GUIDE

STORMSHIELD DATA SECURITY FOR CLOUD & MOBILITY

ARCHITECTURE ET SÉCURITÉ

Version 3

Dernière mise à jour du document : 13 janvier 2021

Référence : sds-fr-sds_for_cloud-architecture_et_sécurité

Table des matières

Dans la documentation, Stormshield Data Security for Cloud & Mobility est désigné sous la forme abrégée : SDS for C&M et Stormshield Network sous la forme abrégée : SN.

Ce document n'est pas exhaustif et d'autres modifications mineures ont pu être incluses dans cette version.

1. Avant de commencer

La solution SDS for C&M est proposée en mode Saas et gérée par l'équipe Cloud Services de SDS for C&M.

Ce document fournit des informations techniques sur la confidentialité, l'intégrité et la disponibilité des données de nos utilisateurs.

2. Types d'informations stockées

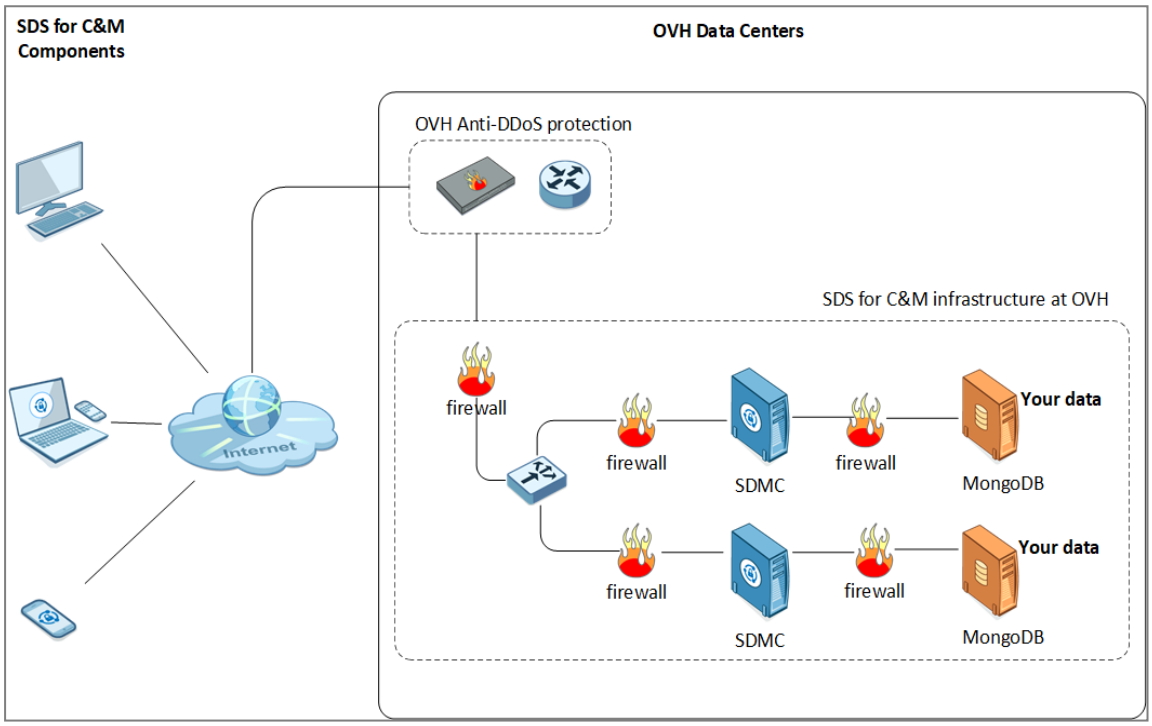
Le tableau ci-dessous décrit le type d'informations stockées par SDS for C&M et la durée de rétention de ces informations :

Données	Type	Emplacement et durée de rétention
Données utilisateurs pour la gestion des accès	• Nom, prénom, adresse e-mail, • Emplacement de l'appareil (pays).	• Logs du système d'exploitation : 1 an • Sauvegardes quotidiennes des bases de données : 7 jours • Logs des utilisateurs SDMC : 30 jours
Logs d'événements pour l'audit et la supervision	• Actions des utilisateurs, date, et heure, • Adresses e-mail (expéditeurs et destinataires), • Nom du fichier (pas le contenu), • Appareil : système d'exploitation, modèle, nom et adresse IP.	• Logs du système d'exploitation : 1 an • Sauvegardes quotidiennes des bases de données : 7 jours • Logs des utilisateurs SDMC : 30 jours
Logs de l'administration système	• Patches et mises à jour logiciels • Création et suppression de comptes, • Actions de gestion du système d'exploitation, • Actions de sauvegarde et restauration, • Opérations et maintenance du serveur.	• Logs du système d'exploitation : 1 an • Sauvegardes quotidiennes des bases de données : 7 jours • Logs des utilisateurs SDMC : 30 jours
Clés des utilisateurs finaux	Magasin de clés de l'utilisateur final	Tant que l'utilisateur existe dans SDMC
Clés des utilisateurs externes	Clés d'utilisateurs finaux	Tant que l'utilisateur existe dans SDMC

3. Protection de l'infrastructure

3.1 Où sont stockées vos informations

Toutes les informations concernant SDS for C&M sont stockées dans les datacenters sécurisés d'OVH France. OVH met en œuvre une solution anti-DDoS qui protège l'infrastructure SDS for C&M contre les attaques par déni de service. De plus, tous les serveurs et bases de données hébergeant vos informations sont protégées par plusieurs niveaux de firewalls Iptables.



3.2 Comment les composants SDS for C&M communiquent

Tous les flux de données entre les différents composants SDS for C&M transitent via le protocole HTTPS et le port 443. La version de TLS utilisée est v1.2.

