3SKey

# Guide d'utilisation du portail pour les entreprises

Ce document décrit les fonctions du portail 3SKey.

20 novembre 2020

# Table des matières

# Préface

## À propos de ce manuel

Ce document décrit les fonctions du portail 3SKey.

## Modifications importantes

Le tableau suivant répertorie les modifications importantes apportées au *Guide d'utilisation du portail 3SKey pour les entreprises*. Ce tableau ne comprend pas les différentes modifications qui ont été apportées.

| Nouvelles informations | Emplacement |
|---|---|
| L'écran de sélection de la règle en matière de code PIN a été déplacé dans la procédure pour activer le premier administrateur. | Gérer les utilisateurs<br>Activer un token |

## Informations associées

Guide d'installation du logiciel du token 3SKey

Guide d'installation de SConnect pour 3SKey

Mise en route de 3SKey pour les entreprises

# 1 Présentation du portail de clé de signature sécurisée SWIFT (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.

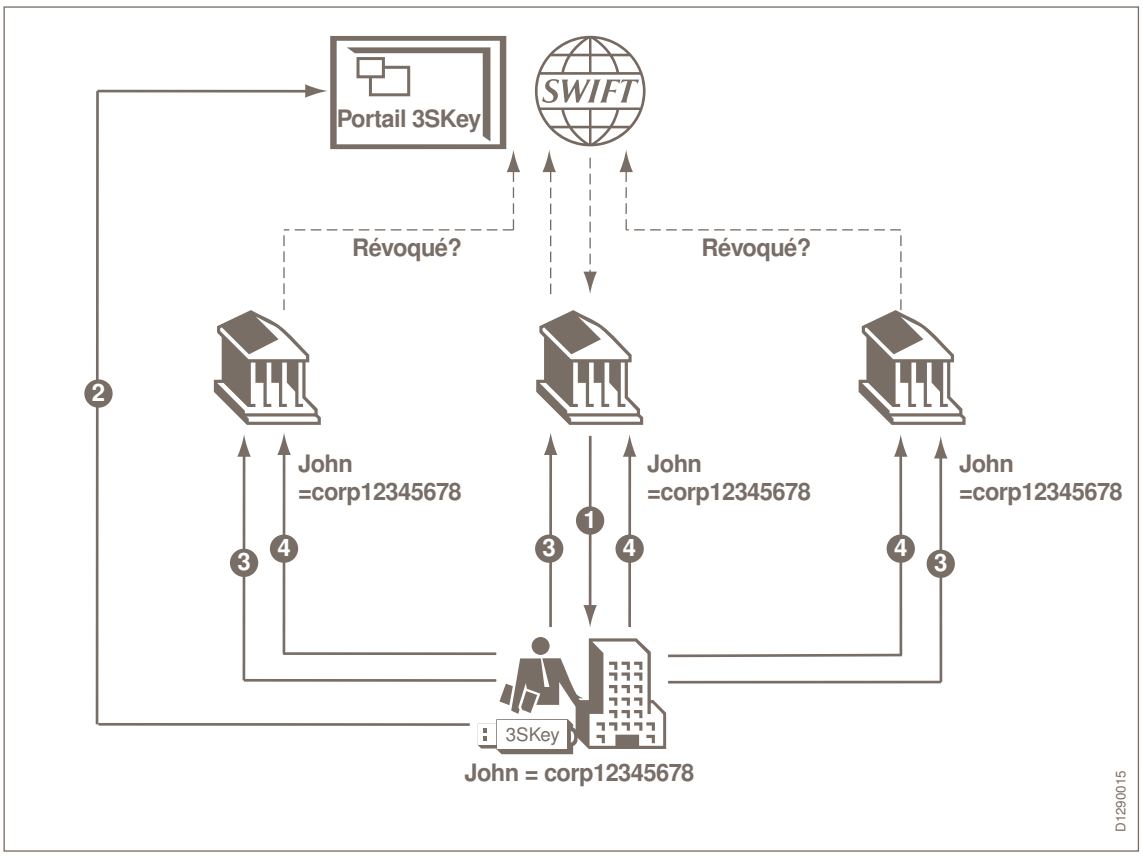
### Présentation

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, les tokens 3SKey et le Kit du développeur 3SKey.

- **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 Fonctions du portail 3SKey

Les utilisateurs accèdent au portail 3SKey pour activer et gérer le certificat stocké sur le token. Les administrateurs disposent de privilèges supplémentaires pour gérer le groupe d'utilisateurs. Le portail 3SKey est utilisé uniquement pour gérer les tokens 3SKey et leurs propriétaires. Les fonctions du portail 3SKey n'ont aucun impact sur le portail de signature.

Pour vous connecter au portail 3SKey vous avez besoin du logiciel 3SKey et de SConnect. Pour plus d'informations, reportez-vous au Guide d'installation du logiciel du token 3SKey et au Guide d'installation de SConnect pour 3SKey.

## 1.2.1 Gérer le groupe d'utilisateurs

Les pages **Gérer le groupe d'utilisateurs** sont disponibles uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

### Créer un groupe d'utilisateurs

Si le portail 3SKey détecte que le token avec lequel vous vous êtes connecté n'appartient pas à un groupe d'utilisateurs, il affiche un écran d'information et vous invite à créer un groupe d'utilisateurs pour votre organisation, avec deux administrateurs.

### Ajouter un utilisateur

Vous pouvez utiliser la page **Ajouter un utilisateur** pour ajouter de nouveaux utilisateurs à un groupe d'utilisateurs et spécifier leur rôle.

Le groupe d'utilisateurs est un ensemble de tokens 3SKey appartenant à une organisation spécifique. Un groupe d'utilisateurs dispose de deux administrateurs, ou plus, qui sont responsables d'ajouter des utilisateurs au groupe.

### Gérer le groupe d'utilisateurs

Vous pouvez utiliser cette page pour afficher et modifier les utilisateurs dans votre groupe d'utilisateurs ou modifier la règle en matière de code PIN du groupe.

### Gérer l'adresse e-mail

Vous pouvez utiliser la page **Gérer l'adresse e-mail** pour enregistrer, modifier ou supprimer votre adresse e-mail. Il s'agit d'un moyen utile pour connaître les informations opérationnelles importantes sur le service 3SKey.

### Informations associées

Groupes d'utilisateurs 3SKey à la page 9
Préparer un nouveau token utilisateur (pour les administrateurs) à la page 18
Gérer les utilisateurs (pour les administrateurs) à la page 21
Gérer votre adresse e-mail (pour les administrateurs) à la page 25

## 1.2.2 Gérer les tokens

Utilisez le portail pour gérer le certificat sur le token. Tous les propriétaires de tokens utilisent le portail pour activer un token, gérer le mot de passe du token or révoquer un token perdu.

### Gérer le certificat sur le token

- Activer un token
- Renouveler un token
- Révoquer un token
- Régénérer un token
- Réinitialiser un token

### Autres fonctions du token

- Modifier le mot de passe du token
- Générer le code de sécurité
- Informations portées par la clé

### Activer le token

Les nouveaux tokens 3SKey contiennent un certificat technique qui n'est pas valide pour les opérations commerciales. Le processus d'activation de 3SKey remplace le certificat technique sur le token par un **certificat métier**. Ce **certificat métier** est utilisé pour sécuriser toutes les transactions commerciales avec les banques.

### Renouveler un token

Le certificat métier sur le token 3SKey est valide 3 ans après activation. Vous pouvez utiliser l'option **Renouveler** sur le portail pour renouveler le certificat métier sur un nouveau token dans les 3 mois qui précèdent sa date d'expiration.

**Remarque** *La durée de validité du certificat métier a été ajustée à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Pour plus d'informations, reportez-vous à l'entrée Durée de validité du certificat dans le glossaire.*

### Révoquer un token

Si un token est perdu ou compromis ou n'est plus nécessaire, le certificat associé au token peut être révoqué. Pour ce faire, il existe trois moyens:

- Si vous possédez toujours le token que vous souhaitez révoquer, et qu'il a été activé, vous pouvez procéder vous-même à la révocation.
- Si vous ne disposez pas du token activé que vous souhaitez révoquer ni de son mot de passe, vous pouvez demander à un administrateur d'effectuer la révocation pour votre compte.
- Si vous avez un token non activé de réserve, vous pouvez révoquer votre token activé. Toutefois, vous devrez également présenter le code de sécurité associé au token que vous souhaitez révoquer.

  **Remarque** *Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est* `code.txt`.

Lorsque le certificat est révoqué, il est ajouté à une liste de certificats révoqués. Les banques peuvent consulter cette liste avant d'autoriser une transaction: lorsqu'elles trouvent un certificat dans la liste de révocation des certificats, elles ne considèrent plus le certificat comme un certificat de confiance.

**Remarque** *Les règles de vérification de la liste de révocation des certificats varie selon la banque. Pour savoir à quel moment elle consulte la liste, et à quelle fréquence elle la met à jour, veuillez contacter votre banque.*

### Configurer en vue d'une régénération

Vous pouvez utiliser la page **Configurer en vue d'une régénération** pour préparer la régénération d'un token perdu ou compromis. Cette page vous permet d'attribuer un token non activé en remplacement du token d'origine.

### Régénérer un token

Si un token est perdu, révoqué, endommagé ou a expiré, vous pouvez régénérer l'identifiant unique sur un token non activé de réserve (fourni par votre banque). En conservant le même identifiant unique, vous n'avez pas à vous enregistrer à nouveau auprès des banques avec lesquelles vous êtes en relation.

L'administrateur doit configurer le nouveau token en vue d'une régénération et le rendre au propriétaire du token de réserve qui doit l'activer. Ce processus nécessite également que vous disposiez du code de sécurité du token d'origine.

**Remarque** *Si vous décidez de ne pas régénérer un certificat révoqué, SWIFT vous conseille de contacter les parties associées (banques) et de les informer qu'elles ne doivent plus considérer ce certificat spécifique comme un certificat de confiance.*

### Réinitialiser un token

Vous pouvez utiliser cette fonctionnalité pour réutiliser un token qui est verrouillé ou dont le mot de passe est perdu. Au préalable, l'administrateur doit préparer le token pour la réinitialisation. Ensuite, l'utilisateur du token doit finaliser la réinitialisation.

### Modifier le mot de passe du token

Vous pouvez modifier le mot de passe protégeant le contenu du token. Le mot de passe doit se conformer aux exigences de complexité minimum définies pour la liste d'utilisateurs par son gestionnaire.

### Générer le code de sécurité

Un code de sécurité est associé au token. Ce code est requis s'il est nécessaire de révoquer le certificat sur le token ou de régénérer le certificat en le transférant sur un nouveau token. Le code de sécurité ne doit pas être communiqué à des tiers.

Si l'ancien code a été perdu ou compromis, vous pouvez utiliser l'option **Générer le code de sécurité**.

### Informations portées par la clé

La page **Informations portées par la clé** affiche des informations détaillées sur le token et le certificat qu'il contient.

### Informations associées

Activer un token à la page 26
Renouveler un token à la page 31
Réinitialiser un token à la page 40
Révoquer un token à la page 41
Régénérer un token à la page 44
Modifier le mot de passe à la page 49
Générer le code de sécurité à la page 48
Informations portées par la clé - détails du certificat et du token à la page 51

## 1.3 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?

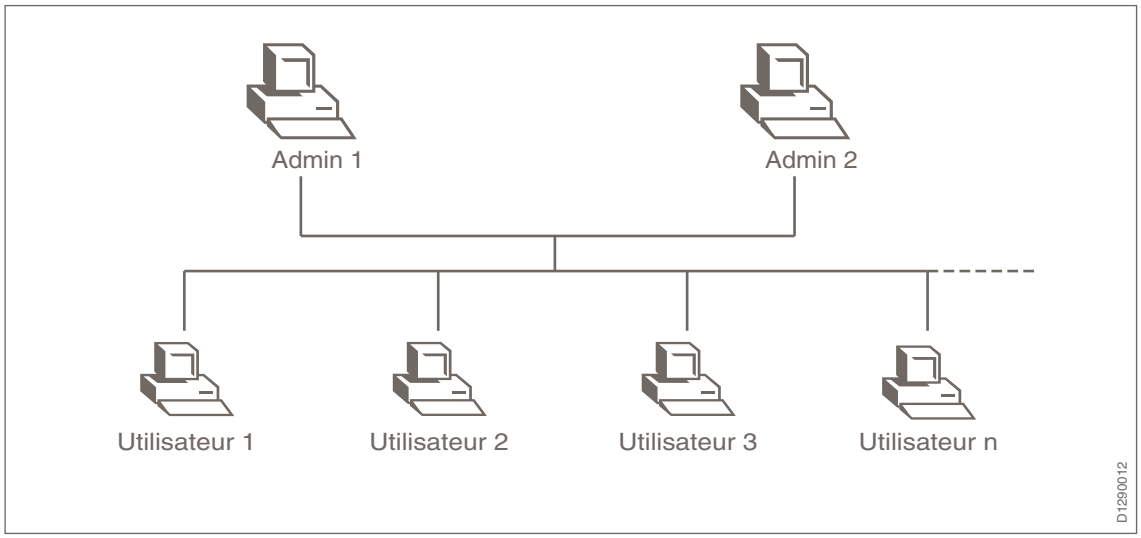
Le groupe d'utilisateurs est une aide pour gérer les tokens de l'organisation: il n'a aucun impact sur la capacité du token à signer des transactions, car l'application de signature ne connaît pas le groupe auquel le token appartient. Il est possible de signer une transaction avec un token appartenant 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 à la page 55.

