3SKey

Description du service

Ce document décrit les fonctionnalités et les fonctions des composants de la solution 3SKey et les rôles et les responsabilités de toutes les parties impliquées dans la solution 3SKey.

24 mai 2019

Table des matières

Préface

Objet de ce document

Ce document décrit les fonctionnalités et les fonctions des différents composants de la solution 3SKey (clé de signature sécurisée SWIFT) et les rôles et les responsabilités de toutes les parties impliquées dans la solution 3SKey.

Remarque *Cette description du service, ainsi que toute autre documentation contractuelle SWIFT pertinente, est partie intégrante des accords contractuels entre SWIFT et les abonnés 3SKey, les utilisateurs 3SKey ou toute autre organisation commandant le Kit du développeur 3SKey pour la fourniture et l'utilisation des composants associés à la solution 3SKey.*

Public

Ce document s'adresse au public suivant:

- Abonnés 3SKey (généralement, les banques) ayant besoin d'informations sur les fonctionnalités et les fonctions des composants de la solution 3SKey, et sur les rôles et les responsabilités de toutes les parties impliquées dans la solution 3SKey.
- Utilisateurs 3SKey (généralement, les clients entreprise des banques, ou leurs représentants) ayant besoin d'informations sur les fonctionnalités et les fonctions des composants de la solution 3SKey, et sur les rôles et les responsabilités de toutes les parties impliquées dans la solution 3SKey.
- Personnes ayant l'intention d'utiliser ou de souscrire à la solution 3SKey, et ayant besoin d'informations sur les fonctionnalités et les fonctions des composants de la solution 3SKey, et sur les rôles et les responsabilités des parties impliquées dans la solution 3SKey.

Modifications importantes

Les tableaux suivants répertorient les changements significatifs apportés au document depuis sa publication en septembre 2016.

Ces tableaux ne comprennent pas les modifications mineures et éditoriales que SWIFT effectue pour améliorer l'utilisation et la compréhension du document.

Nouvelles informations	Emplacement
Responsabilités de l'utilisateur relatives à la mise en oeuvre de la nouvelle topologie hiérarchique PKI (migration des certificats 3SKey de l'autorité de certification SWIFTNet vers la nouvelle autorité de certification subalterne 3SKey).	Composants SWIFT à la page 12

Informations mises à jour	Emplacement
Mise à jour des hyperliens et noms de documents	Tout le document

Termes définis par SWIFT

Dans le contexte de la documentation SWIFT, certains termes ont une signification spécifique. Ces termes sont appelés "termes définis par SWIFT" (par exemple, client, utilisateur, ou produits et services SWIFT). La définition des termes définis par SWIFT apparaît dans le SWIFT Glossary.

Documentation connexe:

- Instructions à l'attention de l'administrateur 3SKey
- Instructions à l'attention de l'utilisateur 3SKey
- 3SKey Getting Started for Banks
- Mise en route de 3SKey pour les entreprises
- Guide d'installation du logiciel du token
- Guide d'utilisation du portail 3SKey pour les entreprises
- Guide de dépannage 3SKey
- 3SKey Token Renewal Instructions for Banks
- Instructions de renouvellement du token 3SKey à l'attention des administrateurs d'entreprise
- Instructions de renouvellement du token 3SKey à l'attention des utilisateurs d'entreprise
- Conditions générales de 3SKey
- 3SKey Tokens Terms and Conditions
- 3SKey Developer Toolkit Terms and Conditions
- SWIFT Advanced Support and Care Services Service Description
- SWIFT Community Support Service Description

1 Introduction

Lorsqu'une banque interagit avec des clients d'entreprise par le biais de canaux de services bancaires électroniques, elle peut avoir besoin d'authentifier les données reçues au niveau du ou des individu(s) autorisé(s) à remettre les instructions. Par exemple, un individu spécifique dans le service trésorerie de l'entreprise doit approuver des instructions de paiement.

En pratique, les banques et leurs clients d'entreprise doivent souvent gérer et utiliser des mécanismes multiples de signature personnelle (par exemple, plusieurs tokens avec des mots de passe différents et des processus différents pour les maintenir). L'utilisation et la maintenance de différentes méthodes d'authentification ajoutent de la complexité et entraînent un risque opérationnel et un coût plus élevés.

Pour résoudre ce problème, SWIFT a créé la solution 3SKey. Grâce à cette solution, SWIFT fournit des tokens qui comprennent des informations d'identification basées sur une infrastructure à clé publique (PKI) pour l'utilisation entre les abonnés 3SKey (généralement, des banques) et les utilisateurs 3SKey (généralement, des entreprises). Les utilisateurs 3SKey configurent ensuite leurs tokens à l'aide d'un certificat unique émis par l'infrastructure à clé publique (PKI) de SWIFT. Les utilisateurs 3SKey utilisent alors ces informations d'identification pour signer les messages et les fichiers échangés avec un ou plusieurs abonnés 3SKey sur un canal convenu mutuellement. La signature fournit l'authentification de l'utilisateur 3SKey et la non-répudiation des transactions signées.

1.1 Avantages de la solution 3SKey

Abonnés 3SKey

La solution 3SKey est conçue pour répondre aux besoins des abonnés et des utilisateurs 3SKey. Les abonnés 3SKey associent chaque utilisateur 3SKey individuel à des informations d'identification uniques indépendamment des autres abonnés 3SKey. Les abonnés 3SKey accèdent à l'infrastructure à clé publique (PKI) de SWIFT afin de s'assurer que le certificat n'a pas été révoqué.

Cette approche laisse chaque abonné 3SKey libre de définir et d'appliquer ses propres règles d'identification de clients lorsqu'il associe des utilisateurs 3SKey. Chaque abonné 3SKey associe ses utilisateurs 3SKey indépendamment et n'a pas besoin de s'appuyer sur l'association effectuée par les autres abonnés 3SKey.

La solution 3SKey permet aux abonnés 3SKey de mettre en oeuvre (ou de renforcer) d'une manière économique l'authentification et la non-répudiation de leurs canaux de services bancaires électroniques existants.

Utilisateurs 3SKey

Un utilisateur 3SKey doit actuellement utiliser plusieurs périphériques de sécurité différents pour s'authentifier auprès de tiers (généralement, des banques). L'utilisation d'un token unique pour plusieurs abonnés 3SKey permet de réduire le coût et le risque opérationnel, en plus d'être plus pratique.

1.2 Critères à remplir

Critères à remplir pour souscrire au service 3SKey

Le service 3SKey est disponible pour tous les utilisateurs de SWIFT et les bureaux de services.

Critères à remplir pour commander et distribuer des tokens 3SKey

Les utilisateurs de SWIFT qui ont souscrit au service 3SKey peuvent commander des tokens 3SKey auprès de SWIFT pour leur propre utilisation ou pour les distribuer à des utilisateurs 3SKey. Les utilisateurs de SWIFT affiliés de l'abonné 3SKey peuvent également commander des tokens 3SKey auprès de SWIFT pour leur propre utilisation ou pour les distribuer aux utilisateurs 3SKey en leur nom propre.

Tous les utilisateurs de SWIFT peuvent commander des tokens 3SKey auprès de SWIFT pour leur propre utilisation ou pour les distribuer à des filiales au sein de leur groupe. Un bureau de services peut distribuer les tokens 3SKey aux utilisateurs de SWIFT qui se connectent à SWIFT par son intermédiaire. Tous les partenaires de SWIFT commandant un Kit du développeur 3SKey peuvent également commander des tokens 3SKey auprès de SWIFT pour leurs propres activités de développement. Les tokens 3SKey ne doivent pas être distribués à des individus à des fins privées.

