

Sécurité et chiffrement des documents

Architecture, gestion des clés et limites du modèle de sécurité

VERSION

1.0

DATE

Octobre 2026

CLASSIFICATION

Public

CONTACT

hello@doksure.com

LSP Labs SAS · 60 rue François Premier, 75008 Paris

Sommaire

Objet et périmètre	3
Public visé.....	3
1. Résumé exécutif	3
2. Notre modèle de sécurité	4
3. Architecture de chiffrement.....	5
4. Gestion des clés et des identités.....	6
5. Cycle de vie des documents	7
6. Contrôle d'accès, traçabilité et exploitation	8
7. Garanties et limites.....	9
8. Conformité, hébergement et contacts.....	10
Glossaire.....	10

Objet et périmètre

Ce dossier présente la sécurité de Doksure et les protections que nous apportons à vos documents. Il décrit le chiffrement, la gestion des clés, le cycle de vie des documents, les contrôles d'accès et l'hébergement.

Il est conçu pour vous accompagner dans votre évaluation : chaque section explique ce que nous protégeons, comment, et ce que cela implique pour votre usage. Les notions clés sont définies dans le glossaire.

Public visé

Ce dossier s'adresse aux directions des systèmes d'information, aux responsables de la sécurité, aux délégués à la protection des données et aux équipes achats ou juridiques. Il présente les mécanismes de façon accessible ; les notions techniques sont définies dans le glossaire.

1. Résumé exécutif

Doksure est un service français de collecte et d'échange de documents sensibles. Vos clients déposent leurs pièces sans créer de compte ; vos équipes les consultent, les valident et les partagent depuis un espace sécurisé.

Le principe est simple : chaque document est chiffré dans le navigateur avant l'envoi. Doksure ne détient pas les clés nécessaires pour lire vos documents, ni vos mots de passe en clair. Nos serveurs et nos hébergeurs stockent des fichiers chiffrés et des clés enveloppées, qu'ils ne peuvent pas ouvrir sans votre mot de passe ou vos codes de récupération.

Vous gardez le contrôle de l'accès à vos documents. Vous décidez qui peut consulter un document, par quel lien, avec quel mot de passe et pour quelle durée. Les accès sont journalisés. Les documents partagés sont également chiffrés avec le mot de passe du lien, que Doksure ne conserve pas.

Cette protection est complétée par des mesures d'exploitation : HTTPS, authentification, double authentification optionnelle et cloisonnement des espaces de travail. Elle ne remplace pas la vigilance sur les postes, les destinataires ou les liens que vous transmettez.

Ce dossier détaille ces mécanismes et leurs limites.

2. Notre modèle de sécurité

Notre modèle repose sur un principe simple : vos documents vous appartiennent. Ils sont chiffrés avant de nous parvenir, et nous ne détenons pas les clés nécessaires pour les lire.

2.1 Ce que nous protégeons

Nous protégeons d'abord le contenu de vos documents : pièces d'identité, justificatifs, contrats, documents financiers. Ce contenu est chiffré avant d'atteindre nos serveurs. Nous protégeons aussi les clés qui permettent de le déchiffrer, les accès à votre espace de travail et les journaux qui retracent les consultations.

Les métadonnées — nom du fichier, type, statut, dates, coordonnées du contact — sont nécessaires au fonctionnement du service. Elles sont protégées par nos contrôles d'accès, mais ne sont pas chiffrées de bout en bout.

2.2 Les menaces que nous neutralisons

Le chiffrement de bout en bout répond à plusieurs risques concrets.

- **Un serveur ou un hébergeur compromis.** Les fichiers stockés restent chiffrés ; sans les clés détenues par les utilisateurs, ils ne peuvent pas être lus.
- **Une copie non autorisée du stockage.** Même si un fichier chiffré était copié, il resterait inutilisable sans la clé correspondante.
- **Un lien de partage intercepté.** Le fichier est chiffré avec le mot de passe du lien ; le lien seul ne suffit pas à lire le document.
- **Un accès non autorisé à votre espace.** Les accès sont authentifiés, les sessions limitées dans le temps et la double authentification disponible.
- **Une altération d'un fichier.** AES-GCM détecte les modifications du contenu chiffré.

