Livre blanc - Retyc

Transfert de fichiers et datarooms chiffrés : architecture, sécurité et indépendance

TripleStack SAS / Version 1.0 / Avril 2026

Ce document est destiné aux décideurs techniques, directeurs des systèmes d'information, responsables de la sécurité des systèmes d'information (RSSI), délégués à la protection des données (DPO) et responsables de la conformité au sein d'organisations opérant dans l'Union européenne.

> ***Primauté de la version originale*** *— Ce livre blanc est initialement rédigé en français. Bien que des traductions puissent être mises à disposition pour la commodité des lecteurs internationaux, seule la version française originale fait foi et prévaut en cas de divergence d'interprétation, de contradiction ou de nuance technique.*

Sommaire

1. Synthèse

Retyc est une plateforme européenne de transfert sécurisé de fichiers et de datarooms collaboratives, développée et opérée par TripleStack SAS, société française indépendante. Elle repose sur trois piliers indissociables : **chiffrement de bout en bout avec mécanismes résistants aux menaces quantiques**, **architecture zero-knowledge** et **indépendance numérique européenne**.

Dans un contexte marqué par l'intensification des cybermenaces, des tensions géopolitiques croissantes, le durcissement du cadre réglementaire européen (RGPD, NIS2, DORA) et la prise de conscience croissante des risques liés aux législations extraterritoriales américaines (Cloud Act, FISA), les organisations ont besoin de solutions qui ne reposent pas uniquement sur des garanties contractuelles ou réglementaires, mais sur des **garanties cryptographiques**.

Par conception, Retyc limite tout accès à vos contenus en clair, y compris par ses propres équipes. Les fichiers sont chiffrés localement sur l'appareil de l'utilisateur avant tout envoi vers nos serveurs. Seuls les destinataires autorisés disposent des clés de déchiffrement.

Ce livre blanc présente l'architecture technique de Retyc, son modèle de sécurité, ses implications pour la conformité réglementaire et ses cas d'usage pour les organisations exigeantes.

> ***Terminologie*** *— Dans ce document, le terme "mot de passe" désigne, selon le contexte, soit un secret d'authentification (connexion), soit une entrée secrète utilisée pour le chiffrement côté client (équivalent technique d'une passphrase).*

2. Le défi : protéger les données sensibles dans un contexte réglementaire exigeant

2.1 Un cadre réglementaire européen en renforcement

Le Règlement Général sur la Protection des Données (RGPD, 2016/679) impose depuis 2018 des obligations strictes sur le traitement des données personnelles. La conformité n'est plus optionnelle : les sanctions peuvent atteindre 4 % du chiffre d'affaires mondial annuel.

Au-delà du RGPD, plusieurs réglementations sectorielles renforcent les exigences de sécurité, telles que :

- **NIS2** (directive sur la sécurité des réseaux et de l'information, 2022) : élargit les obligations de cybersécurité à de nombreux secteurs
- **DORA** (Digital Operational Resilience Act, 2022) : impose des exigences de résilience numérique pour le secteur financier
- **Secret professionnel** (avocats, experts-comptables, médecins) : obligation déontologique renforcée par des risques de sanctions ordinales et juridiques en cas de manquement.

2.2 La menace réelle sur les transferts de fichiers

Le transfert de fichiers entre organisations est l'un des vecteurs les plus exposés de la chaîne de sécurité. Les solutions traditionnelles telles que partages cloud grand public, email avec pièces jointes ou serveurs FTP présentent des vulnérabilités documentées :

- **Données exposées sur les serveurs du fournisseur** : les plateformes de partage grand public chiffrent les données en transit (HTTPS / TLS) et parfois au repos sur leurs serveurs, mais **conservent les clés de déchiffrement**. Un accès non autorisé aux serveurs, une réquisition judiciaire ou une fuite de données exposent intégralement vos contenus.
- **Exposition aux législations extraterritoriales** : les fournisseurs hébergés par des entreprises américaines (même si les centres de données sont physiquement en Union Européenne) sont soumis au *Cloud Act* (2018) et au *Foreign Intelligence Surveillance Act (FISA)*, qui autorisent les autorités américaines à accéder aux données stockées par ces entreprises, y compris pour des données de clients européens, sans nécessairement en informer les personnes concernées.
- **Absence de traçabilité** : les solutions informelles (email, messagerie instantanée) ne permettent aucun audit des accès ni aucune révocation des droits après envoi (même si le fichier est supprimé du serveur, les copies locales restent accessibles).
- **Menaces futures sur les données actuelles** : la stratégie dite *harvest now, decrypt later* consiste à capturer des données chiffrées aujourd'hui en anticipant les progrès matériels (notamment les ordinateurs quantiques) qui pourraient permettre de les déchiffrer dans quelques années. Les données sensibles transmises aujourd'hui avec un chiffrement classique pourraient être compromises demain.

2.3 La limite des approches contractuelles

Face à ces enjeux, de nombreux fournisseurs mettent en avant des garanties organisationnelles et contractuelles : clauses de confidentialité, engagements de sécurité, certifications, audits ou politiques internes. Ces éléments ont leur utilité, mais ils **ne suffisent pas à eux seuls à garantir la confidentialité effective des données**.

En pratique, une protection purement contractuelle ne change pas les capacités techniques réelles du fournisseur. Si les données sont accessibles en clair sur ses serveurs, elles restent exposées en cas de compromission technique, d'erreur humaine, d'abus interne ou de demande d'accès émanant d'une autorité compétente.

Autrement dit, un engagement contractuel peut encadrer un usage. Il ne supprime pas la possibilité technique d'accéder aux données.

La protection la plus robuste repose donc sur l'architecture cryptographique elle-même : lorsque les contenus sont chiffrés côté client et que les clés de déchiffrement ne sont pas accessibles au fournisseur, la confidentialité ne dépend plus uniquement d'une promesse, d'une procédure interne ou d'un cadre contractuel. Elle repose sur une contrainte technique vérifiable.

C'est cette logique qui fonde l'architecture de Retyc.

> *Certains services se réservent la possibilité de faire évoluer leurs conditions d'utilisation, y compris sur des sujets sensibles liés aux données. Cette dépendance à un cadre contractuel évolutif introduit une* ***incertitude sur le niveau réel de confidentialité*** *dans le temps.*
> *Une contrainte cryptographique ne dépend pas d'une politique interne. Retyc ne repose pas sur une promesse contractuelle, mais sur une architecture conçue pour rendre les données inaccessibles en clair au fournisseur.*

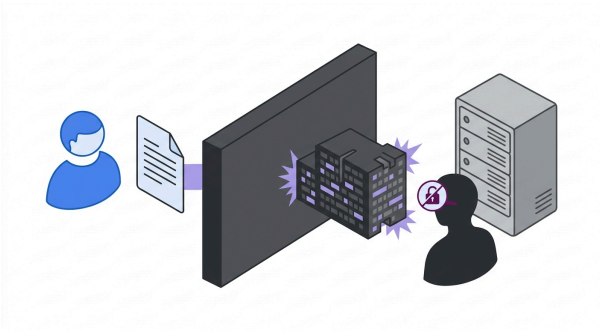
3. Architecture technique et modèle de sécurité

> ***Note*** *— Deux types de mots de passe sont utilisés dans Retyc pour chaque utilisateur enregistré : un mot de passe de connexion (authentification) et un mot de passe de chiffrement (protection de la clé privée). Retyc déconseille fortement l'utilisation du même mot de passe pour les deux fonctions.*

3.1 Principe fondamental

L'architecture de Retyc est conçue pour empêcher tout accès opérateur aux contenus en clair, y compris par l'éditeur du service.

