



GED TECHNIQUE SOUVERAINE · CAO · BIM · SIG

# White Paper

---

La gestion documentaire technique, souveraine et sans compromis

Version 1.4 · Juillet 2026 · DIFFUSION CLIENT

## 1. Le problème

Les bureaux d'études, cabinets d'ingénierie et exploitants industriels manipulent quotidiennement des documents techniques — plans CAO, maquettes BIM, données SIG, nomenclatures, notes de calcul — dont la valeur et la sensibilité exigent bien plus qu'un simple partage de fichiers.

Les solutions en place échouent typiquement sur l'un de ces points :

- **Les serveurs de fichiers classiques** n'offrent ni versionnage fiable, ni verrouillage d'édition, ni traçabilité : deux dessinateurs écrasent mutuellement leur travail, les indices de révision se gèrent à la main dans les noms de fichiers.
- **Les GED bureautiques génériques** ignorent les spécificités des documents techniques : références croisées entre fichiers CAO (xrefs), cycles de vie par phases, volumes importants.
- **Les plateformes cloud SaaS** imposent l'externalisation des données chez un tiers, souvent hors du contrôle juridique du client — inacceptable pour de nombreux projets sensibles.
- **Les GED techniques historiques** reposent sur des architectures lourdes et vieillissantes, coûteuses à déployer et à maintenir.

## 2. La solution : Esovran

Esovran est une solution de gestion documentaire technique conçue pour les flux d'ingénierie, avec un principe fondateur : **les données du client restent chez le client**. La solution se déploie intégralement sur l'infrastructure Windows Server du client — jusqu'à l'annuaire d'identité et l'interface web — et chaque client dispose de sa propre instance dédiée : aucune infrastructure mutualisée ne traite ses données. Il n'y a **pas de plafond applicatif de volumétrie** : nombre de documents, volume total et taille des fichiers sont dimensionnés par l'infrastructure du client, pas par la licence.

### 2.1 Pour qui ?

PROFIL	CE QU'ESOVAN LUI APPORTE
<b>Manager de projet</b>	Vision du cycle de vie documentaire par phases (APS → APD → PRO → DCE → EXE → DOE), workflows de validation avec tampons et notifications, création de projets contrôlée, modèles d'arborescence, traçabilité complète des décisions
<b>Dessinateur / projeteur</b>	Check-out/check-in verrouillé (fini les écrasements), versionnage automatique, intégration native MicroStation / AutoCAD / BricsCAD, gestion des références croisées CAO, ouverture directe dans l'application native, travail hors-ligne jusqu'à 30 jours, cache local rapide
<b>DSI</b>	Déploiement 100 % on-premise en services Windows natifs (sans Docker), aucune télémétrie, chiffrement TLS 1.3, audit immuable, droits fins RBAC + ABAC, outil d'import en masse pour la reprise de l'existant

### 2.2 Deux modes de fonctionnement

Chaque espace documentaire (« datasource ») est créé dans l'un de deux modes, adapté au métier :

- **Mode Projet** — pour les études et projets de construction : les documents vivent au rythme des phases du projet (APS, APD, PRO, DCE, EXE, DOE) et de leurs workflows de validation.

- **Mode Usine** — pour les référentiels d'installations existantes (as-built) : consultation majoritairement en lecture, modifications encadrées par des **demandes de modification** (Change Requests) avec workflow d'approbation, puis réintégration au référentiel.

## 3. Fonctionnalités

### 3.1 Structuration et reprise de l'existant

- **Projets et arborescences** : arborescence de dossiers illimitée par projet (Mode Projet) ou par installation (Mode Usine) ; création de projets réservée aux administrateurs habilités.
- **Modèles d'arborescence** : des templates de structure de dossiers sont enregistrés au niveau de l'espace et appliqués à un nouveau projet en un clic — chaque projet démarre conforme au standard de l'entreprise.
- **Import en masse** : un outil de chargement batch reprend une arborescence de fichiers existante — classification automatique des documents, codification calculée, déduplication des doublons, exclusion des éléments obsolètes ; l'import est idempotent (relançable sans créer de doublons) et contrôle la cohérence avant toute écriture.
- **Modèles de documents** : des modèles réutilisables (classe, métadonnées par défaut, fichier de départ optionnel) permettent de créer un « nouveau document à partir d'un modèle » — une coquille pré-remplie et conforme, sur le même principe que les modèles d'arborescence.
- **Bundles de configuration** : schémas de métadonnées, règles de codification, classes de documents, modèles d'arborescence et workflows s'importent depuis des fichiers de configuration versionnables — la configuration d'un espace est reproductible d'un environnement à l'autre.

