

OPENINTEROP

OpenInterop : note de vision

Stefane Fermigier (Abilian SAS) · 30 octobre 2026 · DRAFT

Version 0.3
Licence CC BY 4.0

Genèse

OpenInterop est une initiative du CSF (comité stratégique de filière « Logiciels et solutions numériques de confiance ») qui concerne l'ensemble des acteurs de la filière des éditeurs de solutions et services numériques français (et, à terme, européen). Elle s'inscrit dans un cadre réglementaire et politique précis :

- Contrat de filière CSF (signé en avril 2025, 3 ministères)
- Circulaire Premier Ministre du 5 février 2026 (sur la commande publique numérique)
- Décisions de la réunion du 10 décembre 2025 concernant la Suite numérique de la DINUM : co-développement avec la filière au-delà du « cœur de suite », que la DINUM développe et opère elle-même. Ce cœur compte trois modules (Tchap, Visio, France Transfert), auxquels s'ajoutent Fichiers et Messagerie, en construction en 2026

L'initiative est hébergée par **OW2**, communauté de logiciels libres européenne, indépendante et à but non lucratif, qui garantit la neutralité et la pérennité open source de l'initiative.

Objectifs

L'initiative poursuit trois objectifs, par ordre croissant d'ambition :

1. **Spécifier** des standards d'interopérabilité et de réversibilité
2. **Documenter** ces standards et les bonnes pratiques associées
3. **Développer** des composants open source mutualisés : implémentations de référence, POC d'interopérabilité, suites de tests de conformité

Les deux propriétés clés visées sont :

- **Interopérabilité** : communication effective entre solutions distinctes (échanges de données, identité, workflows...)
- **Réversibilité** : capacité à migrer d'une solution à une autre sans perte de données ni de fonctionnalités

Les 6 domaines

L'initiative couvre 6 domaines sectoriels, chacun organisé en groupes de travail autonomes :

#	Domaine	Acteurs identifiés / pressentis
1	Outils collaboratifs	Abilian, EXO, Jalios, Jamespot, Netframe, XWiki...
2	Cloud	Fournisseurs de solutions cloud ; premier atelier le 9 octobre 2026, sur la réversibilité du stockage objet
3	Cybersécurité	Hexatrust (soutien et participation confirmés)
4	Outils métier	Éditeurs de solutions métier (à préciser)
5	Collectivités locales	Éditeurs de solutions pour collectivités (intérêt manifesté)
6	Santé	Éditeurs du secteur santé (à préciser)

Chaque domaine a ses propres enjeux d'interopérabilité et ses standards existants. Les groupes de travail avanceront à leur propre rythme selon la volonté et la capacité des participants.

Organisation et gouvernance

Échelle

L'initiative a vocation à rassembler **des dizaines, voire une centaine d'éditeurs**, coordonnés par le CSF et OW2. C'est une initiative de filière, pas un consortium fermé.

Groupes de travail

L'organisation repose sur des **groupes de travail par domaine** (et éventuellement par thématique transverse). Le principe fondateur : **avanceront ceux qui veulent avancer**. Aucun consensus minimal ne bloque un groupe : chacun progresse selon l'engagement de ses membres.

Parties prenantes

- **Éditeurs** : open source ou propriétaires, toute taille ; ils définissent et implémentent les standards
- **Institutions** : ministères, DINUM, ANCT ; cadre réglementaire et levier de la commande publique
- **Utilisateurs** : Cigref, TOSIT, entreprises privées, collectivités ; ils fournissent les **pain points** réels et valident l'utilité des travaux
- **Associations et communautés** : Hexatrust, OW2, ETSI ; structuration, hébergement, animation, méthodologie. ETSI opère à un niveau plus bas (protocoles, télécoms, IoT, eIDAS) mais reste un modèle méthodologique de référence et un partenaire potentiel sur les zones de chevauchement.

Approche technique

Principes directeurs

- **Ouverture** : standards ouverts, logiciels libres, APIs publiques
- **Cloud-agnostique** : portabilité garantie, pas de vendor lock-in
- **API-First** : interfaces programmatiques comme composantes primaires
- **Sécurité by design** : modèle Zero Trust, conformité RGPD/NIS2
- **Approche data-centric** : les données sont un actif partagé, pas un sous-produit enfermé dans les applications ; l'interopérabilité doit porter sur les données autant que sur les interfaces
- **Interopérabilité opposable** : objectif de long terme ; garantir réglementairement la souveraineté, la concurrence et la liberté de choix pour les utilisateurs, par des résultats mesurables plutôt que des déclarations d'intention

La [doctrine OpenInterop](#) précise ces principes : définitions, dix principes, règles d'application, dérogations, rôles et révision.

« *Interoperability [...] should be regarded as a thread running through the entire standards development process and not as an isolated issue to be fixed at the end.* » — ETSI, *Interoperability Best Practices*, 2011-2013.