Ce n'est pas une question de confiance dans nos équipes ou de robustesse de nos politiques internes. C'est une contrainte cryptographique imposée par notre architecture : les clés de déchiffrement (en clair) de vos contenus ne transitent jamais par nos serveurs et ne sont jamais accessibles à notre infrastructure.



3.2 Vue d'ensemble de l'architecture

L'architecture de Retyc articule plusieurs couches complémentaires :

Lorsqu'un utilisateur envoie un fichier via Retyc :

1. Le fichier est **chiffré localement dans le navigateur** avec la clé publique du ou des destinataires autorisés. En cas d'absence de destinataire enregistré, une clé éphémère est générée pour le transfert, chiffrée avec un mot de passe choisi par l'expéditeur.
2. Le fichier chiffré est envoyé vers nos serveurs : nous ne voyons que des données illisibles.
3. Le destinataire récupère le fichier chiffré et le déchiffre **localement dans son navigateur** avec sa clé privée.
4. La clé privée de chaque utilisateur est stockée sur nos serveurs sous forme **chiffrée avec le mot de passe de chiffrement de l'utilisateur**, que nous ne connaissons pas.

3.3 Ce que Retyc peut et ne peut pas faire

Il est essentiel d'être explicite sur les limites techniques de notre accès :

Donnée	Périmètre	Accessible à Retyc ?
Email, nom, prénom	Global	**Oui** — nécessaires au fonctionnement
Contenu des fichiers (en clair)	Retyc	**Non** — chiffré avant envoi
Métadonnées des fichiers (nom, taille, type)	Retyc	**Partiellement** — la taille des fichiers n'est pas chiffrée (nécessaire pour la gestion du stockage), mais les autres métadonnées (type, nom) sont chiffrées.
Cas particulier : nom des fichiers dans une dataroom	Retyc	**Non** — le nom est chiffré ; un hash `sha256` avec un sel aléatoire de 256 bits (CSPRNG), lui-même chiffré E2EE avec la clé de session, est utilisé pour la gestion des versions. Le sel étant inaccessible au serveur en clair, ce dernier ne peut pas inférer les noms de fichiers.
Messages d'un transfert	Retyc	**Non** — chiffrés E2EE
Journal d'activité et messagerie (dataroom)	Retyc	**Partiellement** — le contenu des messages et les métadonnées sensibles sont chiffrés. Les informations nécessaires au fonctionnement (ex. utilisateurs, types d'événements) restent visibles.
Titre d'un transfert / dataroom	Retyc	**Oui** — non chiffré E2EE
Clé privée d'un utilisateur	Retyc	**Non** — stockée uniquement sous forme chiffrée
Mot de passe de connexion	IAM	**Non** — haché avec argon2 (version `1.3`, `type=id`, `iterations=5`, `parallelism=1`, `memory=19 MiB`) côté serveur. **Si authentification via un fournisseur externe, aucun mot de passe n'est stocké**.
Récupération du mot de passe de chiffrement / Clé privée	Retyc	**Non** — en cas de perte du mot de passe de chiffrement, l'accès aux données chiffrées est définitivement perdu.
Adresse email (notifications)	Global	**Oui** — utilisée pour l'envoi de toutes les notifications par email (transfert reçu, invitation dataroom, code de vérification, etc.). Le prestataire d'envoi d'emails ne reçoit ni les fichiers ni les contenus chiffrés.

Cette transparence sur nos limites techniques est un élément constitutif de notre engagement envers nos utilisateurs.

> *Le périmètre "IAM" (Identity and Access Management) couvre les données d'authentification et de gestion des utilisateurs (gérée par l'application Keycloak v26.x). Le périmètre "Retyc" couvre les données liées aux transferts, datarooms et fichiers. Le périmètre "Global" couvre les données présentes dans les deux systèmes.*

3.4 Hypothèses et limites du modèle de sécurité

Retyc réduit fortement plusieurs risques liés au transfert et stockage de fichiers sensibles. Cependant, il est important de reconnaître les limites inhérentes à toute solution de sécurité :

Menace/Risque	Périmètre	Réduction du risque par Retyc	Limites
Compromission de l'appareil de l'utilisateur	Global	-	Si l'appareil de l'utilisateur est compromis par un malware ou un accès physique, les données chiffrées localement peuvent être exposées. Retyc recommande des pratiques de sécurité robustes côté client (antivirus, MFA, gestion des accès).
Attaques automatisées (scans, brute force, etc.)	Global	**Élevée**	Retyc met en œuvre des mécanismes de protection applicative (WAF) et de détection d'intrusion, incluant des solutions telles que CrowdSec, permettant d'identifier et de bloquer les comportements malveillants. Des attaques ciblées ou sophistiquées peuvent néanmoins contourner ces mécanismes.
Attaque par force brute sur le système d'authentification	IAM	**Élevée**	Keycloak implémente des mécanismes de protection contre les attaques par force brute (rate limiting, verrouillage de compte).
Attaque par force brute sur le mot de passe d'une clé privée	Retyc	**Partielle**	La clé privée est chiffrée avec scrypt (`N=2^18`), ce qui rend chaque tentative très coûteuse en temps et en ressources. La résistance effective dépend néanmoins de la robustesse du mot de passe choisi par l'utilisateur : un mot de passe faible réduit significativement cette protection malgré le coût de dérivation.
Attaque sur les algorithmes cryptographiques	Retyc	**Élevée**	Retyc utilise des algorithmes modernes et robustes face aux attaques connues, avec un schéma hybride intégrant des mécanismes résistants aux menaces quantiques à l'état actuel des connaissances.
Erreur de configuration ou de mise en œuvre	Global	**Partielle**	Bien que nous suivions les meilleures pratiques de développement sécurisé, une erreur humaine dans la configuration ou la mise en œuvre pourrait introduire une vulnérabilité. Nous avons mis en place des processus rigoureux de revue de code et de tests de sécurité pour minimiser ce risque.
Menace interne (abus de privilèges)	Global	**Élevée**	En raison de l'architecture zero-knowledge, même un employé malveillant ou un abus de privilèges ne dispose pas des éléments techniques permettant d'accéder aux contenus en clair.
Réquisition judiciaire	Global	**Élevée**	En cas de demande d'accès par une autorité compétente, Retyc et son hébergeur de fichiers ne peuvent fournir que des données chiffrées illisibles et les journaux de connexion. Nous ne pouvons pas déchiffrer ce que nous n'avons pas les moyens de déchiffrer.
Fuite de données sur les serveurs du fournisseur	Global	**Élevée**	En cas de fuite de données sur nos serveurs, les contenus chiffrés restent illisibles. Nous ne stockons pas de données en clair qui pourraient être exposées. Cependant, ces données ne permettent pas d'accéder aux contenus en clair