### 3.2 Maîtrise du cycle de vie documentaire

- **Check-out / check-in strict** : un document en cours d'édition est verrouillé ; chaque check-in crée automatiquement une nouvelle version horodatée et attribuée. Un « release » abandonne le verrou sans créer de version.
- **Ouvrir et modifier** : double-clic sur un document → check-out automatique → ouverture dans l'application native (Word, Excel, AutoCAD, MicroStation, BricsCAD...). L'utilisateur travaille comme sur un disque local, la GED gère le reste.
- **Édition optimiste** : un fichier modifié hors verrouillage (par exemple hors-ligne) est détecté automatiquement (empreinte SHA-256) et réconcilié : promotion en nouvelle version si aucun conflit, sinon arbitrage explicite par l'utilisateur. En cas de travail hors-ligne, l'utilisateur est averti s'il modifie un document non verrouillé.
- **Révisions et tampons** : les workflows de validation apposent des tampons (stamps) et gèrent les indices de révision.
- **Historique et restauration de versions** : chaque version passée est consultable et téléchargeable ; une version antérieure peut être **restaurée** (une nouvelle version réinstalle l'ancien contenu, l'historique reste intact).
- **Annotations (markups)** sur les documents, et **références entre documents** (un document peut en référencer d'autres — nomenclatures, plans liés, bibliothèques).

### 3.3 Métadonnées, codification et recherche

- **Métadonnées dynamiques** : schémas configurables par espace (champs, listes de valeurs, classes de documents).

- **Codification multiple par document** : un espace peut définir **plusieurs schémas de codification coexistants** (par exemple une codification « nomenclature / BOM » et une codification « fichiers de travail »), chacun rattaché aux classes de documents concernées. Un même document peut ainsi porter **plusieurs codes** simultanément — chaque code est composé automatiquement selon les règles du client (segments, compteurs, attributs métier), unique et vérifié à la création.
- **Recherche** : plein texte sur noms, métadonnées et contenu des fichiers (texte, tableurs, PDF), recherche partielle (fragments de code ou de nom), recherche avancée par métadonnées, recherches sauvegardées.
- **Extraction de données** : export de la liste de documents courante (dossier, sous-arbre projet ou résultat de recherche) au format **CSV / XLSX**, avec un jeu de colonnes de métadonnées choisi par l'utilisateur.

### 3.4 Workflows et collaboration

- Moteur de workflow **configurable par espace** (graphes d'états définis en configuration) : circuits type Brouillon → En révision → En validation → Validé → Diffusé, visas, approbations, avec rôles autorisés par transition.
- **Visibilité selon l'état** : la lisibilité d'un document suit son état de workflow — un brouillon reste visible de son auteur, un document en révision de ses relecteurs, un document validé ou diffusé d'un public large.
- **Annotations et commentaires** : fils d'annotations et de commentaires par version, pour la relecture et les visas.
- **Notifications et tâches** générées automatiquement par le moteur ; notifications e-mail avec **accusé de lecture**.
- **Diffusion contrôlée** : listes de diffusion par projet, transition « Diffuser » qui notifie automatiquement la liste, accusés de prise de connaissance internes et externes, et panneau « qui a pris connaissance ».
- **Abonnement à un document ou un dossier** : un « S'abonner » déclenche une notification (in-app, e-mail optionnel) à chaque changement pertinent — nouvelle version, métadonnées, workflow, ajout d'un élément enfant.
- **Rafraîchissement inter-utilisateurs** : lorsqu'un collègue modifie une ressource, les vues concernées (document ouvert, panneau des références, dossier courant) se réactualisent automatiquement.
- **Demandes de modification** (Mode Usine) avec workflow d'approbation et réintégration au référentiel.
- **Partage externe sécurisé** : un destinataire sans compte (ex. fournisseur) reçoit un lien signé et un code à usage unique par e-mail — accès en lecture limité au périmètre partagé (document ou dossier), avec expiration et révocation.
- **Envoi d'un document par e-mail** : depuis la GED, « Envoyer par e-mail » transmet un **lien de partage** (aperçu destinataire → code à usage unique → téléchargement) — jamais le fichier en pièce jointe.
- **Espace de dépôt pour partenaires** : sur autorisation, un intervenant externe peut **déposer** des fichiers dans un dossier partagé (contrôle de taille et de type, mise en quarantaine, audit).
- **Liens directs** entre membres : chaque document, dossier ou vue est adressable par URL.

