im Sicherheitslevel Very High

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels Basic und der Rolle Service Provider (SP)** auf[1]:

SR-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse
C01	**Vertraulichkeit** Der Nutzer und seine Berechtigung müssen für den Zugriff auf die Applikation, die den Service nutzt, eindeutig identifiziert werden und die Vertraulichkeit muss gewährt sein.	F02	Die Authentifizierungsinformation muss sicher gespeichert werden und darf nicht im Klartext ersichtlich sein.	M52	Der vom SP ausgestellte Token darf keine sensitive Information (CID) enthalten. Zudem darf der Token nicht unverschlüsselt gespeichert werden.	TE
C03	Der Zugriff auf Schlüssel für den Service (Token) und die zum SU transferierten Daten muss adäquat geschützt werden (at rest, in transit, at processing).	F26	Der Zugriff auf den Authentifizierungsservice muss geschützt sein.	M56	Der Zugriff aus dem Internet auf den Service (z.B. Online Banking) muss mittels Perimeterschutz (Proxy, WAF) gesichert werden.	TE
		F28	Die Erteilung der Zugriffsrechte muss geregelt sein.	M10	Es muss ein Access Management Prozess definiert und implementiert sein, der Rechtevergabe, -unterhalt und -entzug regelt (inkl. Administratorenrechte). Ausserdem müssen die bestehenden Benutzerrechte periodisch (mindestens jährlich) einer Rezertifizierung unterzogen werden.	Prozess
C05	Bei Datenhaltung oder Zugriff ausserhalb der Schweiz muss der Nutzer klar und verständlich informiert werden und die entsprechende Zustimmung vorhanden sein.	F11	Datenhaltung und Zugriffe (nicht Nutzer-Zugriffe) müssen auf Schweiz einschränkbar sein.	M11	Wenn keine explizite Zustimmung des Nutzer vorhanden ist, darf die Datenhaltung nicht im Ausland sein oder der Zugriff nicht aus dem Ausland erfolgen (z.B. Systemadministratoren, Supportpersonal usw.). Dies wird mit technischen / organisatorischen Massnahmen sichergestellt. Der Nutzer selber darf von überall her auf seine Daten zugreifen.	TE
I01	**Integrität** Zugriff auf den Service des SP muss nachvollziehbar sein.	F13	Alle Ereignisse welche für die Nachvollziehbarkeit (Audit-Trail) benötigt werden müssen protokolliert werden.	M12	Ein Audit-Trail betreffs Service- Authentifizierung (Nutzung des Nutzer-Tokens) muss geführt werden.	TE

[1] Der Sicherheitslevel Basic deckt die Anforderungen für den Austausch von «Client Identifying Data» (CID) auf der bLink Plattform nicht ab.
CID umfassen Informationen über Kunden, die es ermöglichen, direkt oder indirekt Rückschlüsse auf das Bestehen einer Kundenbeziehung mit der Bank zu nehmen.
Ebenso durch den Sicherheitslevel Basic nicht abgedeckt sind wertverändernde d.h. vermögensändernde Transaktionen.

T01	**Technologie** Identifikation der involvierten IT-Systeme.	F21	Der SP kann nachweisen, auf welchen Systemen die bezogenen Daten verarbeitet und gespeichert werden.	M15	Der SP führt eine Inventar der Systeme, die die Zugriffsdaten und übertragenen Daten beinhaltet.	Prozess
P02	Es besteht ein Incident Management Prozess, um Störungen und Sicherheitsvorfälle zu bearbeiten.	F22	Der SP kann Störfälle verwalten und kommuniziert Sicherheitsvorfälle.	M17	- Der SP verfügt über einen Incident Management Prozess, damit Incidents und Sicherheitsvorfälle über den gesamten Lifecycle verwaltet werden können - Der SP besitzt einen dokumentierten und implementierten SIEM Prozess, der auch ein entsprechendes Meldeverfahren an die SIX zulässt. Es gibt generell ein Verfahren, um die beteiligten Parteien (d.h. SIX, Kunden, relevante Behörden) unverzüglich über den Verlust der Vertraulichkeit von Kontoinformationen in ihrem Zuständigkeitsbereich zu informieren (gem. Artikel 92 der PSD2). - Kontaktstelle (inkl. Name und E-Mail) für Kunden in Fällen von Betrug, techn. Problemen und Forderungsmanagement vorhanden und kommuniziert sein.	Prozess
P03	Der SP besitzt einen Change Management Prozess.	F21	Change Management Prozess ist vorhanden und umgesetzt.	M18	Der SP verfügt über einen aktuellen und angemessenen Change Management Prozess, der unter Berücksichtigung von Funktionentrennung, Genehmigung und Testprozess im Rahmen des Change Managements eine zeitnahe, qualitativ angemessene Einführung oder Aktualisierung der APIs garantiert.	Prozess
P04	Der SP besitzt einen Management Prozess für eigene Subunternehmer, die relevante Daten bearbeiten.	F23	Subunternehmen, die Daten verarbeiten muss dieselben Datenhaltungsbedingungen erfüllen, wie der SP.	M19	Es besteht ein Vertrag und Managementprozess für Subunternehmen mit äquivalenten Sicherheitsauflagen.	Prozess
P06	Physischer Zutritt.	F24	Server für Tokenspeicherung müssen physisch angemessen geschützt sein.	M21	Server für Tokenspeicherung sind angemessen physisch geschützt (z.B. Rechenzentrum mit geregeltem und kontrolliertem Zutritt).	TE