Critères à remplir pour commander le Kit du développeur 3SKey

Les utilisateurs 3SKey et tous les partenaires de SWIFT peuvent commander le Kit du développeur 3SKey auprès de SWIFT.

Pour faciliter la mise en oeuvre des fonctions de l'application de l'abonné 3SKey, SWIFT fournit le Kit du développeur 3SKey à tous les abonnés 3SKey qui le demandent.

Pour plus d'informations sur le Kit du développeur 3SKey, reportez-vous au *3SKey Developer Guide*.

2 Fonctionnalités et fonctions

2.1 Présentation

SWIFT fournit la solution 3SKey avec les composants suivants:

- **Infrastructure à clé publique (PKI) SWIFT**

  PKI sous-jacente gérée et exploitée par SWIFT. Les abonnés 3SKey et les utilisateurs 3SKey accèdent à la PKI SWIFT via le portail 3SKey ou la fonction de contrôle de révocation des certificats 3SKey, le cas échéant.

- **Tokens 3SKey**

  Périphériques sécurisés comportant les informations d'identification de signature de l'utilisateur 3SKey ou les informations d'identification d'authentification de l'abonné 3SKey pour accéder au portail.

- **Portail 3SKey**

  Les utilisateurs 3SKey y accèdent pour gérer leurs tokens 3SKey (activation, renouvellement, régénération, réinitialisation et révocation des tokens).

  Les abonnés 3SKey y accèdent pour obtenir les certificats SSL (Secure Socket Layer), pour la fonction de contrôle de révocation des certificats 3SKey, et pour obtenir les rapports sur les tokens qu'ils distribuent.

- **Fonction de contrôle de révocation des certificats 3SKey**

  Les abonnés 3SKey y accèdent pour vérifier si le certificat d'un utilisateur 3SKey (non arrivé à expiration) a été révoqué.

- **Kit du développeur 3SKey**

  Bibliothèques de logiciels, spécifications techniques et 2 tokens de test que les abonnés 3SKey et les intégrateurs utilisent pour permettre à leurs serveurs Web et leurs applications de fonctionner avec le service 3SKey. Ceci inclut les fonctions de signature, de vérification de signature et de contrôle de révocation des certificats.

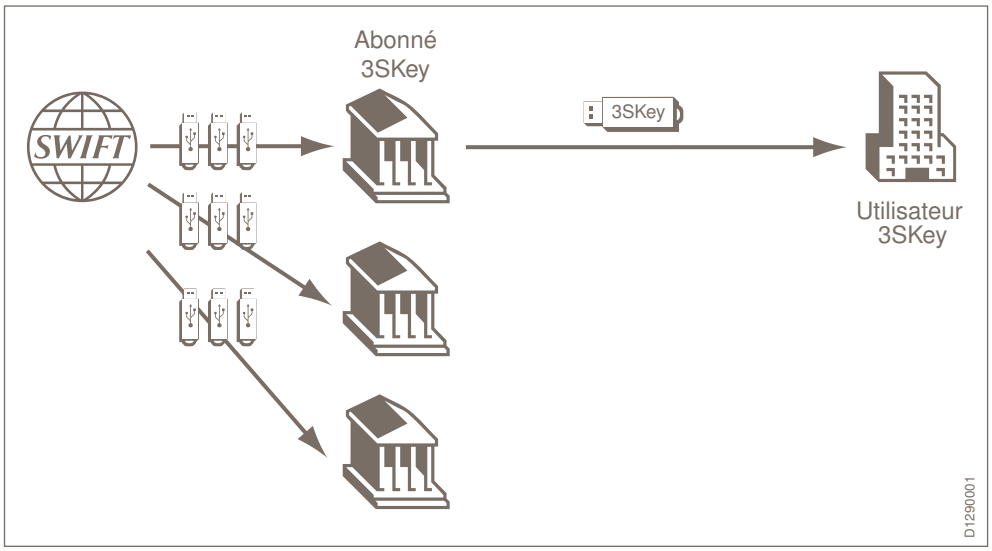
2.2 Description de la solution

2.2.1 Configuration de la solution

Procédure

1. **Fourniture et distribution des tokens 3SKey**

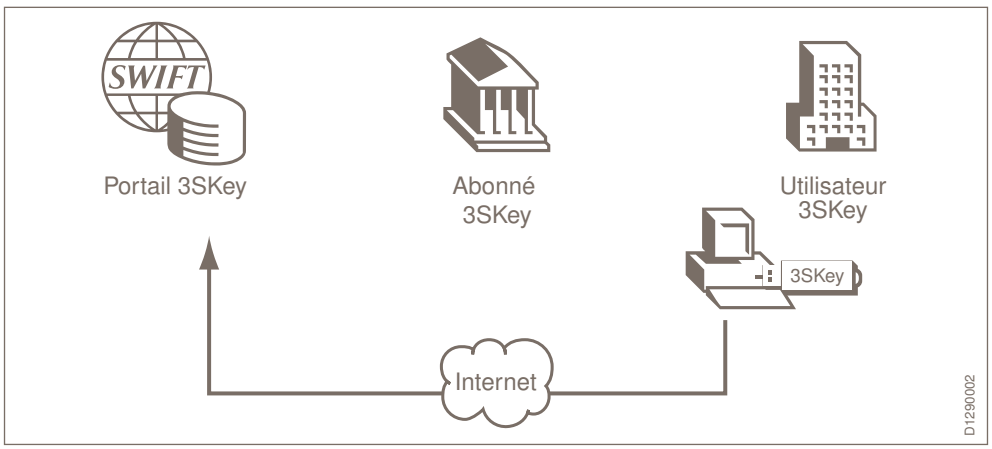
   Si un abonné 3SKey, un bureau de services ou un utilisateur 3SKey a commandé des tokens 3SKey, SWIFT fournit les tokens qui, en fonction des droits de distribution en vigueur (le cas échéant), peuvent être distribués aux utilisateurs 3SKey.



2. **Activation**

   SWIFT fournit des tokens inactifs (qui ne peuvent pas être utilisés pour signer des transactions). L'utilisateur 3SKey doit d'abord activer son token en utilisant l'accès sécurisé (fourni par le token inactif) au portail 3SKey sur Internet et le mot de passe par défaut du token.

   Des informations d'identification métier (c'est-à-dire un certificat et une clé privée) sont ensuite créées et stockées sur le token. Le processus d'activation ne requiert pas la fourniture d'informations d'identification sur l'utilisateur 3SKey, et les informations d'identification métier sont complètement anonymes. Elles ne contiennent aucun nom mais seulement l'identifiant unique utilisé par les abonnés 3SKey pour associer l'utilisateur 3SKey au certificat.



   Le même processus s'applique à l'activation de n'importe quel autre token utilisateur utilisé à des fins de tests.