### 3.5 Intégration CAO native

- **Add-in CAO (MicroStation CONNECT)** : la GED s'intègre nativement dans MicroStation — ouverture d'un document GED depuis la CAO (matérialisation automatique), création, enregistrement (check-in), fermeture (libération du verrou) pilotés depuis la session CAO. L'hôte de plugins du daemon est

**agnostique de l'application**, ce qui ouvre la voie aux autres plateformes CAO (AutoCAD, BricsCAD, Civil 3D) — voir §7.

- **Références croisées (xrefs) résolues par la GED** : à l'ouverture d'un fichier, les références attachées sont résolues, matérialisées localement et re-pointées automatiquement vers les bons fichiers — **sans modifier le fichier CAO** (remappage non persistant, vérifié).
- **Fichiers à leur emplacement naturel** : les documents sont présents sur le disque du poste à leur chemin d'origine — les xrefs des outils CAO fonctionnent sans reconfiguration.
- **Bibliothèques CAO** : un dossier « bibliothèque » désigné est synchronisé DMS → poste (copie locale en lecture seule, à un chemin stable par espace) pour que les chemins de recherche CAO (cellules, gabarits, fonds de plan) résolvent automatiquement.
- **Épinglage transitif** : épingler un document épingle automatiquement ses références (bibliothèques, fonds de plan).
- **Sécurité** : l'add-in ne détient jamais d'identifiants ; il consomme la session du daemon local via un jeton scopé, accordé par consentement explicite de l'utilisateur. L'architecture de plugins est ouverte aux autres outils (add-ins Office).

### 3.6 Travail hors-ligne et performance

- Le poste reste pleinement utilisable sans connexion **jusqu'à 30 jours** : consultation du cache, éditions locales, opérations mises en file. À la reconnexion, la synchronisation rejoue les opérations de façon fiable (idempotence garantie) et réconcilie les éventuels conflits.
- **Cache local intelligent** : les documents consultés restent disponibles localement (quota configurable, éviction automatique des moins utilisés), pour des ouvertures instantanées même sur de gros fichiers.
- **Aperçus visuels** : vignette de contenu par version et icône de type de fichier de l'OS (AutoCAD, MicroStation... lorsque l'application est installée) dans le panneau d'information, les listes et les « documents récents ».
- **Interface installable (PWA)** : la webapp s'installe comme une application de bureau depuis le navigateur.

### 3.7 Administration, audit et exploitation

- **Droits par rôle** : chaque membre reçoit un rôle par espace (owner / editor / reader), en refus par défaut ; le serveur ré-évalue chaque opération. Des contrôles contextuels s'ajoutent par surface (autorité de transition de workflow selon l'état, propriété du verrou de check-out, portée de partage et de plugin, isolation par espace).
- **Droits fins par ressource** : listes de contrôle d'accès (ACL) attribuables par **dossier**, par **document** et par **état de workflow**, façon permissions Windows — héritage (la ressource la plus proche l'emporte), propriétaire de ressource, droits séparés pour la gestion des permissions, et vues de provenance (« pourquoi ce droit »). Déploiement sans rupture : à l'activation, les accès restent identiques tant qu'aucune ACL n'est éditée.
- **Groupes d'utilisateurs** : des groupes nommés deviennent des **principaux de droits** à part entière — l'habilitation se gère par groupe plutôt qu'utilisateur par utilisateur.
- **Rétention et obsolescence** : politiques de conservation par espace / classe (revue par date d'ancrage), balayage planifié qui signale les documents dus et met au statut « Périmé », suppression encadrée (corbeille → délai de grâce → purge optionnelle du contenu), exclusion « legal hold » — le tout audité et ratifié par l'opérateur avant toute purge destructive.
- **Piste d'audit immuable** sur toutes les mutations ; historique complet des workflows.

- **CLI d'administration** : création d'espaces, import des bundles de configuration, gestion des rôles, enregistrement des modèles d'arborescence.
- **API documentée pour intégrateurs** : la surface loopback du daemon (plugin-host) est publiée en spécification **OpenAPI / Swagger**, avec guide d'intégration (consentement + jeton scopé, catalogue d'endpoints) et politique de stabilité de version.
- **Exploitation Windows native** : tous les services serveur s'installent en services Windows à démarrage automatique — supervision et sauvegarde avec les outils standard du client.
- **Archives et réversibilité** : archives ZIP documentées ( `.dmsarc` ), export complet d'espace ( `.dsexport` ).