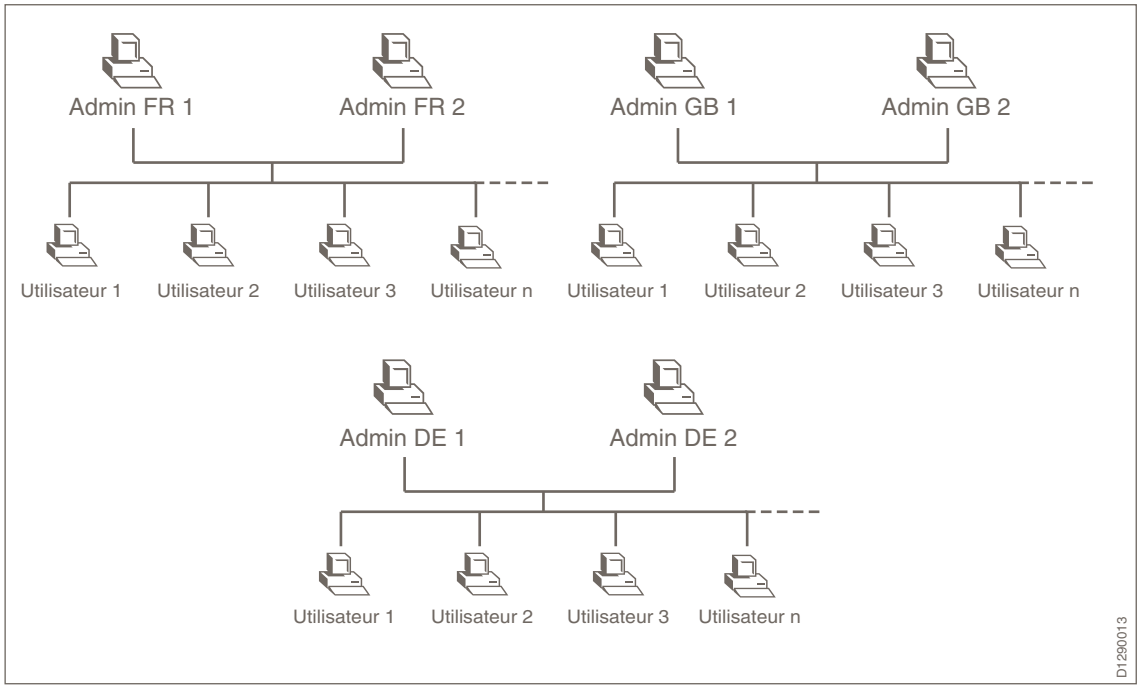
Un token utilisateur 3SKey ne peut pas être activé s'il n'appartient pas à un groupe d'utilisateurs. Un token ne peut appartenir qu'à un seul groupe d'utilisateurs.

**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. Lorsque le token a été activé, il ne peut être déplacé dans un autre groupe. La migration d'un utilisateur d'un groupe à un autre s'effectue en activant un nouveau token dans le nouveau groupe et en révoquant le token du premier groupe.*

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. Des fonctions d'export, de filtre et de tri sont disponibles sur la page **Gérer les utilisateurs** du portail.

### 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 à la section Créer un groupe d'utilisateurs (pour les administrateurs) à la page 17.

Si votre organisation a besoin d'un deuxième 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.

## 1.4 Introduction de 3SKey dans votre organisation

Le processus d'introduction de 3SKey dans votre organisation consiste en les étapes suivantes:

1. **Installer le logiciel du token**

   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.

   Pour plus d'informations, reportez-vous au Guide d'installation du logiciel du token 3SKey.

2. **Créer le groupe d'utilisateurs**

   Tous les tokens 3SKey doivent appartenir à un groupe d'utilisateurs.

   Lorsqu'une entreprise reçoit un lot de tokens de la part de sa banque, un administrateur configure le groupe d'utilisateurs en activant au minimum deux tokens avec des droits d'administrateur. Pour des informations complémentaires, reportez-vous à Créer un groupe d'utilisateurs (pour les administrateurs) à la page 17.

3. **Ajouter des utilisateurs**

   Une fois que les tokens administrateurs ont été activés, l'administrateur ajoute des tokens non activés au groupe d'utilisateurs. Lorsqu'il est connecté au portail 3SKey, l'administrateur insère chaque token non activé à tour de rôle dans un second port USB, et l'ajoute au groupe d'utilisateurs. Pour des informations complémentaires, reportez-vous à Préparer un nouveau token utilisateur (pour les administrateurs) à la page 18.

**Remarque** *Le token administrateur et le token qui est ajouté doivent être tous les deux branchés dans deux ports USB en même temps. Vous devez par conséquent ajouter les tokens au groupe d'utilisateurs avant de les distribuer à leurs propriétaires.*

Un token identifie son propriétaire comme étant un utilisateur 3SKey ou un administrateur 3SKey. Pour des informations complémentaires, reportez-vous à Rôles à la page 55.

L'administrateur répète cette opération pour tous les tokens devant être ajoutés au groupe d'utilisateurs à ce moment-là. Des tokens supplémentaires peuvent être ajoutés au groupe à tout moment.

4. **Distribuer les tokens aux utilisateurs**

   L'administrateur distribue les tokens utilisateurs non activés qui appartiennent maintenant au groupe d'utilisateurs aux administrateurs ou aux utilisateurs de l'entreprise qui utiliseront les tokens.

   Le propriétaire du token a besoin des éléments suivants:

   - Le token 3SKey.
   - Les instructions à l'attention de l'utilisateur 3SKey.
   - L'identifiant unique du token (`corp99999999`). L'utilisateur doit sélectionner l'identifiant unique dans une liste déroulante lorsqu'il se connecte au portail 3SKey.
   - Le mot de passe par défaut du token.
   - Le Guide d'installation du logiciel du token 3SKey, si le logiciel du token n'est pas encore installé sur le PC de l'utilisateur.

5. **Activer les tokens**

   Le propriétaire du token (administrateur ou utilisateur de l'entreprise) active le token en l'insérant dans un port USB sur un PC sur lequel le logiciel du token 3SKey est installé, et se connecte au portail 3SKey.

   Lorsque le propriétaire se connecte avec le token non activé 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.

   Le portail 3SKey génère un certificat métier sur le token, puis génère un code de sécurité personnel qui doit être conservé dans un lieu sûr par l'utilisateur.

   Le token peut alors être enregistré auprès d'une banque et être utilisé pour authentifier des transactions.

   Pour des informations complémentaires, reportez-vous à Activer un token à la page 26.

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

Si un certificat est déjà déclaré à la banque mais que le token est perdu avant d'être activé, il est impossible de régénérer le token et le contrat doit être modifié.

# 2 Conditions préalables à l'installation du logiciel du token

Les clients doivent installer le logiciel du token et SConnect afin de configurer leur système pour 3SKey.

**Exigences de configuration minimum**

| Type | Description |
|---|---|
| Système d'exploitation | Pour les systèmes d'exploitation sur les ordinateurs personnels, SWIFT recommande un PC exécutant Windows 8.1 ou Windows 10 ou une version ultérieure (32 bits ou 64 bits). Pour les systèmes d'exploitation sur les serveurs, SWIFT recommande Windows Server 2012 ou une version ultérieure (32 bits ou 64 bits). |

**Important** L'installation du logiciel du token nécessite des droits d'administrateur.

### Vérifier la configuration du système

Vous pouvez vérifier la configuration de votre système en effectuant un test automatique sous le menu **Démarrer** > **Tous les programmes** > **Swift Token Client**. Les résultats apparaissent après quelques secondes. Effectuer le test automatique nécessite des droits d'administrateur.

**Remarque** *Le test automatique n'est disponible qu'après installation du logiciel du token.*

# 3 Installation de SConnect

SConnect est une extension de navigateur qui permet à une application bancaire Web de communiquer avec les tokens directement dans le navigateur en utilisant JavaScript.

SConnect est nécessaire en plus du logiciel du token 3SKey.

SConnect peut être installé à partir de la page d'installation du logiciel 3SKey sur le site Web 3SKey. SConnect peut également être installé en se connectant au portail 3SKey directement.

Pour plus d'informations, reportez-vous à la page SConnect de l'aide sur le site Web 3SKey et au Guide d'installation de SConnect pour 3SKey.

**Remarque** *Certaines applications tierces ne sont peut-être pas encore passées de Java à SConnect. Veuillez contacter les fournisseurs de vos applications bancaires ou applications de signature pour plus d'informations. Si vos applications n'utilisent pas encore SConnect, vous devez installer Java. Java et SConnect peuvent être installés ensemble sur le même système. Le portail 3SKey utilisera SConnect si Java et SConnect sont installés.*

### Compatibilité du navigateur

SConnect fonctionne avec tous les navigateurs majeurs en ce compris Internet Explorer, Firefox, et Chrome. Toutefois, chaque application à laquelle vous accédez en utilisant votre token peut avoir des exigences de navigateur différentes. Chaque navigateur que vous utilisez avec votre token pour accéder à une application nécessite l'installation de l'extension de navigateur SConnect.

### Informations associées

Page d'aide SConnect
Guide d'installation de SConnect pour 3SKey

# 4 Connexion

L'accès au portail 3SKey nécessite un token, un mot de passe et l'installation de SConnect et du logiciel du token.

### Avant de commencer

La première fois que vous vous connectez avec le token, vous devez utiliser le mot de passe accompagnant le token. Si vous ne disposez pas de ce mot de passe par défaut, contactez votre administrateur 3SKey. Si la banque ayant fourni le token n'a pas envoyé le mot de passe par défaut, l'administrateur doit contacter la banque.

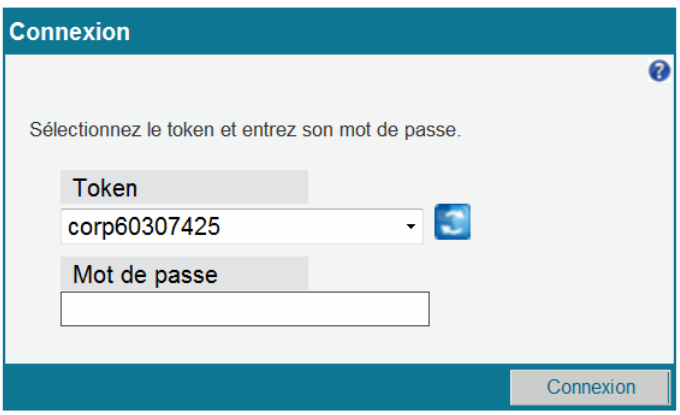
### Procédure

1. Insérez votre token dans un port USB.
2. Ouvrez Internet Explorer et accédez au site http://www.3skey.com.
3. Cliquez sur Connexion.

   Dans une nouvelle session de navigateur, le portail vous invite deux fois à entrer le mot de passe du token:

   - pour ouvrir la session SSL (étapes 4-6 ci-dessous)
   - pour la connexion au portail 3SKey (étapes 8-9 ci-dessous)
4. Si plusieurs certificats personnels sont disponibles dans le navigateur, vous devez en sélectionner un. Le certificat 3SKey est identifié par son identifiant unique, au format corp12345678, et est émis par SWIFT ou par l'AC 3SKey.

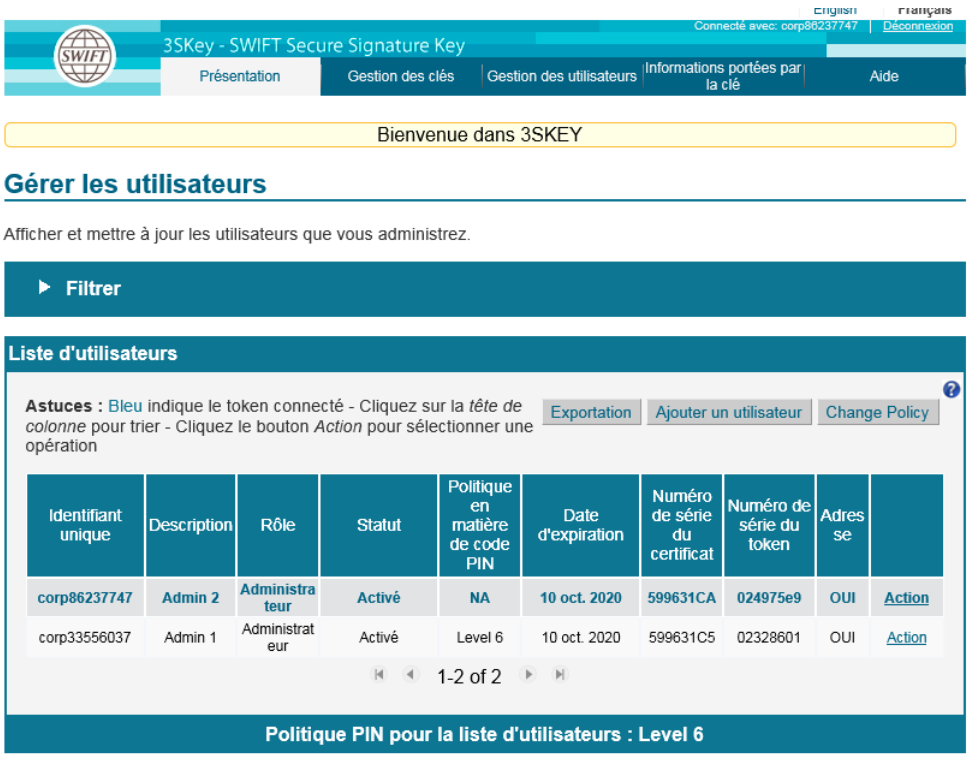
   La liste contient tous les tokens actuellement connectés à votre PC, et peut également inclure les certificats personnels ayant été installés sur votre système par d'autres produits que 3SKey. Si vous ne voyez pas le certificat 3SKey, faites dérouler la liste ou cliquez sur Autres choix en fonction de votre navigateur.
5. Cliquez sur OK.
6. Saisissez le mot de passe du token dans la fenêtre **Token logon** (Se connecter au token) et cliquez sur OK pour vous connecter au site Web sécurisé.
7. Si SConnect n'est pas encore installé sur votre navigateur, il sera installé automatiquement, veuillez suivre la procédure d'installation à l'écran.
8. Sélectionnez l'identifiant unique du token dans la liste déroulante **Token** (si plusieurs tokens sont connectés au PC).