Menace/Risque	Périmètre	Réduction du risque par Retyc	Limites
Fuite des données présentes en base de données (email, nom, prénom)	Global	**Partielle**	En cas de fuite de données personnelles, les informations d'identification des utilisateurs pourraient être exposées.
Vol de cookies de session ou d'autres données d'authentification	Global	**Partielle**	En cas de vol de cookies de session, un attaquant pourrait potentiellement accéder à un compte utilisateur. Nous recommandons l'utilisation de MFA pour réduire ce risque et de ne pas utiliser Retyc sur des appareils partagés ou non sécurisés. Afin de limiter le risque, la durée de validité des sessions est limitée et les sessions inactives sont automatiquement déconnectées.
Attaque par injection de scripts malveillants (XSS) sur l'interface utilisateur	Retyc (web uniquement)	**Élevée**	Nous appliquons des politiques de sécurité strictes (CSP, HSTS) pour réduire les risques d'attaques XSS.
Vol du mot de passe de transfert	Retyc	**Faible**	Si un attaquant obtient le mot de passe d'un transfert, il peut accéder au contenu tant que le transfert est actif. L'expéditeur peut désactiver le transfert à tout moment pour révoquer l'accès. Pour les données sensibles, nous recommandons l'usage de destinataires enregistrés (clés asymétriques).
Utilisateur révoqué ayant déjà téléchargé les fichiers avant la révocation	Retyc	**Faible**	Si un utilisateur révoqué a déjà téléchargé les fichiers avant la révocation, il pourrait conserver une copie locale. La révocation empêche l'accès futur, mais ne peut pas effacer les copies déjà téléchargées. Nous recommandons de limiter la durée de validité des liens pour réduire ce risque.
Oubli de mot de passe de la clé privée	Retyc	-	En l'absence de "Master Key", l'oubli du mot de passe par l'unique détenteur d'un accès entraîne la perte des données. Néanmoins, la multiplicité des membres autorisés assure la redondance de l'accès.
Compromission des codes source	Retyc	**Partielle**	En cas de compromission du code source, un attaquant pourrait théoriquement introduire une vulnérabilité ou un backdoor. Cependant, l'architecture zero-knowledge limite les risques d'accès aux données chiffrées. Nous suivons des pratiques rigoureuses de revue de code et de sécurité pour minimiser ce risque.
Compromission d'une clé privée d'un utilisateur (exfiltration ou attaque ciblée)	Retyc	**Partielle**	En cas de compromission de la clé privée d'un utilisateur, les données chiffrées pour cet utilisateur pourraient être exposées. Cependant, les autres utilisateurs et leurs données restent protégés. En cas de suspicion ou de compromission, la rotation des clés et la modification du mot de passe de chiffrement permettent de limiter l'impact.

Menace/Risque	Périmètre	Réduction du risque par Retyc	Limites
Compromission de l'infrastructure d'hébergement (Scaleway, Clever Cloud)	Hébergement	**Partielle**	En cas de compromission de l'infrastructure d'hébergement, les données chiffrées restent illisibles. Néanmoins, une compromission pourrait entraîner une indisponibilité temporaire du service et une éventuelle exploitation des données non chiffrées
Utilisation d'une clé révoquée pour déchiffrer des données passées	Retyc	**Faible**	Lors d'une rotation de clé, l'ancienne clé privée chiffrée est supprimée au niveau serveur et la clé de session est rechiffrée pour les espaces concernés. Le risque résiduel est limité au cas où l'utilisateur aurait conservé une copie locale de sa clé privée en dehors de Retyc. La rotation de clé d'un utilisateur ne rechiffre la clé de session que sur les transferts qu'il a créés et les datarooms dont il est administrateur. Dans les autres cas, le rekey doit être déclenché par un administrateur de l'espace.

> *Note — La sécurité des mécanismes reposant sur un mot de passe dépend de la robustesse du secret choisi. Nous recommandons l'utilisation de mots de passe forts et uniques.*

3.5 Mécanismes minimisant les risques résiduels

Mécanisme de mitigation	Description	Limites
Authentification forte optionnelle (MFA)	Nous recommandons et supportons l'authentification à deux facteurs pour renforcer la sécurité des comptes utilisateurs.	Ne protège pas contre les attaques ciblant directement l'appareil de l'utilisateur ou les erreurs de configuration côté client.
HSTS, CSP, CORS et permissions policy stricts	Nous appliquons des politiques de sécurité HTTP strictes pour protéger contre les attaques de type man-in-the-middle et les injections de scripts.	Ne protège pas contre les attaques ciblant directement l'appareil de l'utilisateur.
WAF et surveillance des anomalies	Nous utilisons un pare-feu applicatif (WAF) et des systèmes de détection d'intrusion pour surveiller les activités suspectes sur nos serveurs.	Ne protège pas contre les attaques ciblant directement l'appareil de l'utilisateur ou les erreurs de configuration côté client.
Rate limiting et protection contre les attaques par force brute	Nous mettons en œuvre des mécanismes de limitation de débit (rate limiting) afin de réduire l'impact des abus automatisés et de certaines attaques par déni de service	L'hébergement peut être temporairement indisponible en cas d'attaque par déni de service, mais les données restent protégées.
Mises à jour régulières et suivi des vulnérabilités	Nous suivons activement les vulnérabilités de sécurité et appliquons des mises à jour régulières pour corriger les failles potentielles.	Ne protège pas contre les attaques ciblant directement l'appareil de l'utilisateur ou les erreurs de configuration côté client.
Aucun script de tracking tiers et collecte minimale de données personnelles	Nous n'utilisons aucun cookie tiers qui pourrait être exploité pour le suivi publicitaire ou l'analyse comportementale, et nous limitons la collecte de données personnelles au strict nécessaire.	Ne protège pas contre les attaques ciblant directement l'appareil de l'utilisateur ou les erreurs de configuration côté client.
Authentification avec Keycloak et gestion des accès basée sur les rôles (RBAC)	Nous utilisons Keycloak pour gérer l'authentification en limitant les durées de session et en appliquant une gestion granulaire des accès basée sur les rôles.	Ne protège pas contre les attaques ciblant directement l'appareil de l'utilisateur ou les erreurs de configuration côté client.
Rotation des clés de chiffrement	Nous offrons la possibilité de faire tourner les clés de chiffrement pour limiter l'impact d'une éventuelle compromission.	La rotation de clés permet de limiter l'impact d'une compromission, mais ne protège pas des éventuelles données exposées avant la rotation.
Désactivation de compte par un administrateur (Business/Enterprise)	Un administrateur peut désactiver un compte utilisateur, ce qui coupe immédiatement tout accès aux ressources : invalidation des sessions actives (authentification) et révocation des droits d'accès (ACL).	Ne supprime pas les copies de fichiers déjà téléchargés localement par l'utilisateur avant la désactivation.

3.6 Gestion des identités et du cycle de vie des accès

Retyc utilise Keycloak pour la gestion des identités et des accès (IAM).