Service	Source	Destination	Description
Authentification au SDS for C&M Encryption Portal	Appareils de l'utilisateur	https://sds.stormshieldcs.eu/portal	URL d'accès à SDS for C&M Encryption Portal - et - Administration des utilisateurs Assistance et Recouvrement
Serveur Stormshield (SDMC)	Appareils de l'utilisateur	https://sds.stormshieldcs.eu	URL d'accès au serveur Stormshield (SDMC)

Client SDS for C&M	Appareils de l'utilisateur	https://sds.stormshieldcs.eu/api/internal	URL d'accès à la création de compte et aux politiques de sécurité
Stormshield API	Appareils de l'utilisateur	https://sds.stormshieldcs.eu/api	URL d'accès aux informations sur les utilisateurs et les logs pour récupérer les logs
Mailjet API	Serveur Stormshield (SDMC)	Serveur Mailjet	Utilisé par SDMC pour envoyer des e-mails via l'adresse *noreply@stormshieldcs.eu*

3.3 Gestion des vulnérabilités

Les équipes Cloud Services et Recherche & Développement de Stormshield mettent en œuvre une politique de gestion des vulnérabilités à chaque publication sans interruption de service. Le résultat des analyses automatiques des données sensibles est contrôlé par l'officier de sécurité de Stormshield.

4. Algorithmes de chiffrement

Les mots de passe, clés de mots de passe ou de fichiers restent sur les appareils des utilisateurs et ne sont jamais transférés nulle part ni à quiconque. Les clés utilisateurs, les clés de groupes, et les clés de votre entreprise sont stockées chiffrées sur le serveur SDMC. Toutes les opérations de chiffrement ont lieu sur votre appareil, et jamais sur les serveurs de Stormshield. Ni Stormshield, ni l'hébergeur du service, n'a la capacité d'accéder aux clés privées des utilisateurs internes à la solution.

Le tableau suivant liste les algorithmes cryptographiques utilisés dans SDS for C&M.

Traitement	Algorithme	Détails
Chiffrement de la clé asymétrique	RSA PKCS 1.5 et RSA OAEP	2048, 4096 bits
Chiffrement de la clé symétrique	AES Key Wrap	256 bits
Chiffrement symétrique des données	AES CBC Padding PKCS#7	256 bits
HMAC	HMAC SHA-256	256 bits
Protection par mot de passe du magasin de clés	PBKDF2	10 000 rounds et salt 32 bits
Dérivation des mots de passe	SHA-256 et Argon2d	Facteur de parallélisme : 2 Coût en mémoire : 8192 Itérations : 33 Salt : 128 bits

5. Protection des comptes utilisateurs

Il existe plusieurs types d'utilisateurs dans SDS for C&M :

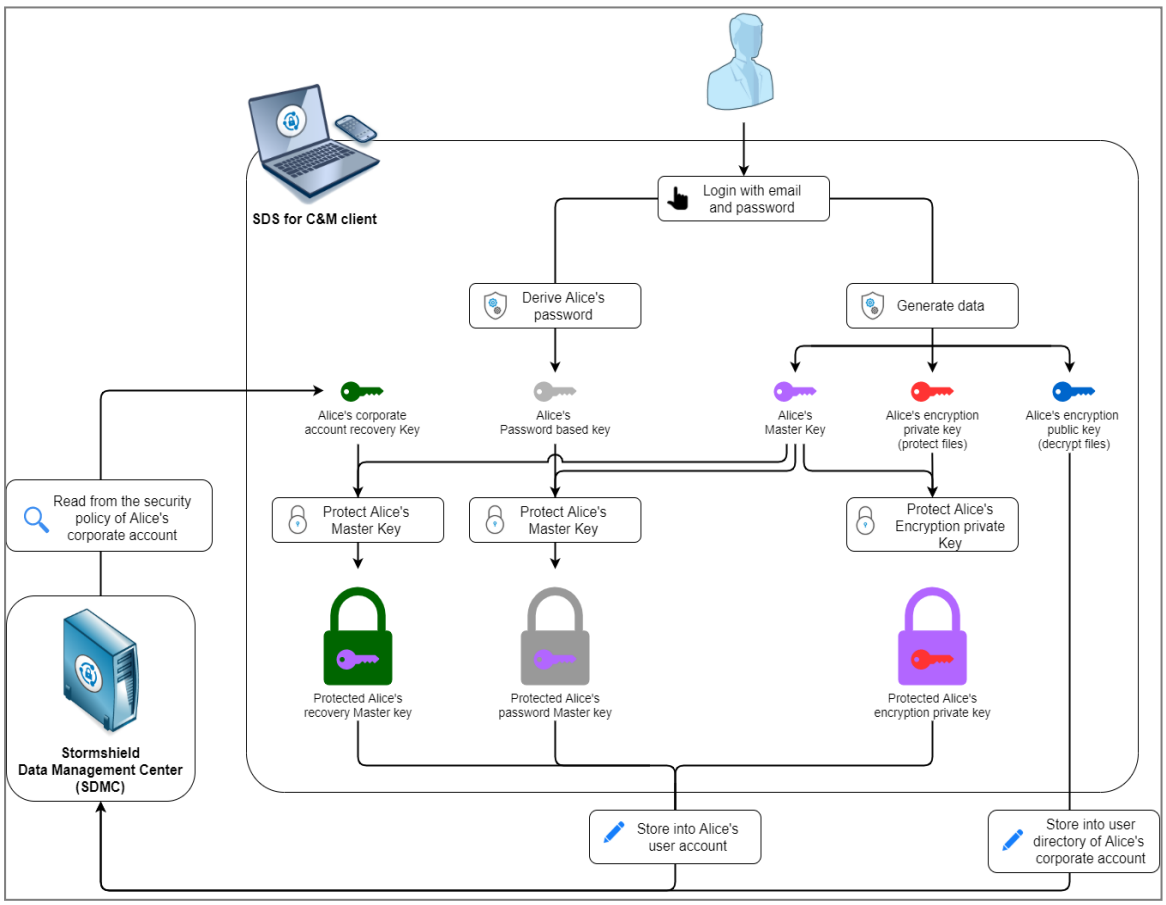
- Les utilisateurs internes qui disposent d'un compte utilisateur payant déclaré sur le compte d'entreprise SDS for C&M de leur société,
- Les utilisateurs externes qui ne disposent pas d'un compte utilisateur.