2.3 Ce que le chiffrement ne couvre pas

Le chiffrement protège le contenu, pas tout. Il ne protège pas un poste compromis, un utilisateur autorisé qui copie un document, les métadonnées, ni un lien de dépôt ou de partage transmis à une personne non prévue. La section 7 détaille ces limites et les bonnes pratiques associées.

3. Architecture de chiffrement

3.1 Le chiffrement de bout en bout, concrètement

Vos documents sont chiffrés dans le navigateur avant l'envoi. Le serveur reçoit un fichier chiffré, des paramètres de déchiffrement et des clés enveloppées. Il ne reçoit ni le contenu en clair, ni votre mot de passe, ni votre clé privée en clair.

Le déchiffrement n'a lieu que dans un navigateur autorisé : le vôtre, celui d'un collaborateur, ou celui d'un destinataire de lien après saisie du mot de passe.

3.2 La hiérarchie des clés

Niveau	Objet	Algorithme	Protection
Clé utilisateur	Paire RSA propre à chaque utilisateur	RSA-OAEP 4096 bits, SHA-256	Clé privée chiffrée avec AES-256-GCM et une clé dérivée du mot de passe par PBKDF2-SHA-256, 1 000 000 itérations, sel de 32 octets. Clé publique en clair.
Clé d'espace de travail	Paire RSA propre à chaque espace de travail	RSA-OAEP 4096 bits, SHA-256	Clé privée enveloppée pour chaque membre avec la clé publique de sa clé utilisateur. Clé publique utilisée pour envelopper les clés de session.
Clé de session de fichier	Clé AES aléatoire propre à chaque fichier	AES-256-GCM, nonce de 12 octets, tag de 16 octets	Clé de session enveloppée avec la clé publique de l'espace de travail. Fichier chiffré avec cette clé.

Votre clé utilisateur protège la clé de votre espace de travail, qui protège les clés de session des fichiers. Cette séparation limite la portée d'une clé compromise.

3.3 Le parcours d'un document

Lors d'un dépôt, votre client ouvre le lien, sélectionne sa pièce et la chiffre dans son navigateur. Le fichier chiffré est envoyé directement au stockage ; Doksure ne voit jamais le contenu.

Pour le consulter, un utilisateur autorisé déchiffre la clé de son espace de travail, puis la clé du fichier, dans son navigateur. Pour partager, le document est ré-chiffré avec le mot de passe du lien ; le destinataire le déchiffre après avoir saisi ce mot de passe.

3.4 Ce que nos serveurs voient

Ce que nos serveurs voient	Ce qu'ils ne voient pas
Fichiers chiffrés, clés publiques et clés enveloppées	Contenu des documents en clair
Empreintes et sels des mots de passe	Clés privées en clair
Métadonnées et journaux d'accès	Mots de passe en clair

Note — Ces éléments sont nécessaires au fonctionnement du service. Ils sont protégés par nos contrôles d'accès et ne permettent pas, à eux seuls, de lire vos documents.

4. Gestion des clés et des identités

4.1 Votre clé, votre contrôle

À l'inscription, votre navigateur génère une paire de clés RSA de 4096 bits. La clé privée est chiffrée avec votre mot de passe et avec quatre codes de récupération. Doksure conserve la clé publique et la version chiffrée de la clé privée ; il ne détient jamais la clé privée en clair.

4.2 Connexion et sessions

Vous vous connectez avec votre mot de passe ; Doksure vérifie une empreinte, jamais le mot de passe en clair. La double authentification TOTP est disponible et optionnelle. Les sessions utilisent des jetons à durée limitée. La clé privée déchiffrée reste dans votre navigateur pendant la session et disparaît lorsque vous vous déconnectez.

4.3 Ajouter un collaborateur

Lorsque vous ajoutez un collaborateur, Doksure enveloppe la clé de votre espace de travail avec la clé publique de ce collaborateur. Il peut alors déchiffrer les documents de l'espace, comme les autres membres.

4.4 Mot de passe oublié

Si vous oubliez votre mot de passe, vous pouvez utiliser l'un de vos codes de récupération pour retrouver l'accès et définir un nouveau mot de passe. Si vous perdez à la fois votre mot de passe et tous vos codes, Doksure ne dispose pas des éléments nécessaires pour déchiffrer vos documents. Conservez ces codes dans un endroit sûr.