Les utilisateurs peuvent se connecter avec :

- un email et un mot de passe
- via des fournisseurs d'identité externes (SSO) compatibles SAML 2.0 ou OpenID Connect.

Les sessions sont **limitées dans le temps** et les utilisateurs inactifs sont automatiquement déconnectés. En cas de suspicion de compromission ou de comportement anormal, les sessions peuvent être invalidées manuellement par un administrateur Retyc.

L'accès au service d'authentification est **restreint au strict périmètre nécessaire** au fonctionnement de Retyc. Un reverse proxy dédié limite l'exposition publique au seul espace d'authentification utilisé par la plateforme, réduisant ainsi la surface d'attaque.

Gestion des accès dans les organisations

Dans le cas d'une gestion avec organisation (plan business et entreprise), les administrateurs peuvent gérer les accès de leurs collaborateurs et révoquer des accès.

Les utilisateurs **invités non inscrits** peuvent être supprimés à tout moment par un administrateur, entraînant la suppression des données dont ils sont propriétaires (transferts, datarooms).

En revanche, lorsqu'un utilisateur **dispose déjà d'un compte au moment de son invitation**, la suppression de son accès à une organisation met fin à ses droits au sein de celle-ci, **sans entraîner la suppression de son compte ni des données** dont il est propriétaire.

Intégration aux environnements d'entreprise

Retyc propose un mécanisme d'affectation automatique des utilisateurs à une organisation basé sur leur adresse email (ex. `@company.tld`).

Retyc permet également l'intégration de fournisseurs d'identité (IdP) propres aux organisations clientes, sous réserve de compatibilité avec Keycloak, notamment via des standards tels que SAML 2.0 ou OpenID Connect.

Cette approche permet de s'appuyer sur les mécanismes d'authentification existants de l'organisation (annuaire interne, SSO, MFA) sans duplication des identités, tout en conservant une gestion cohérente des rattachements utilisateurs. Les politiques de sécurité associées, lorsqu'elles sont déléguées à l'IdP du client, restent sous le contrôle de celui-ci.

---

4. Chiffrement de bout en bout avec mécanismes résistants aux menaces quantiques

4.1 Au-delà du chiffrement classique

Il existe trois niveaux de protection des données dans les solutions de partage de fichiers :

Niveau 1 — Chiffrement en transit (HTTPS / TLS) : protection pendant le transfert réseau. Standard aujourd'hui, mais insuffisant : vos données arrivent déchiffrées sur les serveurs du fournisseur, qui peut y accéder.

Niveau 2 — Chiffrement au repos (server-side encryption) : les fichiers sont chiffrés sur les serveurs du fournisseur. Protection contre les attaques physiques, mais le fournisseur conserve les clés de déchiffrement. Il peut accéder aux contenus pour maintenance, analyse ou sur demande légale.

Niveau 3 — Chiffrement de bout en bout (E2EE) : approche adoptée par Retyc. Les fichiers sont chiffrés sur l'appareil de l'expéditeur avant tout envoi. Seuls les destinataires autorisés peuvent les déchiffrer. Le fournisseur ne dispose pas des éléments lui permettant d'accéder aux contenus en clair.

Ces deux premiers niveaux (transport et stockage) sont aujourd'hui des standards de l'industrie et ne constituent pas, à eux seuls, un mécanisme de protection de la confidentialité vis-à-vis du fournisseur.

> *Le marché du partage de fichiers entretient une **confusion fréquente** : certaines solutions se revendiquant "chiffrées" reposent en réalité sur du chiffrement en transit ou au repos, des mécanismes standards aujourd'hui généralisés et **insuffisants pour garantir la confidentialité** des données.*
> *Ces approches laissent au fournisseur la **capacité technique d'accéder aux données en clair** et ne sont pas équivalentes à un chiffrement de bout en bout. Retyc adopte cette dernière approche.*

4.2 La cryptographie age-encryption

Retyc s'appuie sur le format de chiffrement **age**, conçu pour proposer une approche moderne, simple et robuste du chiffrement de fichiers. Age peut être considéré comme un **composant de confiance** : sa spécification est publique et formelle, il repose sur des primitives cryptographiques éprouvées, et il est conçu et maintenu par Filippo Valsorda, cryptographe reconnu (ancien responsable sécurité de l'équipe Go chez Google).

Côté application web, Retyc utilise age-encryption, l'implémentation TypeScript de la spécification age. Cette approche permet d'exécuter les opérations cryptographiques directement côté client, sans exposer les contenus en clair au serveur.

La transparence du code cryptographique est une garantie supplémentaire : la **bibliothèque** `age-encryption` est open source et son code peut être inspecté et audité par des experts tiers indépendants. Le code source de l'application web (frontend et backend) n'est pas public, mais la **CLI Retyc est open source** et auditable, et les primitives cryptographiques sous-jacentes le sont également.

4.3 Chiffrement avec clés hybrides post-quantique

Les ordinateurs quantiques, lorsqu'ils atteindront une puissance suffisante, seront en mesure de casser les algorithmes asymétriques classiques (RSA, ECC) actuellement utilisés dans la plupart des solutions de sécurité.

La stratégie dite *harvest now, decrypt later* représente une menace concrète : des acteurs malveillants ou étatiques capturent aujourd'hui des données chiffrées en anticipant leur déchiffrement futur. Pour des données ayant une durée de vie longue (contrats, dossiers médicaux, données financières), ce risque est réel.

Retyc utilise par défaut un schéma de clés hybrides intégrant des mécanismes **résistants aux menaces quantiques**, dans le cadre du format age.

Cette approche hybride vise à réduire le risque qu'une faiblesse affectant un seul composant compromette à elle seule la confidentialité des données.

Toutes les clés sont exclusivement générées et chiffrées sur le poste de l'utilisateur. **Les clés privées ne sont pas accessibles en clair à l'infrastructure Retyc**.

4.4 Gestion des clés et rotation

Chaque utilisateur Retyc dispose d'une paire de clés asymétriques (publique/privée) :

- La **clé publique** est stockée sur nos serveurs et utilisée par les expéditeurs pour chiffrer les fichiers à destination de cet utilisateur.
- La **clé privée** est chiffrée avec le mot de passe de chiffrement de l'utilisateur et stockée sur nos serveurs sous forme chiffrée. Nous n'y avons jamais accès en clair.
- La **rotation des clés** est disponible sur tous les plans, permettant de générer de nouvelles clés et de rechiffrer les données existantes.

Principe d'absence de clé maîtresse

> *Contrairement aux architectures "cloud" traditionnelles, Retyc n'implémente aucune clé maîtresse ("Master Key") ni mécanisme de recouvrement d'urgence.* ***Cette architecture ne laisse pas d'accès administrateur aux contenus en clair****. La responsabilité de la conservation des mots de passe* ***incombe exclusivement à l'utilisateur ou à la politique de gestion des secrets de son organisation*** *(coffre-fort de mots de passe, IAM).*

4.5 Implémentation technique détaillée

> *Cette section s'adresse aux équipes techniques et aux auditeurs souhaitant vérifier les propriétés cryptographiques de la plateforme.*

Primitives cryptographiques

Retyc s'appuie sur age-encryption, l'implémentation TypeScript du format age pour les opérations de chiffrement exécutées côté client.