Tabelle 5: Sicherheitskriterien für den Service Provider im Sicherheitslevel Basic

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels High und der Rolle Service Provider (SP)** auf. Die gelisteten Sicherheitskriterien gelten **zusätzlich** zu denen des Security Levels Basic:

SR-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse
C01	**Vertraulichkeit** Der Nutzer und seine Berechtigung müssen für den Zugriff auf die Applikation, die den Service nutzt, eindeutig identifiziert werden und die Vertraulichkeit muss gewährt sein.	F01	Der Nutzer muss vor dem ersten Servicezugriff eineindeutig identifiziert werden.	M51	Der SP prüft den Nutzer mittels starker Authentifizierung.	TE
		F03a	Session-Timeout in der SP Applikation.	M03a	Der Nutzer muss nach längerer Inaktivität der Sitzung (max. 1h) von der SP-Applikation abgemeldet werden.	TE
		F03b	Session-Timeout der SP Administratoren.	M03b	Die Sessions der Administratoren sind bei Inaktivität zeitlich (auf wenige Minuten) zu begrenzen, um das Risiko eines Session-Hijackings und somit u.a. böswillige Konfigurationsänderungen zu minimieren.	TE
		F25	Der Nutzer muss periodisch stark identifiziert werden.	M53	Der Token für den Nutzerzugriff (Refresh-Token) muss nach einem definierten Ablaufdatum revoziert werden, respektive ablaufen, und es muss erneut eine starke Authentifizierung zur Erstellung des Tokens stattfinden.	TE
		F05	Identifikation und Authentifizierung müssen über einen gesicherten Pfad abgewickelt werden.	M05	Der Zugriff vom Nutzer auf die Applikation oder den Webservice des SP muss verschlüsselt über https (TLS Verschlüsselung) erfolgen. Dabei werden keine veralteten Protokolle (z.B. TLS 1.0) respektive Algorithmen eingesetzt.	TE
C02	Die Berechtigung für den Datenzugriff darf nur an Nutzer vergeben werden, die dem Datenzugriff zugestimmt haben und vom Service Provider ermächtigt sind.	F04	Der Consent des Nutzers muss geprüft werden.	M54	Consent für die Datenfreigabe an den SU wird nachweislich und unanfechtbar eingeholt.	TE
				M55	Der Zugriff auf den vom SU bezogenen Service muss auf den Scope (e.g. Account Information und Payment Submission) des gegebenen Nutzer-Consents eingeschränkt werden.	TE
C03	Der Zugriff auf Schlüssel für den Service (Token) und die zum SU transferierten Daten muss adäquat geschützt werden (at rest, in transit, at processing).	F27	Zugriff auf den Service und die Daten muss eingeschränkt und protokolliert sein.	M57	Es müssen Rollen definiert sein, die eine Trennung von technischem Zugriff und Applikationszugriff ermöglichen. Logs müssen auf anomale Service Nutzung überwacht werden.	TE

C04	Die Berechtigung für den Datenzugriff darf nur an SP-Administratoren vergeben werden, wenn diese für die Erbringung der Dienstleistung notwendig ist.	F31	Falls ein Administrator seine Stelle oder Rolle wechselt, müssen die Zugriffsrechte innerhalb angemessener Zeit entzogen oder geändert werden.	M10	Es muss ein Access Management Prozess definiert und implementiert sein, der Rechtevergabe, -unterhalt und -entzug regelt (inkl. Administratorenrechte). Ausserdem müssen die bestehenden Benutzerrechte periodisch (mindestens jährlich) einer Rezertifizierung unterzogen werden.	Prozess
I02	**Integrität** Anomale Nutzung des Service muss detektiert werden.	F14	Es müssen Mechanismen definiert werden, die Abweichungen von vorgesehenem Verhalten detektieren	M13	Die Zugriffe der Nutzer müssen auf sicherheitsrelevante Vorkommnisse (bspw. Verwendung von falschen Passwörtern) überwacht werden.	TE
A01	**Verfügbarkeit, BCP, DR** Es dürfen keine Zugriffsdaten verloren gehen.	F19	Der SP muss den Servicezugriff und den Consent wiederherstellen können.	M14b	Backup oder Datenspiegelung muss für den Servicezugriff und den Consent vorhanden sein oder es besteht ein Data Recovery Konzept. Allfällige Backups sollten die gleichen Schutzmassnahmen wie der Primary Server aufweisen.	TE
P01	**Prozesse** Sicherheits-Policy	F19	Sicherheits-Policy ist vorhanden.	M16	Existenz einer dokumentierten und aktuellen Sicherheits-Policy, welche die grundsätzlichen Sicherheitsziele und Sicherheitsvorgaben des Unternehmens und die Sicherheitsorganisation im Unternehmen festhält.	Prozess
P05	Sicherheitsüberprüfung des Administrators	F23	Strafregisterauszug	M20	Für alle Administratoren des SP müssen die folgenden Dokumente vorhanden sein: Strafregister- und Betreibungsregisterauszug.	Prozess

