Annexe 1
Critères d'admission

pour le contrat de participation à la plate-forme bLink

1. Définitions

Les définitions suivantes sont utilisées dans le présent document:

Application	Une application représente un cas d'utilisation, dans lequel le fournisseur de services met à disposition une ou plusieurs API à disposition de l'utilisateur de service via la plateforme bLink. Les conditions d'utilisation de l'applications sont définies dans une spécification propre à l'application, afin d'assurer un échange de données conforme au contrat d'application.
Contrat d'application	Accord entre le fournisseur de services et l'utilisateur de services, qui est conclu lorsque le fournisseur de services répond à l'appel de service sur la plate-forme conformément aux spécifications d'application (pour plus de détails, voir le contrat de participation, clause 6.2 N° 44 ss.).
Service API	Un service API représente la plus petite unité de l'application proposée via une API, pour laquelle un contrat d'application est établi.
Place de marché bLink	Un service géré par SIX, qui publie et met à disposition toutes les applications.
Client final	Client du fournisseur de services et titulaire de compte/dépôt.
Utilisateur	L'utilisateur utilise le service API mis à disposition par l'utilisateur de services.
API partenaire	API d'un fournisseur de services, lequel peut décider librement de son existence et de son utilisation dans le cadre de l'Annexe 2 - Spécifications d'application de l'API partenaire - et ce, notamment eu égard à l'organisation du service API et aux Spécifications techniques (Ownership).
Plate-forme	Plate-forme bLink exploitée par SIX.
Fournisseur de services	Fournit le service API.
Utilisateur de services	Utilise le service API.
Contrat de participation	En cas de décision d'admission positive à la plate-forme bLink et à au moins une des applications souhaitées, le contrat de participation est conclu par suite de la signature valable des conditions de participation.
Participant	Le participant est le partenaire contractuel de SIX dans le contrat de participation pour la plate-forme bLink. Dans le contrat d'application, le participant a le statut soit de fournisseur de services, soit d'utilisateur de services.

Le contrat de participation utilise la désignation «client». Pour certaines applications, il peut être judicieux d'opérer une différenciation et «client» y est utilisé en tant que terme générique pour «client final» ou «utilisateur», un «client» pouvant être aussi bien un «client final» qu'un «utilisateur».

2. Généralités

La présente annexe décrit les critères d'admissibilité dont la satisfaction est une condition préalable à la participation à la plate-forme bLink. Les critères d'admission se composent des éléments suivants, qui doivent être remplis dans leur intégralité:

1. Critères généraux d'admission

Les critères généraux d'admission sont réglés uniformément pour toutes les applications et doivent être remplis dans tous les cas, quels que soient le rôle demandé (utilisateur ou fournisseur de services) ainsi que le niveau de sécurité défini dans le cadre de toutes les applications.

2. Critères pour la réalisation de la finalité spécifique

Les critères pour la réalisation de la finalité spécifique définissent les preuves à fournir pour démontrer le respect de la réalisation de la finalité spécifique telle que décrite dans les spécifications d'application respectives (annexe 2). Ces critères sont définis dans l'application. Si le participant décide d'avoir accès à une application, les critères pour la finalité spécifique de l'application correspondante doivent être remplis.

3. Critères de sécurité dans le rôle demandé

Les critères de sécurité règlent les objectifs et les mécanismes nécessaires pour un échange de données sécurisé au sens du contrat de participation et reposent sur le besoin de protection de l'application concernée. Le champ d'application des critères de sécurité s'étend donc à toutes les parties impliquées dans la transmission des données et aux composants extérieurs à l'application. Sont également concernés la voie de transmission et les parties et composants impliqués entre le client et l'application, dans la mesure où le client intervient dans l'autorisation et l'authentification des appels de service.

Les critères de sécurité sont déterminés par le niveau de sécurité défini pour le rôle demandé (utilisateur de services ou fournisseur de services) du participant dans l'application concernée.