Selon les mécanismes mis en œuvre par cette bibliothèque :

- **X25519** : pour les échanges de clés.
- **ML-KEM-768** : dans le cadre des clés hybrides intégrant des mécanismes **résistants aux menaces quantiques** connues à ce jour (schéma hybride MLKEM768-X25519). Ce schéma est implémenté via une extension du format age (format de clé `age1pq1...`), en complément du format age standard (FIPS 203).
- **ChaCha20-Poly1305** : pour le chiffrement authentifié des données.
- **scrypt** (`N=2^18`) : dérivation de la clé d'enveloppement lors du chiffrement par passphrase (stanza `scrypt` d'age).
- **HKDF-SHA-256** : dérivation de la clé de chiffrement du payload à partir de la file key (mécanisme interne d'age).

> ***Note** — scrypt est utilisé par age pour la protection de la clé privée, une opération exécutée **côté client** dans le navigateur. Argon2id est utilisé indépendamment par Keycloak pour le hachage des mots de passe d'authentification, côté serveur. Ce sont deux systèmes distincts opérant sur deux périmètres différents.*

Génération des paires de clés utilisateur

Les paires de clés sont générées via `generateHybridIdentity()`, qui produit une identité hybride X25519 + ML-KEM-768. Ce schéma hybride vise à réduire le risque qu'une faiblesse affectant un seul composant compromette à elle seule la confidentialité des données : avancée mathématique contre X25519 ou faiblesse découverte dans ML-KEM-768.

Toutes les identités utilisateur Retyc étant hybrides par défaut, il n'existe pas de mélange entre destinataires hybrides post-quantiques et non post-quantiques (contrainte explicite de la spécification age).

La clé privée brute n'est **jamais transmise ni stockée en clair** sur nos serveurs. Elle est chiffrée côté client avec le mot de passe de chiffrement de l'utilisateur via age en mode passphrase (scrypt), ce qui rend les attaques par force brute prohibitives en termes de coût machine.

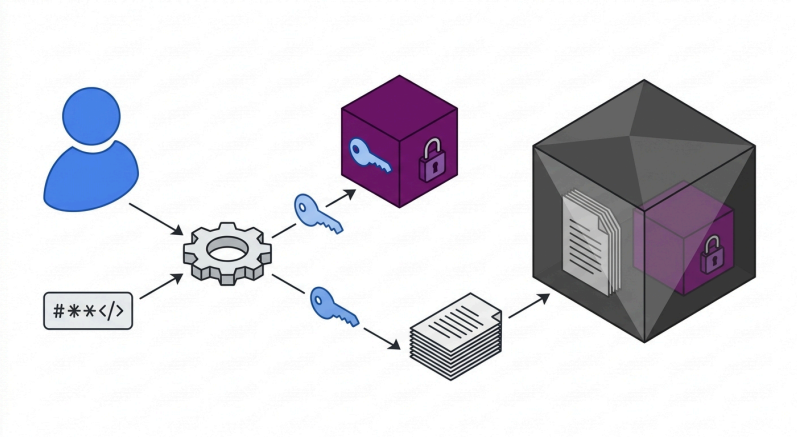
Chiffrement multi-destinataires

> *Le principe décrit ci-dessous constitue le fonctionnement de référence. Des variantes existent selon les cas d'usage (gestion des destinataires, modalités d'accès), tout en conservant les mêmes garanties de sécurité.*

Transferts et datarooms reposent sur un **socle cryptographique commun** :

1. Une paire de clés hybride X25519 + ML-KEM-768 (la **clé de session**) est générée côté client.
2. Les fichiers et les **métadonnées sensibles** (nom de fichier, type MIME) sont chiffrés avec la `session_public_key`. Pour les fichiers volumineux, le chiffrement est appliqué par chunk pour limiter l'impact sur la mémoire.
3. La `session_private_key` est chiffrée pour chaque destinataire enregistré via `encryptStringWithRecipients()`.
4. Au téléchargement, le destinataire déchiffre `session_private_key_enc` avec sa propre clé privée age, puis déchiffre les fichiers localement avec la `session_private_key` obtenue.

Le serveur ne reçoit que des éléments chiffrés : fichiers, métadonnées et clé de session lui sont inaccessibles en clair.



Isolation des opérations cryptographiques dans le navigateur

Toutes les opérations cryptographiques s'exécutent dans un **Web Worker dédié**, isolé du thread principal de l'interface. Ce choix architectural a deux conséquences :

- **Performance** : les opérations de chiffrement, potentiellement longues sur des fichiers volumineux, ne bloquent pas l'interface utilisateur.
- **Isolation** : le contexte cryptographique est séparé du reste de l'application, réduisant la surface d'attaque par injection de scripts malveillants dans le DOM principal.

Les buffers binaires sont transférés entre threads par transfert de propriété plutôt que par copie, limitant la duplication en mémoire des données sensibles.

---

5. Architecture zero-knowledge : la confidentialité par conception

5.1 Définition

> ***Note terminologique*** *— Le terme "zero-knowledge" est employé ici au sens industriel courant : le fournisseur n'a pas accès aux contenus en clair. Ce terme désigne en cryptographie académique les preuves à divulgation nulle de connaissance (Goldwasser-Micali-Rackoff), un concept distinct. L'usage que nous en faisons est répandu dans l'industrie mais doit être distingué de son sens académique strict.*

Une architecture zero-knowledge signifie que le fournisseur de service n'a aucune connaissance (*zero knowledge*) du contenu des données qu'il traite. Cette propriété est garantie par construction cryptographique, pas par une politique interne.

Chez Retyc, zero-knowledge signifie concrètement :

- Nous ne disposons pas des éléments permettant d'accéder en clair au contenu des fichiers, aux noms de fichiers, aux messages associés, ni aux clés privées des utilisateurs.
- Si un utilisateur oublie son mot de passe de chiffrement, nous ne pouvons ni récupérer sa clé privée ni déchiffrer les données associées.
- Isolation cryptographique : chaque espace est indépendant. La compromission d'un compte ou d'un poste administrateur n'offre aucun levier technique pour déchiffrer les données des autres collaborateurs.

5.2 Implications pour la conformité

L'architecture zero-knowledge a des implications directes pour la conformité réglementaire :

Pour le RGPD : les données chiffrées dont nous ne possédons pas les clés nous sont inaccessibles en clair. Nous ne pouvons pas les exploiter à des fins non autorisées et ne disposons pas des éléments permettant d'y accéder en clair. Retyc reste néanmoins **responsable de traitement** au sens RGPD pour les données de compte (email, nom, prénom) et **sous-traitant** pour les contenus chiffrés. L'architecture zero-knowledge réduit notre exposition, elle ne nous exonère pas de nos obligations réglementaires.

Pour les secrets professionnels : les obligations déontologiques des avocats, experts-comptables et professionnels de santé imposent une confidentialité rigoureuse des données confiées. Une garantie purement contractuelle ne suffit pas à y répondre techniquement. L'architecture zero-knowledge de Retyc apporte un renforcement cryptographique que nous ne pouvons pas contourner.