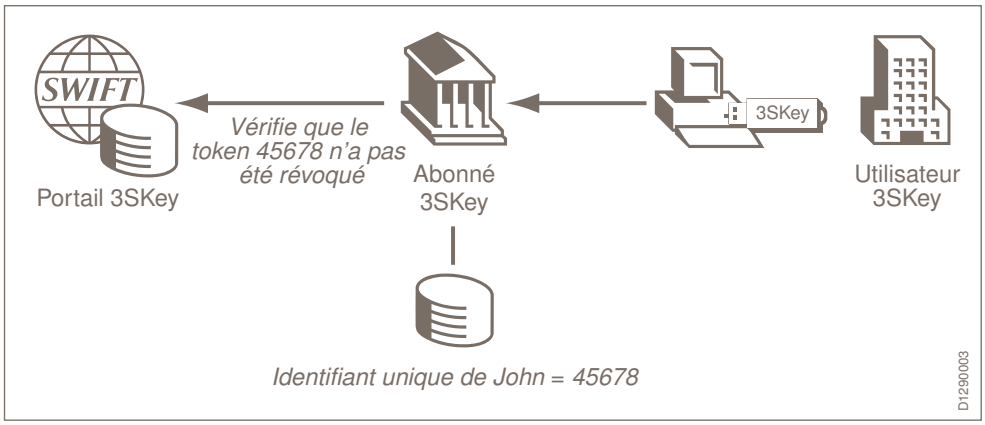
3. **Association**

   L'abonné 3SKey associe le token à son ou ses utilisateurs 3SKey.

   Ensuite, l'application de l'abonné 3SKey associe l'utilisateur 3SKey à son identifiant unique. Cette association est effectuée comme un processus d'enregistrement à convenir entre l'abonné 3SKey et l'utilisateur 3SKey directement (par exemple, via une présence physique ou l'utilisation d'une technologie d'identification à distance sécurisée et pré-existante). Au cours du processus d'association, l'abonné 3SKey doit vérifier que le certificat est valide, en utilisant notamment la fonction de contrôle de révocation des certificats 3SKey.

Lorsque le processus d'association est terminé, l'abonné 3SKey peut associer les messages signés avec les informations d'identification à l'utilisateur 3SKey enregistré ou, si le processus d'enregistrement le permet, à un représentant spécifique de l'utilisateur 3SKey.

Association des tokens 3SKey



2.2.2 Utilisation de la solution

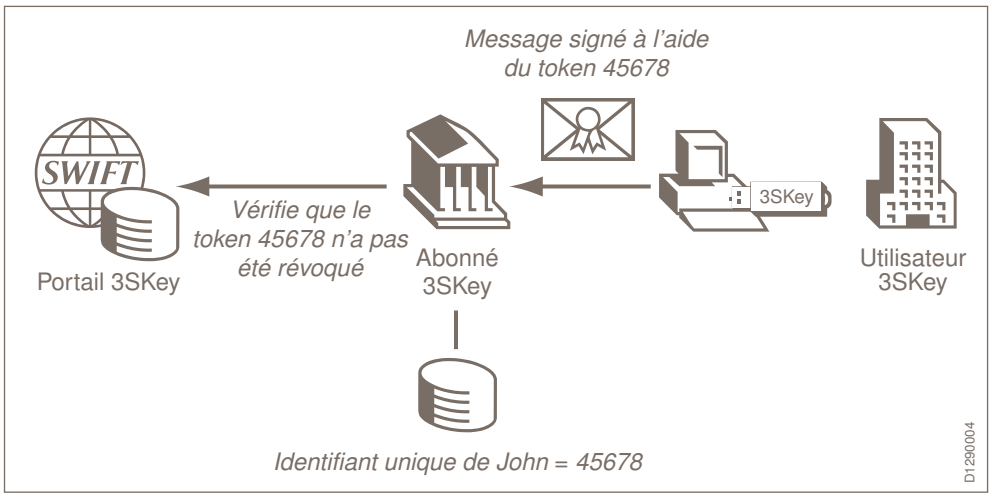
Procédure

1. **Utilisation du token**

   Lorsque les procédures d'activation et d'association ont été effectuées, l'utilisateur 3SKey peut utiliser le token pour signer des messages et des fichiers envoyés à l'abonné 3SKey ou accéder de manière sécurisée aux applications de l'abonné 3SKey à l'aide du token 3SKey.

   Le logiciel d'application de l'utilisateur 3SKey ou le navigateur de l'utilisateur 3SKey qui interagit avec l'application Web de l'abonné 3SKey (un service bancaire électronique par exemple) signe les messages avec le token de l'utilisateur 3SKey.

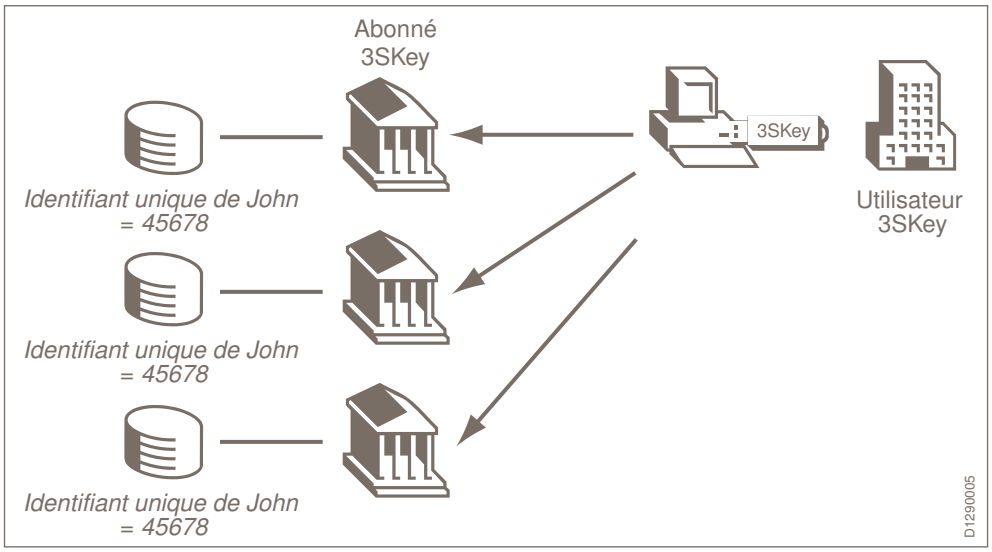
   L'application de l'abonné 3SKey vérifie la signature et accède à la fonction de contrôle de révocation des certificats 3SKey afin de vérifier que le certificat n'a pas été révoqué.



2. **Utilisation des informations d'identification métier avec des abonnés 3SKey multiples**

   Un utilisateur 3SKey peut utiliser les mêmes informations d'identification métier pour signer des messages pour des transactions avec d'autres abonnés 3SKey ou pour accéder de manière sécurisée aux applications d'autres abonnés 3SKey. L'abonné 3SKey doit s'associer avec

chaque utilisateur 3SKey séparément. Il s'agit du même processus que celui décrit dans l'étape 3 à la page 8 de la section "Configuration de la solution".



2.2.3 Maintenance de la solution

Procédure

1. **Révocation**

   Si le token 3SKey a été volé, ou si sa sécurité ou sa fiabilité est compromise d'une autre manière (généralement, la personne qui utilise le token quitte l'entreprise), l'utilisateur 3SKey ou l'administrateur 3SKey peut demander la révocation de son certificat via le portail 3SKey.

   SWIFT met alors à jour la liste de révocation des certificats avec les informations de révocation du certificat. Lorsque l'application de l'abonné 3SKey vérifie la liste de révocation des certificats, le certificat apparaît comme révoqué et, en conséquence, l'application de l'abonné 3SKey arrête de le considérer comme étant de confiance.

