3SKey

Mise en route pour les entreprises

Ce manuel décrit la procédure de configuration de l'environnement 3SKey d'une organisation à des fins de signature des transactions financières.

27 octobre 2017

Table des matières

Préface

Objet de ce document

Ce manuel décrit la procédure de configuration de l'environnement 3SKey d'une organisation à des fins de signature des transactions financières.

Public

Ce document s'adresse aux planificateurs, coordinateurs, administrateurs et utilisateurs de tokens 3SKey.

Modifications importantes

Le tableau suivant répertorie les changements significatifs apportés depuis l'édition précédente. Ce tableau ne comprend pas les modifications générales et mises à jour mineures qui ont été apportées.

Nouvelles informations	Emplacement
Un gestionnaire de liste d'utilisateurs peut définir des **règles en matière de code PIN** pour augmenter la complexité minimum obligatoire des mots de passe pour la liste d'utilisateurs.	Sélectionner une règle en matière de code PIN pour la liste d'utilisateurs

Informations associées

Guide d'installation du logiciel du token 3SKey
Guide d'utilisation du portail 3SKey pour les entreprises
Instructions à l'attention de l'administrateur 3SKey
Instructions à l'attention de l'utilisateur 3SKey
Description du service 3SKey

1 Introduction à 3SKey

1.1 Qu'est-ce que 3SKey?

Le service 3SKey fournit un mécanisme permettant aux clients d'une banque d'authentifier et de signer les messages et les fichiers qu'ils envoient à la banque par l'intermédiaire de réseaux de services bancaires électroniques.

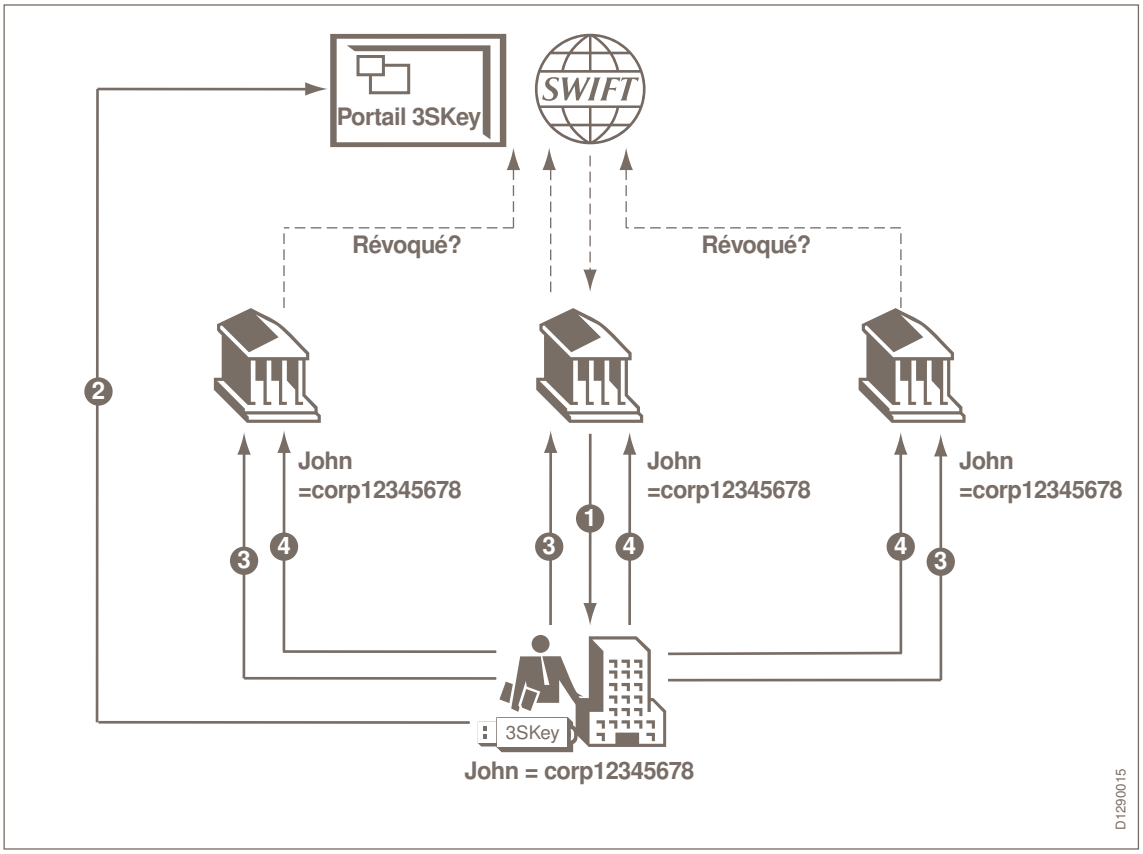
Présentation

Lorsqu'une banque et une entreprise conviennent d'utiliser 3SKey pour authentifier les transactions, la banque fournit un ensemble de tokens 3SKey à l'entreprise, afin que chaque utilisateur individuel au sein de l'entreprise puisse recevoir un token personnel. L'utilisateur de l'entreprise doit activer le token en utilisant le portail 3SKey, puis enregistrer le token auprès de la banque.

Lorsque l'utilisateur envoie une transaction à la banque, le token crée une signature électronique pour accompagner la transaction. La signature est basée sur l'infrastructure à clé publique (PKI) SWIFT. La signature électronique permet à la banque d'identifier la personne spécifique qui a signé la transaction en utilisant la non-répudiation et de vérifier que la transaction n'a pas été modifiée depuis sa signature.

Pour plus d'informations sur 3SKey, reportez-vous à la Description du service 3SKey.

Processus de présentation de 3SKey



Les points suivants décrivent le processus 3SKey:

1. John, l'utilisateur du token 3SKey, reçoit son token de sa banque.
2. Il active son token sur le portail 3SKey.
3. Il enregistre son token auprès des banques dont il doit signer les transactions.
4. Il peut authentifier ou signer des messages en utilisant différents réseaux, tels qu'Internet, le réseau de sa banque ou SWIFT.

Parties 3SKey

Les parties suivantes sont impliquées dans la solution 3SKey:

- **SWIFT**

  SWIFT fournit le service 3SKey, le Kit du développeur 3SKey, les tokens 3SKey ainsi que le portail 3SKey nécessaire à leur gestion.