La manière dont leurs informations sont protégées diffère, de même que la méthode d'authentification.

5.1 Principes généraux pour les utilisateurs internes

En mode Gestion des clés intégrée, lorsqu'un utilisateur crée un compte, SDS for C&M lui génère les clés suivantes :

- Sa clé master (clé violette sur le schéma),
- Sa clé privée (clé rouge sur le schéma),
- Sa clé publique (clé bleue sur le schéma),
- La clé de son mot de passe, à partir d'un hash du mot de passe (clé grise sur le schéma).



5.1.1 La clé publique

Un utilisateur SDS for C&M (Alice sur le schéma) possède une clé publique stockée sur le serveur SDMC et ainsi accessible par tous les utilisateurs du compte d'entreprise. La clé publique permet à ceux-ci de protéger des documents pour Alice. C'est la seule clé stockée en clair sur SDMC car elle ne contient aucune information sensible et n'est donc pas confidentielle.

5.1.2 La clé privée et la clé master

Pour pouvoir lire des documents protégés pour elle, Alice a besoin de sa clé privée. Celle-ci est chiffrée par une clé asymétrique intermédiaire, elle-même chiffrée par la clé master. De son côté la clé master est chiffrée de deux manières différentes :

- Par la clé du mot de passe d'Alice, connue d'elle seule (cadenas gris sur le schéma),
- Par la clé publique de recouvrement (cadenas vert sur le schéma). La clé privée de recouvrement est stockée dans le compte de l'utilisateur de recouvrement et est protégée par la clé master de ce compte, elle-même protégée par un mot de passe.

Par conséquent, Stormshield ne peut en aucun cas lire vos informations et aucune donnée sensible n'est stockée sur SDMC.

5.1.3 La clé du mot de passe

La clé du mot de passe est produite à partir du mot de passe de l'utilisateur et ne quitte jamais l'appareil de l'utilisateur. Elle sert à chiffrer la clé master du compte de l'utilisateur. Cette clé master sera ensuite envoyée la base de données de SDMC : le mot de passe lui-même n'est jamais stocké. Ce double niveau de protection permet de limiter au maximum les possibilités d'attaquants potentiels.

La clé du mot de passe de l'utilisateur est le point de départ pour déchiffrer un document : elle permet de retrouver la clé master qui elle-même permet de retrouver les clés privées indispensables au déchiffrement de données.

SDS for C&M n'utilise jamais le mot de passe lui-même mais seulement des dérivés : la clé du mot de passe et ou cette même clé chiffrée par la clé master.

Le mot de passe permet de :

- Retrouver la clé master pour accéder aux données sensibles du compte utilisateur,
- Authentifier l'utilisateur sur SDMC.

5.1.4 Le magasin de clés

Le magasin de clés de l'utilisateur, qui sera utilisé lors du déchiffrement de documents, contient ses données confidentielles. Il est composé des clés suivantes :

- La clé master chiffrée par la clé du mot de passe,
- La clé master chiffrée par la clé publique de recouvrement,
- La clé privée chiffrée par une clé asymétrique intermédiaire, elle-même chiffrée par la clé master.

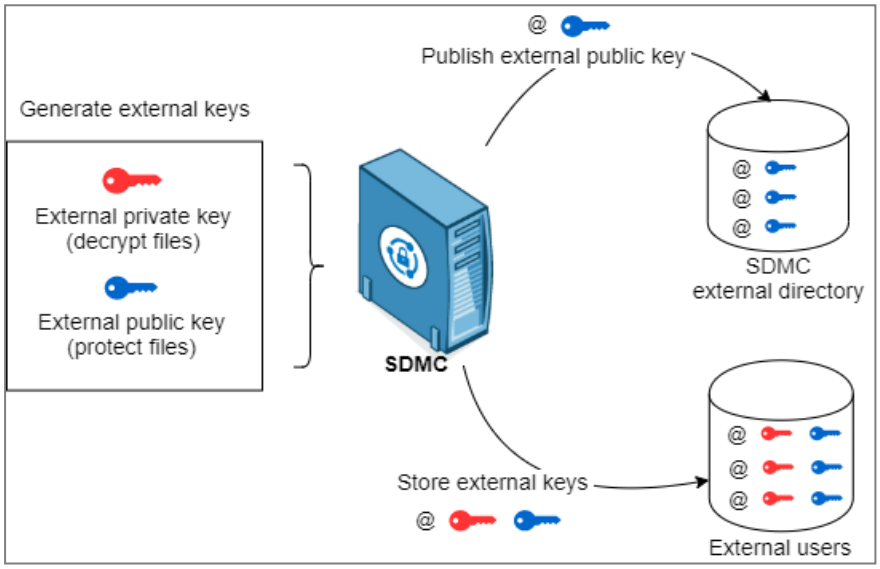
5.2 Principes généraux pour les utilisateurs externes

Un utilisateur externe (Bob) ne dispose pas de compte SDS for C&M payant. Lorsque l'on souhaite chiffrer pour lui, SDS for C&M lui génère les clés suivantes :

- Une clé publique externe (clé bleue sur le schéma). Publiée dans l'annuaire externe sur le serveur SDMC, elle est accessible par tous les utilisateurs externes et internes. Elle permet à ceux-ci de protéger des documents pour Bob.
- Une clé privée externe (clé rouge sur le schéma). Elle permet à Bob de déchiffrer les documents protégés pour lui. Contrairement aux clés des utilisateurs internes, la clé privée externe est stockée sur le serveur SDMC.