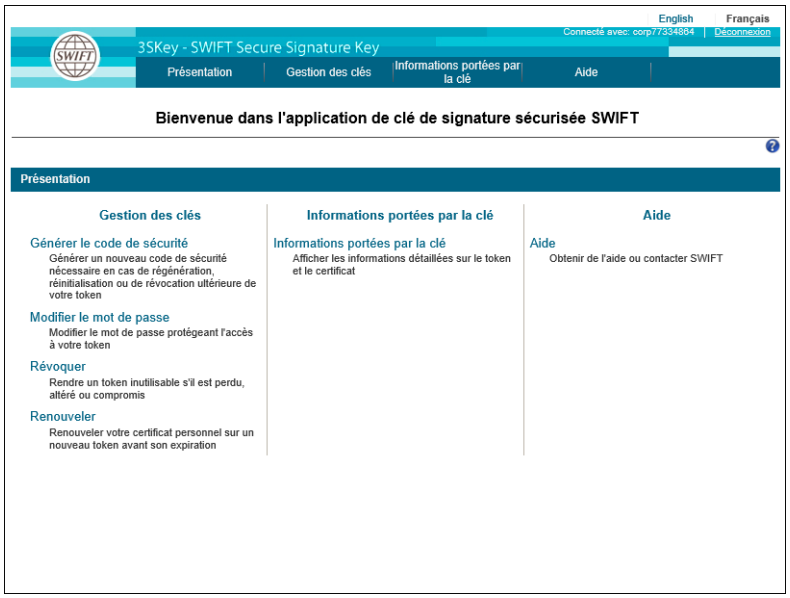

Pour afficher tous les tokens ayant été insérés, cliquez sur l'icône pour rafraîchir .

9. Saisissez le mot de passe du token et cliquez sur Connexion.

Si vous avez le rôle `admin`, la page suivante apparaît.




Si vous avez le rôle `user`, la page suivante apparaît.



# 5 Créer un groupe d'utilisateurs (pour les administrateurs)

Si le portail 3SKey détecte que le token avec lequel vous vous êtes connecté n'appartient pas à un groupe d'utilisateurs, il affiche un écran d'information et vous invite à créer un groupe d'utilisateurs pour votre organisation, avec deux administrateurs.

### Avant de commencer

La création du groupe d'utilisateurs n'est pas terminée tant que vous n'avez pas créé les deux administrateurs. Vous avez par conséquent besoin de deux tokens non activés et de deux ports USB libres.

### À propos de cette tâche

La première connexion avec un token non activé qui n'appartient pas à un groupe d'utilisateurs nécessite l'insertion d'un second token avant de poursuivre l'activation. La création du groupe d'utilisateurs nécessite 2 tokens administrateurs. Vous pouvez ajouter des tokens administrateurs supplémentaires ultérieurement. Les tokens administrateurs sont pareils aux tokens utilisateurs mais disposent de privilèges supplémentaires sur le portail 3SKey pour déverrouiller et révoquer les tokens.

### Procédure

1. Acceptez les **Conditions générales**. Elles n'apparaissent qu'une seule fois lors de votre première connexion.
2. Confirmez que vous êtres l'administrateur.
3. Sans retirer le premier token, insérez un second token **non activé**. Entrez le mot de passe par défaut du token et cliquez ensuite sur Suivant.
4. Retirez le second token administrateur du port USB, **sans retirer le premier token administrateur**. Transmettez le token, le mot de passe par défaut du token ainsi que les *Instructions à l'attention de l'administrateur 3SKey* à l'administrateur.
5. Cliquez sur Suivant et le portail continue automatiquement avec l'activation du premier administrateur.

### Informations associées

Activer un token à la page 26
Instructions à l'attention de l'administrateur 3SKey

# 6 Préparer un nouveau token utilisateur (pour les administrateurs)

Tous les tokens utilisateurs doivent appartenir à un groupe qui inclut les administrateurs. Un administrateur doit tout d'abord ajouter un token utilisateur à la liste d'utilisateurs que gère l'administrateur. Ceci nécessite la connexion au portail avec un token ayant le rôle `admin` et l'insertion d'un nouveau token `non activé` sur la même machine.

## Présentation

Vous pouvez utiliser cette page pour ajouter de nouveaux utilisateurs à la liste d'utilisateurs que vous gérez et spécifier leur rôle. Les utilisateurs sont identifiés par l'identifiant unique sur le token qu'ils utiliseront.

Pour ce faire, il vous sera demandé de vous connecter avec un token `admin`. Le processus d'ajout d'un utilisateur nécessite d'insérer un nouveau token dans le port USB.

Il est important que les deux tokens administrateurs soient activés avant de commencer à ajouter des utilisateurs.

---

**Important** Insérez un nouveau token dans un deuxième port USB mais ne retirez pas le token `admin` avec lequel vous vous êtes connecté au portail 3SKey.

---

## Écran

Si vous êtes un administrateur 3SKey, vous pouvez ajouter des utilisateurs à partir de la page **Gérer les utilisateurs** > Ajouter un utilisateur ou à partir de la page **Présentation** en utilisant **Gestion des utilisateurs** > **Ajouter un utilisateur**.

---

**Important** Utilisez la fonction **Ajouter un utilisateur** pour ajouter un token non activé à la liste d'utilisateurs. Le token peut ensuite être assigné à un nouvel utilisateur, gardé comme token de réserve ou utilisé dans une procédure de régénération. Une fois que le token a été activé et enregistré auprès de la banque, il ne peut plus être réassigné d'un utilisateur à l'autre. Pour plus d'informations, reportez-vous à https://www2.swift.com/3skey/fr/help/reassign_token.html

---

## Champs

L'écran **Ajouter un utilisateur** contient les champs suivants:

**Token** Sélectionnez l'identifiant unique du nouveau token dans la liste déroulante.

Si vous ne voyez pas l'identifiant unique correct, cliquez sur l'icône pour rafraîchir

**Mot de passe** Indiquez le mot de passe fourni avec le nouveau token.

**Description** Vous pouvez utiliser le champ **Description** pour spécifier un nom avec lequel identifier l'identifiant unique, par exemple le rôle de l'utilisateur auquel il a été attribué, ou **Token de réserve**.

La description est utilisée uniquement au sein de votre organisation pour gérer les tokens sur le portail 3SKey. Elle n'a aucune incidence sur l'utilisation du token pour signer des transactions et il n'est pas nécessaire de communiquer la description à la banque.

Vous pouvez utiliser les caractères suivants pour la description:

`A-Z`

`a-z`

`0-9`

`_ - ,` et espace

Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple), ni de signes de ponctuation exceptés ceux qui sont répertoriés.

**Rôle**

Le rôle attribué à un identifiant unique détermine les fonctions auxquelles un utilisateur peut accéder lorsqu'il est connecté avec cet identifiant unique.

Par défaut, les identifiants uniques sont ajoutés avec le rôle `user` standard. Vous pouvez également créer un administrateur en sélectionnant `admin` dans la liste déroulante.

- Un token avec le rôle `user` donne 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.
  - Procéder à la réinitialisation d'un token configuré en vue d'une réinitialisation par un administrateur.
  - Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la période de validité).
  - Renouveler le token avant son expiration.
- Un token avec le rôle `admin` donne accès aux mêmes fonctions qu'un token avec le rôle `user`. Ces fonctions sont identiques pour les deux types d'utilisateurs.

  De plus, les tokens avec le rôle `admin` donnent accès aux fonctions suivantes:
  - Configurer et assurer la maintenance de la liste **Gérer les utilisateurs** qui contient les tokens avec le rôle `admin` et les tokens avec le rôle `user`.
  - Afficher les tokens de la liste et leur statut.
  - Révoquer les tokens des utilisateurs dans la liste.
  - Configurer un token pour la régénération d'un identifiant unique (rôle `user` ou rôle `admin`).
  - Configurer en vue d'une réinitialisation un token verrouillé ou dont le mot de passe est perdu.

### Finaliser l'ajout du token

Lorsque tous les champs sont renseignés correctement, cliquez sur Ajouter.

Le portail 3SKey confirme que le token a été ajouté à la liste **Gérer les utilisateurs**.

Retirez le token que vous avez ajouté du port USB.

- Si d'autres tokens doivent être ajoutés, cliquez sur Ajouter un autre.
- Lorsque vous avez fini d'ajouter tous les tokens, cliquez sur Terminer.

# 7 Gérer les utilisateurs (pour les administrateurs)

Utilisez cette page pour afficher les détails d'un utilisateur au sein de votre groupe et effectuer différentes actions sur un token, comme révoquer un token ou changer les rôles du token. La page **Gérer les utilisateurs** est disponible uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

### Gérer les utilisateurs

Vous pouvez utiliser la page **Gérer les utilisateurs** pour afficher les utilisateurs dans votre groupe d'utilisateurs ainsi que les détails de leurs certificats. Cliquez sur **Action** pour obtenir une liste des différentes fonctions disponibles sur un token.

### Champs

La page **Gérer les utilisateurs** contient les champs suivants:

**Identifiant unique** Identifiant unique du token.

**Description** Nom défini par l'utilisateur pour identifier l'identifiant unique. La description est utilisée uniquement au sein de votre organisation pour gérer les tokens sur le portail 3SKey.

Vous pouvez utiliser les caractères suivants pour la description:

`A-Z`

`a-z`

`0-9`

`_ - ,` et espace

Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple), ni de signes de ponctuation exceptés ceux qui sont répertoriés.

**Important** Une fois qu'un token a été activé et enregistré auprès d'une banque, changer simplement la description ne permet pas de réassigner un token à un autre utilisateur. Pour plus d'informations, reportez-vous à https://www2.swift.com/3skey/fr/help/reassign_token.html.

**Rôle** Utilisez la liste déroulante pour affecter à l'utilisateur le rôle `user` standard ou le rôle `admin`.

- Les utilisateurs avec 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.
- Procéder à la réinitialisation d'un token configuré en vue d'une réinitialisation par un administrateur.
- Afficher les informations portées par la clé stockées sur le token (par exemple, l'identifiant unique et la période de validité).
- Renouveler le token avant son expiration.

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

- Configurer et assurer la maintenance d'un groupe d'utilisateurs contenant des tokens avec le rôle `admin` et des tokens avec le rôle `user`.
- Afficher les tokens et le statut des tokens dans le groupe d'utilisateurs.
- Révoquer les tokens des utilisateurs dans le groupe.
- 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.

**Important** Un administrateur peut modifier le rôle d'un token. Vous devez toujours disposer de 2 tokens administrateurs activés. Pour changer le token `user` en token `admin`, cliquez sur **Action** et sélectionnez **Changer le rôle en**.

**Statut**

Statut actuel du token. Ce champ peut contenir les valeurs suivantes:

| | |
|---|---|
| **Activated** (Activé) | Le token a été activé comme token d'utilisateur ou d'administrateur. |
| **Activated (old)** (Activé (ancien)) | Ce token a été renouvelé mais est toujours valide. |

| | |
|---|---|
| **NotActivated** (Non activé) | Le token est toujours à l'état d'origine, non activé.<br>Lorsque le statut du certificat est **NotActivated** (Non activé), vous pouvez:<br>• Activer le token pour une utilisation normale.<br>Pour des informations complémentaires, reportez-vous à Activer un token à la page 26.<br>• Configurer le token pour régénérer un autre token qui est inutilisable.<br>Pour des informations complémentaires, reportez-vous à Régénérer un token à la page 44.<br>• Utiliser le token pour révoquer un autre token.<br>Pour des informations complémentaires, reportez-vous à Méthode 3: Utiliser un token non activé pour révoquer un token à la page 42.<br>• Utiliser le token pour renouveler un token sur le point d'expirer.<br>Pour des informations complémentaires, reportez-vous à Renouveler un token à la page 31. |
| **NotActivated (Reset Interrupted)** (Non activé (réinitialisation interrompue)) | La procédure de réinitialisation a été interrompue pour une raison quelconque (par exemple, une coupure de réseau). Il est nécessaire de redémarrer la procédure de réinitialisation. |
| **Prepared to recover** (Préparé en vue d'une régénération) | Le token a été configuré pour régénérer un autre token qui est inutilisable. La régénération n'a pas encore été effectuée. |
| **Prepared to reset**<br>(Préparé en vue d'une réinitialisation) | Le token a été configuré par l'administrateur et est prêt à être réinitialisé par l'utilisateur. |
| **Revoked** (Révoqué) | Le token a été révoqué et ne peut plus être utilisé.<br>Ce statut s'applique uniquement aux tokens révoqués par une action **de révocation** explicite, ce statut ne s'applique pas aux tokens révoqués dans le cadre du processus de **régénération**. |
| **Used to recover (corp12345678)** (Utilisé pour la régénération (corp12345678)) | Le token a été utilisé pour régénérer un autre token qui est inutilisable. L'identifiant unique qui était associé à l'origine au token converti n'est plus actif.<br>La liste des utilisateurs contient une seconde entrée avec le même numéro de token mais un identifiant unique différent, avec le statut **Activated** (Activé). L'identifiant unique est celui du token qui a été régénéré. |
| **Used to renew (corp12345678)** (Utilisé pour le renouvellement (corp12345678)) | Ceci signifie que le token contenant le certificat repris sous la colonne **Identifiant unique** a été utilisé pour renouveler un token. L'identifiant unique du nouveau certificat qui en résulte apparaît dans la colonne **Statut**. |

**Règle en matière de code PIN** Niveau de règle en matière de code PIN pour le token. 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.