4.5 Mots de passe des liens de partage

Vous choisissez un mot de passe pour chaque lien de partage. Le fichier est chiffré avec une clé dérivée de ce mot de passe ; Doksure conserve une empreinte pour vérifier la saisie, jamais le mot de passe. Choisissez un mot de passe long et transmettez-le par un canal distinct du lien.

5. Cycle de vie des documents

5.1 Dépôt

Vous créez une demande, choisissez les pièces attendues et envoyez un lien de dépôt à votre client. Il n'a pas besoin de compte : il ouvre le lien, consulte la liste et dépose ses fichiers. Chaque fichier est chiffré dans son navigateur avant l'envoi. Vous pouvez être prévenu à chaque dépôt.

5.2 Revue et validation

Vos équipes consultent les pièces dans la visionneuse, les acceptent ou les refusent avec un motif. Le client peut redéposer la bonne pièce depuis le même lien. Les messages du dossier sont protégés par nos contrôles d'accès, mais ne sont pas chiffrés de bout en bout : ne les utilisez pas pour transmettre des secrets.

5.3 Partage

Pour partager un document, vous choisissez un mot de passe, une date d'expiration et autorisez ou non le téléchargement. Le document est ré-chiffré avec le mot de passe du lien. Le destinataire le déchiffre dans son navigateur. Vous pouvez supprimer le lien à tout moment.

5.4 Téléchargement et export

Un utilisateur autorisé peut télécharger un document ou plusieurs fichiers dans une archive ZIP. Le déchiffrement se fait dans le navigateur ; le document en clair devient un fichier local, soumis à la protection de votre poste. En mode consultation seule, l'interface masque le téléchargement, mais le navigateur déchiffre le fichier pour l'afficher : une capture reste possible.

5.5 Expiration et suppression

Vous pouvez fixer une date d'expiration et supprimer un lien à tout moment. Un lien expiré ou supprimé n'est plus accessible. Les liens expirés sont conservés 30 jours puis supprimés. La suppression d'un document supprime l'objet chiffré du stockage ; elle ne rappelle pas les copies déjà téléchargées. Les formulaires joints à une demande ne sont pas chiffrés de bout en bout : n'y placez pas de données sensibles.

6. Contrôle d'accès, traçabilité et exploitation

6.1 Qui peut accéder à vos documents

Les documents sont rattachés à votre espace de travail. Les membres que vous invitez partagent la clé de cet espace et peuvent déchiffrer les documents qu'il contient. Les liens de dépôt et de partage sont accessibles à toute personne qui les possède ; pour les liens de partage, un mot de passe est requis. Choisissez donc vos destinataires et vos mots de passe avec soin.

6.2 Chaque accès est tracé

Les consultations, téléchargements, partages et modifications sont journalisés avec une date et une adresse IP. Pour les accès internes, l'utilisateur est identifié. Pour les accès externes, l'adresse IP est enregistrée ; elle ne prouve pas l'identité du destinataire. L'historique vous aide à suivre l'usage de vos documents.

6.3 Nos mesures d'exploitation

Nous appliquons HTTPS, des cookies sécurisés, un filtrage CORS, des jetons de session à durée limitée, la double authentification TOTP optionnelle, des URL présignées de courte durée et une séparation des stockages entre documents chiffrés et contenus utilisateur. Ces mesures complètent le chiffrement et protègent l'accès au service.

7. Garanties et limites

7.1 Les garanties

Propriété	Garantie	Limite
Confidentialité vis-à-vis de Doksure et de l'hébergeur	Contenu chiffré dans le navigateur ; nos serveurs stockent le chiffré et les clés enveloppées.	Poste ou navigateur compromis.
Contrôle des clés	Clé privée chiffrée avec votre mot de passe et vos codes de récupération ; Doksure ne la détient pas en clair.	Perte du mot de passe et des codes.
Intégrité	AES-GCM détecte toute modification du contenu chiffré.	Cette vérification ne prouve pas l'identité du déposant.
Liens de partage	Chiffrement dérivé du mot de passe ; mot de passe non stocké en clair.	Toute personne avec le lien et le mot de passe peut ouvrir.
Traçabilité	Consultations, téléchargements, partages et modifications journalisés.	L'identité d'un destinataire externe n'est pas vérifiée.
Cloisonnement	Chaque espace de travail est cloisonné.	Les membres d'un même espace partagent la clé.