Les clés sont liées à l'adresse e-mail de l'utilisateur. Elles restent les mêmes pendant toute la durée de l'utilisation de SDS for C&M Encryption Portal.

Le magasin de clés d'un utilisateur externe utilisé lors du déchiffrement d'un document contient uniquement la clé privée externe.

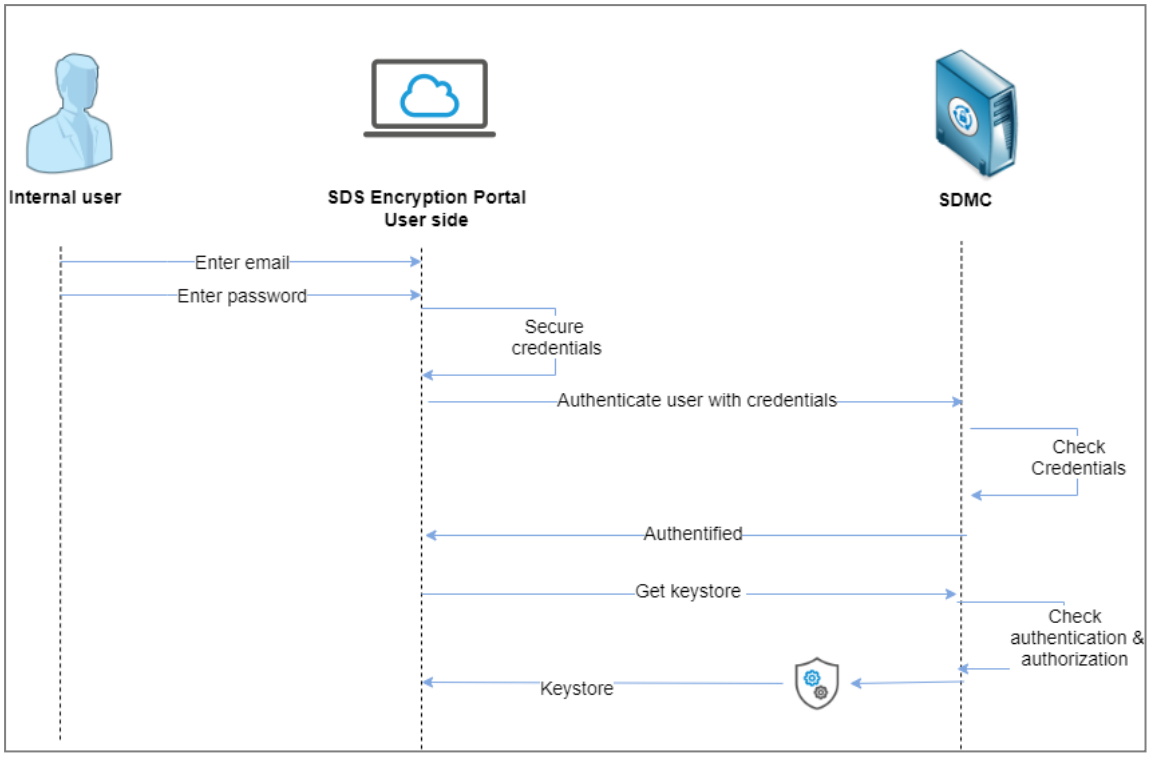


5.3 Authentification des utilisateurs sur SDS for C&M Encryption Portal

L'authentification des utilisateurs pour se connecter au SDMC est différente selon que l'utilisateur est interne ou externe, ou si vous utilisez SDS for C&M en mode Gestion des clés externe.

5.3.1 Connexion de l'utilisateur interne sur SDS for C&M Encryption Portal

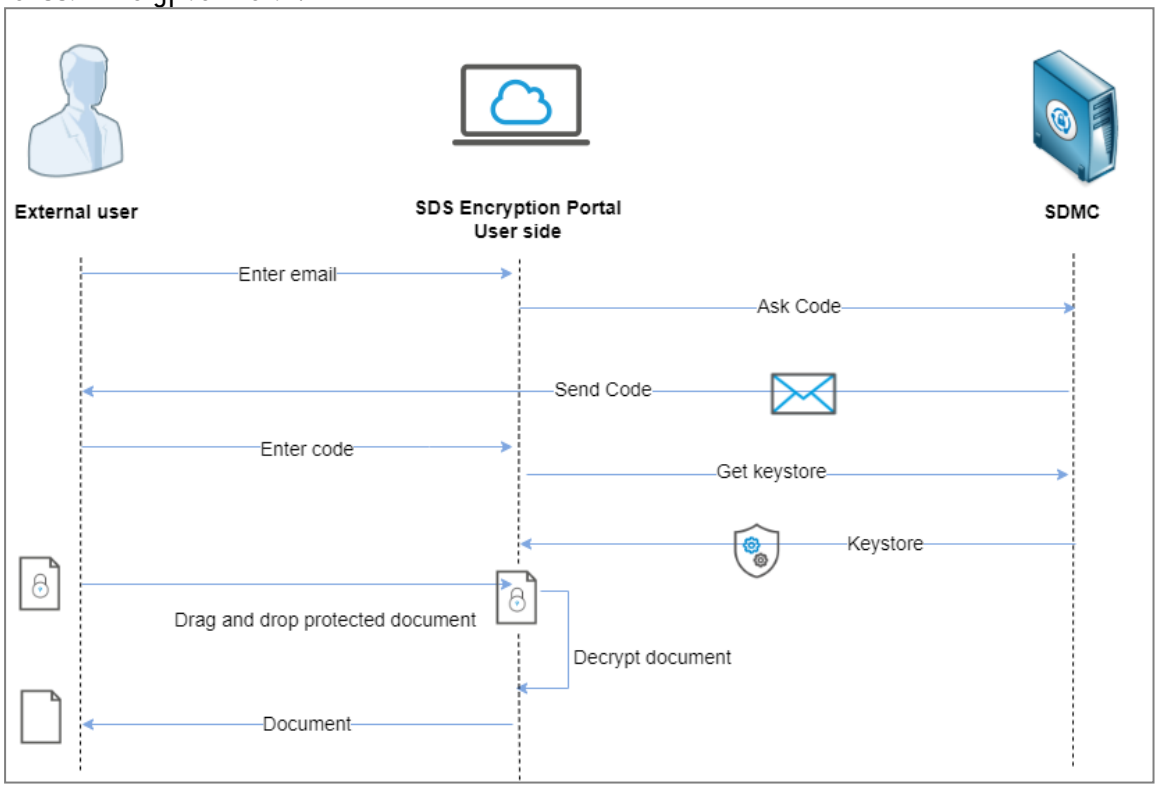
Un utilisateur interne saisit son adresse e-mail et son mot de passe sur SDS for C&M Encryption Portal qui les transmet au serveur SDMC. La transmission du mot de passe s'effectue via un hash en SHA256. SDMC vérifie les identifiants, ce qui permet à l'utilisateur de demander le magasin de clés. Après vérification des autorisations, SDMC met le magasin de clés à disposition de l'utilisateur. Ce dernier est connecté, il peut protéger ou déchiffrer un document.


