SCELLEMENT · GESTION DES CLÉS ET DES SECRETS

Fiche sécurité REVIEWIT SEAL

REVIEWIT SEAL garde les identifiants techniques que nos clients nous confient, signe pour leur compte et scelle chaque jour la piste d'audit. Cette fiche répond aux questions usuelles des responsables de la sécurité et dit aussi ce que nous ne garantissons pas.

VERSION
1.0 · Novembre 2026

PÉRIMÈTRE
REVIEWIT SAS · module REVIEWIT SEAL, toutes régions

DIFFUSION
Public

SOMMAIRE

01 En une page
02 Principes de conception
03 Cryptographie et gestion des clés
04 Contrôle d'accès et isolation
05 Traçabilité et preuve
06 Révocation et continuité
07 Ce que nous ne garantissons pas
08 Pour aller plus loin

OBJET

Pour collecter les accès, REVIEWIT détient des accès techniques aux environnements de ses clients : secrets d'application, jetons, comptes de service, certificats. REVIEWIT SEAL les protège, opère les signatures qui en dépendent et scelle la piste d'audit. La fiche décrit la conception du module ; seuls les engagements du contrat et de l'accord de traitement des données sont opposables.

LECTURE

En service : en fonctionnement à la date de publication. **Prévu** : inscrit à la trajectoire de REVIEWIT, sans engagement de date.

SECTION 01

En une page

QUESTION DU RSSI	RÉPONSE COURTE
Où sont stockés nos identifiants techniques ?	Chiffrés dans notre référentiel sous une clé maître dédiée à votre organisation, conservée dans un service de gestion de clés dont elle ne sort pas. Le chiffrement lie la valeur à son détenteur : une enveloppe présentée pour un autre détenteur ne s'ouvre pas.
Nos clés sont-elles séparées de celles des autres clients ?	Oui : une clé maître par client, sans partage. Les clés de fonctionnement de la plateforme relèvent d'une hiérarchie distincte.
Pouvons-nous apporter notre propre clé ?	Pour la signature, oui : vous pouvez importer votre propre clé privée de connexion dans le coffre SEAL, qui signe avec elle sans jamais l'exporter. Le chiffrement sous une clé que vous détenez ou importez est prévu.
Vos administrateurs peuvent-ils lire nos secrets ?	Non. Aucune fonction, y compris d'administration, ne permet de lister ou de lire la valeur d'un secret.
Comment savons-nous qui a accédé à quoi ?	Chaque accès et chaque refus est tracé dans une piste d'audit dont l'intégrité ne dépend pas de SEAL ; la preuve est enregistrée avant toute restitution.
Que se passe-t-il si nous révoquons un accès ?	L'invalidation au sein de la plateforme prend effet en 60 secondes au plus ; la révocation auprès du système source est déclenchée en complément, lorsque celui-ci le permet.
Les clés sont-elles renouvelées ?	Oui : rotation automatique annuelle de la clé maître de chaque souscription, rotation annuelle des clés de chaque client dans le coffre, échéance et alerte pour la clé de signature de SEAL.

SECTION 02

Principes de conception

PRINCIPE	CE QUE CELA SIGNIFIE
Abstraction du service de clés	Aucun composant applicatif n'appelle directement le service de gestion de clés : un changement de fournisseur ou de modèle de clé n'affecte pas le traitement des secrets.
Le service de clés ne voit pas les secrets	Il n'opère que sur des clés, sans accès à aucune valeur de secret ni à aucune donnée métier.
Contexte prouvé, jamais déclaré	L'appartenance d'un traitement à votre organisation est établie par un contexte d'exécution signé, rattaché à un objet réel, jamais par un paramètre fourni par l'appelant.
Accès par identité	Les composants de la plateforme s'authentifient entre eux par des identités à certificat, renouvelées automatiquement et révocables ; aucun mot de passe statique n'authentifie la plateforme elle-même.
Moindre capacité	Les clés de signature ne sont jamais exportables : elles ne s'utilisent que par opération, à l'intérieur du coffre. Chaque composant n'est autorisé que sur les classes de secrets nécessaires à sa fonction, pour des finalités énumérées et pour la durée du traitement en cours.

Preuve avant divulgation	La preuve d'un accès est enregistrée avant que la valeur ne soit restituée ; si la preuve ne peut être produite, l'accès n'a pas lieu.
Révocabilité bornée	Les délais de révocation sont chiffrés ; les portées que nous ne pouvons pas garantir sont dites plutôt que promises (section 07).
Confinement au client	Un incident touchant une clé maître ou un contexte d'exécution ne produit pas d'effet au-delà de l'organisation concernée ; aucun composant ne détient de droit permanent sur les clés maîtres de plusieurs clients.

