

HOLOVID SAS

DOSSIER DE PRESSE

HOLOVID ID, la sécurité numérique souveraine

Connexion sans code, coffre-fort chiffré et protection en cascade. Conçu et hébergé en France, sans télémétrie ni traceurs tiers.

À propos de Holovid SAS

Holovid SAS est une société française basée à Bergerac (RCS Bergerac 987 882 016). Elle conçoit des outils de sécurité numérique respectueux de la vie privée, reposant sur une architecture zero-knowledge et une infrastructure européenne.

Le principe est constant sur toute la gamme : aucune télémétrie, aucun SDK de pistage tiers, des serveurs hébergés en France, et aucun compte obligatoire pour les fonctions de base. L'indépendance vis-à-vis des grands acteurs technologiques fait partie de l'identité du produit, pas seulement de ses choix techniques.

HOLOVID ID en bref

HOLOVID® Secure Connect

Connexion sans code par scan de QR code. Chaque appareil possède sa propre paire de clés Ed25519, ce qui rend la méthode résistante aux attaques de phishing par proxy (AiTM).

HOLOVID® Sentry

Verrouillage en cascade : code PIN, biométrie, puis détection de vivacité. Toute la vérification se déroule sur l'appareil, sans dépendance au cloud.

HOLOVID® Vault

Coffre-fort chiffré dans le cloud, en architecture zero-knowledge (AES-256-GCM), sur infrastructure HDS française. Disponible en quatre formules : Vault, Vault Pro, Vault Elite, Vault Infinity.

CARACTÉRISTIQUES

Fiche technique

Éditeur	Holovid SAS, Bergerac, France
Produit	HOLOVID ID
Plateformes	iOS et Android
Date de lancement	19 février 2026
Version actuelle	1.2.5
Application	Développée en Flutter
Serveur	Rust, base PostgreSQL
Hébergement	OVH Cloud HDS, 3 zones de disponibilité, France
Chiffrement du coffre-fort	AES-256-GCM, zero-knowledge
Connexion	Clés Ed25519 propres à chaque appareil, stockées dans le stockage sécurisé du système (Keychain iOS, Keystore Android)
Formules Vault	Vault, Vault Pro, Vault Elite, Vault Infinity
Confidentialité	Aucune télémétrie, aucun traceur tiers, aucun compte obligatoire pour les fonctions de base

UN MOT SUR...

La double authentification

« La double authentification classique repose souvent sur un code que l'on recopie, et donc que l'on peut intercepter. Nous le remplaçons par un scan lié au site légitime, puis nous y associons la biométrie et la vérification de présence réelle de la personne. En combinant ces trois protections, nous neutralisons à la fois les attaques par phishing, qui exploitent les codes transmissibles, et les tentatives par deepfake, qui cherchent à se faire passer pour un utilisateur. »

Éric Gatineau, fondateur de Holovid SAS

Quatre angles pour votre article

La souveraineté numérique appliquée : une alternative française aux services dépendants des grands acteurs technologiques

HOLOVID ID est conçu et hébergé en France par Holovid SAS, société basée à Bergerac. Contrairement à de nombreux services dont les données transitent par des infrastructures contrôlées par les grands acteurs technologiques américains, l'application repose entièrement sur une infrastructure européenne : les serveurs sont hébergés chez OVH, sur une infrastructure certifiée HDS répartie sur trois zones de disponibilité en France. L'éditeur a fait le choix de ne dépendre d'aucun service cloud étranger pour le traitement des données sensibles.

Cette indépendance ne se limite pas à la localisation des serveurs. L'application ne contient aucune télémétrie ni aucun SDK de pistage tiers, et la plupart des fonctions sont utilisables sans compte obligatoire. La souveraineté n'est donc pas un argument ajouté après coup, mais un principe de conception présent à chaque niveau du produit.

Double authentification sécurisée : comment fonctionne une connexion par QR code résistante au phishing ?