Phase 1 : État de l'art

La priorité absolue est de **cartographier les standards existants** dans chaque domaine. Hors de question de réinventer la roue. Pour chaque besoin d'interopérabilité identifié, il s'agit de déterminer :

- Quels standards existent déjà (protocoles, formats, API) ?
- Lesquels sont déjà suffisants par rapport aux objectifs du projet ?
- Lesquels nécessitent des extensions ou des profils d'application ?
- Où sont les vrais trous, justifiant un travail de standardisation nouveau ?

Cf. la note d'[état de l'art](#) pour le détail.

Phase 2 : Spécification et implémentation

Chaque standard retenu ou créé reçoit :

- **Implémentation de référence** (si elle n'existe pas déjà)
- **POC d'interopérabilité** entre applications, en interopérabilité verticale (au sein d'un domaine) et horizontale (entre domaines)
- **Suite de tests de conformité (Compliance Test Kit)** : un standard sans modèle de conformité vérifiable est inutile. La méthodologie ETSI (proformas ICS/IFS, langage TTCN-3, événements Plug-tests™, recommandations EG 202 568 et ITU-T I.130) constitue un référentiel mature qu'OpenInterop peut adopter comme inspiration sans s'y inféoder.
- **Contrats sémantiques** : au-delà des API, spécifier les comportements attendus (ex. : comment un service de stockage doit réagir à une exportation massive)
- **Indicateur d'interopérabilité** : une mesure de la facilité de sortie et de transfert des données pour chaque solution, calculée à partir des rapports de conformité selon une méthode publique. L'atelier cloud du 9 octobre 2026 en a fixé la règle : des critères obligatoires sans compensation, les autres mesures publiées à part, aucune moyenne pondérée

Phase 3 : Structuration et influence

- **Livre blanc** sur les enjeux et la vision, incluant le concept d'interopérabilité opposable
- **Guides de bonnes pratiques** pour DSI et architectes (architectures cloud-agnostiques, patrons de portabilité)
- **Clauses types pour la commande publique** : modèles de clauses d'interopérabilité et de réversibilité intégrables dans les marchés publics ; une première proposition d'annexe contractuelle, pour le stockage objet, est prévue en décembre 2026
- **Influence européenne** : présentation des travaux à la Commission (DG CNECT), en coopération avec EuroStack, APELL, OpenForum Europe
- **Lobbying réglementaire** : porter auprès de l'ARCEP et de la DG CNECT une position pour que l'interopérabilité devienne un critère de conformité mesurable techniquement (type Data Act)
- **Hackathons d'interopérabilité** : faire collaborer industriels et fournisseurs pour valider des cas d'usage multi-cloud et multi-éditeurs ; un premier TechSprint, sur le stockage objet, a lieu en novembre 2026

- **Rencontres trimestrielles** de l'écosystème pour partager les avancées et recueillir les retours du terrain

Gouvernance technique

L'initiative s'appuie sur une **autorité technique**, appelée « Design Authority » dans le plan d'action cloud du CSF : une instance experte et indépendante des fournisseurs, qui valide les profils et les suites de tests, délivre les badges de conformité, accorde les dérogations et tranche les différends (cf. [doctrine](#), §7). Elle pourrait être constituée avec le laboratoire I4C (« Interoperability 4 Cloud », laboratoire commun de l'IMT et d'acteurs industriels de l'interopérabilité).

Dynamique écosystémique

Le modèle est celui d'une **coopétition structurée** : des éditeurs concurrents collaborent sur la couche d'interopérabilité (pré-compétitive) tout en se différenciant sur leurs fonctionnalités propres.

Le levier principal est la **commande publique** : en inscrivant l'interopérabilité et la réversibilité comme critères dans les marchés, les institutions créent une incitation forte pour l'ensemble de la filière.

L'enjeu de **souveraineté numérique** est structurant : l'interopérabilité est le moyen de constituer des alternatives crédibles et complètes face aux suites intégrées en position dominante, en permettant de composer une offre modulaire à partir de briques souveraines.

Cadre réglementaire et références

L'initiative s'appuie sur un cadre réglementaire européen et français de plus en plus favorable :

- **Data Act** (règlement (UE) 2023/2854, en vigueur depuis le 11 janvier 2024, applicable depuis le 12 septembre 2025) : portabilité des données, interopérabilité, changement de fournisseur de cloud (chapitre VI), avec suppression des frais de changement au 12 janvier 2027
- **Interoperable Europe Act** : cadre européen d'interopérabilité des services publics
- **Circulaire PM du 5 février 2026** : commande publique numérique
- **European Interoperability Framework (EIF)** : principes et standards pour les services publics européens ; une proposition de cadre technique (EIF-TS, projet de l'auteur) le décline en 7 profils d'interopérabilité concrets
- **Cyber Resilience Act / NIS2** : exigences de SBOM, notification d'incidents, sécurité de la supply chain
- **AI Act** : exigences de transparence pour les systèmes d'IA
- **eIDAS 2.0** : portefeuille d'identité numérique européen (EUDI Wallet)
- **Arrêt CJUE Alphabet e.a. (C-233/23, 25 février 2025)** : une entreprise dominante qui n'assure pas l'interopérabilité de sa plateforme avec l'application d'un tiers peut abuser de sa position ; seuls la justifie une impossibilité technique ou un risque pour l'intégrité ou la sécurité de la plateforme