Face aux réquisitions judiciaires : en cas de demande d'accès par une autorité, Retyc ne peut livrer que des données chiffrées illisibles. Nous ne pouvons pas déchiffrer ce que nous n'avons pas les moyens de déchiffrer.

5.3 Limites assumées et transparentes

La rigueur impose d'être précis sur ce que zero-knowledge couvre et ne couvre pas dans notre architecture :

- Le **titre d'un transfert ou d'une dataroom** n'est pas chiffré E2EE (c'est un choix de conception pour permettre l'affichage dans l'interface et effectuer des notifications).
- La **taille des fichiers** n'est pas chiffrée (nécessaire pour la gestion du stockage).
- La **liste des membres** d'un transfert ou d'une dataroom n'est pas chiffrée E2EE (nécessaire pour la gestion des accès).
- Les **métadonnées de connexion** (adresse IP, date/heure) sont collectées à des fins de sécurité dans notre système d'authentification (Keycloak).
- Dans le cadre d'une dataroom, un hash `sha256` du nom de fichier est calculé avec un sel aléatoire de 256 bits (CSPRNG) chiffré E2EE avec la clé de session de la dataroom. Seul ce hash est transmis au serveur pour la gestion des versions. Le nom du fichier et le sel restent inaccessibles au serveur en clair.

Ces limites sont documentées publiquement dans notre page de transparence. Nous préférons une transparence totale sur nos capacités réelles plutôt que des affirmations invérifiables.

> *Bien que Retyc ne puisse pas restaurer un accès perdu à la clé privée de chiffrement, nous préconisons l'usage de gestionnaires de mots de passe d'entreprise lors de l'enregistrement des comptes critiques.*

Limites structurelles du E2EE dans un navigateur web

Deux limites fondamentales, communes à toute solution de chiffrement opérant dans un navigateur, méritent d'être explicitement assumées :

1. **Substitution de clé publique.** Retyc distribue les clés publiques des destinataires via ses serveurs. Un expéditeur fait confiance à cette distribution. En cas de compromission des serveurs ou d'abus interne, un attaquant pourrait théoriquement substituer une clé publique.
2. **Intégrité du code JavaScript.** Dans un contexte web, le navigateur exécute le code de chiffrement livré par le serveur à chaque chargement de page. Une compromission du serveur de distribution du code frontend pourrait donc potentiellement affecter les opérations cryptographiques avant leur exécution. Pour limiter ce risque, Retyc applique une politique CSP stricte qui **interdit l'exécution de tout script externe** : seuls les scripts servis directement par le frontend Retyc peuvent s'exécuter dans le navigateur. Aucun script tiers,

inline ou provenant d'un domaine externe n'est autorisé. Cette mesure élimine les vecteurs d'injection (XSS, supply chain tiers), mais ne protège pas contre une compromission du serveur d'origine lui-même (limite inhérente à tout modèle E2EE web).

Ces deux vecteurs sont inhérents au modèle E2EE web et reconnus comme tels par l'ensemble de l'industrie. Ils ne remettent pas en cause la solidité du modèle cryptographique, mais doivent être pris en compte dans toute évaluation du niveau de risque résiduel.

---

6. Indépendance technologique européenne

6.1 Hébergement 100% européen

Toutes les données traitées par Retyc sont hébergées **exclusivement dans l'Union européenne**, auprès de prestataires français soumis au droit européen :

Prestataire	Rôle	Localisation
Scaleway SAS	Hébergement applicatif, stockage	France (UE)
Clever Cloud SAS	Hébergement applicatif (Keycloak)	France (UE)
Brevo SAS	Emails transactionnels	France (UE)

Stripe Inc. est utilisé pour le traitement des paiements uniquement. Les données transmises à Stripe se limitent aux informations strictement nécessaires à la transaction (montant, devise, identifiant client). Aucun contenu utilisateur, aucun fichier ni aucune métadonnée de transfert ne sont communiqués à Stripe. En tant qu'entreprise américaine, Stripe reste soumise au Cloud Act pour ces données de paiement — exposition résiduelle assumée et limitée à ce périmètre.

6.2 Certifications hébergement

Scaleway et Clever Cloud sont certifiés **HDS** (Hébergeur de Données de Santé) par des organismes accrédités par le COFRAC.

Ces certifications attestent d'un niveau de maturité élevé en matière de sécurité et de conformité de la part de nos prestataires d'infrastructure.

Retyc n'est pas lui-même certifié HDS ni ISO 27001. En choisissant des prestataires d'infrastructure soumis à ces référentiels exigeants, nous offrons à nos clients un niveau de maturité élevé sur l'ensemble de la chaîne d'hébergement. Les évolutions futures de notre architecture et de nos processus pourraient nous conduire à envisager, le cas échéant, des démarches de certification adaptées.

6.3 Réplication et haute disponibilité

Vos données (fichiers envoyés) sont **répliquées automatiquement sur trois zones de disponibilité européennes** (Scaleway). Cette architecture garantit :

- Une haute disponibilité
- Une résilience face aux pannes d'un datacenter.
- Pas de point de défaillance unique au niveau du stockage des fichiers.

6.4 Indépendance vis-à-vis des GAFAM

> *Certaines solutions assimilent à tort la localisation des données à leur protection juridique. Héberger des données dans un datacenter situé en France ou en Europe via des entreprises soumises à des **législations extraterritoriales** (notamment américaines) ne garantit pas l'absence d'exposition à ces juridictions. Cette confusion peut conduire à **surestimer le niveau réel de protection** offert.*

Retyc n'utilise **aucun service d'hébergement ou d'infrastructure des plateformes américaines** (tels que Google Cloud, Amazon Web Services ou Microsoft Azure). L'intégralité des données utilisateurs est hébergée exclusivement auprès d'opérateurs européens. Stripe Inc. (américain) est utilisé pour le traitement des paiements uniquement (aucune donnée de contenu n'y est stockée ni hébergée).

Cette indépendance n'est pas seulement idéologique : elle réduit significativement l'exposition aux risques d'extraterritorialité. Le **Cloud Act** (2018) contraint les entreprises américaines à fournir aux autorités américaines les données qu'elles hébergent, y compris pour des clients européens, indépendamment du lieu de stockage. En choisissant une infrastructure exclusivement européenne, Retyc réduit significativement les risques liés à ces législations extraterritoriales.

Cette distinction entre localisation physique et juridiction applicable est souvent mal comprise, y compris dans des communications commerciales.

6.5 Souveraineté décisionnelle

TripleStack SAS est une société française indépendante, sans actionnaires étrangers ni dépendance à des groupes internationaux. Les décisions concernant l'architecture, la sécurité et la gestion des données sont prises en France, dans le respect exclusif du droit européen.

---

7. Fonctionnalités : transfert de fichiers et datarooms

7.1 Transfert de fichiers sécurisé

Le transfert de fichiers Retyc est conçu pour combiner simplicité d'usage et sécurité maximale.