- **L'abonné 3SKey**

  L'abonné 3SKey (généralement une banque) souscrit à et intègre le service 3SKey, et distribue les tokens 3SKey aux utilisateurs 3SKey.

- **L'utilisateur 3SKey**

  L'utilisateur 3SKey (généralement une entreprise) intègre et utilise le service 3SKey avec son abonné 3SKey (ou ses abonnés 3SKey). Les utilisateurs 3SKey obtiendront normalement les tokens 3SKey auprès de leur abonné 3SKey initial.

Principes

Les principes de la solution 3SKey sont les suivants:

- SWIFT joue le rôle d'autorité de certification et fournit les certificats aux utilisateurs finals.
- Les banques distribuent des tokens contenant des clés cryptographiques inactives.
- Les utilisateurs accèdent au portail 3SKey sur Internet pour activer le token. L'activation crée des informations d'identification métier (c'est-à-dire, un certificat et une clé privée) et les stocke sur le token.
- Au lieu de contenir l'identification classique des utilisateurs telle que le nom, le prénom ou l'adresse e-mail, les certificats contiennent une identification unique sous la forme `corp12345678`.
- Au sein de la banque, le détenteur du certificat est identifié par une procédure d'association de l'identifiant unique avec l'identité réelle du détenteur.

  La procédure peut varier d'une banque à l'autre. Elle dépend des critères de sécurité propres à la banque, ou de critères établis par les réglementations du pays dans lequel le certificat est utilisé.

- Grâce à cette configuration, l'identité de l'utilisateur n'est jamais communiquée à l'extérieur de la banque. La société SWIFT elle-même ne connaît pas l'identité des détenteurs de certificat.

1.2 Concepts de 3SKey

Tokens 3SKey

Le token 3SKey est un périphérique USB contenant des clés sécurisées pour la signature des transactions financières. Un seul token peut être utilisé pour les transactions avec plusieurs banques, sur des canaux différents.

Le token 3SKey peut être utilisé sur n'importe quel PC sur lequel le logiciel du token 3SKey est installé.

Pour pouvoir utiliser le token pour signer des transactions, le propriétaire du token doit au préalable activer le token et l'enregistrer auprès de chaque banque avec laquelle l'entreprise utilise 3SKey. L'enregistrement associe l'identifiant unique stocké sur le token à l'identité du propriétaire du token.

Portail 3SKey

Le portail 3SKey est un service Web sécurisé permettant de gérer les tokens 3SKey et leurs propriétaires.

Les fonctions du portail 3SKey incluent l'activation du token, la révocation du certificat d'un token compromis, la régénération de l'identifiant unique d'un token perdu ou inutilisable sur un nouveau token et la réinitialisation d'un token verrouillé ou dont le mot de passe est perdu. En outre, un ensemble de fonctions d'administrateur sont relatives à la gestion des utilisateurs au sein de l'entreprise et de leurs tokens.

Les fonctions du portail 3SKey n'ont aucun impact sur l'application de la banque avec laquelle vous signez les transactions.

Le présent manuel décrit les fonctions du portail 3SKey qui sont nécessaires pour configurer l'environnement 3SKey de votre organisation. Pour des informations complètes sur le portail 3SKey, reportez-vous à l'aide en ligne du portail 3SKey ou au Guide d'utilisation du portail 3SKey pour les entreprises.

Activation

Le token fourni par SWIFT initialement contient un certificat garantissant que le token a été émis par SWIFT. Pour signer des messages professionnels, vous devez convertir ce certificat en **certificat métier**. Le processus de création du certificat métier est appelé **activation du token**.

Pour activer le token, le propriétaire du token doit l'insérer dans un port USB et se connecter au portail 3SKey. Pendant le processus d'activation du token, une nouvelle paire de clés est générée sur le token. La clé publique est ensuite envoyée au portail 3SKey pour être certifiée. Le nouveau certificat métier est stocké sur le token, et le certificat technique est supprimé. La clé privée ne quitte jamais le token.

Utilisateurs et listes d'utilisateurs

Chaque token 3SKey est défini comme appartenant à un administrateur ou à un utilisateur dans une entreprise.

- Les **utilisateurs d'entreprise** peuvent utiliser le certificat sur le token pour signer ou authentifier des transactions auprès d'une banque, et peuvent effectuer des tâches administratives sur leur propre token.
- Les **administrateurs** ont accès à toutes les fonctions qu'un utilisateur d'entreprise peut utiliser. Les administrateurs peuvent en outre accéder à toutes les fonctions qui sont nécessaires pour configurer et effectuer la maintenance de l'environnement 3SKey de leur entreprise.

Chaque environnement 3SKey doit avoir au minimum deux tokens d'administrateur, au cas où un des tokens serait verrouillé.

Chaque token doit appartenir à une **liste d'utilisateurs**. Pour plus d'informations sur la gestion des **listes d'utilisateurs**, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises > Gérer les utilisateurs.

Code de sécurité

Le code de sécurité est généré au cours du processus d'activation du token. Le code de sécurité est nécessaire pour révoquer un token perdu ou compromis, régénérer son identifiant unique sur un nouveau token ou réinitialiser un token verrouillé ou dont le mot de passe est perdu.

Il est très important de conserver le code de sécurité dans un lieu sûr mais accessible.

1.2.1 Groupes d'utilisateurs 3SKey

Un groupe d'utilisateurs est un ensemble de tokens 3SKey appartenant à une organisation spécifique.

Qu'est-ce qu'un groupe d'utilisateurs?