Les participants qui satisfont aux critères de sécurité pour un niveau de sécurité défini sont autorisés à utiliser des applications de même niveau de sécurité ou de niveau inférieur dans le même rôle, pour autant que les critères énoncés aux ch. 2 et 4 (respect de la finalité spécifique, spécification technique) soient respectés.

4. Spécifications techniques

Les exigences techniques sont définies dans les spécifications d'application en tant que spécifications techniques et doivent être mises en œuvre par le participant.

5. Répétition régulière de l'examen d'admission

Le participant s'engage à réitérer la vérification des critères d'admission au plus tard 12 mois après le dernier résultat de la vérification conformément au contrat de participation (ch. 3 N 8 et suivants).

3. Dispositions spéciales

1. Dispositions pour les banques réglementées par la FINMA

L'accès à la plate-forme bLink est autorisé pour les participants qui disposent d'une autorisation en tant que banque suisse au sens de l'art. 1 de la loi fédérale suisse sur les banques et les caisses d'épargne et qui remplissent les critères pour la réalisation de la finalité spécifique conformément au ch. 2.

L'existence d'une telle autorisation doit être confirmée par écrit par le participant et est vérifiée par SIX sur la base des informations publiquement disponibles sur le site Internet de l'Autorité fédérale de surveillance des marchés financiers FINMA (www.finma.ch).

SIX se réserve le droit d'examiner le respect de critères supplémentaires dans le cas où ils seraient introduits à l'avenir.

2. Autorité suisse

«Autorité suisse» désigne un organisme public en Suisse, qui assume des fonctions relevant de l'administration publique, dont elle est chargée sur la base des dispositions de droit public. Dans le cadre du contrat de participation, l'autorité intervient en tant que participant ayant le rôle de fournisseur de services ou d'utilisateur de services.

Les participants qui répondent aux critères d'une autorité suisse, aux critères pour la réalisation de la finalité spécifique conformément au chapitre 2, clause 2 ainsi qu'aux critères de sécurité dans le rôle demandé conformément au chapitre 2, clause 3 sont admis sur la plate-forme.

La qualification en tant qu'autorité doit être confirmée par écrit par le participant et être prouvée sur demande (p. ex. présentation sur le site Web, agencement de la structure administrative) et est vérifiée par SIX sur la base des informations accessibles au public sur la page Web correspondante.

SIX se réserve le droit d'examiner le respect des critères supplémentaires s'appliquant aux autorités suisses, introduits dans le cadre d'une application.

3. SIX en tant que participante

SIX est admise en tant que participante à la plate-forme, dans la mesure où les éléments des critères d'admission conformément au chapitre 2 sont remplis. La vérification de la satisfaction des conditions est effectuée conformément au processus défini dans le contrat de participation au chapitre 9.