Processus de transfert :

1. **Chiffrement automatique** : l'utilisateur glisse-dépose ses fichiers dans l'interface. À la validation, les fichiers sont chiffrés localement dans le navigateur avec les clés publiques des destinataires autorisés.
2. **Génération d'un lien sécurisé** : un lien unique est généré instantanément. Seul le ou les destinataires autorisés pourront déchiffrer et accéder au contenu chiffré.
3. **Téléchargement sécurisé** : le destinataire télécharge et déchiffre le fichier directement dans son navigateur. Aucune installation logicielle n'est requise.
4. **Expiration automatique** : le lien expire automatiquement après le délai configuré. Les fichiers sont définitivement supprimés.

Fonctionnalités de contrôle :

- Expiration configurable des transferts
- Protection optionnelle par un mot de passe pour les destinataires sans compte
- Révocation à tout moment des accès (désactivation du lien)
- Réception de fichiers : génération de liens permettant à des tiers de vous envoyer des documents directement dans votre espace sécurisé
- Possibilité de générer des formulaires de collecte de fichiers personnalisés

Compatibilité :

- Fonctionnement depuis tout navigateur web moderne
- Prise en charge de tous les types de fichiers, y compris les fichiers volumineux
- **Aucune restriction sur le type de fichier** : les fichiers sont traités sans filtrage ni restriction liée à leur format.
- Aucune installation requise pour les destinataires

7.2 Datarooms collaboratives chiffrées

Les datarooms Retyc sont des espaces collaboratifs sécurisés permettant de centraliser et gérer des documents confidentiels avec des équipes ou des partenaires externes. Contrairement aux solutions de stockage partagé classiques, la sécurité n'est pas gérée uniquement par des listes de contrôle d'accès (ACL) sur un serveur, mais sur le chiffrement lui-même.

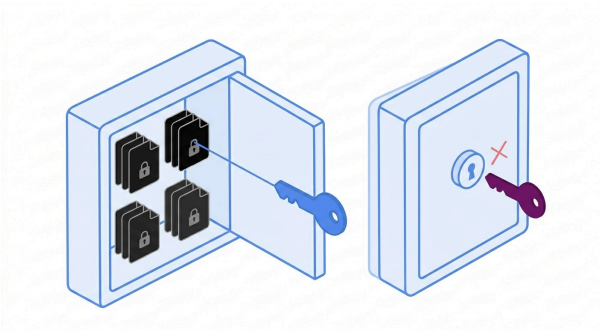
Architecture de sécurité des datarooms :

- **Isolation cryptographique** : chaque dataroom est cryptographiquement isolée des autres

- **Gestion des accès cryptographiques par utilisateur** : chaque dataroom repose sur une isolation cryptographique propre, et l'accès aux clés de session est géré individuellement pour chaque utilisateur autorisé.
- **Zéro accès Retyc** : nous ne pouvons pas lire les documents ni les noms de fichiers stockés dans une dataroom.
- **Rekey cryptographique** : lors de l'ajout ou de la suppression d'un membre, un administrateur peut déclencher un rechiffrement de la clé de session pour la liste exacte des membres autorisés. Après cette opération, un membre révoqué ne peut plus obtenir la clé de session depuis le serveur. Cette opération est à la discrétion de l'administrateur et doit être réalisée explicitement.
- **Responsabilité de l'accès** : aucun "accès de secours" n'est maintenu par Retyc. La disponibilité des données au sein d'une dataroom est assurée par la multiplicité des utilisateurs autorisés : tant qu'un membre actif peut accéder, les données restent disponibles.

Gestion documentaire :

- Organisation et gestion centralisée des fichiers
- **Versioning automatique** : chaque mise à jour crée une nouvelle version sans écraser les précédentes. Historique complet et restauration possible
- Gestion de l'historique des versions : consultation, restauration ou suppression
- Messagerie chiffrée intégrée



Gestion des accès :

- **Permissions granulaires par rôle** : lecture seule, ajout de documents, gestion complète par utilisateur
- Invitation de collaborateurs internes (organisation) et externes (invités)
- Révocation instantanée des accès
- Journal d'activité complet : tous les accès, téléchargements et modifications sont tracés

8. Transparence opérationnelle

8.1 Cryptographie open source

Retyc s'appuie sur la bibliothèque age-encryption pour les opérations de chiffrement côté client. Cette bibliothèque est open source, son code source est publiquement accessible pour audit. Le code source de l'application web (frontend et backend) n'est pas public, mais la **CLI Retyc est open source** et les primitives cryptographiques sous-jacentes le sont également.

Cette transparence sur les fondations cryptographiques permet une vérification indépendante : la bibliothèque peut être inspectée et auditée par des experts tiers, ce qui renforce la confiance dans les propriétés de sécurité annoncées.

8.2 Page de transparence publique

Retyc publie une page de transparence détaillée sur son site, accessible à tous, qui documente de manière exhaustive :

- La liste exhaustive des cookies utilisés et leur finalité
- Les données stockées dans le navigateur de l'utilisateur
- Le détail de toutes les données stockées en base de données, leur finalité, leur durée de conservation et leur niveau de chiffrement

Cette transparence sur nos pratiques est accessible publiquement sur notre site.

8.3 Politique zéro IA

Retyc n'utilise **aucune intelligence artificielle dans son produit** : pas d'IA générative, pas de fonctionnalités assistées par IA, pas d'analyse de contenu par algorithme d'apprentissage automatique.

Ce choix délibéré répond à une demande de nos utilisateurs professionnels pour qui l'utilisation de leurs contenus sensibles à des fins d'entraînement de modèles d'IA représente un risque inacceptable. Chez Retyc, vos fichiers ne servent pas à entraîner des modèles tiers. C'est un engagement produit, qui est restreint par la nature même de notre application : nous ne pouvons pas analyser les contenus que nous ne pouvons pas lire.

8.4 Audit de sécurité externe

Retyc intègre des audits de sécurité réalisés par des tiers indépendants dans son processus de développement, couvrant notamment les aspects cryptographiques, l'infrastructure et les tests d'intrusion. Les conclusions significatives, ainsi que les corrections apportées, font l'objet d'une communication transparente auprès de nos utilisateurs.

8.5 Signalement des vulnérabilités

Retyc prend la sécurité très au sérieux. Notre politique de *responsible disclosure* est accessible via le fichier `/.well-known/security.txt` sur notre domaine, conformément aux bonnes pratiques de la communauté de sécurité (RFC 9116). Toute vulnérabilité découverte doit être signalée selon les modalités décrites dans ce fichier.

8.6 Outils open source et interopérabilité

Retyc propose également une interface en ligne de commande (CLI) open source, permettant d'interagir avec la plateforme de manière automatisée ou intégrée dans des workflows techniques.

Le code source de la CLI est disponible sur notre dépôt GitHub : github.com/retyc/retyc-cli

Cette CLI s'adresse notamment aux équipes techniques souhaitant :

- automatiser des transferts de fichiers
- intégrer Retyc dans des pipelines (CI/CD, scripts, outils internes)
- auditer et contrôler les opérations réalisées

Le code source est public et auditable, s'inscrivant dans la démarche de transparence et d'ouverture de Retyc.

---

9. Cas d'usage

9.1 Cabinets d'avocats et directions juridiques

Les professionnels du droit sont soumis à des obligations de secret professionnel qui ne peuvent reposer sur de simples engagements contractuels. L'architecture zero-knowledge de Retyc permet d'offrir une protection robuste et de limiter les risques de fuite de données sensibles.