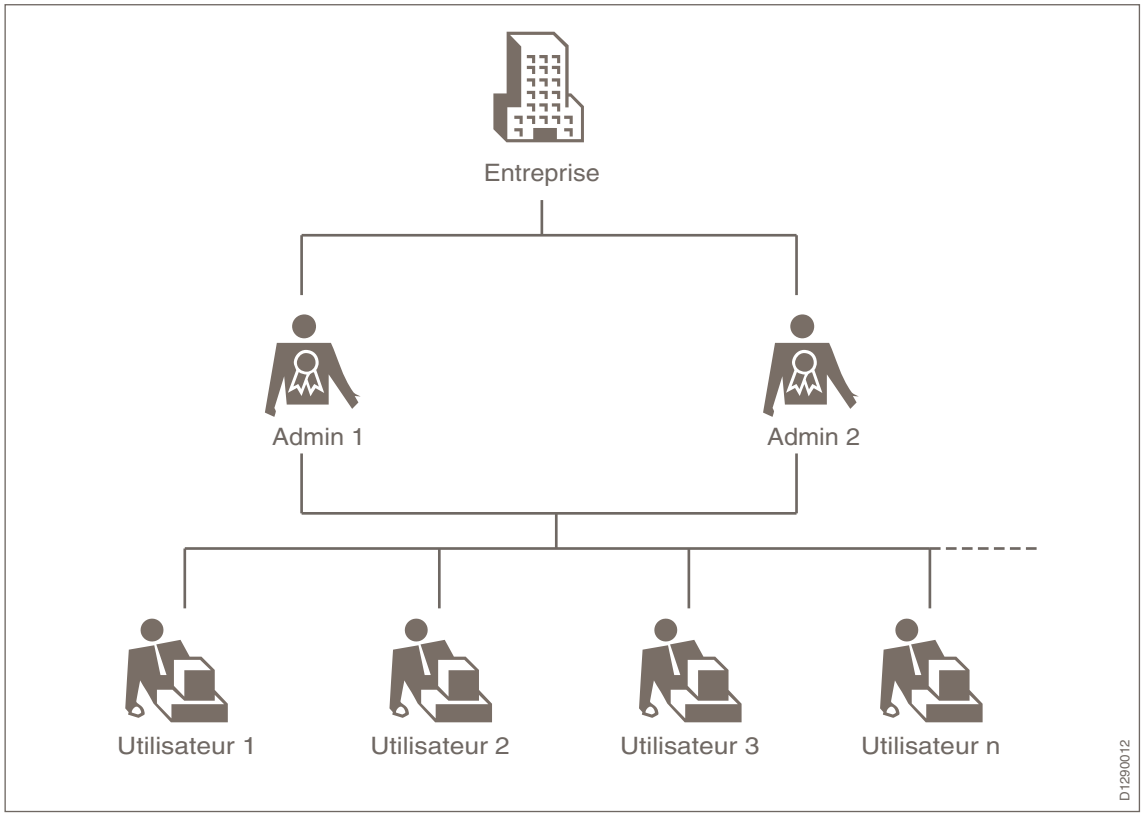
Le groupe d'utilisateurs est une aide pour gérer les tokens de l'organisation: il n'a aucun impact sur la capacité du token à signer des transactions, car l'application de signature ne connaît pas le groupe auquel le token appartient. Il est même possible de signer une transaction avec un token appartenant à un groupe, et d'approuver la transaction avec un token appartenant à un autre groupe.

Le rôle `user` est attribué à la plupart des tokens dans un groupe d'utilisateurs, mais au moins deux tokens, même s'il peut y en avoir plus, doivent avoir le rôle `admin`. Le rôle `admin` attribue la responsabilité de la gestion du groupe d'utilisateurs. Pour plus d'informations sur les différents types d'utilisateurs, reportez-vous à Rôles.

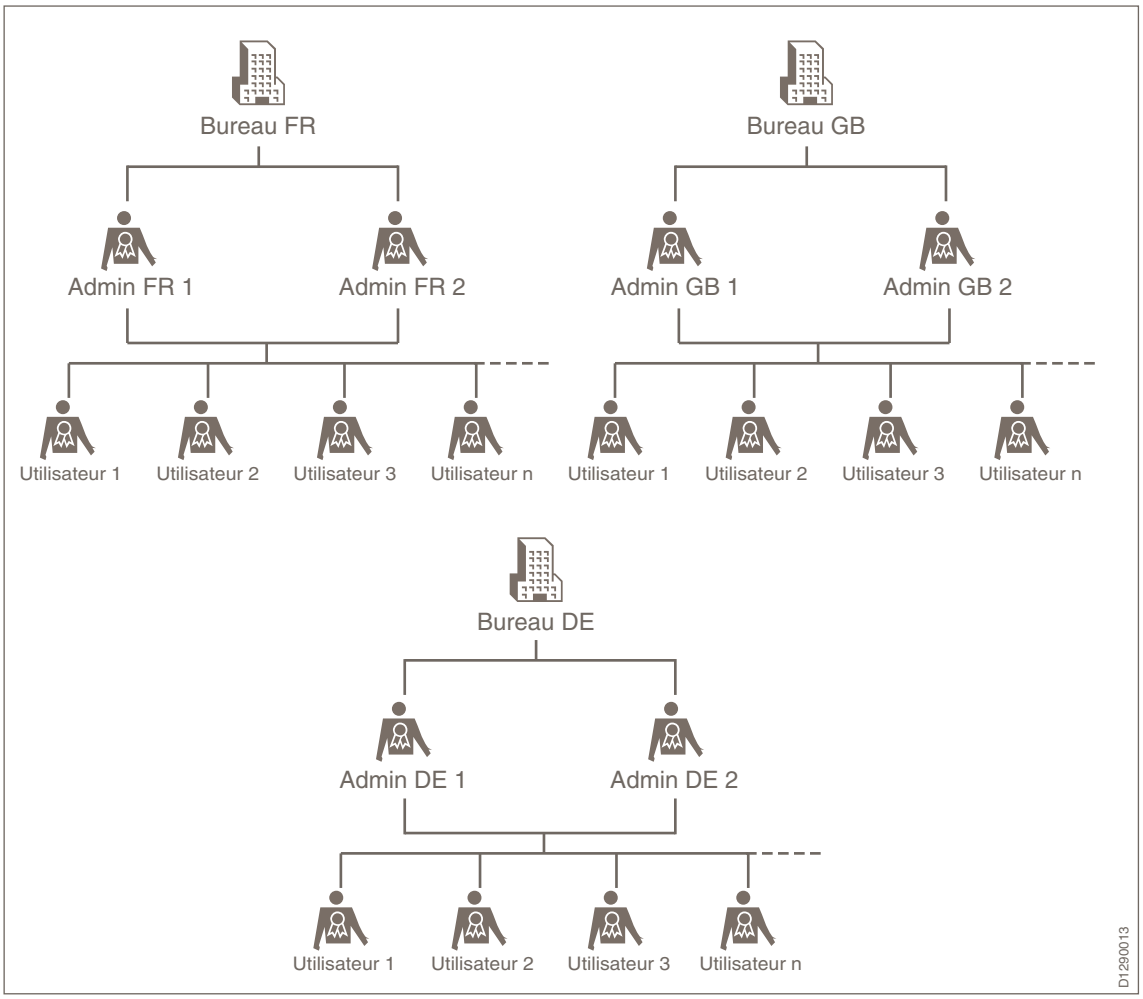
Un token utilisateur 3SKey ne peut pas être activé s'il n'appartient pas à un groupe d'utilisateurs. Un token ne peut appartenir qu'à un seul groupe d'utilisateurs.