4. Critères généraux d'admission

ID	Catégorie	Critère	Quel est l'objectif?	Informations / sujets couverts	Données à fournir par le participant
1	Identification	Dispose d'une inscription au registre du commerce en tant que personne morale	- Confirmation que la société est enregistrée en tant que personne morale au registre du commerce et qu'elle est active- Identification de l'adresse de la société et direction enregistrée	Dénomination sociale et forme juridique Adresse Numéro d'identification Identification de la direction / des signataires autorisés	- Documents constitutifs
2	Modèle d'entreprise	dispose d'un modèle d'entreprise documenté avec les services prévus	- Identification des activités commerciales du demandeur- Comparaison et coordination du modèle d'entreprise avec les services prévus	Identification et résumé des activités et des services de l'entreprise	- Modèle d'entreprise / plan d'affaires
3	Liquidité	dispose d'un plan d'affaires solide et d'un plan budgétaire pour 1 à 3 ans	- Analyse des comptes annuels et de la planification budgétaire pour résumer la situation financière du demandeur	Aperçu des ratios financiers et calcul des ratios clés	- Comptes annuels
4	Structure organisationnelle	crée un organigramme avec les fonctions clés, les succursales	- Obtenir une vue d'ensemble de la structure du demandeur avec les fonctions clés et les personnes responsables- Aperçu des pays et des sites où le demandeur est actif	Autre identification de la direction si impossible via registre du commerce Récapitulatifs des autres sites et services	- Organigramme
5	Audit	Normes comptables Liste des réviseurs	- S'assurer que le demandeur dispose d'un processus comptable approprié et de contrôles internes correspondants	Noms des réviseurs	- Liste des réviseurs / assortie des comptes annuels
6	Respect des sanctions, lutte contre le blanchiment d'argent et le financement du terrorisme	ne figure pas en tant que société ou avec ses membres de la direction / propriétaire sur les listes de sanctions et les listes d'avertissement des autorités de surveillance	- Création de profils de la direction du demandeur, par exemple gérant, directeur financier, employés responsables de la demande- Identification des incidents négatifs de criminalité financière dans lesquels des membres de la direction étaient/sont impliqués- Déterminer si l'entreprise et sa direction sont politiquement exposées	Pots-de-vin, corruption, fraude Relations avec les fonctionnaires (statut PEP) Activités illégales et criminelles Non-conformité financière Non-conformité réglementaire Litiges juridiques Rapports préjudiciables Inscription sur la liste des sanctions	n. d.

7	Respect des lois	- aucun membre de la direction / propriétaire ayant des inscriptions aux casiers judiciaires, aux registres des faillites et des poursuites qui empêcheraient une gestion irréprochable de l'entreprise	- liste les procédures d'autorisation et procédures pénales en cours- Identification des incidents négatifs, par exemple des procédures pénales ou des procédures d'insolvabilité dans lesquels des membres de la direction sont impliqués	Casiers judiciaires / registres des faillites / registres des poursuites couverts par le critère 6	- Extraits de casiers judiciaires de la direction - Confirmation que le fournisseur n'est pas impliqué dans une procédure judiciaire
8	Autorisations rejetées d'autres banques, régulateurs	Informations indiquant si une évaluation pertinente de l'autorisation par une autre autorité a déjà été rejetée, avec indication du motif	- Confirmer si la société est agréée/autorisée par les autorités compétentes	Licences et approbations active et valides disponibles Si aucune licence ou approbation disponible, couvert par le critère 6 «non-conformité réglementaire»	- Licences / confirmations des autorités compétentes
9	Fiabilité, probité, intégrité de la direction	Preuves de connaissances / compétences / expérience selon le curriculum vitae	- Création de profils, p. ex. CV. de la direction du demandeur, p. ex. gérant, directeur financier, employés responsables de la demande - Identification des incidents négatifs concernant l'emploi, tels que la perte d'emploi ou le licenciement de l'employeur	Informations de base (par exemple Informations de base (par exemple nationalité, lieu de résidence, études) Activités passées Respect des lois et intégrité de la personne (couverts par les critères 6 et 7)	- Curriculum vitae des principaux membres de la direction

Tableau 1: Critères généraux d'admission1

5. Critères de sécurité dans le rôle demandé

Le tableau suivant énumère les critères de sécurité pour les spécifications d'application du niveau de sécurité de base et du rôle «Utilisateur de services» (SU):

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
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.	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 réduire au minimum le risque de détournement de session et donc, entre autres, de modification malveillante de la configuration.	TE
		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
C03	L'accès aux données transférées par le SP doit être protégé de manière adéquate (at rest, in transit, at processing)	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
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 et les accès aux données (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 ne doit pas avoir lieu à l'étranger et l'accès ne doit pas avoir lieu depuis l'étranger (par exemple les administrateurs de système, le personnel d'assistance, etc.). Cela est assuré par des mesures techniques/organisationnelles. L'utilisateur lui-même peut accéder à ses données depuis n'importe où.	TE
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
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

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
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
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

Tableau 2: Critères de sécurité pour l'utilisateur de services dans le niveau de sécurité de base2