Internal user
SDS Encryption Portal
User side
SDMC
Enter email
Enter password
Secure
credentials
Authenticate user with credentials
Check
Credentials
Authentified
Get keystore
Check
authentication &
authorization
Keystore

5.3.2 Connexion de l'utilisateur externe sur SDS for C&M Encryption Portal

Lors de chaque connexion sur SDS for C&M Encryption Portal via son adresse e-mail, l'utilisateur externe reçoit un code d'accès unique qui est valide pendant deux heures et supprimé après utilisation. Ce code permet de s'authentifier et de récupérer le magasin de clés nécessaire pour le déchiffrement du fichier.

Un utilisateur externe n'ayant pas été invité une première fois ne peut pas se connecter au SDS for C&M Encryption Portal.



5.3.3 Mode Gestion des clés externe (PKI)

Si vous utilisez SDS for C&M en mode gestion des clés externe (PKI), SDS for C&M ne stocke jamais la clé privée dans le magasin de clés du serveur SDMC, et ne publie jamais la clé publique associée. Un utilisateur peut se connecter à SDS for C&M Encryption Portal mais ne peut pas y protéger un document ou le déchiffrer. Il doit le faire via le Client SDS for C&M car les clés se trouvent sur chaque appareil des utilisateurs finaux.

En revanche, si quelqu'un protège un document pour un utilisateur en mode PKI via SDS for C&M Encryption Portal, celui-ci disposera de clés externes générées par SDS for C&M Encryption Portal, et pourra déchiffrer le document.

Les clés externes sont liées à l'adresse e-mail de l'utilisateur. Si son compte est supprimé, les clés externes sont conservées et peuvent être récupérées après la création d'un nouveau compte associé à cette adresse e-mail.

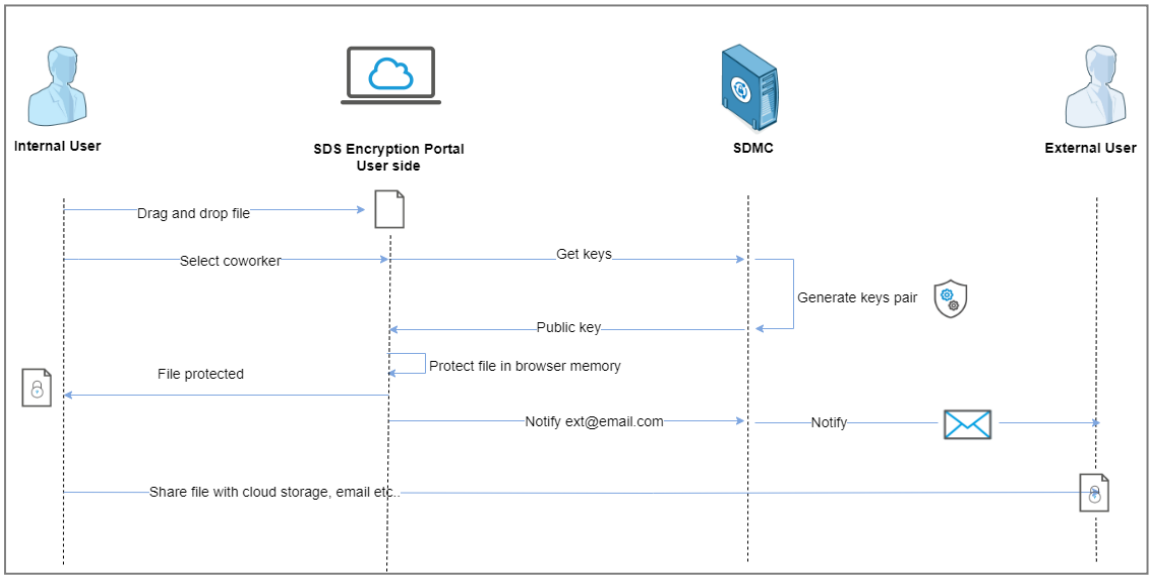
6. Protection des documents dans SDS for C&M Encryption Portal

SDS for C&M combine le chiffrement asymétrique avec RSA et le chiffrement symétrique avec AES. Chaque fichier dispose de sa propre clé aléatoire qui est générée lors de sa création et de chaque modification du contenu. La clé de fichier est utilisée pour protéger le contenu du fichier puis le déchiffrer. Pour plus d'informations, reportez-vous à la section Algorithmes de chiffrement

Cette section décrit comment se déroule la protection et le déchiffrement de documents via SDS for C&M Encryption Portal.