   Certains abonnés 3SKey peuvent également demander à leurs utilisateurs 3SKey de désassocier le certificat avec eux directement.

   Pour plus d'informations, les utilisateurs 3SKey doivent vérifier les conditions régissant l'utilisation du certificat avec leurs abonnés 3SKey.

2. **Renouvellement**

   Le token de l'utilisateur 3SKey expire après 3 ans. Avant l'expiration du token, l'utilisateur 3SKey doit renouveler le certificat sur un nouveau token via le portail. L'utilisateur 3SKey peut renouveler le token durant 90 jours avant sa date d'expiration. Après, le token devient inutilisable et le certificat devra être régénéré.

   Le nouveau token héritera de l'identifiant unique d'origine. L'ancien token peut toujours être utilisé jusqu'à ce que le certificat expire.

   Ceci s'applique également aux tokens utilisateurs utilisés à des fins de tests. Les tokens utilisateurs **non activés** ne peuvent pas être renouvelés.

3. **Régénération**

   Il peut être nécessaire de régénérer un certificat si le certificat a été révoqué ou si le token portant le certificat est perdu ou n'est plus utilisable (par exemple, s'il est endommagé) ou si le certificat a expiré. Dans ce cas, l'utilisateur 3SKey demande à un administrateur 3SKey de

configurer le certificat en vue d'une régénération sur un nouveau token. Par l'intermédiaire du portail 3SKey, l'utilisateur 3SKey peut régénérer son certificat sur un nouveau token ayant été configuré en vue d'une régénération par l'administrateur. Pour procéder à la régénération, l'utilisateur 3SKey doit fournir son code de sécurité.

Le nouveau token comprendra un nouveau certificat métier avec l'identifiant unique d'origine, et sera valide pendant 3 ans. L'ancien certificat ne peut plus être utilisé.

Ceci s'applique également aux tokens utilisateurs utilisés à des fins de tests. Les tokens utilisateurs **non activés** ne peuvent pas être régénérés.

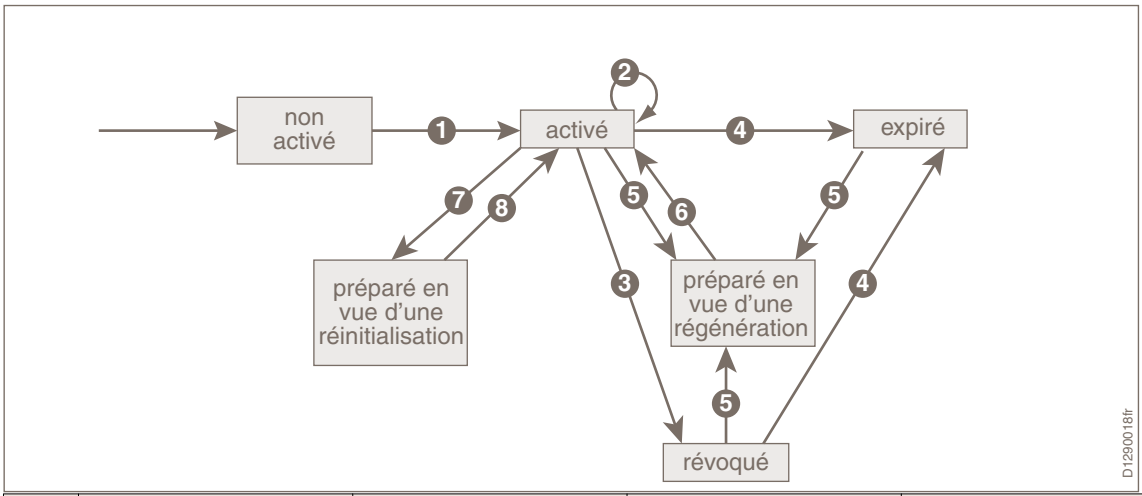
4. **Réinitialisation**

   Il peut être nécessaire de réinitialiser un token si le token est verrouillé après une série de saisie de mots de passe incorrects ou si l'utilisateur 3SKey a perdu son mot de passe. Dans ce cas, l'utilisateur 3SKey demande à un administrateur 3SKey de configurer le token verrouillé en vue d'une réinitialisation. Par l'intermédiaire du portail 3SKey, l'utilisateur 3SKey peut réinitialiser son token avec un nouveau certificat et définir un nouveau mot de passe. Pour procéder à la réinitialisation, l'utilisateur 3SKey doit fournir son code de sécurité.

   Après réinitialisation, le token détient un nouveau certificat métier ou, le cas échéant, un nouveau certificat technique, portant l'identifiant unique d'origine et la même date d'expiration que l'ancien certificat. Ceci s'applique également aux tokens utilisateurs utilisés à des fins de tests.

2.2.4 Gestion et cycle de vie du token 3SKey

Le diagramme suivant indique les différents statuts par lesquels un token 3SKey peut passer ainsi que l'auteur du changement.



	Statut précédent du token	Nouveau statut du token	Action	Auteur
1	**Non activé**	**Activé**	activer	utilisateur
2	**Activé**	**Activé**	renouveler	utilisateur
3	**Activé**	**Révoqué**	révoquer	administrateur ou utilisateur

	Statut précédent du token	Nouveau statut du token	Action	Auteur
4	**Activé**	**Expiré**	expirer	automatiquement
4	**Révoqué**	**Expiré**	expirer	automatiquement
5	**Activé**	**Préparé en vue d'une régénération)**	configurer en vue d'une régénération	administrateur
5	**Révoqué**	**Préparé en vue d'une régénération**	configurer en vue d'une régénération	administrateur
5	**Expiré**	**Préparé en vue d'une régénération**	configurer en vue d'une régénération	administrateur
6	**Préparé en vue d'une régénération**	**Activé**	régénérer	utilisateur
7	**Activé**	**Préparé en vue d'une réinitialisation**	configurer en vue d'une réinitialisation	administrateur
8	**Préparé en vue d'une réinitialisation)**	**Activé**	réinitialiser	utilisateur

2.3 Composants de la solution 3SKey

Les composants de la solution 3SKey sont déployés par les différentes parties, de la manière suivante:

- **SWIFT**: PKI SWIFT, portail 3SKey et fonction de contrôle de révocation des certificats 3SKey
- **Abonné 3SKey**: application de l'abonné 3SKey, tokens de l'abonné 3SKey et Kit du développeur 3SKey
- **Utilisateur 3SKey**: application de l'utilisateur 3SKey, tokens de l'utilisateur 3SKey, Kit du développeur 3SKey et navigateur Web

2.3.1 Composants SWIFT

PKI SWIFT

La PKI SWIFT supporte les opérations PKI suivantes:

- émission de nouveaux certificats
- renouvellement de certificat
- révocation de certificat
- régénération de certificat

Modifications de l'infrastructure PKI SWIFT

SWIFT introduit une nouvelle topologie hiérarchique PKI. Une nouvelle autorité de certification racine SWIFT émettra un certificat vers une nouvelle autorité de certification subalterne. Cette nouvelle autorité de certification subalterne 3SKey émettra tous les nouveaux certificats pour les

utilisateurs 3SKey. Actuellement, l'autorité de certification SWIFTNet émet tous les certificats pour les utilisateurs 3SKey.