Cadre français :

- **RGI v2.0** (référentiel général d'interopérabilité) : approuvé par arrêté du 20 avril 2016, jamais mis à jour depuis, jugé « en friche » par le CNLL. Une commission d'enquête de l'Assemblée nationale propose de l'actualiser et de le rendre obligatoire dans les marchés (rapport n° 3054, juillet 2026, proposition n° 12)
- **LCEN (2004)** : définition du standard ouvert (article 4), que la doctrine retient avec celle de l'EIF 2004

Références complémentaires :

- Position du CNLL sur l'interopérabilité cloud
- Travaux de la Fondation EuroStack, APELL, OpenForum Europe
- Réponses CNLL et Euclidia à la consultation ARCEP
- Étude OPIIEC sur l'interopérabilité
- Stefane Fermigier, « *L'interopérabilité, clé de l'efficacité collaborative et de la souveraineté* », Abilian, novembre 2025 : note de positionnement sur l'interopérabilité opposable. <https://abilian.com/fr/news/interopabilite-efficacite-collaborative-souverainete/>
- ETSI, *Interoperability Best Practices*, 2011-2013 : brochure méthodologique du Centre for Testing and Interoperability (sponsorisée par la Commission européenne).
- ETSI White Paper n° 3, *Achieving Technical Interoperability: the ETSI Approach*.
- Définition EIFv1 (2004) des normes ouvertes : spécifications publiées, librement accessibles, sans restrictions juridiques, opérationnelles ou financières, relevant d'une gouvernance indépendante et transparente ; à privilégier sur la définition affaiblie de l'EIFv2 (2010)

Concept clé : l'interopérabilité opposable

L'interopérabilité opposable est un concept central de l'initiative. Elle se distingue d'une simple recommandation de standards par :

- **Des résultats mesurables** plutôt que des déclarations de conformité : la portabilité et l'interopérabilité doivent fonctionner effectivement ; le support nominal d'un standard ne suffit pas.
- **Des mécanismes d'exigibilité** : APIs obligatoires pour l'exportation en format ouvert, tests de conformité vérifiables, recours en cas de non-conformité, sanctions dissuasives.
- **Un arbitrage technique** : possibilité de recourir à un tiers pour trancher les litiges techniques d'interopérabilité.
- **Une approche pragmatique** : on ne prescrit pas une technologie spécifique, on exige un résultat (la portabilité, l'échange de données) et on vérifie qu'il est atteint.

Ce concept est aligné avec la définition stricte de l'EIFv1 (2004) et avec les principes du Data Act. Il s'oppose à la « conformité apparente » : des implémentations partielles qui affichent le support d'un standard tout en maintenant un verrouillage effectif.

L'atelier cloud du 9 octobre 2026 a précisé la portée du concept. Un kit de test apporte une preuve technique ; son usage dans un contrat suppose une rédaction propre, qui fixe le périmètre, la mesure, les conditions de test et les conséquences d'un écart. La [doctrine](#) (principe 1 et section 5) en tire les règles de preuve.

Les 5 niveaux d'interopérabilité

Niveau	Focus	Exemple
Technique	Connectivité matérielle et logicielle	TLS, HTTP, IP
Syntactique	Structure et format des données	JSON, XML, ODF
Sémantique	Signification univoque des données	Schémas partagés, vocabulaires
Organisationnelle	Alignement des processus métier	Workflows inter-organisations
Juridique	Cadres légaux et contractuels	Licences, CGU, RGPD

OpenInterop doit couvrir les 5 niveaux, pas seulement le technique.

Documents OpenInterop

Cette note de vision est le document d'entrée du corpus OpenInterop. Elle est complétée par :

- [État de l'art des standards d'interopérabilité](#) (cartographie transversale et sectorielle des standards existants)
- [Fiche transverse](#) (chantiers T1-T6 : identité, APIs, schémas, notifications, portail, EUDI Wallet)
- [Fiche collaboratif](#) (chantiers C1-C7, dont fédération OCM / CS3 et recherche fédérée)
- [Fiche cloud](#) (chantiers CL1-CL5 autour de SECA, observabilité, secrets, indicateur d'interopérabilité)
- [Fiche cybersécurité](#) (chantiers CS1-CS5 autour d'OCSF, Sigma, SBOM, CACAO, OWASP CRS)
- [Doctrine](#) (définitions, principes, règles de preuve, rôles)
- **Atelier cloud du 9 octobre 2026** : réversibilité du stockage objet (position, contrats comportementaux, scorecard, scénarios de test, compte rendu, kit de test S4), résumé dans la [fiche cloud](#), §1.4

Trois fiches restent à produire (outils métier, collectivités locales, santé), en lien avec les acteurs de ces domaines.