Combien de groupes d'utilisateurs?

L'environnement 3SKey le plus simple est constitué d'un groupe d'utilisateurs unique contenant tous les tokens 3SKey appartenant à l'organisation:



Une organisation peut également avoir plusieurs groupes d'utilisateurs. Dans ce type d'environnement 3SKey, les tokens sont généralement regroupés en fonction du lieu ou du service dans lequel ils sont utilisés:



Remarque *Chaque groupe d'utilisateurs est entièrement indépendant de tous les autres groupes d'utilisateurs, y compris de ceux qui peuvent exister dans la même organisation.*

Il n'est pas possible de combiner 2 groupes d'utilisateurs existants ni de diviser un groupe d'utilisateurs en 2 groupes.

Il n'y a pas de limite technique au nombre de tokens pouvant appartenir à un groupe. La principale considération pour la taille d'un groupe d'utilisateurs est l'aspect pratique. Par exemple, si un groupe d'utilisateurs devient si important qu'il couvre plusieurs écrans sur la page **Gérer le groupe d'utilisateurs**, il peut être difficile d'effectuer le suivi des tokens individuels.

Création du groupe d'utilisateurs

Lorsque vous vous connectez au portail 3SKey avec le premier token de votre organisation, il n'y a pas de groupe d'utilisateurs pour votre organisation. Le portail 3SKey détecte que votre token n'appartient à aucun groupe d'utilisateurs, et vous fait suivre le processus de création du groupe d'utilisateurs. Dans le cadre de ce processus, le portail attribue le rôle `admin` à votre token. Vous pouvez alors activer votre token et affecter d'autres tokens au groupe d'utilisateurs.

Remarque *Il doit y avoir 2 administrateurs pour la même entreprise lorsque vous commencez la création des groupes d'utilisateurs. Il est conseillé de garder quelques tokens non activés de réserve à des fins de régénération, renouvellement ou de révocation.*

Pour plus d'informations, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

Si votre organisation a besoin d'un second groupe d'utilisateurs, connectez-vous au portail 3SKey avec un token que vous n'avez pas encore affecté au premier groupe d'utilisateurs. Le portail 3SKey détecte à nouveau que votre token n'appartient à aucun groupe d'utilisateurs, et vous fait suivre le processus de création du groupe d'utilisateurs.

2 Introduction de 3SKey dans votre organisation

L'introduction de 3SKey nécessite une certaine préparation et administration. Avant de commencer à utiliser vos tokens 3SKey, procédez comme suit:

- Identifiez les PC qui seront utilisés pour 3SKey, et sur lesquels vous devrez installer le logiciel du token.
- Assurez-vous que les PC remplissent les conditions préalables à l'installation du logiciel du token. Le *Guide d'installation du logiciel du token* détaille les exigences en matière de configuration.
- Désignez 2 gestionnaires de liste d'utilisateurs pour gérer les tokens utilisateur au nom de votre organisation. Les gestionnaires de listes d'utilisateurs disposent d'un token avec le rôle `admin`.
- Identifiez les utilisateurs 3SKey qui signeront des transactions.
- Identifiez les membres de chaque **liste d'utilisateurs**.

Informations associées

Rôles d'utilisateur et d'administrateur à la page 15
Guide d'installation du logiciel du token 3SKey

2.1 Désigner les 2 gestionnaires de liste d'utilisateurs

Les gestionnaires de liste d'utilisateurs doivent gérer les tokens au nom de l'organisation. Au moins 2 gestionnaires sont requis. Les gestionnaires de liste d'utilisateurs disposent d'un token avec le rôle `admin`.

- Fournissez les documents suivants à chaque administrateur:
  - Mise en route de 3SKey pour les entreprises
  - Instructions à l'attention de l'administrateur 3SKey

Remarque *Un token administrateur peut également être utilisé pour authentifier des transactions, au même titre que n'importe quel token utilisateur.*

2.2 Activer 2 tokens administrateur

Il est important que votre organisation dispose de 2 gestionnaires de liste d'utilisateurs disposant chacun d'un token 3SKey avec le rôle `admin`.

Le premier gestionnaire de la liste d'utilisateurs à activer un token doit ajouter le second token `admin` à la liste d'utilisateurs et sélectionner une règle en matière de code PIN pour l'organisation. Ce gestionnaire aura besoin des 2 tokens lors de l'activation. La règle en matière de code PIN peut être modifiée ultérieurement.

Important Il est nécessaire d'installer le logiciel du token sur chaque PC à partir duquel un utilisateur utilisera un token 3SKey pour accéder au portail 3SKey ou au portail de signature.

Après ajout des 2 administrateurs à la liste d'utilisateurs sur le portail 3SKey, le second gestionnaire de liste d'utilisateurs active le second token administrateur en l'insérant dans un port USB sur un PC sur lequel le logiciel du token 3SKey est installé, et effectue l'activation sur le portail 3SKey.

Informations associées

Guide d'installation du logiciel du token 3SKey

2.3 Sélectionner une règle en matière de code PIN pour la liste d'utilisateurs

La règle en matière de code PIN pour la liste d'utilisateurs détermine les exigences de complexité minimum du mot de passe pour un token. Lorsque le token est activé ou réinitialisé, la règle en matière de code PIN est appliquée au token.

Le premier gestionnaire de liste d'utilisateurs à activer un token administrateur doit sélectionner une règle en matière de code PIN pour la liste d'utilisateurs. Chaque propriétaire d'un token `admin` peut modifier cette règle à tout moment sur le portail 3SKey.