La migration des utilisateurs 3SKey de l'autorité de certification SWIFTNet vers la nouvelle autorité de certification subalterne 3SKey (date de commencement prévue en décembre 2019) se produira de manière graduelle en fonction de la durée de validité du certificat. Durant la phase de migration, les abonnés 3SKey doivent se fier à la fois à l'autorité de certification SWIFTNet et à l'autorité de certification subalterne 3SKey afin de valider correctement le certificat de l'utilisateur 3SKey. Ils doivent également se fier à la nouvelle autorité de certification racine SWIFT qui émet le certificat vers l'autorité de certification subalterne 3SKey.

Pour obtenir un aperçu du projet d'évolution PKI et de l'impact sur les rôles et responsabilités des abonnés 3SKey, reportez-vous à PKI Evolution - Impact to 3SKey Service Providers.

Pour obtenir les dernières informations sur l'évolution de l'infrastructure PKI, consultez l'article 5022693 de la Knowledge Base.

Portail 3SKey

SWIFT fournit un portail Web.

- Un utilisateur 3SKey dûment authentifié peut accéder au portail 3SKey pour effectuer les fonctions suivantes sur le token 3SKey:
  - activation
  - renouvellement (sur un nouveau token)
  - révocation
  - régénération (sur un nouveau token)
  - réinitialisation (sur le même token)
  - gestion du mot de passe et du code de sécurité
  - fonctions de gestion de listes d'utilisateurs
- Un abonné 3SKey authentifié peut accéder au portail pour effectuer les fonctions suivantes:
  - récupérer les certificats SSL (utilisés pour accéder de manière sécurisée à la fonction de contrôle de révocation des certificats 3SKey)
  - récupérer un rapport sur les tokens distribués par l'abonné 3SKey et leur statut

Fonction de contrôle de révocation des certificats 3SKey

L'abonné 3SKey peut accéder à la liste de révocation des certificats pertinente en utilisant un accès sécurisé à la fonction de contrôle de révocation des certificats 3SKey via Internet. Cette opération nécessite un certificat SSL que l'abonné 3SKey obtient sur le portail.

La fonction de contrôle de révocation des certificats 3SKey est disponible uniquement pour les abonnés 3SKey.

Pour plus d'informations, reportez-vous au document 3SKey Getting Started for Banks.

2.3.2 Composants de l'abonné 3SKey

Application de l'abonné 3SKey

Pendant la phase d'association, l'abonné 3SKey doit effectuer les activités suivantes par le biais de son application:

- établissement de la correspondance entre l'identifiant unique et une identité (nom ou poste de la personne par exemple)
- vérification de la signature
- vérification que le certificat est un certificat métier 3SKey en vérifiant qu'il comporte l'identifiant 1.3.21.6.3.20.200.1
- vérification que le certificat a été émis par l'autorité de certification SWIFTNet ou l'autorité de certification subalterne 3SKey
- vérification que le certificat n'est pas arrivé à expiration
- vérification que le certificat n'a pas été révoqué

Lorsqu'il traite des transactions commerciales, l'abonné 3SKey doit effectuer les activités suivantes par le biais de son application:

- vérification de la signature des messages ou des fichiers ayant été signés avec un token 3SKey
- vérification que le certificat de signature est un certificat métier 3SKey en vérifiant qu'il comporte l'identifiant 1.3.21.6.3.20.200.1
- vérification que le certificat a été émis par l'autorité de certification SWIFTNet ou l'autorité de certification subalterne 3SKey
- vérification que le certificat de signature n'est pas arrivé à expiration
- vérification que le certificat de signature n'a pas été révoqué
- conservation des journaux de non-répudiation des transactions signées

Remarque *L'abonné 3SKey est chargé de l'intégration du service 3SKey avec sa ou ses application(s) en utilisant le Kit du développeur 3SKey ou avec l'aide d'un fournisseur de son choix.*

Tokens de l'abonné 3SKey

Les abonnés 3SKey reçoivent des tokens spécifiques pour accéder au portail afin de récupérer un certificat SSL et d'accéder à un rapport sur les tokens. Le certificat SSL permet aux abonnés d'accéder de manière sécurisée à la fonction de contrôle de révocation des certificats 3SKey. Le rapport sur les tokens répertorie les tokens commandés par l'abonné 3SKey ainsi que leur statut.

Kit du développeur 3SKey

Pour faciliter la mise en oeuvre des fonctions de l'application de l'abonné 3SKey, SWIFT fournit le Kit du développeur 3SKey à tous les abonnés 3SKey qui le demandent.

Pour plus d'informations sur le Kit du développeur 3SKey, reportez-vous au *3SKey Developer Guide*.

Navigateur Web

Le navigateur de l'abonné 3SKey accède au portail 3SKey pour récupérer les certificats SSL et obtenir un rapport sur les tokens commandés et leur statut. L'abonné 3SKey doit s'assurer que son navigateur Web répond aux spécifications applicables définies dans le Guide d'installation du logiciel du token.

2.3.3 Composants de l'utilisateur 3SKey

Application de l'utilisateur 3SKey

L'application doit permettre aux utilisateurs 3SKey de signer des fichiers et des messages avec le token 3SKey et de les envoyer à l'application de l'abonné 3SKey ou d'accéder de manière sécurisée aux applications de l'abonné 3SKey.

Remarque *L'utilisateur 3SKey est chargé de l'intégration du service 3SKey avec sa ou ses application(s) en utilisant le Kit du développeur 3SKey ou avec l'aide d'un fournisseur de son choix.*

Tokens de l'utilisateur 3SKey

Les utilisateurs 3SKey installent le logiciel pour les tokens 3SKey. Ils activent leurs tokens via le portail 3SKey et ils les associent à leur(s) abonné(s) 3SKey. Les utilisateurs 3SKey peuvent alors utiliser leurs tokens avec leur(s) abonné(s) 3SKey par l'intermédiaire du navigateur ou de l'application de l'utilisateur 3SKey.

Remarque *Pour éviter toute confusion, SWIFT recommande de ne pas ré-assigner un token à une autre personne une fois que l'association a été effectuée.*

Navigateur Web

L'utilisateur 3SKey accède au portail 3SKey en utilisant un navigateur Web. Le portail est utilisé pour la gestion des tokens (activation, révocation, régénération, réinitialisation et renouvellement). Le navigateur Web est nécessaire pour permettre d'accéder à des services basés sur le Web (gestion de la trésorerie par exemple). L'utilisateur 3SKey doit s'assurer que son navigateur Web répond aux spécifications applicables définies dans le Guide d'installation du logiciel du token.

2.4 Disponibilité du service 3SKey

Disponibilité de la fonction de contrôle de révocation des certificats 3SKey

La fonction de contrôle de révocation des certificats 3SKey est conçue pour être disponible 24 heures sur 24 et 7 jours sur 7, via des canaux LDAPS et HTTPS, sous réserve de toute indisponibilité comme stipulé ci-après.

SWIFT n'est pas responsable s'il est impossible d'accéder à la fonction de contrôle de révocation des certificats 3SKey en raison de problèmes avec les canaux Internet utilisés par l'abonné 3SKey.

Indisponibilité planifiée

SWIFT planifie des dates et des heures spécifiques auxquelles le service 3SKey, généralement l'accès au portail 3SKey, sera indisponible. SWIFT publie les notifications d'indisponibilité à l'avance sur le site www.swift.com.

