Annexe 1
Critères d’admission

applicable au service Consent-as-a-Service pour la plate-forme bLink

Le tableau suivant énumère les critères de sécurité pour les spécifications d'application du **niveau de sécurité «Élevé»** et du **rôle «Utilisateur de services» (SU)** énoncés dans les **Conditions de participation pour la plate-forme bLink Annexe 1**, et indique quels critères sont couverts par CaaS et lesquels doivent continuer à être fournis par l'utilisateur de services.

SZ-ID	Objectif/exigence de sécurité	SF-ID	Fonction / processus d'intégration	PZ-ID	Objectif d'évaluation / mécanisme de sécurité	Champ d'application du contrôle de conformité technique (TE) ou des processus	Couvert par	Remarques
C01	**Confidentialité** L'utilisateur et son autorisation doivent être identifiés de manière unique pour l'accès à l'application utilisant le service et la confidentialité doit être garantie.	F01	L'utilisateur doit être clairement identifié avant le premier accès au service.	M01	L'authentification de la session par le SU est **clairement liée** à la connexion fortement authentifiée dans la banque en ligne (approbation par l'utilisateur dans l'application de banque en ligne) et à l'accès au service – liaison Token-ID utilisateur dans l'application du SU	TE	CaaS	Données de l'utilisateur au sens de données de client
		F02	Solides mécanismes d'accès à l'application du SU par l'utilisateur	M02	Soit une authentification à deux facteurs est utilisée, soit au moins une politique de mot de passe technique fort ayant les caractéristiques suivantes doit être mise en œuvre dans l'application du SU: - Longueur minimale: 8 caractères - Complexité: combinaison de majuscules et minuscules, chiffres, caractères spéciaux requis - Intervalle de changement: au moins tous les six mois	TE	SU	
		F03a	Délai d'expiration de session dans l'application du SU	M03a	L'utilisateur doit être déconnecté de l'application SU après une longue inactivité de la session (max. 1h)	TE	SU	

		F03b	Délai d'expiration de session des administrateurs du SU	M03b	Les sessions des administrateurs doivent être limitées dans le temps (à quelques minutes) en cas d'inactivité afin de minimiser le risque de détournement de session et donc, entre autres, de modification malveillante de la configuration.	TE	CaaS SU	Les administrateurs CaaS du côté de SIX sont limités à un délai d'expiration de session de 15 minutes. Pour les administrateurs du SU qui gèrent les critères M02, M03a, M05, M13 ainsi que les critères M07 & M10 dans les cas particuliers décrits. S'applique également aux administrateurs du SU qui reçoivent, dans le contexte d'un accès M08, des données non cryptées.
		F04	Les informations d'authentification doivent être stockées en toute sécurité et ne doivent pas être visibles en texte clair.	M04	Le stockage des informations d'authentification (token) doit être crypté (à l'aide de méthodes de cryptage approuvées par SIX). Les clés cryptographiques utilisées ont un propriétaire défini qui est responsable de leur protection. Si l'utilisateur clé n'est pas une personne, une personne doit lui être assignée.	TE	CaaS	
		F05	L'identification et l'authentification doivent être effectuées par un chemin sécurisé.	M05	L'accès de l'utilisateur à l'application ou au service web du SU doit être crypté via https (cryptage TLS). Aucun protocole (par exemple TLS 1.0) ou algorithme obsolète n'est utilisé.	TE	SU	