**Date d'expiration** Date et heure d'expiration du certificat.

**Numéro de série du certificat** Numéro de série du certificat.

**Numéro de série du token** Numéro de série imprimé sur le token.

**Adresse e-mail** Indique si un utilisateur avec le rôle `admin` a enregistré une adresse e-mail pour le service:

- **Oui**: une adresse e-mail a été enregistrée.
- Un champ vide indique qu'aucune adresse e-mail n'a été enregistrée.

**Action** Lorsque vous cliquez sur **Action**, une liste de fonctionnalités apparaît. En fonction du statut du token sur lequel vous souhaitez effectuer l'action, toutes les fonctionnalités ne sont pas disponibles. Par exemple, vous ne pouvez **Modifier le mot de passe** ou **Générer le code de sécurité** que sur le token actuellement connecté.

**Remarque** *Si vous changez un token `admin` en token `user`, assurez-vous de toujours maintenir un minimum de 2 administrateurs activés.*

**Filtrer** Lorsque vous cliquez sur la barre de menu **Filtrer**, vous pouvez diminuer le nombre d'utilisateurs qui apparaissent sur la page **Gérer les utilisateurs** selon les options de filtrage sélectionnées.

# 8 Gérer votre adresse e-mail (pour les administrateurs)

SWIFT recommande vivement aux administrateurs 3SKey d'enregistrer une adresse e-mail pour le service, afin de pouvoir recevoir les notifications opérationnelles concernant le service 3SKey.

### Présentation

Utilisez la page **Gérer l'adresse e-mail** pour enregistrer, modifier ou supprimer votre adresse e-mail. Cette page est disponible uniquement lorsque vous vous êtes connecté avec un token ayant le rôle `admin`.

SWIFT utilise cette adresse e-mail uniquement pour communiquer des informations opérationnelles importantes sur le service 3SKey, telles qu'une mise à niveau obligatoire de logiciel, une modification apportée aux fonctions, ou une modification des conditions générales que vous devez connaître.

Pour des informations sur la protection des données et la manière dont SWIFT traite vos données personnelles, reportez-vous à la section **Protection des données personnelles** dans les Conditions générales de 3SKey. Seule fait foi la dernière version en anglais disponible sur www.swift.com > About Us > Legal > SWIFT Terms and Conditions > Other Terms and Conditions.

### Rapport de certificats arrivant à expiration

Si vous avez enregistré votre adresse e-mail, vous recevrez régulièrement le **rapport de certificats arrivant à expiration** de 3skey.noreply@swift.com.

Ce rapport contient une liste de tous les certificats métier au sein de votre groupe d'utilisateurs qui arrivent à expiration dans les 90 jours.

#### Exemple de rapport

| Identifiant unique | Numéro de série du token | Date d'expiration |
|---|---|---|
| corp14829882 | 01dd9762 | 08/01/2020 14:31 |
| corp21580981 | 01dd971a | 08/01/2020 14:39 |

Ce rapport est uniquement envoyé s'il y a au moins un token qui arrive à expiration dans votre groupe d'utilisateurs et sera renvoyé toutes les 3 semaines. Vous recevrez par e-mail un rapport similaire à celui qui suit. Dans le rapport, le format de date d'expiration est `mm/jj/aaaa`. Dans l'exemple ci-dessus, les tokens expirent le 1er août 2020.

```
Cher Administrateur 3SKey,

Certains tokens 3SKey dans votre groupe d'utilisateurs arrivent à expiration
(vous en trouverez la liste en pièce jointe). Avant que ces tokens ne deviennent
inutilisables, leurs utilisateurs doivent renouveler leurs certificats sur de
nouveaux tokens 3SKey.
Nous vous invitons à contacter la banque qui vous a fourni ces tokens 3SKey pour
en commander de nouveaux.

Le processus de renouvellement est décrit sur le site 3SKey sous http://
www.swift.com/3skey/fr/renewal.html.
```

**Remarque** *Si vous ne souhaitez plus recevoir de notifications par e-mail concernant un token arrivant à expiration que vous ne souhaitez pas renouveler ni régénérer, vous devez le révoquer.*

# 9 Activer un token

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

### Activer le token avant expiration de son certificat technique

Lorsque vous recevez votre token de la banque, il contient un **certificat technique** qui garantit que le token a été personnalisé par SWIFT. Vous devez activer le token avant que le **certificat technique** n'expire. Si vous gardez des tokens de réserve et que vous ne prévoyez pas d'activer tous les tokens immédiatement, il est recommandé d'activer les tokens dans l'ordre de leur date d'expiration.

**Important** Un certificat technique est normalement valide 5 ans après personnalisation par SWIFT. Toutefois, le token peut avoir passé un certain temps dans le stock du distributeur avant de vous être livré. Pour des raisons techniques, la durée de validité a été ajustée à 3 ans entre le 27 mai 2017 et le 15 juin 2019, et à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Vérifiez toujours la date d'expiration du certificat technique sur le nouveau token si vous prévoyez de ne pas l'activer immédiatement. Pour plus d'informations, reportez-vous à l'entrée Durée de validité du certificat dans le glossaire.

### Activer le token crée un certificat métier

Pour préparer votre token pour pouvoir l'utiliser, vous devez l'**activer**. Le processus d'activation crée un **certificat métier** sur le token. Ce certificat est utilisé pour sécuriser toutes les transactions commerciales avec la banque et est valide durant 3 ans. Avant que le **certificat métier** n'expire, vous devez renouveler le token.

**Remarque** *La durée de validité du certificat métier a été ajustée à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Pour plus d'informations, reportez-vous à l'entrée Durée de validité du certificat dans le glossaire.*

**Remarque** *Si vous avez le rôle* `admin`*, vous ne pouvez pas accéder aux fonctions d'administrateur sur le portail 3SKey tant que vous n'avez pas activé le token.*

### Enregistrer le token après son activation

Activez le token **avant** de communiquer son identifiant unique à votre banque. Si vous enregistrez un token non activé et que vous ne parvenez pas à l'activer (car vous l'avez perdu ou endommagé), il est nécessaire de modifier tout contrat associé que vous avez déjà envoyé à votre banque. Il est impossible de régénérer l'identifiant unique d'un token non activé.

### Informations associées

Groupes d'utilisateurs 3SKey à la page 9

# 9.1 Présentation de la procédure d'activation

### Avant de commencer

- Chaque token doit appartenir à un groupe d'utilisateurs. Pour ajouter un token à un groupe d'utilisateurs, l'administrateur doit se connecter au portail 3SKey et insérer un token `non activé` dans un port USB sur la même machine.

- Le logiciel du token est requis. Les tokens peuvent être activés et utilisés sur n'importe quel ordinateur sur lequel le logiciel du token est installé. Un ordinateur peut être utilisé par plusieurs utilisateurs de tokens.

**Procédure**

1. Connectez-vous avec un token non activé, acceptez les **Conditions générales** et initialisez le processus d'activation en cliquant sur Suivant.
2. Modifiez le mot de passe qui protège le token.

   Vous utilisez ce mot de passe pour vous connecter au portail 3SKey et pour signer vos transactions.
3. **Enregistrez une adresse e-mail (pour les administrateurs 3SKey uniquement).**
4. Le portail génère le code de sécurité que vous devez télécharger et conserver dans un lieu sûr.
5. Le portail génère le certificat métier et le stocke sur le token.

**Informations associées**

Guide d'installation du logiciel du token 3SKey
Préparer un nouveau token utilisateur (pour les administrateurs) à la page 18

# 9.2 Démarrer l'activation

Pour procéder à l'activation, connectez-vous avec un token non activé, acceptez les **Conditions générales** et initialisez le processus d'activation en cliquant sur Suivant.

Si vous cliquez sur Annuler par erreur, vous pouvez reprendre l'activation en cliquant sur **Activer**.

**Important**

- **Ne fermez pas le navigateur et ne retirez pas le token du port USB.**

  Le token risquerait d'être altéré. Si une autre tentative d'activation du token échoue, vous devez alors utiliser un nouveau token.
- **Expiration de l'activation**

  Effectuez l'activation du début jusqu'à la fin sans interruption, sinon la session va expirer et vous devrez vous reconnecter à 3SKey pour continuer l'activation.

# 9.3 Sélectionner une règle en matière de code PIN (premier administrateur uniquement)

Si vous activez le premier token administrateur d'un groupe pour lequel aucune règle en matière de code PIN n'a encore été définie, il vous sera demandé de sélectionner une règle pour votre organisation.

Tous les utilisateurs que vous ajoutez à la liste d'utilisateurs doivent créer des mots de passe qui respectent les exigences de complexité minimum définies par la règle sélectionnée. Si nécessaire, vous pouvez modifier la règle en matière de code PIN ultérieurement.

Pour plus d'informations, reportez-vous à Règles en matière de code PIN.

# 9.4 Modifier le mot de passe par défaut

**Procédure**

1. Lorsque vous cliquez sur Suivant sur la page **Activation du token**, la fenêtre **Modifier le mot de passe du token** apparaît.

   Entrez le mot de passe initial fourni avec le token dans le champ **Mot de passe actuel**.

   Fournissez un mot de passe sécurisé. Votre token doit respecter les exigences de complexité minimum pour les mots de passe définies par votre **règle en matière de code PIN**.

   - La longueur minimale varie en fonction de la règle en matière de code PIN.
   - La longueur maximale est de 20 caractères.
   - Vous pouvez utiliser les caractères suivants:
     - `0-9 A-Z a-z` et espace
     - `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`
   - Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple).
   - Vous ne pouvez pas réutiliser les 5 mots de passe précédents.

2. Cliquez sur Modifier.

   La page **Modifier le mot de passe du token** apparaît avec le texte `Le mot de passe a été modifié avec succès.`

   **Remarque** *La durée de validité du mot de passe varie en fonction de la règle en matière de code PIN. Modifiez le mot de passe avant qu'il n'expire.*

3. Cliquez sur Suivant.

   Si vous vous êtes connecté avec un token `admin` la prochaine étape consiste à enregistrer une adresse e-mail.

   Si vous vous êtes connecté avec un token `user` la prochaine étape consiste à générer le code de sécurité.

**Informations associées**

Règles en matière de code PIN à la page 50
Enregistrer une adresse e-mail (pour les administrateurs) à la page 28
Générer le code de sécurité à la page 29

# 9.5 Enregistrer une adresse e-mail (pour les administrateurs)

La page **Enregistrer une adresse e-mail** s'affiche uniquement lors de l'activation d'un token auquel le rôle `admin` est affecté.

SWIFT recommande vivement aux administrateurs 3SKey d'enregistrer une adresse e-mail pour le service, afin de pouvoir recevoir les notifications opérationnelles concernant le service 3SKey.

SWIFT utilisera cette adresse e-mail uniquement pour communiquer des informations opérationnelles importantes sur le service 3SKey, telles qu'une mise à niveau obligatoire de logiciel, une modification apportée aux fonctions, ou une modification des conditions générales que vous devez connaître.

Pour des informations sur la protection des données et la manière dont SWIFT traite vos données personnelles, reportez-vous à la section **Protection des données personnelles** dans les Conditions générales de 3SKey. Seule fait foi la dernière version en anglais disponible sur www.swift.com > About Us > Legal > SWIFT Terms and Conditions > Other Terms and Conditions.

L'enregistrement et la gestion de votre adresse e-mail sont entièrement sous votre contrôle. Sur le portail 3SKey, vous pouvez enregistrer, modifier ou supprimer votre adresse e-mail à tout moment.

1. **Entrer une adresse e-mail**

   Entrez l'adresse e-mail que vous souhaitez que SWIFT utilise pour les notifications opérationnelles.

2. **Confirmer l'adresse e-mail**

   Confirmez votre adresse e-mail en la saisissant de nouveau.

3. Cliquez sur Enregistrer.

# 9.6 Générer le code de sécurité

**Procédure**

1. Le portail génère ensuite le code de sécurité. Cliquez sur Télécharger pour enregistrer le code de sécurité dans un fichier.

   Le portail vous invite à enregistrer le fichier, avec le nom `code.txt` dans le dossier par défaut de votre navigateur. Le cas échéant, vous pouvez modifier le nom du fichier et le dossier.

2. Vérifiez si le fichier téléchargé contient un code de 16 caractères (quatre groupes de quatre caractères, séparés par des tirets).

   **Important** Vous devez conserver le code de sécurité dans un endroit sûr. S'il est nécessaire de régénérer ou de réinitialiser le token, ceci est impossible sans le code de sécurité.

   Ne stockez pas le code de sécurité 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.

3. Après téléchargement du fichier, le bouton Confirmer est disponible.

   Cliquez sur Confirmer lorsque le téléchargement est terminé.

**Remarque** *Si vous avez perdu le code de sécurité, vous pouvez vous connecter au portail 3SKey et générer un nouveau code pour autant que votre token fonctionne toujours. Si votre token ne fonctionne pas (s'il est verrouillé, expiré ou révoqué), vous aurez besoin de votre code de sécurité parce que vous ne pouvez pas en générer un nouveau avec un token qui ne fonctionne pas.*

*Pour plus d'informations sur comment générer le code de sécurité, reportez-vous à* Générer le code de sécurité *à la page 48.*

# 9.7 Générer la clé

Le portail affiche la page **Générer la clé** pour afficher sa progression lors des étapes suivantes:

- Générer la demande d'activation.
- Obtenir le certificat auprès de SWIFT.
- Enregistrer le nouveau certificat sur le token.
- Confirmer l'activation du token à SWIFT.