6.1 Protection d'un document

1. Lorsque l'utilisateur Alice, qu'elle soit interne ou externe, dépose un document sur SDS for C&M Encryption Portal, elle doit préciser l'adresse e-mail de l'utilisateur externe (Bob) pour qui elle souhaite protéger le document.
2. Si Bob ne dispose pas encore d'une clé publique externe, une paire de clés externes est alors générée pour lui.
3. SDS for C&M Encryption Portal utilise la clé publique externe de Bob pour protéger le document pour lui.
4. Alice met le document protégé à la disposition de Bob.



6.2 Déchiffrement d'un document protégé

1. Après s'être connecté à SDS for C&M Encryption Portal, l'utilisateur externe Bob y dépose un document protégé.
2. Le document est déchiffré directement sur le portail en utilisant la clé privée externe de l'utilisateur.
3. Le document est téléchargé et sauvegardé sur le poste de l'utilisateur.

7. Le compte d'entreprise

Le compte d'entreprise contient toutes les informations liées à votre société. Il est créé dès le début de la procédure d'enregistrement de votre société auprès de la solution SDS for C&M.

Le compte d'entreprise est dédié à une seule société et n'est jamais partagé avec d'autres sociétés.

7.1 Informations stockées dans le compte d'entreprise

Le compte d'entreprise contient les informations suivantes :

Type d'information	Description
Tableau de bord	• Statistiques sur l'utilisation des espaces collaboratifs, • Liste des utilisateurs et des appareils associés.
Espaces collaboratifs	Informations sur les espaces collaboratifs.
Administrateurs	Informations sur les administrateurs.
Utilisateurs	• Actions effectuées par les utilisateurs, • Caractéristiques des utilisateurs, dont les rôles d'assistance et recouvrement dédiés au compte d'entreprise, • Informations sur le compte utilisateur et les clés publiques (en mode gestion des clés intégré uniquement).
Politiques	Informations sur les politiques des postes de travail et appareils mobiles.
Licence	Informations sur la licence qui définit les composants et le nombre d'utilisateurs autorisés à utiliser le service.
Paramètres	Informations sur votre société, les domaines associés à votre compte d'entreprise, la collaboration avec des sociétés externes.

7.2 Lien entre la société et le compte d'entreprise

Lors de la création de votre compte d'entreprise, vous devez utiliser une adresse e-mail de votre société. Le nom de domaine qu'elle contient sera automatiquement considéré comme le domaine par défaut : seuls les utilisateurs disposant d'une adresse e-mail avec ce nom de domaine seront autorisés à créer un compte SDS for C&M sur votre compte d'entreprise.

Vous pouvez par la suite ajouter un ou plusieurs domaines à votre compte d'entreprise afin que les utilisateurs appartenant à ces domaines puissent également créer un compte SDS for C&M. Ceci permet d'inclure les utilisateurs des sous-domaines ou des filiales de votre société.

7.3 Collaboration avec d'autres comptes d'entreprise

La collaboration entre sociétés permet de partager ses annuaires avec d'autres comptes d'entreprise. Ainsi, vos utilisateurs sont capables d'échanger des données protégées facilement avec tous les utilisateurs de la société partenaire.

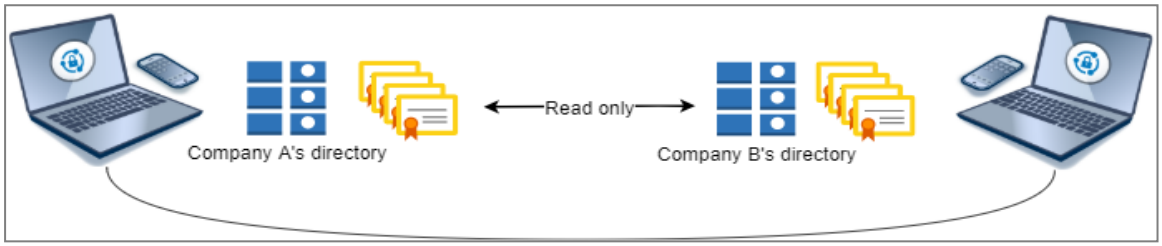
Les utilisateurs d'une société non partenaire sont considérés comme externes et doivent utiliser SDS for C&M Encryption Portal.

7.3.1 Avec collaboration

Lorsque deux sociétés sont partenaires, elles partagent leur annuaire de clés publiques.

Leurs utilisateurs sont considérés comme des utilisateurs standard : leur clé interne est utilisée pour le chiffrement et ils ne reçoivent pas d'e-mail avec un code d'accès pour déchiffrer le document dans le SDS for C&M Encryption Portal. Ils peuvent déchiffrer le document directement à partir du client SDS for C&M en utilisant leur clé privée.