Déterminer la meilleure règle en matière de code PIN pour votre organisation

Paramètre	Description	Niveau 6 (par défaut)	Niveau 8	Niveau 12
Longueur	Nombre minimum de caractères	6	8	12
Expiration	Période de validité (en jours) avant de devoir modifier le mot de passe	90	180	365
Ensemble de caractères	Ensemble minimum de caractères qui doivent être utilisés	Chiffre (0-9)		• Lettre (a-z) • Chiffre (0-9) • Lettre majuscule (A-Z) • Symbole
Complexité	Règles en matière de composition d'un mot de passe	Maximum 2 caractères répétés		• Maximum 2 caractères répétés • Au moins un caractère de chacun des 4 groupes de caractères

Paramètre	Description	Niveau 6 (par défaut)	Niveau 8	Niveau 12
Historique	Nombre de mots de passe précédents qui ne peuvent pas être réutilisés	5		
Verrouillage	Nombre de tentatives erronées avant verrouillage du compte	5		

2.4 Gérer les utilisateurs 3SKey

Une fois que les tokens administrateur ont été activés, le gestionnaire de liste d'utilisateurs peut gérer les tokens utilisateur de l'entreprise.

Lorsqu'il est connecté au portail 3SKey, l'administrateur insère chaque token non utilisé à tour de rôle dans un second port USB, et l'ajoute à la **liste d'utilisateurs**.

Remarque *Le token administrateur et le token utilisateur qui est ajouté doivent être tous les deux branchés dans deux ports USB du même ordinateur en même temps.*

L'administrateur répète cette opération pour chaque token utilisateur qu'il souhaite ajouter à sa **liste d'utilisateurs**. Des utilisateurs supplémentaires peuvent être ajoutés à tout moment.

Lorsque vous avez ajouté les tokens utilisateur à la **liste d'utilisateurs**, vous devez distribuer les tokens aux utilisateurs.

Informations associées

Instructions à l'attention de l'administrateur 3SKey

2.5 Distribuer les tokens aux utilisateurs

L'administrateur distribue les tokens non utilisés (qui ont été ajoutés à la **liste d'utilisateurs**) aux personnes qui utiliseront les tokens.

L'administrateur doit également faire parvenir les Instructions à l'attention de l'utilisateur 3SKey aux utilisateurs 3SKey. Ce document explique les actions que l'utilisateur doit entreprendre avant de commencer à travailler avec 3SKey.

Important Il est nécessaire d'installer le logiciel du token sur chaque PC à partir duquel un utilisateur utilisera un token 3SKey pour accéder au portail 3SKey ou au portail de signature.

Informations associées

Guide d'installation du logiciel du token 3SKey

2.6 Activation du token utilisateur

Le propriétaire du token utilisateur doit se connecter au portail 3SKey pour activer le token. Après activation, l'utilisateur peut enregistrer le token auprès de la banque et l'utiliser pour authentifier des transactions.

Remarque *Il est important d'activer les tokens avant d'envoyer les contrats d'enregistrement à la banque.*

Lorsque le propriétaire se connecte avec un token non utilisé et démarre l'activation, le portail 3SKey demande à l'utilisateur de remplacer le mot de passe par défaut par un mot de passe personnel. La règle en matière de code PIN de la liste d'utilisateurs détermine les exigences de complexité minimum pour les mots de passe personnels sur le token.

L'activation génère un code de sécurité personnel et télécharge le certificat métier utilisé pour signer des transactions. L'utilisateur doit stocker ce code de sécurité dans un endroit sûr et se souvenir du mot de passe du token. Ce code est utilisé pour réinitialiser ou régénérer un token si un utilisateur le verrouille. Sans le code, le token peut devenir inutilisable.

Après activation, le token peut alors être enregistré auprès d'une banque et être utilisé pour authentifier des transactions.

Informations associées

Instructions à l'attention de l'utilisateur 3SKey

3 Meilleures pratiques pour la mise en oeuvre de 3SKey

3.1 Rôles d'utilisateur et d'administrateur

Présentation

Les utilisateurs individuels de 3SKey peuvent avoir deux rôles différents, selon leur niveau de droits d'accès. Ces rôles sont les suivants:

- **Administrateur**
- **Utilisateur**

Fonctions du portail disponibles aux administrateurs

L'administrateur est la personne au sein de l'organisation des utilisateurs 3SKey qui reçoit, prépare, distribue et effectue la maintenance des tokens.

Les utilisateurs ayant le rôle `admin` ont accès à toutes les fonctions d'utilisateur sur le portail, ainsi qu'aux fonctions suivantes:

- Configurer et assurer la maintenance de la **liste d'utilisateurs** contenant des tokens avec le rôle `admin` et des tokens avec le rôle `user`.
- Sélectionner la règle en matière de code PIN pour l'organisation.
- Afficher les tokens et leur statut dans la **liste d'utilisateurs**.
- Révoquer les tokens dans la **liste d'utilisateurs**.
- Configurer un token pour la régénération d'un identifiant unique.
- Réinitialiser un token **non activé**.
- Configurer en vue d'une réinitialisation un token **activé** verrouillé ou dont le mot de passe est perdu.

Remarque *Chaque **liste d'utilisateurs** 3SKey doit avoir au moins deux administrateurs. SWIFT vous recommande d'ajouter un troisième token administrateur à la liste, laissé non activé en tant que token de réserve si les deux autres tokens étaient verrouillés.*

Tâches de l'administrateur

Dans le cadre de leurs responsabilités, les administrateurs doivent effectuer les tâches suivantes:

- Ajouter des tokens non activés à la **liste d'utilisateurs**.
- Distribuer les tokens 3SKey aux utilisateurs.
- Conserver une liste des identifiants uniques et des utilisateurs associés.
- S'assurer qu'une procédure est en place pour révoquer un token perdu ou volé.
- S'assurer qu'une procédure est en place pour régénérer l'identifiant unique d'un token perdu ou endommagé sur un autre token.
- S'assurer qu'une procédure est en place pour réinitialiser un token verrouillé.
- S'assurer qu'une procédure est en place pour le renouvellement des tokens utilisateur avant leur date d'expiration.

- S'assurer qu'il existe suffisamment de tokens de réserve.
- S'assurer que le token d'un utilisateur quittant l'organisation est révoqué.
- S'assurer qu'un administrateur quittant l'organisation est remplacé par un nouvel administrateur.

Rôle de l'utilisateur

L'utilisateur 3SKey reçoit le token de la part de l'administrateur 3SKey et l'active sur le portail 3SKey.