Si l'étape **Génération de la clé** a été effectuée avec succès, cela signifie que le nouveau certificat métier a été généré et certifié.

**Important** L'activation de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Vous devrez vous connecter en utilisant le nouveau mot de passe.

# 9.8 Activation effectuée

La page **Activation effectuée** apparaît. Votre token est à présent activé, et vous pouvez l'enregistrer auprès de votre banque. Vous pouvez alors l'utiliser pour authentifier et signer des transactions commerciales. Vous pouvez utiliser le token sur n'importe quel PC qui respecte les exigences de configuration.

**Remarque** *Retirez le token en toute sécurité et déconnectez-vous de 3SKey. Ré-insérez le token pour ajouter les informations du certificat du token au magasin de certificats du navigateur et commencez à utiliser le token.*

### Enregistrement du token

Suivez les instructions de votre banque ou de votre partenaire pour enregistrer le token. L'enregistrement associe l'identifiant unique à l'identité de l'utilisateur. L'enregistrement nécessite les informations du certificat métier disponibles sur la page **Activation effectuée** ou sur la page **Informations portées par la clé**.

**Informations du certificat métier pour l'enregistrement**

| | |
|---|---|
| **DN** | `CN=corp48228194, OU=section_6, OU=personalid, O=swift, C=ww` |
| **Numéro de série du certificat** | `1427861058 (Hex: 551B6E42)` |
| **Expiration** | `20 juillet 2021 4:52:45 PM CEST` |

# 10 Renouveler un token

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 2017 comprend un certificat qui expire le 1er janvier 2020.

**Remarque** *La durée de validité du certificat métier a été ajustée à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Pour plus d'informations, reportez-vous à l'entrée Durée de validité du certificat dans le glossaire.*

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

---

**ATTENTION** Il est important de renouveler le certificat à temps. Si le certificat expire, il ne peut plus être utilisé pour signer des transactions ni accéder au portail 3SKey et doit être régénéré.

---

Les administrateurs 3SKey peuvent enregistrer une adresse e-mail afin de recevoir les détails des certificats arrivant à expiration. Pour plus d'informations, reportez-vous à la section Gérer votre adresse e-mail (pour les administrateurs) à la page 25.

## 10.1 Renouveler un token

### Avant de commencer

Avant qu'un utilisateur ne puisse renouveler le certificat métier contenu sur le token, les conditions suivantes doivent être remplies:

- Le certificat à renouveler doit se trouver dans sa période de renouvellement (c'est-à-dire dans les 3 mois avant son expiration).
- L'utilisateur doit avoir reçu un nouveau token et un mot de passe par défaut de son administrateur.
- Le PC utilisé pour le renouvellement doit disposer de 2 ports USB libres.

**Remarque** *Il n'est pas nécessaire d'ajouter le nouveau token à un groupe d'utilisateurs avant la procédure de renouvellement.*

### Procédure

1. Insérez votre token actuel dans un port USB de votre PC et accédez à 3SKey.com, cliquez sur Connexion et saisissez le mot de passe de votre token actuel.

   Un avertissement indiquant le nombre de jours avant l'expiration du certificat sur le token apparaît.

   Cliquez sur Continuer.

2. Cliquez sur **Renouveler** sur la page **Présentation**.

   Cliquez sur l'onglet **Présentation** à partir de n'importe quelle page pour accéder à la page **Présentation**.

3. La fenêtre **Renouvellement du token** apparaît. Insérez le nouveau token dans le PC sans retirer le token actuel et cliquez sur Suivant.

   ---

   **ATTENTION** Ne retirez aucun des deux tokens durant le processus de renouvellement.

   ---

4. La fenêtre **Sélectionner le nouveau token** apparaît.

   Dans la liste déroulante à droite du champ **Numéro de série du token**, sélectionnez le numéro de série de votre nouveau token (disponible sur le token même).

   Introduisez le mot de passe par défaut que vous avez reçu de votre banque ou de votre administrateur et cliquez sur Suivant.

5. La fenêtre **Modifier le mot de passe du token** apparaît.

   Introduisez le mot de passe par défaut du nouveau token dans le champ **Mot de passe actuel**.

   Introduisez un nouveau mot de passe, conforme aux règles qui apparaissent à l'écran et ré-introduisez le nouveau mot de passe

   Cliquez sur Modifier.

   **Remarque** *Gardez votre mot de passe en sécurité. Si vous perdez le mot de passe ou que vous entrez 5 mots de passe incorrects consécutifs, le token se verrouille et il est nécessaire de le réinitialiser.*

   *Le nouveau mot de passe est défini pour le nouveau token uniquement. Le mot de passe de l'ancien token reste inchangé.*

6. Un message confirmant que la modification du mot de passe a réussi s'affiche.

   Cliquez sur Suivant.

7. Le processus de renouvellement du certificat se lance automatiquement.

   Lorsque le processus de renouvellement est terminé, la fenêtre **Renouvellement terminé** apparaît.

   **Remarque** *Le renouvellement de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token.*

   Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Veuillez noter que le mot de passe sur le nouveau token sera celui que vous avez modifié. Vous devrez fournir ce mot de passe dans la fenêtre **Sélectionner le nouveau token** (voir étape 4) et le modifier à nouveau dans la fenêtre **Modifier le mot de passe du token** (voir étape 5).

8. **Renouvellement terminé**

   Cliquez sur Terminer.

   Vous êtes automatiquement déconnecté. Le certificat métier a été renouvelé sur le nouveau token (et activé avec le même identifiant unique) et est prêt à être utilisé.

## 10.2 Renouvellement terminé

Suite au processus de renouvellement, vous disposez de 2 tokens. Un ancien token (renouvelé) contenant l'ancien certificat (toujours valide) et un nouveau token contenant un nouveau certificat valide pour une durée de 3 ans. Jusqu'à ce que l'ancien token expire, les 2 tokens apparaissent sur la page **Gérer les utilisateurs** (fonctionnalité uniquement disponible pour les administrateurs d'entreprise).

Durant la période où vous disposerez de 2 tokens, SWIFT vous recommande de différencier le nouveau token de l'ancien token (en utilisant un porte-clés ou un autocollant par exemple) pour éviter toute confusion.

Afin de vérifier si vous utilisez un ancien token (non expiré) ou un token contenant un certificat renouvelé, connectez-vous avec le token que vous souhaitez vérifier et consultez la date

**d'émission** sur la page **Informations portées par la clé**. De même, si vous accédez au portail avec un ancien token (non expiré qui a déjà été renouvelé, les seules fonctions disponibles sur la page **Présentation** sont **Modifier le mot de passe**, **Révoquer** et **Informations portées par la clé**.

Consultez les instructions de votre banque afin de savoir si votre nouveau certificat doit être enregistré auprès de la banque et la procédure requise, si nécessaire.

- Si vous ne devez pas enregistrer votre nouveau token auprès de votre banque, SWIFT vous recommande de commencer à utiliser votre nouveau token même si l'ancien token est encore valide.
- Si votre banque requiert que le nouveau token soit enregistré, veuillez procéder à l'enregistrement immédiatement afin d'être en mesure d'utiliser le nouveau token le plus rapidement possible. Votre ancien token peut toujours être utilisé temporairement.

Lorsque toutes vos banques ont enregistré le nouveau token, SWIFT recommande d'utiliser uniquement le nouveau certificat sur le nouveau token.

Vous ne pouvez vous séparer de l'ancien token qu'après expiration de son certificat. Séparez-vous de l'ancien token de la même manière que vous le feriez pour n'importe quel autre outil électronique au sein de votre organisation.

**Remarque** *Le code de sécurité du token d'origine reste valide. Si vous souhaitez remplacer le code de sécurité, reportez-vous à* Générer le code de sécurité *à la page 48.*

# 11 Configurer un token en vue d'une réinitialisation (pour les administrateurs)

### Présentation

Vous devez procéder à la réinitialisation du token lorsque vous devez:

- Réinitialiser un token verrouillé ou dont le mot de passe est perdu. La réinitialisation ne s'applique qu'aux tokens dont le statut est:
  - **Activated** (Activé)
  - **Activated (Reset Interrupted)** (Activé (réinitialisation interrompue))
  - **NotActivated** (Non activé)
  - **NotActivated (Reset Interrupted)** (Non activé (réinitialisation interrompue))
  - **Prepared to recover** (Préparé en vue d'une régénération)
  - **Prepared to reset** (Préparé en vue d'une réinitialisation)
- Retirer un token **non activé** de son groupe d'utilisateurs.
- Faire passer le statut d'un token de **Prepared to Recover** (Préparé en vue d'une régénération) à **Not Activated** (Non activé) et le retirer de son groupe d'utilisateurs.

Vous devez remplir les conditions préalables suivantes pour réinitialiser un token:

- Vous devez disposer du rôle `admin`.
- Vous devez vous assurer que deux ports USB libres sont disponibles sur le PC sur lequel vous souhaitez procéder à la réinitialisation.
- Pour réinitialiser un token activé, l'utilisateur du token doit disposer de son code de sécurité.

---

**Important** Si l'utilisateur du token ne dispose pas du code de sécurité, l'utilisateur ne doit pas réinitialiser le token et doit activer un nouveau token avec un identifiant unique différent. Un token qui a été configuré en vue d'une réinitialisation dont le code de sécurité a été perdu est inutilisable.

Le code de sécurité a été téléchargé dans un fichier par la personne qui a activé le token. Par défaut, le nom du fichier est `code.txt` et il est stocké dans le dossier par défaut du navigateur.

---

**Remarque** *Le nombre maximum de réinitialisations par token est de 5. Si un token se verrouille ou devient inutilisable après 5 réinitialisations, un nouveau token est nécessaire.*

### Quand ne puis-je pas réinitialiser un token?

Vous ne pouvez pas réinitialiser un token expiré, révoqué ou qui se verrouille durant sa période de renouvellement (c'est-à-dire 90 jours avant son expiration). Vous devrez régénérer son identifiant unique sur un nouveau token.

Pour régénérer un token, reportez-vous à Configurer un token en vue d'une régénération (pour les administrateurs) à la page 44.

# 11.1 Comment configurer un token en vue d'une réinitialisation

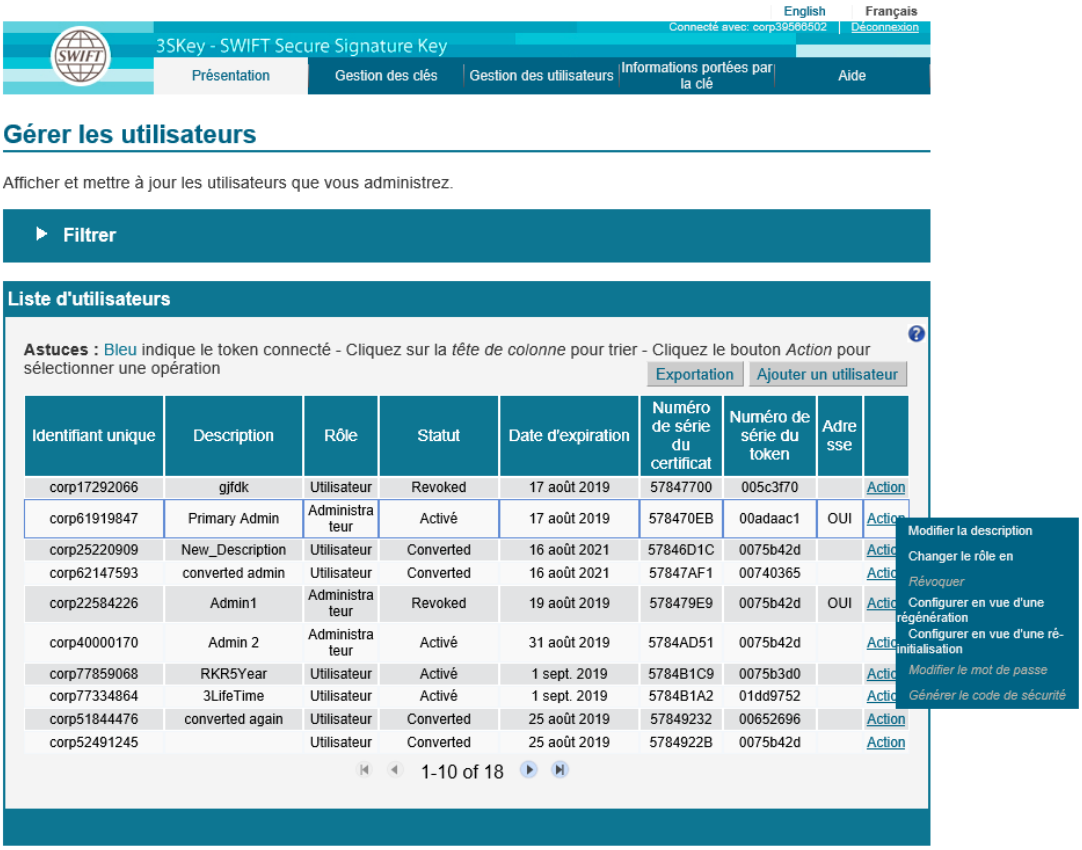
Réinitialisez un token pour déverrouiller un token ou supprimer un token non activé d'une liste d'utilisateurs.

**Procédure**

1. Connectez-vous au portail 3SKey en utilisant votre token `admin`.

   La page **Gérer les utilisateurs** apparaît.

2. Cliquez sur **Action** et **Configurer en vue d'une réinitialisation**.




   Vous pouvez également configurer un token en vue d'une réinitialisation via le menu **Présentation** < **Gestion des utilisateurs** < **Configurer en vue d'une réinitialisation**.