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)**: Les critères de sécurité énumérés s'appliquent en plus de ceux du niveau de sécurité de base:

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
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 identifié de manière unique 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
		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 doit être mise en œuvre dans l'application du SU ayant les caractéristiques suivantes: - Longueur minimale: 8 caractères- Complexité: combinaison de majuscules et minuscules, chiffres, caractères spéciaux requis- Intervalle de changement: au moins tous les six mois	TE
		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
		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
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 de l'utilisateur 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
				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
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	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

			sécurité et protégées contre tout accès non autorisé	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
		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 des administrateurs du SU.	Processus et TE
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 des administrateurs du SU.	Processus et TE
		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
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
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
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
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
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

Tableau 3: Critères de sécurité pour l'utilisateur de services dans le niveau de sécurité élevé3

Le tableau suivant énumère les critères de sécurité pour les spécifications d'application du niveau de sécurité «Très élevé» et du rôle «Utilisateur de services» (SU). Les critères de sécurité énumérés s'appliquent en plus de ceux du niveau de sécurité élevé:

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
I03	**Intégrité** La non-contestation d'une transaction doit être garantie. Sont considérés comme transactions tous les appels de requête/réponse API qui forment une unité logique.	F25	La transaction doit être complète.	M22	L'utilisateur de services doit transmettre au fournisseur de services les mêmes informations que si l'utilisateur effectuait lui-même la transaction.	TE
		F26	La transaction doit pouvoir être clairement référencée.	M23	La transaction doit posséder un ID de transaction unique.	TE
		F27	Vérification de la réponse à la transaction	M24a	Le SU est tenu de vérifier que l'ordre envoyé et la confirmation reçue du fournisseur de services concordent, respectivement que les non-concordances soient immédiatement communiquées à l'utilisateur et que d'éventuelles mesures correctives soient rendues possibles.	Processus
		F28	Identification d'ordres automatisés	M25	Les transactions basées sur des règles ou automatisées doivent être identifiables par le fournisseur de services.	TE
		F29	Non-contestation d'ordres d'utilisateurs	M26	Lorsqu'un utilisateur passe des ordres automatisés (basés sur des règles), l'utilisateur de services doit garantir la traçabilité et la non-contestation de ces ordres.	TE
		F30	Conservation de la réponse à la transaction (recommandation)	M27	La réponse à la transaction du fournisseur de services doit être conservée de manière à pouvoir être utilisée ultérieurement en cas d'éventuels sinistres.	n. d.

Tableau 4: Critères de sécurité pour l'utilisateur de services dans le niveau de sécurité très élevé4

Le tableau suivant énumère les critères de sécurité pour les spécifications d'application du niveau de sécurité de base et du rôle «Fournisseur de services» (SP):[1]

SR-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
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	F02	Les informations d'authentification doivent être stockées en toute sécurité et ne doivent pas être visibles en texte clair	M52	Le token délivré par le SP ne doit pas contenir d'informations sensibles (CID). En outre, le token ne doit pas être stocké en clair.	TE
C03	L'accès aux clés pour le service (jeton) et aux données transférées au SU doit être protégé de manière adéquate (at rest, in transit, at processing)	F26	L'accès au service d'authentification doit être protégé	M56	L'accès au service depuis Internet (banque en ligne, par exemple) doit être sécurisé par une protection périmétrique (proxy, WAF).	TE
		F28	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
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	F11	Le stockage ou l□es accès aux données (pas les accès des utilisateurs) doivent être limités à la Suisse	M11	En l'absence de consentement explicite de l'utilisateur, le stockage des données ne doit pas avoir lieu à l'étranger et l'accès ne doit pas avoir lieu depuis l'étranger (par exemple les administrateurs de système, le personnel d'assistance, etc.). Cela est assuré par des mesures techniques/organisationnelles. L'utilisateur lui-même peut accéder à ses données depuis n'importe où.	TE
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

[1] Le niveau de sécurité Basic ne répond pas aux exigences de l'échange de «Client Identifying Data» (CID) sur la plate-forme bLink.
Les CID contiennent des informations sur les clients, qui permettent de déduire directement ou indirectement l'existence d'une relation client avec la banque.
De même, les transactions qui modifient la valeur, c'est-à-dire le patrimoine, ne sont pas non plus couvertes par le niveau de sécurité Basic.