Les utilisateurs possédant un token activé ayant le rôle **user** ont accès aux fonctions suivantes:

- Utiliser le certificat sur le token pour signer ou authentifier des transactions avec une banque.
- Modifier le mot de passe du token.
- Générer un nouveau code de sécurité.
- Révoquer le certificat sur le token.
- Effectuer la régénération du certificat sur le token. Pour ce faire, un second token préparé par un administrateur en vue d'une régénération est nécessaire.
- Effectuer la réinitialisation du token. Pour cela, un administrateur doit avoir préparé le token en vue d'une réinitialisation.
- Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la date d'expiration).
- Renouveler le token avant son expiration (au bout de trois ans).

Commentaires

- La présence physique du token 3SKey de l'administrateur et du token 3SKey de l'utilisateur est toujours requise lors de l'ajout d'un token utilisateur à la liste gérée par l'administrateur.
- Le code de sécurité est requis dans certaines situations exceptionnelles (par exemple, révocation d'un token par l'utilisateur, réinitialisation d'un token verrouillé ou régénération du certificat sur un token perdu ou volé). Pour plus d'informations sur la révocation ou la réinitialisation des tokens et la régénération des identifiants uniques, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

3.2 Directives en matière de sécurité

Accès Internet

L'utilisateur 3SKey doit s'assurer qu'une connexion Internet est active et sécurisée, et résoudre tout autre problème provoqué par ou survenant pendant la connexion Internet à l'application Web de l'abonné 3SKey.

En particulier, l'utilisateur 3SKey doit résoudre les problèmes liés à sa connexion Internet, ou les problèmes de configuration de l'accès Internet du côté de l'utilisateur.

Sécurité des tokens et mots de passe

L'utilisateur 3SKey est entièrement responsable de la sécurité du token. En particulier, il est de la seule responsabilité de l'utilisateur 3SKey d'empêcher un tiers non autorisé d'utiliser son token et son mot de passe pour initier une transaction.

Les utilisateurs 3SKey doivent prendre toutes les précautions possibles pour protéger physiquement leurs tokens contre tout prêt non autorisé, perte ou vol. Ils doivent également

prendre toutes les mesures nécessaires pour empêcher toute divulgation non autorisée du mot de passe du token.

Important Le token d'un utilisateur qui quitte la société ou change de rôle ne peut jamais être réassigné à un nouvel utilisateur. Ceci est en contradiction avec les directives en matière de sécurité et rend la piste d'audit des transactions effectuées avec le token difficile à suivre.

Si un utilisateur quitte la société ou change de rôle, le token doit être révoqué. Un nouveau token peut alors être assigné au remplaçant de l'utilisateur.

- **Ce que doit faire l'utilisateur 3SKey**

  En particulier, les utilisateurs 3SKey doivent s'assurer qu'ils respectent la liste non-exhaustive suivante de directives en matière de sécurité:

  - S'assurer que chaque token est associé à une personne unique et autorisée.
  - Stocker les tokens dans un endroit sûr lorsqu'ils ne sont pas nécessaires.
  - Révoquer tout token non utilisé, obsolète ou perdu.
  - Fermer le navigateur ou l'application de signature et retirer le token pour terminer la session complètement.

- **Ce que ne doit pas faire l'utilisateur 3SKey**

  L'utilisateur de 3SKey ne doit jamais:

  - Prêter les tokens à des tiers.
  - Laisser le token inséré dans un PC sans surveillance qui est utilisé pour les transactions 3SKey.
  - Laisser la session de signature dans le navigateur ou l'application de signature ouverte.
  - Noter un mot de passe ou communiquer un mot de passe à des personnes non autorisées.
  - Utiliser un mot de passe pouvant être facilement deviné.
  - Laisser quelqu'un regarder lors de la saisie du mot de passe.

Directives générales en matière de sécurité

- **Ce que doit faire l'utilisateur 3SKey**

  L'utilisateur 3SKey doit protéger les systèmes utilisés pour accéder au portail 3SKey et signer des transactions bancaires conformément aux pratiques de sécurité du secteur. Par exemple:

  - Protéger le PC de l'utilisateur 3SKey contre tout accès physique et au réseau non autorisé. Utiliser un pare-feu afin de protéger le PC du trafic Internet entrant et de tout accès non autorisé sur le réseau interne. Le pare-feu doit être à la fois une barrière physique pour protéger le trafic entrant et un pare-feu de PC local pour garantir que seuls les programmes autorisés communiquent avec l'extérieur.
  - Installer uniquement des logiciels autorisés et nécessaires sur le PC.
  - S'assurer que toutes les applications logicielles exécutées sur le PC sont mises et jour et que les correctifs sont appliqués régulièrement. Ceci inclut Windows, le navigateur Internet et des fonctionnalités supplémentaires.
  - Restreindre le trafic sortant du PC aux sites essentiels pour l'entreprise, ainsi qu'à des sites provenant de sources sûres pour les mises à jour des logiciels.
  - Utiliser des détecteurs de virus et des détecteurs de programmes malveillants pour protéger le PC des menaces telles que les virus, les vers informatiques, les enregistreurs de saisie et les chevaux de Troie.

  L'utilisateur 3SKey doit s'assurer que les utilisateurs finals du système respectent des pratiques de navigation sécurisée, telles que:

  - Réserver certains PC strictement pour accéder aux sites et aux applications avec un niveau élevé de criticité, tels que 3SKey et les autres applications Web vitales utilisées pour les transactions bancaires, et accéder à ces sites uniquement depuis ces PC réservés.

  L'utilisateur 3SKey doit appliquer les principes de gestion suivants afin de réduire les risques pour son système:

  - Établir des pratiques de gestion des utilisateurs afin de garantir que seuls des utilisateurs autorisés sont créés et restent sur le système.
  - Établir des pratiques de gestion des droits afin de garantir que l'accès aux fonctions 3SKey est accordé uniquement à des utilisateurs qui en ont besoin.
  - Lorsque des utilisateurs changent de rôle ou quittent l'entreprise, s'assurer que le client maintient une liste précise et à jour des utilisateurs autorisés.

Important Lorsqu'un utilisateur quitte la société ou change de rôle, son token doit être révoqué. Un token enregistré existant ne doit pas être transféré à un autre membre du personnel. Associer un nouvel utilisateur à un identifiant unique existant interrompt la piste d'audit et il n'existe plus de lien unique entre le token et le signataire.