3. La page **Réinitialisation du token** s'affiche et explique dans quelles circonstances la réinitialisation du token peut être utilisée.

   Insérez le token que vous souhaitez réinitialiser et cliquez sur Suivant.

4. La fenêtre **Configurer en vue d'une réinitialisation** s'ouvre et affiche le numéro de série du token à réinitialiser.

   Sélectionnez le numéro de série du token dans la liste déroulante et cliquez sur Suivant.

5. La fenêtre **Confirmer la réinitialisation** s'affiche et fournit les détails du token à réinitialiser.

   Vérifiez le statut du token. Voici les scénarios possibles:

   - Si vous disposez d'un token dont le statut est **Activated** (Activé) qui ne se trouve pas en période de renouvellement (90 jours avant expiration), cliquez sur Confirmer et suivez la procédure décrite ici.
   - Si vous disposez d'un token dont le statut est **Activated** (Activé) qui se trouve en période de renouvellement (90 jours avant expiration), vous devez configurer le token en vue d'une régénération. Pour ce faire, reportez-vous à la section Configurer un token en vue d'une régénération (pour les administrateurs) à la page 44.
   - Si vous disposez d'un token verrouillé dont le statut est **NotActivated** (Non activé) ou **Prepared to Recover** (Préparé en vue d'une régénération), cliquez sur Confirmer et suivez la procédure décrite ici.
   - Si vous disposez d'un token non verrouillé dont le statut est **NotActivated** (Non activé) ou **Prepared to Recover** (Préparé en vue d'une régénération), la fenêtre **Confirmation de la réinitialisation** propose 2 options:

     1. `Je ne connais pas le mot de passe du token` - dans ce cas, vous devez procéder à une réinitialisation complète qui supprimera du token toutes les informations relatives au certificat et génèrera un nouveau certificat technique.

        Sélectionnez l'option de mot de passe appropriée, cliquez sur Confirmer et suivez la procédure décrite ici.

     2. `Je connais le mot de passe du token` - dans ce cas, vous pouvez procéder à une réinitialisation rapide et garder le même certificat technique.

        Sélectionnez l'option de mot de passe appropriée, cliquez sur Confirmer et suivez la procédure décrite ici.

## 11.2 Réinitialiser un token activé

La procédure de réinitialisation d'un token activé se déroule en deux étapes:

1. L'administrateur doit configurer le token en vue d'une réinitialisation.
2. L'utilisateur du token peut ensuite réinitialiser le token.

---

**Important** Avant de configurer un token pour sa réinitialisation, vérifiez que le propriétaire du token à réinitialiser dispose du code de sécurité de ce token.

Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser le token et vous devez activer un nouveau token avec un identifiant unique différent. Un token qui a été configuré en vue d'une réinitialisation dont le code de sécurité a été perdu est inutilisable.

Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est `code.txt` et il est stocké dans le dossier par défaut de votre navigateur.

---

Lorsque vous réinitialisez un token activé, la procédure est similaire à celle de la régénération d'un token sauf que, dans le cas d'une réinitialisation, vous utilisez le même token et non un nouveau token.

## 11.3 Configurer le token en vue d'une réinitialisation

**Procédure**

1. En cliquant sur Confirmer, la fenêtre **Réinitialiser le mot de passe** s'ouvre.

   Introduisez un nouveau mot de passe en respectant les règles qui apparaissent à l'écran. Ré-introduisez le mot de passe et cliquez sur Suivant.

   **Remarque** *Veuillez noter que ce mot de passe devra à nouveau être modifié lorsque l'utilisateur finalisera la réinitialisation.*

2. La fenêtre **Configurer en vue d'une réinitialisation** s'ouvre.

   Cette étape génère un nouveau certificat technique avec le même identifiant unique que le certificat précédent et le stocke sur le token. Le statut du token passe à **Prepared to Reset** (Préparé en vue d'une réinitialisation).

   ---

   **Important** Ce processus peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

   Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération.

   ---

3. La fenêtre **Configuration en vue de la réinitialisation terminée** s'ouvre.

   Lorsque la configuration est terminée, vous recevrez une confirmation indiquant que l'identifiant unique du token a été réinitialisé.

   Cliquez sur Terminer.

4. Le token apparaît dans le groupe d'utilisateurs avec le statut **Prepared to Reset** (Préparé en vue d'une réinitialisation).

   L'administrateur doit ensuite transférer le token avec le statut **Prepared to Reset** (Préparé en vue d'une réinitialisation) et son mot de passe à l'utilisateur du token. L'utilisateur doit se connecter au portail et terminer la réinitialisation. Reportez-vous à la section Réinitialiser un token à la page 40 pour terminer la réinitialisation.

## 11.4 Réinitialiser un token: Un token non activé ou préparé en vue d'une régénération qui est verrouillé

**Procédure**

1. En cliquant sur Confirmer, la fenêtre **Réinitialiser le mot de passe** s'ouvre.

   Introduisez un nouveau mot de passe en respectant les règles qui apparaissent à l'écran. Ré-introduisez le mot de passe et cliquez sur Suivant.

2. La fenêtre **Configurer en vue d'une réinitialisation** s'ouvre.

   Cette étape génère un nouveau certificat avec le même identifiant unique que le certificat précédent.

**Important** Ce processus peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération.

3. Après quelques instants, la fenêtre **Réinitialisation du token terminée** s'ouvre.

   Elle affiche le numéro de série du token qui a été réinitialisé.

   Cliquez sur Terminer et la page **Présentation** s'ouvre.

   Au cours de cette procédure, le token est retiré du groupe d'utilisateurs. Et le statut du token passe de **Prepared to Recover** (Préparé en vue d'une régénération) à **Not Activated** (Non activé).

   Le token peut maintenant être ajouté à un groupe d'utilisateurs et activé.

# 11.5 Réinitialiser un token: Un token non activé ou préparé en vue d'une régénération qui n'est pas verrouillé

Si vous connaissez le mot de passe du token, procédez comme suit:

1. Cliquez sur `Je connais le mot de passe du token.`

   Cliquez sur Confirmer.

2. La fenêtre **Réinitialisation du token terminée** s'ouvre et affiche le numéro de série du token qui a été réinitialisé.

   Après réinitialisation le statut du token passe à **NotActivated** (Non activé) et le token n'appartient plus à un groupe d'utilisateurs.

   Cliquez sur Terminer.

   Au cours de cette procédure, le token est retiré du groupe d'utilisateurs. Et le statut du token passe de **Prepared to Recover** (Préparé en vue d'une régénération) à **NotActivated** (Non activé).

3. Vous pouvez maintenant ajouter le token à un groupe d'utilisateurs et l'activer.

Si vous ne connaissez pas le mot de passe du token, procédez comme suit:

1. Cliquez sur `Je ne connais pas le mot de passe du token.`
2. Cliquez sur Confirmer. La fenêtre **Réinitialiser le mot de passe** s'ouvre.

   Introduisez un nouveau mot de passe en respectant les règles qui apparaissent à l'écran. Ré-introduisez le mot de passe et cliquez sur Suivant.

3. La fenêtre **Réinitialisation du token** s'ouvre.

   Cette étape génère un nouveau certificat avec le même identifiant unique que le certificat précédent.

**Important** Ce processus peut prendre quelques secondes. N'abandonnez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération.

4. La fenêtre **Réinitialisation du token terminée** s'ouvre.

   Elle affiche le numéro de série du token qui a été réinitialisé.

   Cliquez sur Terminer et la page **Présentation** s'ouvre.

   Au cours de cette procédure, le token est retiré du groupe d'utilisateurs. Et le statut du token passe de **Prepared to Recover** (Préparé en vue d'une régénération) à **Not Activated** (Non activé).

   Le token peut maintenant être ajouté à un groupe d'utilisateurs et activé.

# 12 Réinitialiser un token

Le token doit être réinitialisé si le token est verrouillé après de trop nombreuses tentatives de saisies de mot de passe erroné. Votre administrateur doit tout d'abord préparer votre token et vous fournir un mot de passe temporaire. Connectez-vous à 3SKey en utilisant le mot de passe temporaire et votre code de sécurité personnel afin de compléter la réinitialisation.

**Avant de commencer**

- Votre administrateur doit avoir configuré votre token en vue d'une réinitialisation.
- Vous devez avoir reçu votre token et son nouveau mot de passe de votre administrateur.
- Vous devez disposer de votre code de sécurité.

---

**Important** Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser le token et vous devez activer un nouveau token avec un identifiant unique différent. Un token qui a été configuré en vue d'une réinitialisation dont le code de sécurité a été perdu est inutilisable.

Le format du code de sécurité est `XXXX-XXXX-XXXX-XXXX`. Le code est sensible à la casse. Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est `code.txt`.

---

**Procédure**

1. Connectez-vous au portail à l'aide du token qui doit être réinitialisé.
2. La fenêtre **Réinitialiser votre token** s'ouvre automatiquement. Cliquez sur Suivant.
3. La fenêtre **Valider le code de sécurité** s'ouvre. Introduisez le code de sécurité du token. Cliquez sur Valider.
4. La fenêtre **Modifier le mot de passe du token** s'ouvre. Introduisez le mot de passe actuel du token, et introduisez ensuite un nouveau mot de passe pour le token en respectant les règles qui s'affichent à l'écran. Confirmez le nouveau mot de passe et cliquez sur Modifier.

   Vous recevrez une confirmation indiquant que le nouveau mot de passe a été modifié avec succès. Cliquez sur Suivant.
5. La fenêtre **Générer la clé** s'ouvre. La réinitialisation de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token. Le token risquerait de devenir inutilisable.

   Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Vous devrez vous connecter en utilisant le nouveau mot de passe. Vous devrez à nouveau modifier le mot de passe dans la fenêtre **Modifier le mot de passe du token**.
6. La fenêtre **Réinitialisation du token terminée** s'ouvre. Cliquez sur Terminer.

La réinitialisation de votre token est maintenant terminée. Le token stocke un nouveau certificat avec le même identifiant unique et la même date d'expiration que le certificat précédent.

**Remarque** *Le code de sécurité du token reste valide. Si vous souhaitez remplacer le code de sécurité, reportez-vous à* Générer le code de sécurité *à la page 48.*

**Que faire ensuite**

Votre token est maintenant prêt à l'emploi. Enregistrez le nouveau certificat auprès des banques qui ont requis des informations supplémentaires autres que l'identifiant unique `corpxxxxxxxx`.

Si vous souhaitez utiliser le token immédiatement sur le PC que vous avez utilisé pour l'activation, vous devez vous déconnecter du portail 3SKey, et retirer le token du port USB.

# 13 Révoquer un token

### Présentation

La révocation d'un token a les conséquences suivantes:

- La révocation du token rend non valides tous les certificats associés à l'identifiant unique du token.
- Une fois que le token a été révoqué, 3SKey l'ajoute à la liste de révocation des certificats. Les applications destinées à vérifier la liste de révocation des certificats ne considèrent alors plus les certificats correspondant à l'identifiant unique associé au token comme des certificats de confiance.
- Un token révoqué ne peut pas être réutilisé.

Révoquer un token est nécessaire si, par exemple, vous avez perdu le token, vous suspectez qu'il a été compromis, ou que l'utilisateur du token a quitté votre organisation.

Si vous souhaitez continuer à utiliser l'identifiant unique qui se trouvait sur le token d'origine, vous devez régénérer cet identifiant. Le processus de régénération révoque automatiquement le token d'origine. Pour de plus amples informations, reportez-vous à Configurer un token en vue d'une régénération (pour les administrateurs) à la page 44 et Régénérer un token à la page 44.

Si vous révoquez un token ayant le rôle `admin`, il peut être nécessaire de régénérer l'identifiant unique ou de configurer un nouveau token, afin que votre organisation ait toujours au moins deux tokens d'administrateur.

**Remarque** *Il est impossible de révoquer un token non activé.*

*Lorsqu'une opération requiert que vous fournissiez deux informations différentes, vous devez fournir la seconde information dans les **cinq minutes** suivant la première. Sinon, votre session peut arriver à expiration et vous devez recommencer le processus de révocation.*

### Comment révoquer un token

Il existe trois moyens pour révoquer un token activé:

- Se connecter avec le token suspect et le révoquer. Voir Méthode 1: Révoquer le token avec lequel vous vous êtes connecté à la page 42.
- Se connecter en tant qu'administrateur du groupe d'utilisateurs auquel le token appartient, et révoquer le token suspect. Voir Méthode 2: Révoquer un token en tant qu'administrateur à la page 42.
- Dans des situations exceptionnelles, si la méthode 1 et la méthode 2 ne sont pas possibles, vous pouvez vous connecter avec un token non activé et révoquer le token suspect. Par exemple, vous pouvez utiliser cette troisième méthode s'il est nécessaire de révoquer un token perdu en urgence en l'absence des administrateurs.

  Pour utiliser cette méthode, vous avez besoin du code de sécurité du token que vous souhaitez révoquer. Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est `code.txt`.

  Voir Méthode 3: Utiliser un token non activé pour révoquer un token à la page 42.

**Remarque** *Si vous devez révoquer un token qui a été renouvelé et que l'ancien token n'a pas encore expiré, vous aurez la possibilité de révoquer l'ancien ou le nouveau token lorsque vous sélectionnez l'identifiant unique.*

# 13.1 Méthode 1: Révoquer le token avec lequel vous vous êtes connecté

**Procédure**

1. Connectez-vous au portail 3SKey avec le token que vous souhaitez révoquer.
2. Si vous êtes un administrateur 3SKey, sur la page **Gérer les utilisateurs**, cliquez sur **Action** > **Révoquer**.