T01	**Technologie** Identification des systèmes informatiques concernés	F21	Le SP peut prouver sur quels systèmes les données correspondantes sont traitées et stockées	M15	Le SP tient un inventaire des systèmes, qui contient les données d'accès et les données transférées.	Processus
P02	Un processus de gestion des incidents est en place pour traiter les dysfonctionnements et les incidents de sécurité.	F22	Le SP peut gérer les cas de dysfonctionnement et communique les incidents de sécurité	M17	- Le SP 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 SP 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
P03	Le SP dispose d'un processus de gestion du changement	F21	Le processus de gestion du changement est en place et mis en œuvre	M18	Le SP 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
P04	Le SP dispose d'un processus de gestion pour ses propres sous-traitants qui traitent les données pertinentes	F23	Les sous-traitants qui traitent les données doivent satisfaire aux mêmes exigences de stockage des données que le SP	M19	Il existe un contrat et un processus de gestion pour les sous-traitants ayant des exigences de sécurité équivalentes.	Processus
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

Tableau 5: Critères de sécurité pour le fournisseur de services dans le niveau de sécurité de base5

Le tableau suivant énumère les critères de sécurité pour les spécifications d'application du niveau de sécurité élevé et du rôle «Fournisseur de services» (SP). Les critères de sécurité énumérés s'appliquent en plus de ceux du niveau de sécurité de base:

SR-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
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 identifié de manière unique avant le premier accès au service	M51	Le SP contrôle l'utilisateur au moyen d'une authentification forte.	TE
		F03a	Délai d'expiration de session dans l'application du SP	M03a	L'utilisateur doit être déconnecté de l'application SP après une longue inactivité de la session (max. 1h).	TE
		F03b	Délai d'expiration de session des administrateurs du SP	M03b	Les sessions des administrateurs doivent être limitées dans le temps (à quelques minutes) en cas d'inactivité afin de réduire au minimum le risque de détournement de session et donc, entre autres, de modification malveillante de la configuration.	TE
		F25	L'utilisateur doit être fortement identifié périodiquement	M53	Le token pour l'accès de l'utilisateur (token de rafraîchissement) doit être révoqué ou expirer après une date d'expiration définie, et un processus d'authentification strict doit être répété pour créer le token.	TE
		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 SP doit être crypté via https (cryptage TLS). Aucun protocole (par exemple TLS 1.0) ou algorithme obsolète n'est utilisé	TE
C02	L'autorisation d'accès aux données ne peut être accordée qu'aux utilisateurs qui ont accepté l'accès aux données et qui sont autorisés par le fournisseur de services	F04	Le consentement du client doit être vérifié	M54	Le consentement à la communication des données au SU est obtenu de manière vérifiable et incontestable.	TE
				M55	L'accès au service obtenu par le SU doit être limité au champ d'application (informations de compte et livraison de paiements, par exemple) du consentement donné par l'utilisateur.	TE
C03	L'accès aux clés pour le service (jeton) et aux données transférées au SU doit être protégé de manière adéquate (at rest, in transit, at processing)	F27	L'accès au service et aux données doit être limité et consigné	M57	Des rôles permettant de séparer l'accès technique et l'accès aux applications doivent être définis. Les journaux doivent être contrôlés pour détecter toute utilisation anormale du service.	TE

C04	L'autorisation d'accès aux données ne peut être donnée aux administrateurs des SP que si elle est nécessaire à la fourniture du service	F31	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
I02	**Intégrité** 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
A01	**Disponibilité, BCP, DR** Aucune donnée d'accès ne doit être perdue	F19	Le SP doit être en mesure de rétablir l'accès au service et le consentement	M14b	Une sauvegarde ou une mise en miroir des données doit être disponible pour l'accès au service et le consentement 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
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
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 SP: extrait du casier judiciaire et du registre des poursuites.	Processus