7.2 Ce que le chiffrement ne couvre pas

- **Un poste compromis.** Protégez vos appareils, activez la double authentification et verrouillez vos sessions.
- **Un utilisateur autorisé qui copie un document.** Choisissez avec soin les personnes que vous invitez et les liens que vous partagez.
- **Les métadonnées.** Elles sont protégées par nos contrôles d'accès, mais pas chiffrées de bout en bout ; évitez d'y placer des informations sensibles.
- **Les liens de dépôt et de partage.** Toute personne qui possède le lien, et le mot de passe pour un partage, peut accéder au contenu ; utilisez un mot de passe fort et une date d'expiration, et ne transférez pas les liens à des tiers.
- **La perte des identifiants.** Conservez vos codes de récupération ; sans eux, Doksure ne peut pas déchiffrer vos documents.

7.3 Notre engagement

Le chiffrement de bout en bout est un moyen de protection, pas une promesse d'invulnérabilité. Nous documentons ici ce qu'il protège et ce qu'il ne protège pas, pour que vous puissiez l'utiliser en confiance. La sécurité de vos documents repose aussi sur vos pratiques : mots de passe robustes, appareils à jour et accès limités aux personnes concernées.

8. Conformité, hébergement et contacts

8.1 Conformité RGPD

Doksùre traite les données personnelles dans le cadre du RGPD. La politique de confidentialité décrit les catégories de données, les finalités, les bases légales, les durées de conservation et vos droits. Lorsque vous utilisez Doksùre pour vos clients, vous restez responsable du traitement et Doksùre agit comme sous-traitant ; un contrat de sous-traitance est disponible. Vous pouvez nous écrire à hello@doksùre.com.

8.2 Hébergement et prestataires

Le site doksùre.com est hébergé par OVH SAS à Roubaix. Les documents chiffrés sont stockés sur Cloudflare R2 avec un endpoint européen. La politique de confidentialité recense également PostHog (analyse), Crisp (support), Stripe et Chargebee (paiements). Ces prestataires ne disposent pas des clés nécessaires pour lire vos documents.

8.3 Nous contacter

Pour toute question de sécurité, écrivez à hello@doksùre.com avec « Sécurité » dans l'objet. Nous répondons en français.

Glossaire

Chiffrement de bout en bout. Chiffrement sur l'appareil de l'émetteur avant l'envoi, dont le déchiffrement n'a lieu que sur l'appareil d'un destinataire autorisé. Le serveur stocke le chiffré et les clés enveloppées.

Clé publique / clé privée. La clé publique est diffusée sans secret et sert à chiffrer ou envelopper une clé. La clé privée est secrète et sert à déchiffrer.

Clé utilisateur. Paire RSA propre à un utilisateur, dont la clé privée est chiffrée avec le mot de passe et les codes de récupération.

Clé d'espace de travail. Paire RSA propre à un espace de travail ; sa clé publique enveloppe les clés de session, sa clé privée est enveloppée pour chaque membre.

Clé de session de fichier. Clé AES aléatoire propre à un fichier, enveloppée avec la clé publique de l'espace de travail.

Enveloppe de clé. Chiffrement d'une clé avec une autre clé, pour la stocker ou la transmettre sans la révéler.

AES-GCM. Chiffrement authentifié assurant confidentialité et intégrité ; il produit un chiffré, un nonce et un tag.

RSA-OAEP. Chiffrement asymétrique utilisé pour envelopper des clés AES, pas pour chiffrer des fichiers volumineux.

PBKDF2. Dérivation de clé à partir d'un mot de passe, avec un sel et un nombre d'itérations, pour ralentir les attaques par force brute.

Métadonnées. Informations décrivant un document sans en constituer le contenu : nom, taille, type, contact, statut, horodatage, adresse IP.

Pour toute question complémentaire, écrire à hello@doksure.com.