Tabelle 6: Sicherheitskriterien für den Service Provider im Sicherheitslevel High

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels Very High und der Rolle Service Provider (SP)** auf. Die gelisteten Sicherheitskriterien gelten **zusätzlich** zu denen des Security Levels High.:

SZ-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse
I03	**Integrität** Die Nichtabstreitbarkeit einer Transaktion muss gewährleistet sein. Als Transaktionen gelten alle API-Request-/Response-Calls, die eine logische Einheit bilden.	F31	Der Empfang der Transaktion muss vollständig bestätigt werden.	M58	Der Service Provider muss direkt nach Empfang der Transaktion dem Service User mindestens mit der erhaltenen Transaktions-Information und dem Status der Transaktion den Empfang bestätigen.	TE
		F26	Die Transaktion muss eindeutig referenzierbar sein.	M23	Die Transaktion muss eine eineindeutige Transaktions-ID besitzen.	TE
TM01	**Transaktionsüberwachung**	F32	Es müssen Parameter der Transaktionen zur Bewertung von Risiken, Fraud oder Sicherheitsvorfällen überwacht und geloggt werden.	M59	"Service Provider besitzen ein Transaktionsmonitoring, dass ihnen ermöglicht fraudulente Transaktionen möglichst gut festzustellen.	Prozess
D01	**Eineindeutige Verlinkung der Transaktionsautorisierung mit der Transaktion**	F33	Dynamic Linking von Transaktionen	M59	Der Service Provider muss die Transaktion (sofern keine Exemption vorliegt) mittels MFA durch den Nutzer autorisieren. Der MFA hat folgende Eigenschaften: - der Nutzer (e.g. Initiator) erhält Information über die getätigte Transaktion (e.g. Betrag) und den Transaktionsempfänger - der generierte Authentifizierungscode ist spezifisch für die Transaktion, dem der Transaktions-Initiator bei der Einleitung der Transaktion zugestimmt hat und dies ist für den Initiator transparent verifizierbar; - der Authentifizierungscode ist eineindeutig mit der Transaktion verlinkt, d.h. die Transaktion darf nur bei Übereinstimmung von einem Kennzeichen und bestätigter Transaktionsinformation akzeptiert werden.	TE
		F34	Dynamic Linking von Batch-Transaktionen	M60	Im Falle der Autorisierung von mehreren Transaktionen als Batch muss (sofern keine Exemption vorliegt) der Authentifizierungscode des MFA spezifisch für den Batch sein und dem Nutzer eine verifizierbare Information über den Batchauftrag anzeigen.	TE
		F35	Kennzeichnung von fehlgeschlagener Transaktionsautorisierung.	M61	Im Falle einer fehlgeschlagenen Autorisierung der Transaktion muss der Service User informiert werden.	TE

P07	**Prozesse** **Umgang mit Ausnahmen**	F35	Die Sicherheitsmassnahmen der Transaktionen müssen regelmässig überprüft werden.	M62	Die Sicherheitsmassnahmen müssen dokumentiert und von einem unabhängigen Experten, periodisch getestet, evaluiert und auditiert werden: Transaktionen werden mittels Multifactor Authentication (MFA) des Nutzers, die eineindeutig mit der Transaktion verlinkt ist, autorisiert, es sei denn, es liegt eine dokumentierte Exemption basierend auf einem dokumentierten Fraud-Management Prozess vor.	Prozess
		F36	Exemptions sind in den Anwendungsspezifikationen geregelt und sind nur für solche Fälle möglich, welche einer Risikoüberwachung unterliegen.	M63	Auf den MFA zur Transaktionsautorisierung darf nur in spezifischen Fällen verzichtet werden, wenn z.B.: - spezifische und limitierende Bedingungen betreffs der Risiken definiert sind - Betrag, wiederkehrende Transaktionen oder Transaktionskanäle definiert sind. Bei Anomalien oder Fraud muss der MFA sofort aktiviert werden oder die Transaktion blockiert, respektive suspendiert und gesondert geprüft werden.	Prozess

Tabelle 7: Sicherheitskriterien für den Service Provider im Sicherheitslevel Very High