Anhang 1
Zulassungskriterien

für Consent-as-a-Service für die bLink Plattform

Die folgende Tabelle listet die Sicherheitskriterien für Anwendungsspezifikationen des **Sicherheitslevels High** und der **Rolle Service User (SU)** aus den **Teilnahmebedingungen bLink Plattform, Anhang 1** auf, und zeigt, welche Kriterien durch CaaS abgedeckt werden und welche weiterhin durch den Service User zu erbringen sind.

SZ-ID	Sicherheitsziel/-anforderung	SF-ID	Sicherheitsfunktion/-prozess	PZ-ID	Assessment-Ziel / Sicherheitsmechanismus	Scope technische Einhalteprüfung (TE) oder Prozesse	Abgedeckt durch	Anmerkungen
C01	**Vertraulichkeit** Der Nutzer und seine Berechtigung müssen für den Zugriff auf die Applikation, die den Service nutzt, eindeutig identifziert werden und die Vertraulichkeit muss gewährt sein.	F01	Der Nutzer muss vor dem ersten Servicezugriff eineindeutig identifiziert werden.	M01	Session-Authentisierung seitens SU wird mit dem stark authentisierten 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	CaaS	Nutzerdaten im Sinne von Kundendaten
		F02	Starke Zugriffsmechanismen auf die SU Applikation durch den Nutzer	M02	Entweder wird eine Zwei-Faktor-Authentisierung 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	SU	

		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	SU	
		F03b	Sessiontimeout 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	CaaS SU	CaaS-Administratoren seitens SIX sind auf eine Session-Timeout von 15 Minuten eingeschränkt. Für SU Administratoren, welche die Kriterien M02, M03a, M05, M13 verwalten sowie M07 & M10 in den beschriebenen Sonderfällen. Gilt auch für SU Administratoren die im Kontext von M08 Zugriff auf unverschlüsselte Daten erhalten.
		F04	Die Authentisierungsinformation muss sicher gespeichert werden und darf nicht im Klartext ersichtlich sein	M04	Die Speicherung der Authentisierungsinformationen (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	CaaS	

		F05	Identifikation und Authentisierung 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	SU	
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-Authentisierung seitens SU wird mit dem stark authentisierten 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	CaaS	
				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	SU	Der SU muss den Nutzer informieren seinen Consent zu revozieren. Zusätzlich muss der SU SIX informieren, den zugehörigen Provider Token zu löschen.
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.	TE	SU	Falls die SU Applikation keine Zwischenablage nutzt, erfüllt CaaS diese Kriterium vollumfänglich

					den Schlüssel, der zur Verschlüsselung verwendet wurde.			
				M08	Weitere Sicherheitsmassnahmen bestehen (e.g. Firewalls, Antivirus, IDS, usw.), um die Token und Nutzerdaten zu schützen.	TE	CaaS	Die Nutzerdaten inkl Consumer Token müssen mit geschäftsüblicher Sorgfalt geschützt werden. CaaS erfüllt dieses Kriterium für die Provider Token vollumfänglich.
		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 (durch Nutzer oder Administratoren beim SU) überwacht werden.	Prozess & TE	CaaS	CaaS erfüllt dieses Kriterium für die Provider Token vollumfänglich.
		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	CaaS SU*	Das Access Management für den Zugriff auf Providertoken liefert CaaS. *Falls der SU die Verwaltung von CaaS über ein API bei sich integriert, müssen die Sicherheitkriterien (M10) durch den SU sichergestellt werden.
C04	Die Berechtigung für den Datenzugriff darf nur an SU-Administratoren vergeben werden, wenn diese für die Erbringung	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	Prozess & TE	CaaS	CaaS erfüllt dieses Kriterium für die Provider Token vollumfänglich.

	der Dienstleistung notwendig ist				(durch Nutzer oder Administratoren beim SU) überwacht werden.			
		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	CaaS SU*	Das Access Management für den Zugriff auf Provider Token liefert CaaS. *Falls der SU die Verwaltung von CaaS über ein API bei sich integriert, müssen die Sicherheitkriterien (M10) durch den SU sichergestellt werden.
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 Nutzers 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	SU	Für die Provider Token erfolgt die Speicherung seitens SIX in der Schweiz.
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 Serviceauthentisierung (Nutzung des Nutzer-Tokens) muss geführt werden.	TE	CaaS	

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	SU	Falsche Logins müssen überwacht werden.
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	CaaS	
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	CaaS	SIX führt ein Inventar über die CaaS Umgebung
P01	**Prozesse** Sicherheits-Policy	F19	Sicherheits-Policy ist vorhanden	M16	Existenz einer dokumentierten und aktuellen Sicherheitspolicy, welche die grundsätzlichen Sicherheitsziele und Sicherheitsvorgaben des Unternehmens und die Sicherheitsorganisation im Unternehmen festhält.	Prozess	CaaS	
P02	Es besteht ein Incidentmanagement 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	Prozess	CaaS	Beim SU muss eine Kontaktstelle (inkl. Name und E-Mail) für Kunden in Fällen von Betrug, techn. Problemen und Forderungsmanagement

					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			vorhanden und kommuniziert sein.
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	SU	CaaS verfügt über einen Change Management 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 Subcontractors mit äquivalenten Sicherheitsauflagen	Prozess	SU	

P05	Sicherheitsüberprüfung des Administrators	F23	Strafregisterauszug	M20	Für alle Administratoren des SU müssen die folgenden Dokumente vorhanden sein: Strafregister- und Betreibungsregisterauszug	Prozess	CaaS SU	Für SU Administratoren, welche die Kriterien M02, M03a, M05, M13 verwalten sowie M07 & M10 in den beschriebenen Sonderfällen. Gilt auch für SU Administratoren die im Kontext von M08 Zugriff auf unverschlüsselte Daten erhalten.
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	CaaS	