- **Ce que ne doit pas faire l'utilisateur 3SKey**

  L'utilisateur 3SKey ne doit pas:

  - Naviguer sur des sites Internet suspectés d'être non sécurisés, lorsqu'il utilise le même PC pour accéder au portail 3SKey ou aux applications Web de la banque.
  - Cliquer sur des liens dans des e-mails semblant provenir de SWIFT ou d'une autre organisation, même si le lien semble parfaitement valide d'un point de vue commercial. Ce type d'attaques de hameçonnage peut conduire vers un site malveillant pouvant voler des informations ou infecter le PC.

    S'il est nécessaire d'un point de vue professionnel de visiter le site, l'utilisateur doit saisir à nouveau le lien tel qu'il apparaissait dans l'e-mail au sein du navigateur.
  - Accepter une fenêtre contextuelle demandant à l'utilisateur de télécharger et d'installer un logiciel exécutable.

4 Glossaire

Activer

Le token fourni par SWIFT contient initialement un certificat technique qui ne peut pas être utilisé pour signer des messages commerciaux. Le processus de conversion du certificat technique sur le token en un certificat métier est appelé **activation du token**.

Certificat métier

Le processus d'activation 3SKey remplace le certificat technique du token par le certificat métier. Le certificat métier est utilisé pour sécuriser toutes les transactions commerciales avec les banques.

Le certificat métier est valide pendant trois ans à partir de la date d'activation.

Certificat technique

Le certificat technique est le certificat initial stocké par SWIFT sur un token non activé qui garantit que le token a été personnalisé par SWIFT. Il fournit une piste d'audit incontestable pour la création du certificat métier associé.

Le certificat technique n'est pas accepté pour l'authentification de transactions commerciales. Le token doit d'abord être activé pour produire un certificat métier.

Le certificat technique est valide pendant cinq ans. Après l'activation, le certificat métier est valide pendant trois ans.

Remarque *Les certificats techniques issus après le 27 mai 2017 sont valides 3 ans. En 2019, les nouveaux certificats techniques seront à nouveau valides 5 ans.*

Code de sécurité

Le code de sécurité est généré au cours du processus d'activation du token.

Il est utilisé pour:

- révoquer un token perdu ou compromis
- réinitialiser un token verrouillé ou dont le mot de passe est perdu
- régénérer l'identifiant unique sur un nouveau token

Le code de sécurité est téléchargé dans un fichier. Par défaut, le nom du fichier est `code.txt`.

Vous devez conserver le code de sécurité dans un endroit sûr mais accessible. Ne stockez pas le code de sécurité sur le token 3SKey NG-FLASH lui-même, ou avec votre token.

Si vous stockez le code de sécurité sur votre PC et que vous changez de PC, n'oubliez pas de supprimer le code de sécurité de l'ancien PC et stockez-le sur le nouveau.

Identifiant unique

SWIFT crée un identifiant unique pour chaque token et le stocke dans le certificat technique sur le token non activé.

Lorsque le token est activé, l'identifiant unique est transféré sur le certificat métier. L'identifiant unique doit ensuite être enregistré auprès de la banque associée pour identifier un utilisateur spécifique comme propriétaire d'un identifiant unique spécifique.

L'identifiant unique est préservé durant le processus de renouvellement étant donné que le certificat sur le nouveau token aura le même identifiant unique que le certificat précédent sur l'ancien token.

Si le token est perdu ou compromis, il est possible de régénérer l'identifiant unique en le transférant sur un autre token. Pour plus d'informations, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

Régénération

Vous pouvez utiliser le processus de régénération si un token a été perdu, endommagé, si le certificat a été révoqué ou a expiré, ou encore si un token se trouve en période de renouvellement (90 jours avant expiration) et se verrouille.

Le processus de régénération vous permet de réutiliser l'identifiant unique de l'ancien token, et de l'associer à un autre token.

Pour plus d'informations, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

Règle en matière de code PIN pour la liste d'utilisateurs

Le gestionnaire de la liste d'utilisateurs sélectionne une règle en matière de code PIN pour la liste d'utilisateurs. Cette règle s'applique au token lors de sa nouvelle activation ou lors de son renouvellement, de sa régénération ou de sa réinitialisation.

Règle en matière de code PIN pour le token

Il s'agit du niveau de règle en matière de code PIN défini pour le token au moment de son activation ou de sa réinitialisation. Les règles en matière de code PIN pour le token et la liste d'utilisateurs peuvent avoir différentes valeurs si le gestionnaire de la liste d'utilisateurs modifie le niveau des règles après que les règles précédentes ont été appliquées au token.

Réinitialisation

Les utilisateurs d'entreprise peuvent réinitialiser leur token dont le mot de passe est perdu ou lorsque le token est verrouillé après saisie de 5 mots de passe incorrects. Le processus de réinitialisation permet aux utilisateurs de ré-initialiser leur token avec leur identifiant unique.

Pour plus d'informations, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

Renouvellement

Les tokens 3SKey comprennent un certificat métier qui reste valide 3 ans à partir de la date d'activation du token. Par exemple, un token activé le 1er janvier 2016 comprend un certificat qui expire le 1er janvier 2019.

SWIFT recommande aux utilisateurs de renouveler les certificats sur un nouveau token au moins 2 mois avant la date d'expiration du certificat.

Pour plus d'informations, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

Révocation

La révocation d'un token est nécessaire si vous avez perdu le token ou si vous suspectez qu'il a été compromis. La révocation du token rend non valides tous les certificats associés à votre identifiant unique.

Vous pouvez régénérer l'identifiant unique d'un token révoqué sur un nouveau token, mais le token révoqué lui-même ne peut plus être utilisé.

Pour plus d'informations, reportez-vous au Guide d'utilisation du portail 3SKey pour les entreprises.

Rôles

Les rôles déterminent les fonctions qu'un utilisateur du service 3SKey peut effectuer sur le portail 3SKey. La plupart des utilisateurs ont le rôle `user`, mais des administrateurs ont également le rôle `admin`.