## 4. Architecture : le poste comme point de confiance



### Le poste comme point de confiance

Les identifiants ne transitent jamais par le navigateur ni par la CAO — seul le daemon détient la session et dialogue avec le serveur.

Figure 1 — Topologie : le daemon local, unique intermédiaire entre le poste et le serveur.

- La **webapp** (interface web moderne, installable) ne détient aucun secret : elle n'accède aux données qu'à travers le daemon.
- L'**add-in CAO** suit la même règle : aucune donnée d'authentification dans l'application CAO (MicroStation, AutoCAD, BricsCAD).
- Le **daemon**, discret dans la zone de notification Windows, est le point de confiance unique du poste : c'est lui — et lui seul — qui détient la session et dialogue avec le serveur. Les identifiants ne transitent **jamais** par le navigateur ni par la CAO.
- Le **Filer**, sur le Windows Server du client, est la source de vérité : documents, versions, droits, workflows, audit.
- Le **Directory** assure l'annuaire des espaces et l'identité ; il se déploie sur le serveur du client (topologie 100 % on-premise) ou en service mutualisé.

Ce découpage apporte une propriété rare : la surface d'exposition réseau du serveur se limite aux postes internes (et, en option, au seul chemin de partage externe). Le détail figure dans le document « Architecture réseau ».

## 5. Sécurité et souveraineté

- **Données chez le client** : instance dédiée, déployable 100 % on-premise, sans plafond de volumétrie imposé.

- **Aucune télémétrie** : le daemon n'appelle aucun autre serveur que ceux configurés — cette garantie est vérifiée par des tests automatisés en continu. Aucun outil d'analytics tiers dans l'interface.
- **Chiffrement moderne** : TLS 1.3 exigé sur les flux réseau, secrets stockés dans le magasin Windows (DPAPI), mots de passe hachés en Argon2id.
- **Droits fins** : contrôle par rôle (owner / editor / reader par espace) en refus par défaut, renforcé par des contrôles contextuels appliqués par surface (autorité de transition de workflow, propriété du check-out, portée de partage et de plugin, isolation par espace) ; le serveur ré-évalue chaque opération. À la première version, ce modèle s'enrichit de **droits fins par ressource (ACL par dossier / document / état) et de groupes d'utilisateurs** — détaillé dans le « Dossier sécurité ».
- **Plugins sous contrôle** : chaque application tierce (add-in CAO) est autorisée explicitement par l'utilisateur — consentement par binaire (chemin + empreinte SHA-256), jetons scopés et révocables.
- **Clients enregistrés** : seules les applications explicitement autorisées peuvent dialoguer avec le daemon (jeton de capacité émis par le daemon, appairage du navigateur par consentement unique, add-in CAO par jeton scopé) — le tout révocable dans « Applications autorisées ».
- **Audit immuable** : chaque mutation est journalisée dans une piste d'audit non modifiable.
- **Formats ouverts** : archives ZIP documentées, exports complets — aucune captivité des données.

Le flux d'authentification illustre ce principe : les identifiants ne sont saisis que dans le daemon, qui échange des jetons à durée de vie courte avec l'annuaire d'identité puis le Filer — la webapp n'en voit jamais.