   Ou sur la page **Présentation**, dans la colonne **Gestion des clés**, cliquez sur **Révoquer**.

   3SKey affiche votre identifiant unique.

   Terminez la procédure de révocation en suivant les étapes décrites dans la section Terminer la révocation du token à la page 43.

# 13.2 Méthode 2: Révoquer un token en tant qu'administrateur

**Procédure**

1. Connectez-vous au portail 3SKey en utilisant un token `admin` du même groupe d'utilisateurs que celui devant être révoqué.
2. Si vous êtes un administrateur 3SKey, sur la page **Gérer les utilisateurs**, cliquez sur **Action** > **Révoquer**.

   Ou sur la page **Présentation**, dans la colonne **Gestion des clés**, cliquez sur **Révoquer**.
3. Sélectionnez l'identifiant unique que vous souhaitez révoquer dans la liste déroulante.

   Cette liste contient tous les tokens qui sont membres du groupe d'utilisateurs auquel le token administrateur appartient.

   Terminez la procédure de révocation en suivant les étapes décrites dans la section Terminer la révocation du token à la page 43.

# 13.3 Méthode 3: Utiliser un token non activé pour révoquer un token

**Procédure**

1. Connectez-vous au portail 3SKey en utilisant un token non activé.

   3SKey affiche la page **Activation du token**.
2. Cliquez sur Annuler.

   La page principale du portail 3SKey s'affiche.
3. Dans la colonne **Gestion des clés**, cliquez sur **Révoquer**.
4. Entrez l'identifiant unique et le code de sécurité du token que vous souhaitez révoquer.

   Le format du code de sécurité est `XXXX-XXXX-XXXX-XXXX`. Le code est sensible à la casse.

   Terminez la procédure de révocation en suivant les étapes décrites dans la section Terminer la révocation du token à la page 43.

# 13.4 Terminer la révocation du token

**Avant de commencer**

Suivez les étapes décrites dans la Méthode 1, 2, ou 3 et terminez la procédure de révocation comme suit.

**Procédure**

1. Cliquez sur Soumettre.

   3SKey affiche les informations relatives à votre identifiant unique. La **Date de révocation** est l'horodatage sur le serveur. L'**Identifiant unique** est l'utilisateur que vous souhaitez révoquer.

   Si votre token a été renouvelé et que l'ancien token n'a pas encore expiré, vous verrez 2 certificats avec le même identifiant unique et vous serez en mesure de sélectionner l'ancien ou le nouveau token.

2. Vérifiez que l'**identifiant unique** affiché est celui que vous souhaitez révoquer, et cliquez sur Confirmer.
3. Le portail affiche une confirmation indiquant que la révocation du token a réussi.

   Cliquez sur Effectué. Si vous utilisez la Méthode 1, votre session est clôturée.

# 14 Régénérer un token

Le processus de régénération vous permet de réutiliser l'identifiant unique d'un ancien token et de l'associer à un autre token. Pour utiliser le processus de régénération, vous devez disposer du code de sécurité du token d'origine et votre administrateur doit avoir configuré un nouveau token en vue d'une régénération.

### Qu'est-ce que la régénération et quand l'utiliser

Si possible, vous devez utiliser le processus de régénération dans les situations suivantes:

- Si un token est perdu ou endommagé.
- Si le token a expiré.
- Si le token a été révoqué.

**Remarque** *La régénération nécessite le code de sécurité du token. Si vous ne disposez pas de votre code de sécurité, vous devez activer un nouveau token avec un identifiant unique différent.*

### Quand ne pas utiliser la régénération

Dans les cas suivants, le token doit être réinitialisé:

- Si le propriétaire du token a oublié le mot de passe.
- Si le propriétaire a verrouillé le token en entrant cinq mots de passe incorrects consécutifs.

**Remarque** *Si votre token est verrouillé et qu'il se trouve en période de renouvellement, vous ne pouvez pas réinitialiser votre token et vous devez le régénérer. Si vous ne disposez pas de votre code de sécurité, vous ne pouvez pas réinitialiser ni régénérer le token et vous devez activer un nouveau token avec un identifiant unique différent.*

*Si votre token n'est pas encore activé, il n'est pas possible de le régénérer.*

### Présentation de la régénération

La procédure de régénération se déroule en 2 parties:

1. Un utilisateur avec le rôle `admin` configure un token de réserve pour la régénération.
2. L'utilisateur de l'ancien token se connecte avec le token de réserve préparé, fournit le code de sécurité et modifie le mot de passe.

**Remarque** *Durant la régénération, le portail 3SKey configure le nouveau token pour qu'il ait l'identifiant unique du token d'origine. Dans le cadre de ce processus, le portail révoque le certificat sur l'ancien token. L'ancien token ne peut par conséquent plus être utilisé.*

### Informations associées

Configurer un token en vue d'une régénération (pour les administrateurs) à la page 44
Régénérer l'identifiant unique à la page 46

# 14.1 Configurer un token en vue d'une régénération (pour les administrateurs)

Un administrateur doit préparer un token en vue d'une régénération avant que le propriétaire du token ne puisse régénérer l'identifiant unique sur le token.

### Avant de commencer

Avant de configurer un token pour sa régénération, vérifiez que le propriétaire du token à régénérer dispose du code de sécurité de ce token.

Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est `code.txt`. Le format du code de sécurité est `XXXX-XXXX-XXXX-XXXX`. Le code est sensible à la casse.

---

**Important** Sans le code de sécurité, le token que vous avez configuré en vue d'une régénération ne peut pas être utilisé pour régénérer cet identifiant unique particulier. Vous pouvez réinitialiser le token configuré en vue d'une régénération afin de le faire revenir à son état d'origine non activé.

---

#### Comment configurer un token en vue d'une régénération

1. Connectez-vous au portail 3SKey en utilisant votre token `admin`.
2. Cliquez sur **Configurer en vue d'une régénération** sur la page **Présentation**.

   Vous pouvez également configurer un token en vue d'une régénération via la page **Gérer les utilisateurs** en cliquant sur **Action** à côté de l'identifiant unique que vous souhaitez régénérer.

   La fenêtre **Configurer en vue d'une régénération** s'ouvre.

### Champs

**Sélectionner l'identifiant unique à régénérer**
La liste déroulante contient l'identifiant unique et la description (le cas échéant) de chaque token activé dans votre groupe d'utilisateurs. Sélectionnez l'identifiant unique à régénérer.

Si vous avez accédé à cette page en cliquant sur **Action** à côté d'un token sur la page **Gérer les utilisateurs**, l'identifiant unique de ce token sera pré-sélectionné.

**Sélectionner le nouveau token**
La liste déroulante contient les numéros de série de tous les tokens non activés ayant été ajoutés au groupe d'utilisateurs. Ils sont disponibles pour la régénération du token inutilisable.

Sélectionnez le numéro de série qui est imprimé sur le token que vous souhaitez utiliser.

Si le token que vous souhaitez utiliser ne se trouve pas dans la liste, ajoutez-le au groupe d'utilisateurs. Pour plus d'informations, reportez-vous à Préparer un nouveau token utilisateur (pour les administrateurs) à la page 18.

### Terminer la configuration

**Cliquer sur Effectué**
Lorsque tous les champs sont renseignés correctement, cliquez sur Effectué pour terminer la configuration.

**Transférer le token**
Lorsque la configuration est terminée, transférez le nouveau token au propriétaire du token devant être régénéré.

Assurez-vous que le propriétaire dispose également du mot de passe d'activation que votre banque a fourni avec le token.

Pour plus d'informations sur le processus de régénération, reportez-vous à Régénérer un token à la page 44.

# 14.2 Régénérer l'identifiant unique

Utilisez le code de sécurité de votre ancien token pour associer l'identifiant unique de votre ancien token au nouveau token.

**Avant de commencer**

- Vous devez connaître le code de sécurité de votre ancien token.
- Vous devez disposer d'un nouveau token qui a été préparé en vue d'une régénération par le gestionnaire de la liste d'utilisateurs.
- Vous devez disposer du mot de passe qui accompagne le nouveau token.

**Procédure**

1. Connectez-vous au portail 3SKey avec un token ayant été configuré en vue d'une régénération.

   À ce stade, l'identifiant unique et le mot de passe d'origine du token sont toujours associés au token. Le processus de régénération remplace l'identifiant unique par celui que vous régénérez.

   Dans le champ **Mot de passe**, indiquez le mot de passe initial qui accompagnait le token avec lequel vous êtes connecté.

2. Cliquez sur Suivant.

   Le portail 3SKey affiche une page contenant les informations relatives à l'identifiant unique pour lequel le token de réserve a été configuré.

3. Vérifiez que l'identifiant unique affiché est celui que vous souhaitez régénérer et entrez le code de sécurité associé à cet identifiant unique. Les caractères sont masqués et ne sont donc pas visibles.

   **Remarque** *Le format du code de sécurité est `XXXX-XXXX-XXXX-XXXX`. Le code est sensible à la casse.*

   *Le code de sécurité a été téléchargé dans un fichier lors de l'activation du token. Par défaut, le nom du fichier est `code.txt`.*

4. Cliquez sur Valider pour vérifier que le code de sécurité correspond à l'identifiant unique régénéré.

5. Vous devez maintenant modifier le mot de passe. Entrez un nouveau mot de passe dans la zone d'édition **Nouveau mot de passe**, confirmez le mot de passe en l'entrant à nouveau dans la zone d'édition **Confirmation du nouveau mot de passe**, et cliquez sur Modifier.

   Fournissez un mot de passe sécurisé. Suivez les directives ci-après lorsque vous créez un mot de passe:

   - La longueur minimale varie en fonction de la **règle en matière de code PIN**.
   - La longueur maximale est de 20 caractères.
   - Vous pouvez utiliser les caractères suivants:
     - `0-9 A-Z a-z` et espace
     - `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`
   - Vous devez utiliser au moins deux caractères différents. Par exemple, le mot de passe ne peut pas être `aaaa` ni `11111`.
   - Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple).
   - Vous ne pouvez pas ré-utiliser le mot de passe initial qui accompagnait le nouveau token.

La page **Modifier le mot de passe du token** apparaît avec le texte `Le mot de passe a été modifié avec succès.`

6. Cliquez sur Suivant.

   3SKey génère la clé.

   Une fois que l'opération a été effectuée avec succès, l'identifiant unique de l'ancien token est recréé sur le nouveau token.

---

**Important** La génération de la clé peut prendre quelques secondes. N'annulez pas l'opération en fermant le navigateur ou en déconnectant le token.

Si le portail ne répond plus pendant plus de 5 minutes (en raison d'un problème de réseau), vous devez redémarrer le navigateur et ré-essayer l'opération. Veuillez noter que le mot de passe sur le nouveau token aura été modifié. Vous devrez à nouveau le modifier dans la fenêtre **Modifier le mot de passe du token** (voir étape 5).

---

La régénération de votre identifiant unique est maintenant terminée et vous pouvez utiliser le nouveau token pour authentifier des transactions commerciales. Toutefois - en fonction de la manière dont votre banque enregistre les tokens - il peut être nécessaire d'informer la banque du remplacement.

Vous pouvez utiliser le nouveau token sur n'importe quel PC sur lequel les pilotes de token 3SKey sont installés. Si vous souhaitez utiliser le token immédiatement sur le PC que vous avez utilisé pour l'activation, vous devez vous déconnecter du portail 3SKey, et retirer le token du port USB. Réinsérez ensuite le token dans le port USB: cette opération ajoute les informations sur le certificat du nouveau token dans le magasin des certificats.

**Remarque** *Le code de sécurité du token d'origine reste valide. Si vous souhaitez remplacer le code de sécurité, reportez-vous à* Générer le code de sécurité *à la page 48.*

# 15 Générer le code de sécurité

Le code de sécurité est utilisé pour:

- Régénérer l'identifiant unique d'un token expiré, perdu, endommagé ou révoqué sur un nouveau token. Pour des informations complémentaires sur la régénération, reportez-vous à Régénérer un token à la page 44.
- Révoquer un token en utilisant un token non activé si ni le propriétaire du token ni l'administrateur ne peut le révoquer. Pour des informations complémentaires sur la révocation, reportez-vous à Révoquer un token à la page 41.
- Réinitialiser un token activé qui est verrouillé ou dont le mot de passe est perdu et qui a été configuré en vue d'une réinitialisation. Pour des informations complémentaires sur la réinitialisation, reportez-vous à Réinitialiser un token à la page 40.

Le code de sécurité est généré au cours du processus d'activation du token. Si le code de sécurité est perdu mais que le token est encore utilisable, vous pouvez générer un nouveau code de sécurité comme décrit ci-dessous.

**ATTENTION** Toutefois, ne perdez pas le code de sécurité. Si un token est inutilisable car il est verrouillé, perdu, révoqué ou expiré, il n'est pas possible de réinitialiser ni de régénérer le token sans le code de sécurité. Vous ne pouvez plus utiliser ce token et un nouveau token doit être obtenu et activé pour générer un nouveau code de sécurité.

**Procédure**

1. Connectez-vous au portail 3SKey avec le token pour lequel vous souhaitez générer un code de sécurité.
2. Sur la page **Gérer les utilisateurs**, cliquez sur **Action** > **Générer le code de sécurité**.

   Ou sur la page **Présentation**, dans la colonne **Gestion des clés**, cliquez sur **Générer le code de sécurité**.
3. La page **Générer le code de sécurité** apparaît. Cliquez sur Générer.
4. Cliquez sur Télécharger pour enregistrer le code de sécurité dans un fichier.

   Le portail vous invite à enregistrer le fichier, avec le nom `code.txt` dans le dossier par défaut de votre navigateur. Le cas échéant, vous pouvez modifier le nom du fichier et le dossier.
5. Cliquez sur Confirmer.