Cas d'usage typiques :

- Transmission sécurisée de contrats, actes notariés et pièces sensibles à des clients.
- Datarooms pour opérations M&A, due diligence et gestion de contentieux.
- Réception sécurisée de pièces justificatives sans recours à l'email non chiffré.
- Collaboration sur dossiers avec confrères, experts ou parties prenantes externes.

Valeur ajoutée : le journal d'activité complet constitue une preuve de diligence en matière de confidentialité en cas de litige ou de contrôle ordinal.

9.2 Cabinets d'expertise comptable

Les données financières (bilans, relevés bancaires, bulletins de paie, liasses fiscales) sont parmi les plus sensibles. Leur transmission par email représente un risque majeur.

Cas d'usage typiques :

- Réception sécurisée de pièces comptables clients via un lien unique personnalisé.
- Envoi chiffré de déclarations fiscales, bulletins de paie et documents de clôture.
- Datarooms pour audits, due diligence et transmissions de cabinet.
- Collaboration avec confrères ou experts sur des dossiers complexes.

Valeur ajoutée : la collecte de pièces clients via lien unique remplace l'email non sécurisé pour les échanges quotidiens. La centralisation des documents dans des datarooms sécurisées facilite la gestion documentaire et la traçabilité.

9.3 Équipes techniques et ingénierie

Les équipes techniques manipulent régulièrement des informations hautement sensibles : clés d'API, dumps de base de données, rapports de sécurité, propriété intellectuelle.

Cas d'usage typiques :

- Partage sécurisé de rapports de tests d'intrusion et d'audits de sécurité.
- Transmission de fichiers de configuration contenant des secrets.
- Datarooms pour la gestion documentaire de projets confidentiels.

Valeur ajoutée : l'absence de dépendance aux GAFAM répond aux exigences de sécurité des organisations les plus rigoureuses.

9.4 Entreprises et secteurs régulés

Pour les organisations soumises à NIS2, DORA ou à des réglementations sectorielles, Retyc peut contribuer à répondre à certaines exigences de sécurité et de confidentialité, notamment sur le chiffrement des données en transit et au repos, la traçabilité des accès et l'indépendance vis-à-vis des fournisseurs extraterritoriaux.

> ***Périmètre*** *— Retyc est un outil de transfert et de collaboration chiffrée. Il ne couvre pas l'ensemble des exigences NIS2 ou DORA (gouvernance, tests de résilience, registre des prestataires TIC, etc.). Son adoption doit s'inscrire dans une démarche de conformité plus large portée par l'organisation.*

Cas d'usage typiques :

- Échange de documents confidentiels avec des partenaires, prestataires ou régulateurs.
- Datarooms pour les processus RH sensibles (contrats, évaluations).
- Transmission sécurisée de données dans le cadre de processus de due diligence ou d'appels d'offres.

Valeur ajoutée : selon le plan retenu, Retyc peut intégrer le SSO (SAML/OIDC), un branding personnalisé et un déploiement on-premises pour les organisations ayant des exigences d'intégration spécifiques.

---

10. Offres et déploiement

10.1 Modèle freemium avec plans progressifs

Retyc propose quatre niveaux d'offre permettant à chaque organisation de démarrer gratuitement et d'évoluer selon ses besoins :

	Free	Solo	Business	Enterprise
Transferts sortants	Limité	Étendu	Étendu	Personnalisé
Réception de fichiers	Oui	Oui	Oui	Oui
Datarooms	Oui	Oui	Oui	Personnalisé
Membres internes par dataroom	—	—	Illimité	Illimité
Chiffrement E2EE	**Oui**	**Oui**	**Oui**	**Oui**
Rotation des clés	Oui	Oui	Oui	Oui
SSO (SAML/OIDC)	Non	Non	Sur demande	Oui
Support premium	Non	Non	Non	Oui
Domaine personnalisé	Non	Non	Non	Oui
Déploiement on-premises	Non	Non	Non	Oui

Les détails de chaque plan sont disponibles sur notre site : retyc.com/fr/pricing.

> *Le chiffrement de bout en bout et la rotation des clés sont disponibles sur **tous les plans, y compris Free**.*

10.2 Déploiement SaaS

Le déploiement standard de Retyc est en mode SaaS (Software as a Service) : aucune installation côté client, accessible depuis tout navigateur moderne. L'ensemble de l'infrastructure est géré par Retyc, hébergée auprès de prestataires européens.

10.3 Déploiement on-premises (Enterprise)

Pour les organisations ayant des contraintes réglementaires ou de sécurité spécifiques imposant que les données ne quittent pas leur infrastructure, Retyc propose un **déploiement on-premises** dans le cadre de l'offre Enterprise.

Ce modèle de déploiement permet à l'organisation cliente de faire tourner l'ensemble de la plateforme Retyc sur sa propre infrastructure, en conservant le contrôle total de ses données.

10.4 Intégrations avancées

L'offre Enterprise inclut la possibilité d'intégrations personnalisées, notamment :

- **SSO SAML/OIDC** : intégration avec l'annuaire d'entreprise existant (Active Directory, Okta, etc.).
- **Branding personnalisé** : adaptation de l'interface aux couleurs et au logo de l'organisation.
- **Domaine personnalisé** : accès via votre propre nom de domaine.

---

11. Conclusion

Face aux enjeux croissants de cybersécurité, d'indépendance et de conformité réglementaire, les organisations européennes ont besoin de solutions de transfert de fichiers qui offrent une sécurité supérieure et qui ne reposent pas uniquement sur des engagements contractuels.

Retyc apporte cette garantie en combinant :

- **Chiffrement de bout en bout** : vos fichiers sont illisibles sur nos serveurs, aujourd'hui et face aux menaces futures (schéma hybride intégrant des mécanismes résistants aux menaces quantiques connues à ce jour).
- **Architecture zero-knowledge** : sans clés de déchiffrement, nous ne pouvons pas accéder à vos contenus en clair.
- **Infrastructure exclusivement européenne** : hébergement en France sur des infrastructures européennes, avec une exposition directe très limitée aux législations extraterritoriales.
- **Transparence totale** : cryptographie open source auditable, documentation publique de nos pratiques, honnêteté sur les limites de notre architecture.

Retyc est développé et opéré par TripleStack SAS, société française indépendante. Notre mission est de fournir aux organisations et aux professionnels une alternative européenne, transparente et techniquement rigoureuse pour gérer leurs contenus sensibles.

Contact

TripleStack SAS - Retyc

- Site web : retyc.com
- Contact sécurité : voir `/.well-known/security.txt`
- Contact RGPD / DPO : privacy@retyc.net
- Contact commercial : via retyc.com/about/contact-us

Ce document est fourni à titre informatif. Les informations qu'il contient reflètent l'état de la plateforme au moment de sa rédaction. Retyc se réserve le droit de faire évoluer son architecture et ses fonctionnalités. La version en vigueur des politiques de confidentialité et des conditions d'utilisation est celle publiée sur retyc.com.

— TripleStack SAS, Avril 2026