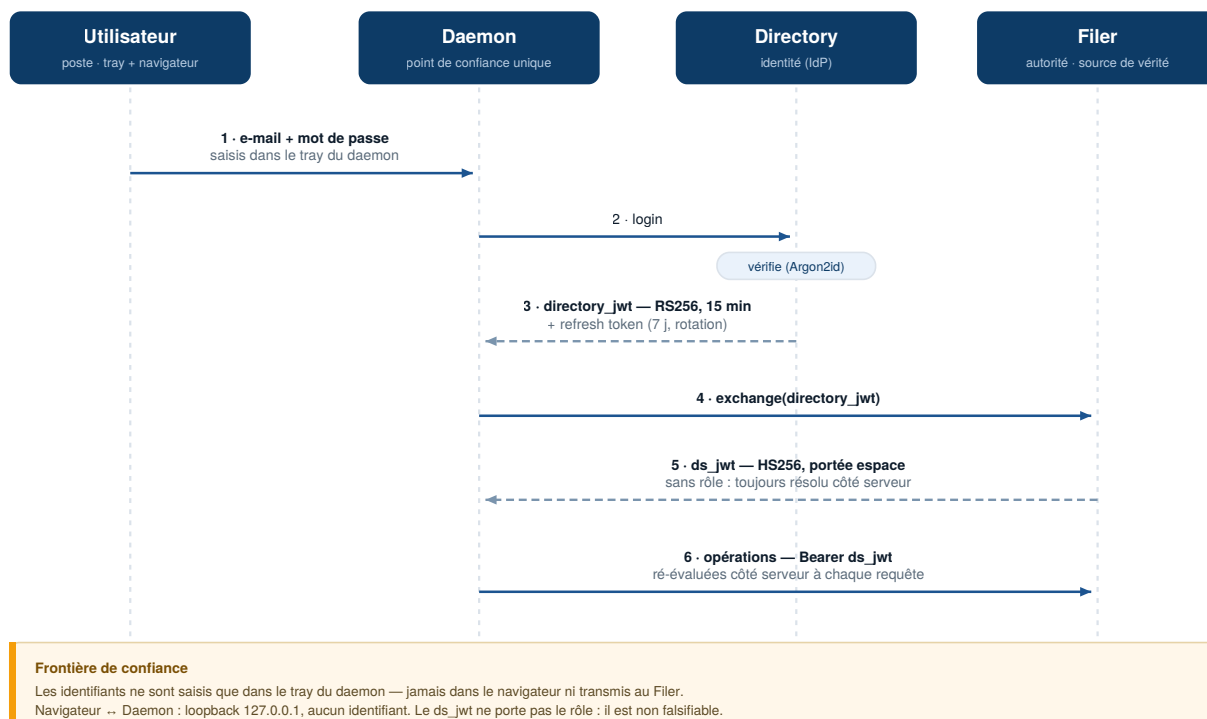


Figure 2 — Flux d'authentification et d'échange de jetons (identité globale → jeton d'espace).

Le détail complet figure dans le « Dossier sécurité ».

## 6. Une stack 2026-native

COMPOSANT	TECHNOLOGIES
Serveur (Filer, Directory)	.NET 10 (ASP.NET Core), PostgreSQL 16/17, services Windows natifs
Poste (daemon)	Tauri 2, .NET 10, SQLite (recherche FTS5)
Interface (webapp)	Vue 3, Quasar 2, PWA installable
Add-in CAO	.NET Framework 4.8, SDK natifs MicroStation CONNECT / AutoCAD / BricsCAD (cœur DmsCad.Core commun)

Frameworks récents et maintenus, builds reproductibles, architecture documentée en continu. Empreinte légère sur les postes (quelques centaines de Mo de RAM au plus).

## 7. Au-delà de la première version

**Rythme de livraison** : au moins une **release majeure par an**, et un **patch mensuel au maximum** pour les améliorations et corrections remontées par les clients.

Les axes suivants sont prévus **après** la première version :

HORIZON	AXE MAJEUR
<b>Après V1</b>	<b>CAO étendue</b> : add-ins AutoCAD, BricsCAD et Civil 3D (références DREF / data-shortcuts), sur l'hôte de plugins déjà agnostique de l'application
<b>Après V1</b>	<b>SSO d'entreprise</b> (Kerberos / Microsoft Entra ID) et interface d'administration web étendue
<b>2027</b>	<b>Indexation et recherche IA</b> : compréhension du contenu des documents techniques, recherche en langage naturel
<b>2028</b>	<b>Contrôle de conformité des dossiers</b> : vérification automatique contre les normes de l'industrie — référentiels standards et normes propres au client

Côté sécurité et conformité, une **certification ISO/IEC 27001** de l'éditeur est un objectif de feuille de route (voir « Dossier sécurité »).

## 8. En résumé

Esovrان réunit ce que les organisations d'ingénierie attendaient sans le trouver dans une seule solution : la rigueur documentaire d'une GED technique (verrouillage, versions, workflows, codification, audit), l'intégration native avec les outils CAO, le confort d'un outil moderne (interface web installable, cache local, hors-ligne, import en masse), et la souveraineté d'un déploiement 100 % on-premise sans télémétrie ni plafond de volumétrie.

**Vos documents. Votre serveur. Votre contrôle.**

*Pour aller plus loin : « Prérequis techniques », « Architecture réseau », « Dossier sécurité » — disponibles sur demande.*