Les utilisateurs avec le rôle `user` ont accès aux fonctions suivantes:

- Utiliser le certificat sur le token pour authentifier ou signer des transactions avec une banque.
- Modifier le mot de passe du token.
- Générer un nouveau code de sécurité.
- Révoquer le certificat sur le token.
- Effectuer la régénération du certificat sur un token. Pour ce faire, un second token préparé par un administrateur en vue d'une régénération est nécessaire.
- Effectuer la réinitialisation du token. Pour cela, un administrateur doit avoir préparé le token en vue d'une réinitialisation.
- Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la période de validité).
- Renouveler le certificat sur un nouveau token avant son expiration (au bout de trois ans).

Les utilisateurs avec le rôle `admin` ont accès à toutes les fonctions `user`, ainsi qu'aux fonctions suivantes:

- Configurer et assurer la maintenance d'une **liste d'utilisateurs** contenant des tokens avec le rôle `admin` et des tokens avec le rôle `user`.
- Afficher les tokens et leur statut dans la **liste d'utilisateurs**.
- Révoquer les tokens dans la **liste d'utilisateurs**.
- Configurer un token pour la régénération d'un identifiant unique (rôle `user` ou rôle `admin`).
- Réinitialiser un token **non activé**.
- Configurer en vue d'une réinitialisation un token **activé** verrouillé ou dont le mot de passe est perdu.

Utilisateur

Un utilisateur 3SKey est une personne individuelle associée à un identifiant unique. L'identifiant unique se trouve dans le certificat stocké sur un token spécifique que l'utilisateur utilise pour signer des transactions avec une ou plusieurs banques.

5 Assistance 3SKey

Assistance pour les clients 3SKey

Cette section décrit les types d'assistance fournis par SWIFT aux utilisateurs 3SKey.

SWIFT est l'unique point de contact pour reporter tous les problèmes et requêtes relatifs à l'installation des tokens 3SKey, à l'activation et à la gestion sur le portail 3SKey.

Pour toute autre question, les clients d'entreprises sont priés de contacter leur banque.

Procédez par étapes pour résoudre votre problème:

1. Consultez le Guide de dépannage 3SKey.

   Si le problème n'est pas résolu, passez à l'étape suivante.

2. Consultez les liens vers l'aide sur le portail.

   Pour accéder à l'assistance 3SKey, accédez à **www.3skey.com**, cliquez sur **Aide**.

   La liste des sujets traités dans l'aide s'affiche.

   Si le problème n'est pas résolu, passez à l'étape suivante.

3. Consultez le tableau ci-dessous pour identifier le point de contact le plus approprié.

Type de problème	Contact = SWIFT 3SKey	Contact = votre banque
Installation du logiciel du token	X	
Connexion au portail 3SKey	X	
Gestion du token sur le portail 3SKey	X	
Commande de tokens		X
Mot de passe, après activation	X	
Mot de passe, initial pour les nouveaux tokens		X
Enregistrement du token auprès de l'application bancaire		X
Transactions rejetées		X
Application de signature/ trésorerie		X

Si le point de contact le plus approprié est une entité autre que SWIFT, veuillez contacter cette entité.

Si le point de contact le plus approprié est SWIFT, passez à l'étape suivante.

4. Contactez l'assistance 3SKey par e-mail (reportez-vous à la section **Assistance par e-mail** ci-dessous).

   Si le problème n'est pas résolu, passez à l'étape suivante.

5. Contactez un analyste du service d'assistance (reportez-vous à la section **Assistance téléphonique** ci-dessous).

Assistance par e-mail

Si vous n'avez pas été en mesure de résoudre votre problème à l'aide du Guide de dépannage 3SKey ou de l'aide 3SKey, envoyez un e-mail à 3skey.support@swift.com.

Veuillez inclure les informations suivantes dans le message électronique. Un analyste du service d'assistance étudiera votre problème et vous contactera.

Remarque *L'analyste vous fournira un numéro de dossier qui servira de référence si vous devez contacter l'assistance téléphonique.*

1. Coordonnées
   - Prénom et nom
   - Adresse e-mail
   - Numéro de téléphone
   - Numéro de téléphone mobile
   - Nom de l'entreprise
   - Description claire du problème
   - Numéro de série indiqué sur le token
2. Quelle opération effectuez-vous sur le portail 3SKey?
   - Installation du logiciel du token
   - Définition des administrateurs pour votre organisation
   - Connexion
   - Activation
   - Régénération
   - Révocation
   - Réinitialisation
   - Renouvellement
3. Quel message d'erreur avez-vous reçu?
4. Quel est votre rôle sur 3SKey et êtes-vous le propriétaire du token?

Important Veuillez zipper et joindre les fichiers journaux d'installation à l'e-mail.

Voici les différents emplacements par défaut où sont disponibles les fichiers journaux en fonction de la version du programme d'installation que vous utilisez:

- 3SKey_token_install.exe (mars 2013)
  - **C:\Program Files\Swift\Swift Token Client\logs** (système 32 bits)
  - **C:\Program Files (x86)\Swift\Swift Token Client\logs** (système 64 bits)
- SwiftTokenClient-2.0x64wrapper.exe ou SwiftTokenClient-2.0x32wrapper.exe (février 2012)
  - **C:\Programmes\Swift\Swift Token Client 2.0\logs**
- 3SKeyinstall.exe (avant février 2012)
  - **C:\Programmes\3SKey\logs**

Si vous n'avez pas encore installé le logiciel 3SKey, veuillez fournir les détails de votre système d'exploitation. Ces détails comprennent la version et le service pack de Windows, la version d'Internet Explorer ainsi que la version de Java que vous utilisez.

Assistance téléphonique

Si votre question n'a pu être résolue par les moyens décrits ci-avant, vous pouvez contacter un analyste du service d'assistance par téléphone. Nos analystes du service d'assistance sont disponibles pour vous aider pendant les heures de bureau, du lundi au vendredi.

Asie-Pacifique:	**+33-1 57 32 35 36** de 09h00 à 12h00 et de 14h00 à 17h00 CET (GMT+2)
Europe, Moyen-Orient et Afrique:	**+33-1 57 32 35 36** de 09h00 à 12h00 et de 14h00 à 17h00 CET (GMT+2)
Amériques:	**+1-540 727 1685** de 08h00 à 11h00 EST (GMT-4). En dehors de ces heures, vous pouvez laisser un message vocal ou, de préférence, envoyer un e-mail à l'adresse 3skey.support@swift.com et demander d'être contacté par un analyste du service d'assistance 3SKey.

Mentions légales