Une indisponibilité planifiée peut être due aux événements suivants:

- interruption en raison d'une maintenance planifiée de l'équipement
- modifications planifiées apportées au système (par exemple, modifications apportées aux logiciels ou aux configurations matérielles ou test de continuité de l'activité)

SWIFT effectue des modifications du système et des opérations de maintenance pendant les fenêtres d'interruption autorisées. Ces fenêtres ont lieu pendant les week-ends (samedi et dimanche).

Pendant une fenêtre d'interruption autorisée, le portail 3SKey peut être indisponible pendant toute la durée de l'interruption ou seulement par intermittence.

Pour plus d'informations sur les interruptions planifiées, reportez-vous à www.swift.com > Ordering & Support > SWIFT Operational Status.

Indisponibilité non planifiée

Si la société SWIFT est informée d'un problème avec le service 3SKey, elle initialise toute opération de régénération ou de secours dont elle est responsable pour restaurer le service.

SWIFT peut suspendre ou modifier le service 3SKey, dans son intégralité ou en partie, à tout moment en donnant autant d'informations que possible à l'avance afin d'éviter ou de limiter les effets défavorables sur la sécurité, la fiabilité ou la résilience du service 3SKey ou, de manière plus générale, l'image, la réputation ou le bon vouloir de SWIFT (typiquement si l'abonné 3SKey et l'utilisateur 3SKey sont sujets à des programmes de sanctions tel que le programme de sanctions de l'Union européenne).

Les niveaux de service spécifiés par ce document supposent des conditions de fonctionnement normales. Celles-ci incluent les opérations résilientes pendant la plupart des scénarios de défaillance de composant unique au sein des centres d'exploitation SWIFT de production et de secours où SWIFT exécute la fonction de contrôle de révocation des certificats 3SKey. La conception de la fonction de contrôle de révocation des certificats 3SKey est résiliente, et peut traiter la plupart des événements anormaux sans impact sur les activités des utilisateurs et des abonnés 3SKey. Cependant, dans certains scénarios très improbables de sinistre (par exemple, la destruction d'un centre d'exploitation SWIFT, des défaillances doubles de composants similaires, ou des défaillances de composants pendant les basculements de centre d'exploitation SWIFT), SWIFT peut ne pas être en mesure de se conformer à ces niveaux de service, en totalité ou en partie. Dans de tels cas, le risque de perdre des données est réel. En pareille situation, SWIFT informera les abonnés 3SKey concernés et les utilisateurs 3SKey qui ont enregistré une adresse e-mail via le portail 3SKey.

Par exemple, si un sinistre frappait un centre d'exploitation SWIFT où SWIFT exécute le service 3SKey, ceci pourrait empêcher SWIFT de traiter entièrement toutes les demandes de révocation reçues dans les 15 minutes précédant le sinistre. Dans ce cas, les utilisateurs 3SKey peuvent contacter SWIFT pour obtenir une assistance pour assurer le suivi des demandes affectées.

3 Commandes et assistance

3.1 Passation de commandes

Souscription au service 3SKey

Les utilisateurs de SWIFT et les bureaux de services peuvent souscrire au service 3SKey en utilisant le formulaire de souscription 3SKey. Il est obligatoire de souscrire au service 3SKey pour se fier à un certificat 3SKey.

En tant que partie intégrante de sa souscription, l'abonné 3SKey a droit à ce qui suit:

- accès au portail 3SKey
- accès à la fonction de contrôle de révocation des certificats 3SKey (10 accès au maximum)
- des tokens 3SKey comme spécifié dans le formulaire de souscription

Les abonnés 3SKey qui souhaitent obtenir le Kit du développeur 3SKey doivent en faire la demande via une commande séparée comme spécifié ci-dessous.

Remarque *La souscription au service 3SKey par un utilisateur de SWIFT permet à l'abonné 3SKey d'étendre, sous sa seule responsabilité, les avantages de la souscription à ses filiales au sein de son groupe. Dans le cas contraire, la souscription au service 3SKey est personnelle. En conséquence, l'abonné 3SKey ne peut communiquer la liste de révocation des certificats à un tiers (ou, dans le cas d'un utilisateur de SWIFT, à une entité non-affiliée), ou ne peut vérifier le statut d'un certificat 3SKey pour le compte d'un tiers (ou, dans le cas d'un utilisateur de SWIFT, d'une entité non-affiliée).*

Pour plus d'informations sur le droit des abonnés 3SKey d'utiliser le service 3SKey, reportez-vous aux 3SKey Tokens Terms and Conditions*.*

Commande de tokens 3SKey

Les utilisateurs de SWIFT, les bureaux de services et les partenaires peuvent commander des tokens 3SKey pour leur utilisation personnelle et, en fonction de leurs droits de distribution respectifs (le cas échéant), pour la distribution à des utilisateurs 3SKey en utilisant le formulaire de commande de tokens 3SKey.

La fourniture, l'utilisation et, si autorisée, la distribution des tokens 3SKey sont soumises aux restrictions d'exportation des États-Unis et autres programmes de sanction. Les personnes situées à Cuba, en Corée du Nord, en Iran, au Soudan ou en Syrie et/ou 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, à utiliser, ni à distribuer des tokens 3SKey.

Commande du Kit du développeur 3SKey

Les utilisateurs de SWIFT, les bureaux de services et les partenaires peuvent commander le Kit du développeur 3SKey en utilisant le formulaire de commande du Kit du développeur 3SKey. Le Kit du développeur 3SKey comprend un guide du développeur incluant les spécifications techniques, les bibliothèques de logiciels et 2 tokens de test.

3.2 Assistance

Assistance pour les abonnés 3SKey et le Kit du développeur 3SKey

SWIFT est l'unique point de contact pour reporter tous les problèmes et requêtes relatifs au service 3SKey et au Kit du développeur 3SKey. Une assistance est également disponible pour le Kit du développeur 3SKey. Les utilisateurs individuels au sein de leur organisation respective doivent s'inscrire pour utiliser le service d'assistance.

Informations connexes

Pour plus d'informations sur la procédure d'inscription au service d'assistance, reportez-vous à la section **Customer login** (Connexion client) sur la page d'accueil de www.swift.com.

Pour plus d'informations sur les services d'assistance, reportez-vous aux documents suivants:

- SWIFT Advanced Support and Care Services Service Description
- SWIFT Community Support Service Description

Assistance pour les utilisateurs 3SKey

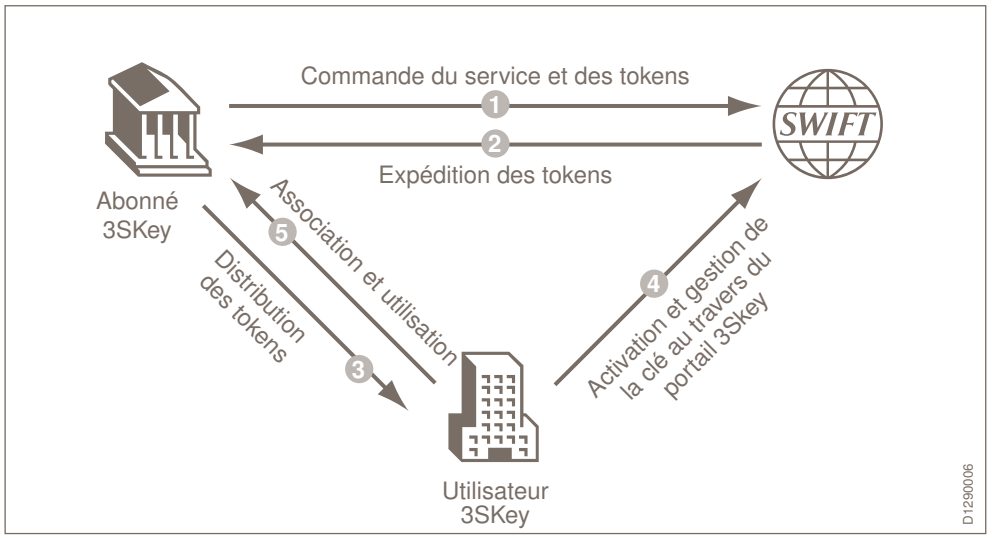
Une assistance en ligne pour les fonctions de gestion des tokens est disponible pour les utilisateurs 3SKey via le site Web 3SKey.