   **Important** Le code de sécurité généré est effectif uniquement après que vous ayez cliqué sur Confirmer et reçu une confirmation positive du serveur. Vous devez cliquer sur Confirmer dans les cinq minutes après que le code de sécurité a été généré ou le processus arrive à expiration.

**ATTENTION** Vous devez conserver le code de sécurité dans un endroit sûr. S'il est nécessaire de régénérer ou de réinitialiser le token, ceci est impossible sans le code de sécurité.

Ne stockez pas le code de sécurité avec votre token.

Si vous stockez le code de sécurité sur votre PC et que vous changez de PC, vous devez supprimer le code de sécurité de l'ancien PC et le stocker sur le nouveau.

Seul le code de sécurité le plus récent est valide. Si un nouveau code de sécurité est généré pour un token, l'ancien code de sécurité deviendra invalide.

# 16 Modifier le mot de passe

**Procédure**

1. Connectez-vous au portail 3SKey avec le token pour lequel vous souhaitez modifier le mot de passe.
2. Sur la page **Gérer les utilisateurs**, cliquez sur **Action** > **Modifier le mot de passe**.

   Ou sur la page **Présentation**, dans la colonne **Gestion des clés**, cliquez sur **Modifier le mot de passe**.

   La page **Modifier le mot de passe du token** apparaît.
3. Entrez le nouveau mot de passe dans le champ **Nouveau mot de passe**. Ce mot de passe doit se conformer aux exigences minimum des règles en matière de code PIN pour être valide.
4. Confirmez le mot de passe en le saisissant à nouveau dans la zone d'édition **Confirmation du nouveau mot de passe**.
5. Cliquez sur Modifier.

   L'application vous signale que le mot de passe a été modifié avec succès. Cliquez sur Effectué pour fermer la page.

Le token est maintenant protégé par le nouveau mot de passe.

**Remarque** *Si vous avez perdu ou oublié votre mot de passe, ou si votre token se verrouille après saisie de 5 mots de passe incorrects, contactez votre administrateur qui préparera votre token en vue d'une réinitialisation.*

# 16.1 Règles en matière de mot de passe

Le certificat du token est protégé par un mot de passe. Vous utilisez ce mot de passe pour accéder à 3SKey et pour signer vos transactions.

**Présentation**

Le gestionnaire de la liste d'utilisateurs définit les exigences de complexité minimum du mot de passe pour la liste d'utilisateurs lorsqu'il sélectionne une **règle en matière de code PIN**. Le gestionnaire de la liste d'utilisateurs peut modifier le niveau de la règle à tout moment. Toutefois, la modification du niveau de la règle ne prendra effet que lors de la réinitialisation, du renouvellement ou de la régénération du token.

**Directives en matière de mot de passe**

Fournissez un mot de passe sécurisé. Suivez les directives ci-après lorsque vous créez un mot de passe:

- La longueur minimale varie en fonction de la **règle en matière de code PIN**.
- La longueur maximale possible du mot de passe est de 20 caractères.
- Vous pouvez utiliser les caractères suivants:
  - `0-9 A-Z a-z` et espace
  - `! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~`
- Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple).
- Vous ne pouvez pas réutiliser les 5 mots de passe précédents.

**Informations associées**

Règles en matière de code PIN à la page 50

# 16.2 Règles en matière de code PIN

Au cours de l'activation du premier token administrateur d'un groupe d'utilisateurs, il est demandé à l'administrateur de sélectionner une règle en matière de code PIN qui déterminera les exigences de complexité minimum des mots de passe pour les utilisateurs de la liste d'utilisateurs. La règle en matière de code PIN peut être modifiée ultérieurement en accédant à la page **Gérer les utilisateurs** et en cliquant sur Modifier la règle.

**Remarque** *La règle par défaut est de niveau 6.*

| 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)<br>• Chiffre (0-9)<br>• Lettre majuscule (A-Z)<br>• Symbole |
| Complexité | Règles en matière de composition d'un mot de passe | Maximum 2 caractères répétés | | • Maximum 2 caractères répétés<br>• Au moins un caractère de chacun des 4 groupes de caractères |
| Historique | Nombre de mots de passe précédents qui ne peuvent pas être réutilisés | 5 | | |
| Verrouillage | Nombre de tentatives erronées avant verrouillage du compte | 5 | | |

# 17 Informations portées par la clé - détails du certificat et du token

La page **Informations portées par la clé** affiche des informations détaillées sur le token avec lequel vous êtes connecté et le certificat qu'il contient. Ces détails du certificat et du token sont également disponibles sur la page **Gérer les utilisateurs** > **Action**.

### Exemple de détails du certificat métier

#### Certificat métier

| | |
|---|---|
| DN | `CN=corp06604282,OU=section_7, OU=personalid, O=swift, C=ww` |
| Numéro de série du certificat | `1503011101 (Hex: 5996211D)` |
| Émetteur | `O=SWIFT` |
| Émis | `7 septembre, 2017 10:07:49 AM EDT` |
| Expiration | `7 septembre, 2020 10:37:49 AM EDT` |
| OID | `1.3.21.6.3.20.200.1` |
| Numéro de série du token | `00adaa8c` |
| Règle en matière de code PIN pour la liste d'utilisateurs | `Niveau 12` |
| Règle en matière de code PIN pour le token | `Niveau 6` |

### Champs

**DN** Nom distinctif du certificat du token.

L'élément **CN** du nom distinctif contient l'identifiant unique du certificat.

**Remarque** *Même si le numéro de série du certificat change, l'identifiant unique d'un certificat métier d'entreprise est préservé s'il est nécessaire de renouveler le certificat, de le régénérer sur un autre token ou de réinitialiser un token.*

**Numéro de série du certificat** Numéro de série du certificat, au format décimal et hexadécimal.

**Émetteur** Émetteur du token. Il s'agit toujours de SWIFT.

**Émis** Date et heure d'émission du certificat.

**Expiration** Date et heure d'expiration du certificat.

**OID** Identifiant d'objet du certificat du token.

| | |
|---|---|
| **Numéro de série du token** | Numéro de série du fabricant imprimé sur le token. |
| **Règle en matière de code PIN pour la liste d'utilisateurs** | Niveau de règle en matière de code PIN qu'un administrateur a défini pour la liste d'utilisateurs. |
| **Règle en matière de code PIN pour le token** | Niveau de règle en matière de code PIN défini pour le token. 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. |

# 18 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.

**Remarque** *La durée de validité du certificat métier a été ajustée à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Pour plus d'informations, reportez-vous à la section Durée de validité du certificat ci-après.*

**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** *La durée de validité des certificats techniques a été ajustée à 3 ans entre le 27 mai 2017 et le 15 juin 2019 et à moins de 3 ans entre le 15 juin 2019 et décembre 2019. La durée de validité du certificat métier a été ajustée à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Pour plus d'informations, reportez-vous à la section Durée de validité du certificat ci-après.*

**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 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.

**Description**

Un administrateur 3SKey peut attribuer une **Description** à un token, pour spécifier un nom avec lequel identifier le propriétaire du token. Par exemple, la description peut spécifier le nom ou le rôle

de l'opérateur auquel le token a été attribué, ou peut être simplement un libellé tel que **Token de réserve**.

La description est utilisée pour faciliter la gestion des tokens anonymes sur le portail 3SKey. Elle n'a aucune incidence sur le portail de signature, et elle n'est pas connue de la banque.

La description peut contenir les caractères suivants:

`A-Z`

`a-z`

`0-9`

`_ - ,` et espace

Vous ne pouvez pas utiliser de caractères accentués (é ou ö par exemple), ni de signes de ponctuation exceptés ceux qui sont répertoriés.

**Remarque** *Pour rappel, les tokens ne doivent pas être réassignés à un autre utilisateur. La description ne doit pas être utilisée pour changer le nom d'utilisateur d'un token.*

### Durée de validité du certificat

Les certificats métier sont valides 3 ans. Avant activation, les certificats techniques sont valides 5 ans.

Il y a une exception temporaire pour les certificats émis avant le 15 décembre 2019. La durée de validité de ces certificats a été ajustée pour expirer avant le 15 juin 2022.

Les détails de l'ajustement sont les suivants:

- Les certificats techniques 3SKey émis entre le 17 mai 2017 et le 15 juin 2019 sont valides pendant seulement 3 ans.
- Les certificats techniques et métier 3SKey émis entre le 15 juin 2019 et le 15 décembre 2019 ont une durée de validité ajustée à moins de 3 ans.

Avant le 15 décembre 2019, les certificats 3SKey étaient émis par l'autorité de certification SWIFT qui expire le 15 juin 2022. Des ajustements étaient nécessaires car un certificat ne peut pas avoir une durée de validité qui dépasse celle de l'autorité de certification. Après le 15 décembre 2019, les certificats 3SKey sont émis par une nouvelle autorité de certification 3SKey dédiée et ont une durée de validité normale.

### 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 des informations complémentaires, reportez-vous à Régénérer un token à la page 44.

### Nom distinctif

Le nom distinctif (DN) est l'identification du certificat en suivant la notation X.500. Il est converti au format `cn=corp<nnnnnnnn>, ou=section_n, ou=personalid, o=swift, c=ww`.

L'élément `cn` du nom distinctif est l'identifiant unique du token.

**Régénération**

Utilisez 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 des informations complémentaires, reportez-vous à Régénérer un token à la page 44.

**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 qui est défini pour le token lors de l'activation ou de la 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 des informations complémentaires, reportez-vous à Réinitialiser un token à la page 40.

**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 des informations complémentaires, reportez-vous à Renouveler un token à la page 31.

**Remarque** *La durée de validité du certificat métier a été ajustée à moins de 3 ans entre le 15 juin 2019 et décembre 2019. Pour plus d'informations, reportez-vous à la section Durée de validité du certificat ci-dessus.*

**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 des informations complémentaires, reportez-vous à Révoquer un token à la page 41.

**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 ce faire, 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.

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.

**Important** Les administrateurs 3SKey doivent s'assurer que minimum 2 tokens administrateurs sont activés et valides à tout moment. Lorsqu'un administrateur quitte l'organisation, cet administrateur ou le second administrateur doit préparer un nouveau token administrateur pour l'administrateur qui le remplacera.

**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.

# 19 Conditions générales

La fourniture et l'utilisation du service 3SKey sont régies par les Conditions générales de 3SKey. Seule fait foi la dernière version en anglais disponible sur www.swift.com > About Us > Legal > SWIFT Terms and Conditions > Other Terms and Conditions.

Pour plus d'informations sur les fonctionnalités et les fonctions de la solution 3SKey, et sur vos rôles et responsabilités en tant qu'utilisateur 3SKey ou abonné 3SKey ou sur ceux de SWIFT en tant que fournisseur de la solution 3SKey, consultez régulièrement la dernière version disponible de la Description du service 3SKey (version anglaise officielle disponible sur www.swift.com > Ordering & Support > Knowledge Centre).

**Important** La fourniture et l'utilisation des tokens 3SKey sont soumises aux restrictions d'exportation des États-Unis et autres programmes de sanction. **Les personnes situées à ou originaires de Cuba, de Corée du Nord, d'Iran, du Soudan, de Libye ou de Syrie et les personnes identifiées sur des listes du gouvernement des États-Unis ou de l'Union européenne comme "partie refusée", ou sur des listes nationales désignées spécifiquement, ne sont pas autorisées à posséder ni à utiliser des tokens 3SKey**.

# 20 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. L'assistance n'est disponible qu'en anglais et français.

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

Procédez par étapes pour résoudre votre problème:

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

   Pour accéder à l'aide 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.

2. Contactez l'assistance appropriée pour votre question.

   Si vous êtes une banque, contactez votre SWIFT Support Centre habituel.

   Pour toute questions relative à l'application bancaire, contactez le fournisseur de l'application.

   Si vous rencontrez des problèmes dans l'application bancaire, essayez de vous connecter au portail 3SKey. Si la connexion est réussie et que la page **Informations portées par la clé** affiche un certificat métier, votre token est correctement configuré et vous devez contacter le fournisseur de l'application.

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

| Type de problème | Contact = SWIFT 3SKey | Contact = votre banque |
|---|---|---|
| Installation de SConnect ou 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 |

| Type de problème | Contact = SWIFT 3SKey | Contact = votre banque |
|---|---|---|
| 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.

3. 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.

4. 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 grâce à 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 de SConnect ou 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:

- **C:\Program Files\Swift\Swift Token Client\logs** (système 32 bits)
- **C:\Program Files (x86)\Swift\Swift Token Client\logs** (système 64 bits)

Si vous n'avez pas encore installé SConnect ou le logiciel du token, veuillez fournir les détails de configuration de votre système. Veuillez fournir les informations suivantes:

- Version du système d'exploitation et service pack
- Navigateur et version

### 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

**Copyright**

SWIFT © 2020. Tous droits réservés.

**Clause de protection**

Les informations contenues dans cette publication sont susceptibles d'être modifiées ponctuellement. Vous devez toujours vous reporter à la dernière version disponible.

**Traductions**

La version anglaise de la documentation SWIFT est la seule version officielle et contraignante.

**Marques commerciales**

SWIFT est le nom commercial de S.W.I.F.T. SC. Les noms suivants sont des marques déposées de SWIFT: 3SKey, Innotribe, MyStandards, Sibos, SWIFT, SWIFTNet, SWIFT Institute, le logo Standards Forum, le logo SWIFT, SWIFT gpi avec logo, le logo SWIFT gpi, et UETR. Les autres noms de produit, de service ou d'entreprise dans cette publication sont des noms commerciaux, des marques commerciales ou des marques déposées de leurs propriétaires respectifs.