C02	L'autorisation d'accès aux données ne peut être accordée qu'aux utilisateurs qui ont accepté l'accès aux données de l'utilisateur au fournisseur de services et qui sont autorisés par le fournisseur de services	F06	Le consentement du client à l'utilisation du service doit être entretenu	M01	L'authentification de la session par le SU est **clairement liée** à la connexion fortement authentifiée dans la banque en ligne (approbation par l'utilisateur dans l'application de banque en ligne) et à l'accès au service – liaison Token-ID utilisateur dans l'application du SU	TE	CaaS	
				M06	Si un utilisateur annule le service du SU, le token correspondant doit être supprimé par le SU dans son application dans les 24 heures. Le SU doit également informer l'utilisateur qu'il retirera son consentement dans l'application de banque en ligne auprès de la banque.	Processus + contrat entre le SU et l'utilisateur	SU	Le SU doit informer l'utilisateur qu'il révoque son consentement. Par ailleurs, le SU doit informer SIX qu'il efface le token du fournisseur afférent.
C03	L'accès aux données transférées par le SP doit être protégé de manière adéquate (at rest, in transit, at processing).	F07	Les données «at rest» (y compris les sauvegardes de données) doivent être stockées en toute sécurité et protégées contre tout accès non autorisé.	M07	Il existe un cryptage de stockage pour les données de l'utilisateur transférées par le SP si elles sont stockées **en dehors** de l'application. Seules les personnes autorisées (besoin d'en connaître) ont accès à ces données (dans l'application et en dehors) ou à la clé utilisée pour le cryptage.	TE	SU	Si l'application SU n'utilise pas de presse-papiers, le CaaS remplit pleinement ce critère.
				M08	D'autres mesures de sécurité sont en place (par exemple: pare-feu, antivirus, IDS, etc.) pour protéger les tokens et les données de l'utilisateur.	TE	CaaS	Les données de l'utilisateur y compris le token de client doivent être protégés avec la diligence habituellement requise. Le CaaS remplit pleinement ce critère pour les tokens du fournisseur.

		F08	L'accès aux données doit être limité et consigné.	M09	Des rôles séparant l'accès technique, l'accès aux applications et l'accès des utilisateurs (données) doivent être définis. Les journaux doivent être surveillés pour détecter toute activité suspecte (par les utilisateurs ou les administrateurs du SU).	Processus et TE	CaaS	Le CaaS remplit pleinement ce critère pour les tokens du fournisseur.
		F09	L'octroi des droits d'accès doit être réglementé	M10	Un processus de gestion des accès qui réglemente l'attribution, le maintien et la révocation des droits (y compris les droits d'administrateur) doit être défini et mis en œuvre. En outre, les droits d'utilisation existants doivent être périodiquement (au moins une fois par an) soumis à une recertification.	Processus	CaaS SU*	La gestion des accès pour l'accès au token du fournisseur est assurée par le CaaS. Si le SU intègre la gestion du CaaS par le biais d'une API, les critères de sécurité (M10) doivent être assurés par le SU.
C04	L'autorisation d'accès aux données ne peut être donnée aux administrateurs des SU que si elle est nécessaire à la fourniture du service	F08	L'accès aux données doit être limité et consigné	M09	Des rôles séparant l'accès technique, l'accès aux applications et l'accès des utilisateurs (données) doivent être définis. Les journaux doivent être surveillés pour détecter toute activité suspecte (par les utilisateurs ou les administrateurs du SU).	Processus et TE	CaaS	Le CaaS remplit pleinement ce critère pour les tokens du fournisseur.
		F11	Si un administrateur change d'emploi ou de rôle, les droits d'accès doivent être révoqués ou modifiés dans un délai raisonnable	M10	Un processus de gestion des accès qui réglemente l'attribution, le maintien et la révocation des droits (y compris les droits d'administrateur) doit être défini et mis en œuvre. En outre, les droits d'utilisation existants doivent être périodiquement (au moins une fois par an) soumis à une recertification	Processus	CaaS SU*	La gestion des accès pour l'accès au token du fournisseur est assurée par le CaaS. Si le SU intègre la gestion du CaaS par le biais d'une API, les critères de sécurité (M10) doivent être assurés par le SU.

C05	En cas de stockage ou d'accès aux données en dehors de la Suisse, l'utilisateur doit être informé de manière claire et compréhensible et le consentement approprié doit être obtenu	F12	Le stockage des données et les accès (pas l'accès de l'utilisateur) doivent être limités à la Suisse.	M11	En l'absence de consentement explicite de l'utilisateur, le stockage des données à l'étranger ou l'accès depuis l'étranger (par exemple les administrateurs de système, le personnel d'assistance, etc.) n'est pas autorisé. Cela est assuré par des mesures techniques/organisationnelles. L'utilisateur lui-même peut accéder à ses données depuis n'importe où.	TE	SU	En ce qui concerne le token du fournisseur, l'enregistrement a lieu, du côté de SIX, en Suisse.
I01	**Intégrité** L'accès au service du SP doit être traçable	F13	Tous les événements nécessaires à la traçabilité (piste d'audit) doivent être consignés.	M12	Une piste d'audit concernant l'authentification du service (utilisation du token de l'utilisateur) doit être conservée.	TE	CaaS	
I02	L'utilisation anormale du service doit être détectée	F14	Des mécanismes doivent être définis pour détecter les écarts par rapport au comportement prévu.	M13	Les accès des utilisateurs doivent être surveillés pour détecter les incidents de sécurité (utilisation de mots de passe incorrects, par exemple)	TE	SU	Il convient de surveiller les mauvaises connexions.
A01	**Disponibilité, BCP, DR** Aucune donnée d'accès ne doit être perdue	F16	Le SU doit pouvoir restaurer les tokens et les liens.	M14a	Une sauvegarde ou une mise en miroir des données doit être disponible pour les tokens et les liens ou il doit exister un concept de récupération des données. Toute sauvegarde doit être assortie des mêmes mesures de protection que le serveur principal.	TE	CaaS	