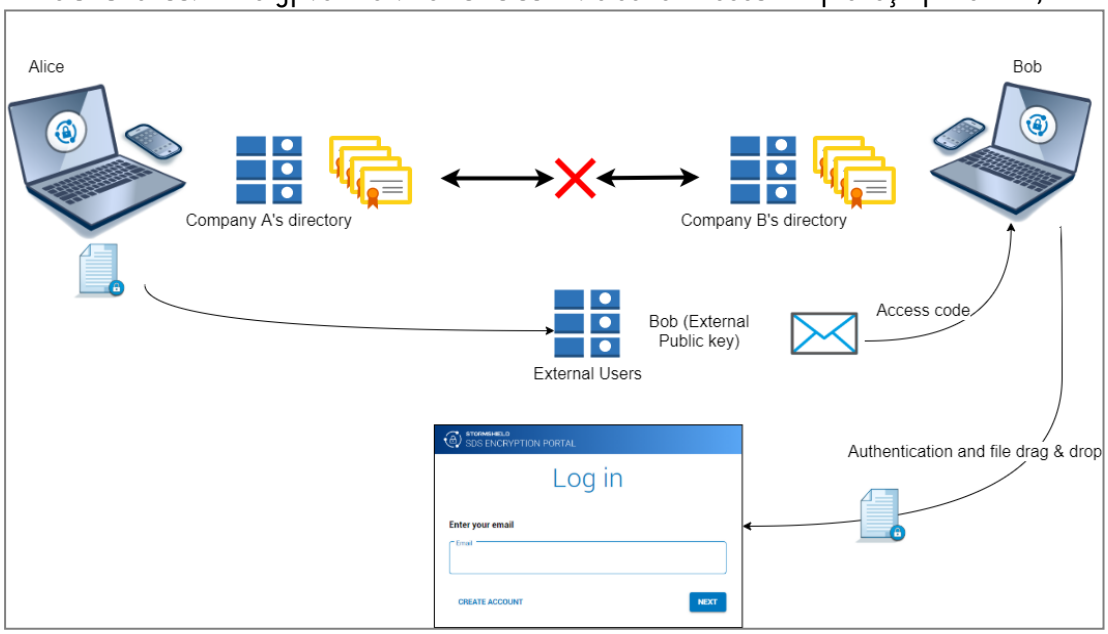
Les annuaires sont partagés en lecture seule : les utilisateurs ou administrateurs de la société A ne peuvent pas modifier les informations contenues dans le compte d'entreprise de la société B.



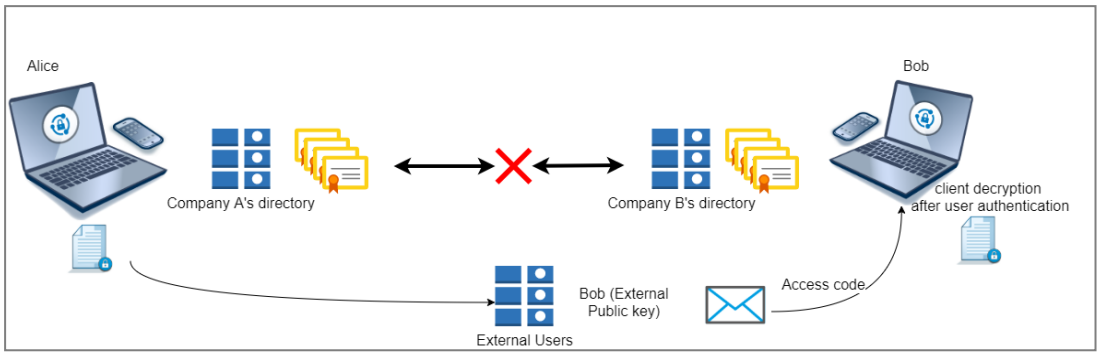
7.3.2 Sans collaboration

Si le compte d'entreprise n'est pas partenaire, alors ses utilisateurs sont inconnus et considérés comme externes. C'est donc leur clé privée externe qui sera utilisée pour déchiffrer le document. Si vous protégez un document pour eux et que vous leur mettez à disposition, ils recevront un e-mail avec un code d'accès, et ils pourront le déchiffrer de deux manières :

- Par le SDS for C&M Encryption Portal en saisissant le code d'accès unique reçu par e-mail,



- Directement par le Client SDS for C&M car leur compte SDS for C&M contient une clé publique externe.



8. Assistance et recouvrement

En mode Gestion des clés intégrée, le déploiement d'une solution de chiffrement nécessite la mise en place d'un système de recouvrement permettant de récupérer les informations chiffrées et de répondre aux exigences légales.

Dans SDS for C&M, le premier compte utilisateur créé devient compte de recouvrement et son détenteur est administrateur de la sécurité. Ce compte est indispensable au bon fonctionnement de la solution et il ne sera jamais supprimé. Lors de sa création, assurez-vous d'appliquer toutes les **préconisations importantes**.

Les rôles de l'administrateur de la sécurité sont les suivants :

Assistance : Il attribue un nouveau mot de passe à un utilisateur si le mot de passe est perdu ou si sa confidentialité est compromise.

Recouvrement : Il donne à un utilisateur les accès à tous les documents protégés d'un autre utilisateur, au cas où ce dernier quitterait la société par exemple.

Un utilisateur externe ne dispose pas de compte payant SDS for C&M. Il n'a donc pas besoin d'un système d'assistance ou de recouvrement. Il n'a pas de mot de passe et s'authentifie au moyen d'un code unique temporaire. Pour récupérer ses documents protégés, il suffit d'utiliser son adresse e-mail.

8.1 Génération des clés de recouvrement

En mode Gestion des clés intégrée, lorsque le premier utilisateur crée un compte, SDS for C&M génère les clés de recouvrement sur le même principe que pour la génération de clés de chiffrement d'un utilisateur standard.

Tous les comptes utilisateurs créés par la suite seront à la fois protégés avec la clé du mot de passe utilisateur puis avec la clé publique du compte de recouvrement.