4 Rôles et responsabilités

Les trois parties suivantes sont impliquées dans la solution 3SKey:

- **SWIFT**: fournit le service 3SKey, les tokens 3SKey et le Kit du développeur 3SKey.
- L'**abonné 3SKey**: fournit et intègre le service 3SKey, et distribue les tokens 3SKey aux utilisateurs 3SKey.
- L'**utilisateur 3SKey**: 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.

Le graphique suivant présente les interactions entre les différentes parties:



4.1 Rôles et responsabilités de SWIFT

Les principales responsabilités de SWIFT sont les suivantes:

- fourniture du service tel que décrit dans la description du service
- gestion et exploitation des PKI SWIFT
- qualification des tokens
- personnalisation des tokens avec un identifiant unique
- fourniture et mise en oeuvre des règles de certification
- vérification du caractère unique de l'identifiant d'un certificat depuis l'activation et pendant tout son cycle de vie
- fourniture de tokens inactifs
- fourniture d'un portail pour les utilisateurs 3SKey pour les fonctions de gestion des tokens
- fourniture de la fonction de contrôle de révocation des certificats 3SKey aux abonnés 3SKey et plus particulièrement, la mise à disposition d'une version mise à jour de la liste de révocation des certificats aux abonnés 3SKey (dans les 4 heures pour la liste de révocation des certificats combinée et dans les 7 minutes pour les listes de révocation des certificats partitionnées) après la révocation d'un token 3SKey par un utilisateur 3SKey

- lorsque spécifiquement commandé, fourniture du Kit du développeur 3SKey, incluant les spécifications techniques, les bibliothèques de logiciels pertinentes et 2 tokens de test pour intégrer le service 3SKey dans les applications de l'abonné et de l'utilisateur 3SKey
- fourniture d'assistance aux abonnés 3SKey, utilisateurs 3SKey et partenaires pour les composants de la solution 3SKey qui sont pertinents pour eux
- mise à disposition de la documentation 3SKey sur www.swift.com et le site Web 3SKey.
- fourniture d'un rapport aux abonnés 3SKey sur le statut (activé, non activé, préparé en vue d'une régénération, préparé en vue d'une réinitialisation, révoqué, utilisé pour la régénération, utilisé pour le renouvellement) des certificats qui sont stockés sur les tokens qu'ils ont commandés
- révocation des certificats métier via une procédure exceptionnelle hors ligne en contactant l'assistance SWIFT
- confirmation, à la demande de l'utilisateur 3SKey, des détails de l'activation, du renouvellement, de la réinitialisation, de la révocation ou de la régénération d'un certificat sur le portail 3SKey pendant 6 mois au maximum après la date d'expiration de ce certificat. Les actions effectuées sur un certificat par un utilisateur 3SKey sont non-répudiées et horodatées. Par conséquent, SWIFT peut confirmer l'identifiant unique de l'utilisateur 3SKey qui a initié le changement ainsi que la date et l'heure du changement.
- fourniture, à la demande de l'utilisateur ou de l'abonné 3SKey, de la preuve du statut de révocation d'un certificat spécifique pendant 10 ans au maximum

SWIFT se réserve le droit de révoquer unilatéralement des certificats dans des circonstances spécifiques (par exemple, s'il apparaîtrait ou deviendrait probable, sur la base de fondements raisonnables, qu'un certificat a été, est ou pourrait être utilisé à des fins illégales, illicites ou frauduleuses, d'une façon qui pourrait créer la confusion ou présenter de manière inexacte une personne normalement associée au certificat).

Utilisation des données à des fins d'enquêtes et de contrôles de sécurité

Conformément à la SWIFT Data Retrieval Policy (règles de récupération des données) et des principes de Distributed Architecture (architecture distribuée), SWIFT peut traiter et stocker les données du trafic et des messages afin de supporter les mesures de protection ainsi que les capacités forensiques de SWIFT contre les menaces de cybersécurité. SWIFT traite et stocke ces données sur des systèmes de sécurité dédiés en stricte conformité avec ses règles et ses procédures de sécurité et peut analyser ces données dans le cadre d'une enquête spécifique de sécurité dans le contexte de ses processus d'enquêtes et de contrôles de sécurité.

Information associée

Pour plus d'informations sur les rôles et les responsabilités de SWIFT concernant la solution 3SKey, reportez-vous aux documents suivants:

Conditions générales de 3SKey
3SKey Tokens Terms and Conditions
3SKey Developer Toolkit Terms and Conditions

4.2 Rôles et responsabilités de l'abonné 3SKey

Description

Les principales responsabilités de l'abonné 3SKey sont les suivantes:

1. Pour son utilisation personnelle et, le cas échéant, pour la distribution des tokens 3SKey aux utilisateurs 3SKey:
   - commande des tokens 3SKey auprès de SWIFT
   - sous réserve de toutes les restrictions d'exportation et des autres programmes de sanctions applicables, distribution des tokens 3SKey et du mot de passe associé aux utilisateurs 3SKey qui en font la demande, association des utilisateurs 3SKey ou fourniture aux utilisateurs 3SKey des instructions et logiciels d'installation associés
   - gestion du processus de renouvellement de token avec les utilisateurs 3SKey
2. Pour l'utilisation du service 3SKey:
   - souscription au service 3SKey
   - intégration du service 3SKey avec l'application de l'abonné 3SKey (et alignement conformément à l'évolution du service 3SKey par SWIFT)
   - fourniture de la documentation pertinente pour l'utilisation du service 3SKey et des tokens aux utilisateurs 3SKey
   - fourniture des directives de meilleures pratiques aux utilisateurs 3SKey
   - association et conservation de l'association des tokens avec les utilisateurs 3SKey utilisant le service 3SKey
   - obtention et gestion d'un certificat client SSL valide afin de sécuriser l'accès à la fonction de contrôle de révocation des certificats 3SKey
   - obtention et gestion d'une connexion Internet au portail 3SKey et à la fonction de contrôle de révocation des certificats 3SKey
   - mise en place et application d'une obligation de s'informer sur les clients pour associer les utilisateurs 3SKey à leur(s) token(s)
   - notification à SWIFT de toutes les menaces de sécurité liées au service 3SKey
   - vérification des signatures des messages reçus de la part des utilisateurs 3SKey et vérification que les certificats de signature sont des certificats métier 3SKey valides

Dans la mesure où cela s'avère nécessaire pour son utilisation de la solution 3SKey, l'abonné 3SKey a le droit, à ses propres frais et sous sa seule responsabilité, de traduire les informations fournies par SWIFT et d'inclure ces informations dans sa documentation d'utilisateur final. Ces traductions doivent toutefois confirmer que, vis-à-vis de SWIFT, la version anglaise de la documentation SWIFT est la seule version officielle et contraignante.