SECTION 03 Cryptographie et gestion des clés

EXIGENCE	RÉPONSE DE REVIEWIT	ÉTAT
Chiffrement des identifiants	Chiffrement par enveloppe sous la clé maître dédiée à votre organisation. L'organisation, le détenteur et la classe du secret sont liés cryptographiquement à l'enveloppe et vérifiés à chaque déchiffrement.	EN SERVICE
Séparation par client	Une clé maître dédiée par client, sans mutualisation : la compromission d'un périmètre client ne donne accès à aucun autre.	EN SERVICE
Clé gérée par REVIEWIT	Modèle standard : clé maître dédiée à votre organisation, générée, conservée et tournée par REVIEWIT.	EN SERVICE
Votre clé pour la signature	Import de votre clé privée de connexion dans le coffre SEAL, qui signe avec elle ; la clé n'est jamais exportée.	EN SERVICE
Clé maître détenue par le client	Clé maître conservée dans votre propre service de gestion de clés, dont vous déléguez l'usage, révocable à tout moment.	PRÉVU
Matériau de clé importé	Clé maître générée par vous et importée dans notre service de gestion de clés.	PRÉVU
Rotation	Clé maître de chaque souscription : rotation automatique annuelle. Clés de chaque client dans le coffre : rotation annuelle. Rotation par phases : un traitement engagé garde l'accès à la version qu'il a référencée pendant la fenêtre de recouvrement, sauf révocation d'urgence.	EN SERVICE
Identités des composants	Autorité de certification interne : identités renouvelées automatiquement avant leur échéance, liste de révocation des appelants.	EN SERVICE
Fin de vie d'un secret	La suppression retire la valeur chiffrée du référentiel actif : elle n'est plus restituable. Elle devient complète à l'expiration des copies de sauvegarde.	EN SERVICE

SECTION 04 Contrôle d'accès et isolation

EXIGENCE	RÉPONSE DE REVIEWIT	ÉTAT
Isolation entre clients	Contrôles superposés : contexte d'exécution signé, politique d'autorisation par type de composant, contrôle de finalité à chaque lecture, liaison cryptographique vérifiée indépendamment de la logique applicative, autorité cryptographique bornée à une seule organisation par autorisation temporaire.	EN SERVICE
Accès des administrateurs	Aucune énumération ni lecture des valeurs, y compris pour les administrateurs. Opérations sensibles sous authentification renforcée et séparation des rôles, avec validation à quatre yeux.	EN SERVICE
Assistant RITA	Exclu par conception de tout accès aux valeurs de secrets : aucune valeur ne peut figurer dans une requête, une trace ou un résultat d'outil.	EN SERVICE
Configuration et journaux	Aucune valeur de secret en variable d'environnement, en fichier de configuration ni dans les journaux.	EN SERVICE

SECTION 05 Traçabilité et preuve

EXIGENCE	RÉPONSE DE REVIEWIT	ÉTAT
Journalisation des accès	Chaque accès, refus, rotation et révocation produit un événement horodaté : identité appelante, organisation, référence du secret, opération, finalité, résultat. Jamais la valeur.	EN SERVICE
Intégrité indépendante	La piste d'audit est signée et séquencée indépendamment de SEAL : une compromission de SEAL ne permet pas d'effacer une trace a posteriori.	EN SERVICE
Preuve préalable	Enregistrée avant la restitution, complétée après ; un accès sans preuve préalable est refusé.	EN SERVICE
Sceau quotidien	SEAL scelle chaque jour chaque chaîne de la piste d'audit. Sa clé de signature porte une échéance, avec une alerte avant son terme.	EN SERVICE
Journal de vos secrets	Restitution au client du journal relatif à ses secrets, refus compris.	PRÉVU

SECTION 06 Révocation et continuité

EXIGENCE	RÉPONSE DE REVIEWIT	ÉTAT
Révocation locale	Invalidation au sein de la plateforme en 60 secondes au plus, sur l'ensemble des nœuds.	EN SERVICE
Révocation à la source	Déclenchée auprès du système émetteur lorsqu'il le permet ; le résultat vous est restitué.	EN SERVICE

Indisponibilité du service de clés	Les traitements de l'organisation concernée sont suspendus de manière ordonnée et le client est notifié ; aucune autre organisation n'est affectée.	EN SERVICE
Changement de fournisseur de clés	Ré-enveloppement des secrets sous une nouvelle clé maître, sans déplacement des valeurs.	PRÉVU

SECTION 07 Ce que nous ne garantissons pas

Une limite tue est une promesse implicite. Nous énonçons donc les suivantes.

- La cessation d'usage d'une valeur déjà transmise à un traitement en cours n'est pas instantanée : elle est bornée par une durée d'usage maximale, communiquée par classe de secret.
- La révocation auprès d'un système tiers dépend des capacités de ce système : nous la déclenchons et vous en restituons le résultat, sans pouvoir en garantir le délai.
- Les identifiants déposés avant la mise en service de la garde sont repris sous la clé maître de leur organisation, détenteur par détenteur ; jusqu'à leur reprise, ils ne sont protégés que par le chiffrement au repos des bases.
- Nous ne mettons en œuvre aucune destruction cryptographique : un secret supprimé disparaît du référentiel actif, ses copies de sauvegarde s'effacent à leur expiration, et nous ne revendiquons aucune suppression opposable avant ce terme.
- La clé privée que vous importez pour la signature n'est jamais exportée, y compris à la fin du contrat : conservez-en l'original.
- Le changement de fournisseur de clés et les modèles de clé détenue ou importée par le client ne sont pas disponibles aujourd'hui.

SECTION 08 Pour aller plus loin

DOCUMENT	ACCÈS
Annexe « Gestion des clés et des secrets » : modèles de clé, responsabilités, révocation, suppression	Clients et prospects sous accord de confidentialité
Livre blanc sécurité de REVIEWIT	Public
Mesures techniques et organisationnelles (annexe 1 du DPA)	Clients · accès authentifié

REVIEWIT SAS · Sécurité : security@we-reviewit.com. Document revu annuellement et après tout changement majeur du module. La version française fait foi.