Tableau 6: Critères de sécurité pour le fournisseur de services dans le niveau de sécurité élevé6

Le tableau suivant énumère les critères de sécurité pour les spécifications d'application du niveau de sécurité très élevé et du rôle «Fournisseur de services» (SP). Les critères de sécurité énumérés s'appliquent en plus de ceux du niveau de sécurité élevé:

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
I03	**Intégrité** La non-contestation d'une transaction doit être garantie. Sont considérés comme transactions tous les appels de requête/réponse API qui forment une unité logique.	F31	La réception de la transaction doit être entièrement confirmée.	M58	Le fournisseur de services doit, immédiatement après la réception de la transaction, en accuser réception à l'utilisateur de services, au moins avec les informations de transaction reçues et le statut de la transaction.	TE
		F26	La transaction doit pouvoir être clairement référencée.	M23	La transaction doit posséder un ID de transaction unique.	TE
TM01	**Surveillance des transactions**	F32	Les paramètres des transactions doivent être surveillés et consignés pour évaluer les risques, la fraude ou les incidents de sécurité.	M59	Les fournisseurs de services disposent d'un système de surveillance des transactions qui leur permet de détecter au mieux les transactions frauduleuses.	Processus
D01	**Liaison unique de l'autorisation de transaction avec la transaction**	F33	Liaison dynamique de transactions	M59	Le fournisseur de services doit autoriser la transaction (en l'absence d'exemption) au moyen de la MFA par l'utilisateur. La MFA présente les caractéristiques suivantes: - l'utilisateur (p. ex. l'initiateur) reçoit une information sur la transaction effectuée (p. ex. le montant) et le destinataire de la transaction; - le code d'authentification généré est spécifique à la transaction, auquel l'initiateur de la transaction a consenti lors de l'introduction de la transaction et cela peut être vérifié par l'initiateur de manière transparente; - le code d'authentification est clairement lié à la transaction, à savoir que la transaction ne peut être acceptée qu'en cas de concordance entre un indicateur et une information de transaction confirmée.	TE
		F34	Liaison dynamique de transactions Batch	M60	En cas d'autorisation de plusieurs transactions en tant que Batch, le code d'authentification de la MFA doit (en l'absence d'exemption) être spécifique au Batch et indiquer à l'utilisateur une information vérifiable sur l'ordre du Batch.	TE
		F35	Identification d'autorisation de transaction échouée	M61	En cas d'autorisation de transaction échouée, l'utilisateur de services doit être informé.	TE

P07	**Processus** **Traitement des exceptions**	F35	Les mesures de sécurité des transactions doivent être vérifiées régulièrement.	M62	Les mesures de sécurité doivent être documentées et testées, évaluées et auditées périodiquement par un expert indépendant: Les transactions sont autorisées au moyen de la Multifactor Authentication (MFA) de l'utilisateur, qui est clairement liée à la transaction, à moins qu'il n'existe une exemption documentée reposant sur un processus de gestion de la fraude documenté.	Processus
		F36	Les exemptions sont réglées dans les spécifications d'application et ne sont possibles que pour les cas qui sont soumis à une surveillance des risques.	M63	La renonciation à la MFA pour l'autorisation de transaction ne peut avoir lieu que dans des cas spécifiques, par exemple lorsque: - des conditions spécifiques et limitatives concernant les risques sont définies; - le montant, des transactions récurrentes ou des canaux de transaction sont définis. En cas d'anomalies ou de fraude, la MFA doit être activée immédiatement ou la transaction doit être bloquée, voire suspendue et vérifiée séparément.	Processus

Tableau 7: Critères de sécurité pour le fournisseur de services dans le niveau de sécurité très élevé7