T01	**Technologie** Identification des systèmes informatiques concernés	F18	Le SU peut prouver sur quels systèmes les données correspondantes sont traitées et stockées.	M15	Le SU tient un inventaire des systèmes, qui contient les données d'accès et les données transférées.	Processus	CaaS	SIX tient un inventaire de l'environnement CaaS
P01	**Processus** Politique de sécurité	F19	Politique de sécurité en place	M16	Existence d'une politique de sécurité documentée et actualisée, qui définit les objectifs et les spécifications de sécurité de base de l'entreprise et de l'organisation de la sécurité au sein de l'entreprise.	Processus	CaaS	
P02	Un processus de gestion des incidents est en place pour traiter les dysfonctionnements et les incidents de sécurité.	F20	Le SU peut gérer les cas de dysfonctionnement et communique les incidents de sécurité	M17	- Le SU dispose d'un processus de gestion des incidents pour gérer les incidents et les incidents de sécurité tout au long du cycle de vie - Le SU dispose d'un processus SIEM documenté et mis en œuvre, qui permet également une procédure de déclaration correspondante à SIX. En général, il existe une procédure pour informer immédiatement les parties concernées (c'est-à-dire SIX, les clients, les autorités compétentes) de la perte de confidentialité d'informations sur les comptes dans leur domaine de responsabilité (conformément à l'article 92 de la DSP2) - Point de contact (y compris nom et e-mail) pour les clients en cas de fraude, de problèmes techniques et de gestion des réclamations disponible et communiqué	Processus	CaaS	Au niveau du SU, un point de contact (y compris nom et e-mail) doit être disponible pour les clients en cas de fraude, de problèmes techniques et de gestion des réclamations et leur être communiqué.

P03	Le SU dispose d'un processus de gestion du changement	F21	Le processus de gestion du changement est en place et mis en œuvre	M18	Le SU dispose d'un processus de gestion du changement actualisé et approprié, qui garantit une introduction ou une mise à jour des API en temps voulu et de manière appropriée sur le plan qualitatif, en tenant compte de la séparation des fonctions, du processus d'approbation et de test dans le cadre de la gestion des changements	Processus	SU	Le CaaS dispose d'un processus de gestion du changement
P04	Le SU dispose d'un processus de gestion pour ses propres sous-traitants qui traitent les données pertinentes	F22	Les sous-traitants qui traitent les données doivent satisfaire aux mêmes exigences de stockage des données que le SU.	M19	Il existe un contrat et un processus de gestion pour les sous-traitants ayant des exigences de sécurité équivalentes	Processus	SU	
P05	Vérification de sécurité de l'administrateur	F23	Extrait du casier judiciaire	M20	Les documents suivants doivent être mis à la disposition de tous les administrateurs du SU: extrait du casier judiciaire et du registre des poursuites	Processus	CaaS SU	Pour les administrateurs du SU qui gèrent les critères M02, M03a, M05, M13 ainsi que les critères M07 & M10 dans les cas particuliers décrits. S'applique également aux administrateurs du SU qui reçoivent, dans le contexte d'un accès M08, des données non cryptées.
P06	Accès physique	F24	Les serveurs de stockage de tokens doivent être protégés physiquement de manière adéquate	M21	Les serveurs de stockage de tokens sont suffisamment protégés physiquement (centre de données à accès réglementé et contrôlé, par exemple)	TE	CaaS	