HOLOVID® Secure Connect intervient comme deuxième facteur d'authentification (2FA). L'utilisateur saisit son identifiant et son mot de passe habituels sur le site, puis, au lieu de recopier un code à usage unique reçu par SMS ou généré par une application, il scanne un QR code affiché à l'écran avec l'application HOLOVID ID. Chaque appareil dispose de sa propre paire de clés Ed25519, conservée dans le stockage sécurisé du système (Keychain sur iOS, Keystore sur Android), et c'est cette clé qui prouve l'identité de l'utilisateur.

L'intérêt tient à la nature de cette seconde étape. Un code à taper peut être intercepté, notamment lors d'une attaque par proxy (dite AiTM, pour adversary-in-the-middle), où un site frauduleux relaie en temps réel le code saisi par la victime vers le vrai service. Avec Secure Connect, il n'y a aucun code à recopier : la preuve cryptographique est liée au site légitime et ne peut pas être réutilisée par un intermédiaire. Le maillon faible classique de la double authentification, le code transmissible, disparaît.

Le zero-knowledge expliqué simplement : un coffre-fort dont l'éditeur lui-même ne peut pas lire le contenu

HOLOVID® Vault est un coffre-fort numérique dont le contenu est chiffré directement sur l'appareil de l'utilisateur, avant tout envoi vers le cloud, à l'aide d'un chiffrement AES-256-GCM. La clé permettant de déchiffrer les documents ne quitte jamais l'appareil et n'est jamais transmise aux serveurs. C'est le principe du zero-knowledge : l'éditeur héberge des données qu'il est techniquement incapable de lire.

Concrètement, même Holovid SAS, qui exploite l'infrastructure, ne peut pas accéder au contenu d'un coffre-fort. On peut le comparer à un coffre dont le prestataire entreposerait le contenu sans jamais en détenir la combinaison. Les données restent par ailleurs hébergées sur une infrastructure HDS française, ce qui combine confidentialité technique et localisation européenne.

La vérification de présence en cascade : sécuriser l'accès sans envoyer aucune donnée biométrique dans le cloud

HOLOVID® Sentry protège l'accès à l'application par une série de vérifications successives : d'abord un code PIN, puis la biométrie de l'appareil, puis une détection de vivacité (liveness). Cette dernière étape confirme qu'une personne réelle est bien présente devant l'écran, et non une simple photo ou une vidéo, à l'aide de modèles d'analyse faciale exécutés localement.

Le point déterminant est que l'ensemble de ces traitements se déroule sur l'appareil. Aucune donnée biométrique, aucune image de visage n'est envoyée vers un serveur ou stockée dans le cloud. La sécurité repose donc sur une vérification forte sans contrepartie en matière de vie privée, ce qui distingue cette approche des solutions reposant sur une reconnaissance faciale centralisée.

RESSOURCES

Liens utiles

Télécharger (iOS) apps.apple.com/app/id6758670759

Télécharger (Android) play.google.com/store/apps/details?id=fr.holovid.holoid

Sites internet holovid.fr . holovid.cloud

Coffre-fort HOLOVID® Vault vault.holovid.fr

Site corporate (en cours) holovid.eu

Plugin WordPress wordpress.org/plugins/holovid-secure-connect

CONTACT PRESSE

Une question, un visuel, un entretien ?

Nous avons mis en place une adresse dédiée aux journalistes et aux créateurs de contenu. Nous nous efforçons de répondre rapidement, généralement sous 24 heures ouvrées.

presse@holovid-corp.com

HOLOVID® et Twist To Unlock® sont des marques déposées de Holovid SAS auprès de l'INPI. Les autres dénominations sont protégées par enveloppe Soleau.

Apple and the Apple logo are trademarks of Apple Inc., registered in the U.S. and other countries and regions. App Store is a service mark of Apple Inc., registered in the U.S. and other countries and regions. Google Play and the Google Play logo are trademarks of Google LLC.

Apple et le logo Apple sont des marques d'Apple Inc., déposées aux États-Unis et dans d'autres pays et régions. App Store est une marque de service d'Apple Inc., déposée aux États-Unis et dans d'autres pays et régions. Google Play et le logo Google Play sont des marques de Google LLC.