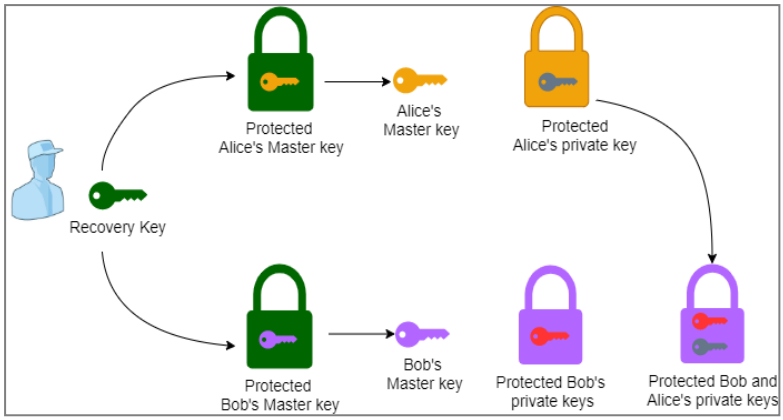
Pour plus d'informations, reportez-vous au schéma de la section **Principes généraux pour les utilisateurs internes**.

Dans SDS for C&M, le compte de recouvrement est un compte de type utilisateur et non pas administrateur car les opérations de recouvrement nécessitent la génération de clés. Les comptes administrateurs ne disposent pas de clés.

8.2 Fonctionnement du rôle Recouvrement

Le rôle Recouvrement permet à l'administrateur de la sécurité de déléguer la clé privée d'un utilisateur A (Alice) à un utilisateur B (Bob) afin que Bob ait accès à tous les documents protégés d'Alice. Pour effectuer cette opération :

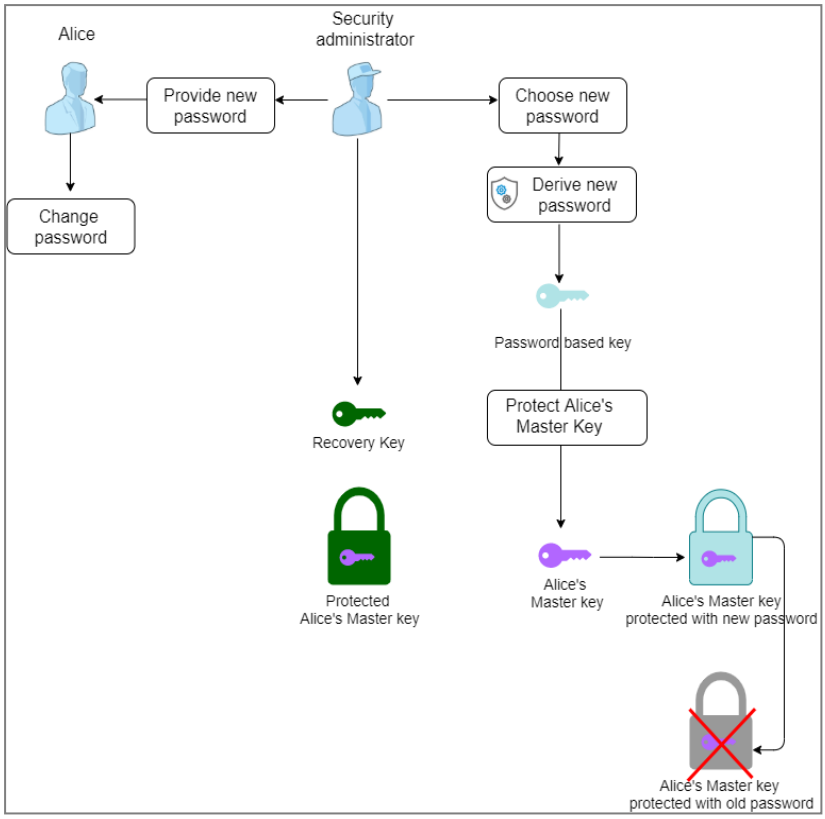
1. Grâce à la clé privée de recouvrement, l'administrateur de la sécurité récupère la clé master d'Alice.
2. La clé master déchiffre le magasin de clés d'Alice.
3. De la même manière, l'administrateur de la sécurité récupère la clé master de Bob.
4. On utilise alors la clé master de Bob pour rechiffrer la clé privée d'Alice et on l'ajoute dans le magasin de clés de Bob. Elle servira uniquement à déchiffrer des documents.



8.3 Fonctionnement du rôle Assistance

Le rôle Assistance permet à l'administrateur de la sécurité de modifier le mot de passe d'un utilisateur (Alice) si celui-ci est perdu ou plus suffisamment sécurisé. Pour effectuer cette opération :

1. Alice contacte l'administrateur de la sécurité en charge de l'assistance pour lui signaler la perte de son mot de passe.
2. Grâce à la clé privée de recouvrement, l'administrateur de la sécurité déchiffre la clé master d'Alice.
3. L'administrateur de la sécurité choisit un nouveau mot de passe à partir duquel SDS for C&M génère une clé de mot passe.
4. La clé master est chiffrée par la nouvelle clé de mot de passe.
5. L'administrateur de la sécurité transmet à Alice le nouveau mot de passe qu'il lui a attribué.
6. Alice se connecte à SDS for C&M avec ce nouveau mot de passe et il lui est demandé de le remplacer par un mot de passe de son choix. L'administrateur de la sécurité n'a pas connaissance du mot de passe final d'Alice.


Alice
Security administrator
Provide new password
Choose new password
Change password
Derive new password
Password based key
Protect Alice's Master Key
Recovery Key
Protected Alice's Master key
Alice's Master key
Alice's Master key protected with new password
Alice's Master key protected with old password

9. Contact

Pour contacter notre Technical Assistance Center (TAC) Stormshield :

- https://mystormshield.eu/
  La soumission d'une requête auprès du TAC doit se faire par le biais du gestionnaire d'incidents dans l'espace privé https://mystormshield.eu/, menu **Support technique** > **Rapporter un incident/Suivre un incident**.
- +33 (0) 9 69 329 129
  Afin d'assurer un service de qualité, veuillez n'utiliser ce mode de communication que pour le suivi d'incidents auparavant créés par le biais de l'espace https://mystormshield.eu/.

documentation@stormshield.eu