Tests effectués par le client

Les clients ne doivent pas procéder à des tests de performance ou de vulnérabilité sur ou via des produits et services SWIFT sauf si expressément autorisé dans la SWIFT Customer Testing Policy. Si les clients pensent avoir identifié une potentielle menace de performance ou de vulnérabilité, ils doivent immédiatement en informer SWIFT et considérer tous les matériels, données ou informations y afférents comme des informations SWIFT confidentielles.

Information associée

Pour plus d'informations sur les rôles et les responsabilités de l'abonné 3SKey concernant la solution 3SKey, les abonnés 3SKey peuvent se reporter aux documents suivants:

Conditions générales de 3SKey
3SKey Tokens Terms and Conditions
3SKey Developer Toolkit Terms and Conditions

4.3 Rôles et responsabilités de l'utilisateur 3SKey

Description

Les principales responsabilités de l'utilisateur 3SKey sont les suivantes:

- effectuer le travail d'intégration relatif au fonctionnement du service 3SKey avec l'abonné 3SKey (ou les abonnés 3SKey)
- activer le token via le portail 3SKey
- à des fins d'authentification auprès de SWIFT, conserver en sécurité l'identifiant unique et le code de sécurité associé
- associer un ou plusieurs tokens avec l'abonné 3SKey (ou les abonnés 3SKey)
- effectuer la gestion des tokens conformément aux directives fournies dans la documentation sur 3SKey
- conserver en sécurité le récépissé de toutes les fonctions de gestion effectuées sur le portail 3SKey
- obtenir de nouveaux tokens avant l'expiration des tokens
- protéger physiquement les tokens d'un accès non-autorisé (emprunt, perte, et vol) et prendre toutes les mesures nécessaires pour empêcher la divulgation du mot de passe du token. L'utilisateur 3SKey doit maintenir la confidentialité, l'intégrité et la disponibilité de sa clé privée à tout moment.
- révoquer les tokens en cas de menace de sécurité, si le token n'est plus utilisé, ou pour toute raison jugée nécessaire ou souhaitable. Après avoir demandé la révocation d'un certificat 3SKey, vérifier dès que possible sur le portail 3SKey que le certificat a dûment été révoqué par SWIFT.
- informer le ou les abonné(s) 3SKey et SWIFT de toute menace de sécurité pouvant affecter l'utilisation du service 3SKey
- respecter les directives de meilleures pratiques fournies par l'abonné 3SKey
- se conformer à toutes les obligations convenues avec son ou ses abonné(s) directement

Tests effectués par le client

Les clients ne doivent pas procéder à des tests de performance ou de vulnérabilité sauf si expressément autorisé dans la SWIFT Customer Testing Policy.

Si les clients pensent avoir identifié une potentielle menace de performance ou de vulnérabilité, ils doivent immédiatement en informer SWIFT et considérer tous les matériels, données ou informations y afférents comme des informations SWIFT confidentielles.

Information associée

Pour plus d'informations sur les rôles et les responsabilités de l'utilisateur 3SKey concernant la solution 3SKey, les utilisateurs 3SKey peuvent se reporter aux documents suivants:

Conditions générales de 3SKey
3SKey Tokens Terms and Conditions
3SKey Developer Toolkit Terms and Conditions

5 Tarifs et facturation

Frais

L'abonné 3SKey doit régler à SWIFT tous les frais et honoraires pour les différents composants de la solution 3SKey.

Les frais pour la souscription à la solution 3SKey sont les suivants:

- un investissement initial pour la souscription par les abonnés 3SKey au service 3SKey
- un montant annuel récurrent pour la souscription par les abonnés 3SKey au service 3SKey
- un investissement fixe pour la fourniture des tokens 3SKey

Informations connexes

Pour plus d'informations sur la tarification, contactez votre SWIFT Account Manager.

6 Cadre contractuel

Conditions générales

Les Conditions générales de 3SKey régissent la fourniture et l'utilisation du service 3SKey.

Les 3SKey Tokens Terms and Conditions régissent la fourniture, la distribution et l'utilisation des tokens 3SKey.

Les 3SKey Developer Toolkit Terms and Conditions régissent la fourniture et l'utilisation du Kit du développeur 3SKey.

Consultez toujours la Legal page on www.swift.com pour obtenir la dernière version de ces documents.

Autres accords contractuels entre les abonnés 3SKey et les utilisateurs 3SKey

Il est de la responsabilité des abonnés 3SKey et des utilisateurs 3SKey d'envisager tout autre accord contractuel nécessaire ou souhaitable entre eux en relation avec leur utilisation du service 3SKey. L'utilisation des tokens 3SKey est régie par l'accord entre l'utilisateur et l'abonné.

Par exemple, ces accords contractuels peuvent définir le processus que l'utilisateur 3SKey doit suivre lorsqu'il enregistre ses tokens 3SKey auprès de l'abonné 3SKey, l'obligation pour l'utilisateur 3SKey de demander à l'abonné de désassocier un certificat lorsqu'il devient obsolète, les règles que l'abonné 3SKey applique pour vérifier la révocation du certificat et, plus particulièrement, la fréquence de ces vérifications ainsi que le processus de traitement des litiges, en ce compris la période de réclamation compte tenu de la période de rétention des journaux de la liste de révocation des certificats par SWIFT.

Assistance SWIFT

En cas de litige entre un utilisateur 3SKey et un abonné 3SKey, SWIFT agira en tant que partie de confiance neutre en fournissant les preuves pertinentes en sa possession.

7 Glossaire des termes

Terme	Définition
3SKey	Signifie SWIFT Secure Signature Key (clé de signature sécurisée SWIFT).
Abonné 3SKey	Organisation participant au service 3SKey, client de SWIFT, dans le but de proposer une application sécurisée à ses clients. Généralement, une banque.
Administrateur	Personne désignée dans l'organisation de l'utilisateur 3SKey, chargée d'attribuer les tokens à une liste d'utilisateurs, de distribuer les tokens aux utilisateurs, de révoquer les certificats et de les configurer en vue d'une réinitialisation ou d'une régénération et rappelant aux utilisateurs de renouveler leurs certificats. Les administrateurs peuvent également avoir accès au statut des certificats de tous les tokens présents dans leur liste d'utilisateurs. Les administrateurs peuvent également accéder à toutes les fonctions de l'utilisateur 3SKey avec leurs propres tokens.
Certificat métier	Certificat valide pour la signature d'une transaction métier. Ce certificat 3SKey est identifié avec l'identifiant 1.3.21.6.3.20.200.1.
Code de sécurité	Chaîne d'authentification personnelle générée par le portail au moment de l'activation ou plus tard à la demande de l'utilisateur, et que l'utilisateur 3SKey peut utiliser pour révoquer son certificat, et qu'il doit fournir pour réinitialiser ou régénérer son certificat.
Portail 3SKey	Serveur applicatif Web pour les opérations de gestion du token 3SKey et du certificat: activation, renouvellement, réinitialisation, régénération, administration de la liste d'utilisateurs, modification du code de sécurité, modification du mot de passe et révocation.
Token actif	Token 3SKey comprenant un certificat métier valide.
Utilisateur 3SKey	Organisation, ou utilisateur individuel dans cette organisation, client d'un abonné 3SKey, dans le but d'utiliser l'application sécurisée fournie par l'abonné 3SKey. Généralement, une entreprise.

Mentions légales