

Doctrine OpenInterop : l'interopérabilité vérifiable

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

Version 0.1

Licence CC BY 4.0

Note préalable (*hors doctrine*). Ce texte est proposé à la discussion du groupe de travail OpenInterop, à côté du projet « Éléments de base pour la constitution de la doctrine OpenInterop » du 29 octobre 2026. Ce projet traite surtout de deux questions : la répartition des rôles entre l'État et les entreprises, la place du logiciel libre dans les achats publics. Elles constituent un sujet à part entière, en grande partie indépendant d'OpenInterop, et ne fixent ni les livrables de l'initiative ni les critères de sa réussite. Le présent texte part de l'objet que l'appel fondateur lui a fixé : « spécifier, documenter et éventuellement développer des composants standards open source pour garantir l'interopérabilité entre les outils informatiques », au service des « utilisateurs publics et privés ». Il en tire des définitions, des principes, des règles d'application et des rôles. Les deux annexes, qui décrivent l'état de l'art et les premiers chantiers, reprennent des notes rédigées depuis avril 2026 ; elles seront mises à jour plus souvent que la doctrine elle-même.

1. Objet et champ d'application

1.1. La présente doctrine fixe les principes qui guident les travaux d'OpenInterop et l'usage de leurs résultats. Elle sert à décider de l'ouverture d'un chantier, du contenu d'un livrable, de la preuve d'interopérabilité recevable et de l'instance qui tranche en cas de désaccord.

1.2. Elle s'applique aux six domaines de l'initiative (outils collaboratifs, cloud, cybersécurité, outils métier, collectivités locales, santé) et aux standards transverses qui leur sont communs (identité, API, formats, sémantique).

1.3. Elle s'applique à tous les participants : éditeurs, quelle que soit la licence de leurs produits, hébergeurs, intégrateurs, utilisateurs publics et privés, institutions et associations. Elle s'applique de la même façon aux solutions publiques et privées.

1.4. Elle traite de l'interopérabilité et de la réversibilité. La politique d'achat des organisations, le choix de licence des produits et la répartition des rôles entre l'État et le secteur privé relèvent d'autres cadres. La doctrine ne les tranche pas. Elle reste compatible avec les règles qui les encadrent, y compris la priorité au logiciel libre que la loi pose dans l'enseignement supérieur depuis 2013 et l'encouragement que demande l'article 16 de la loi pour une République numérique.

2. Définitions

- **Interopérabilité** : capacité de solutions distinctes, issues de fournisseurs indépendants, à échanger des données et à les utiliser, à coopérer dans un même processus et à partager une identité commune. Elle se joue à cinq niveaux : technique (connectivité), syntaxique (formats), sémantique (signification des données), organisationnel (processus) et juridique (licences, conditions d'utilisation, protection des données).
- **Réversibilité** : capacité d'un client à quitter une solution pour une autre, dans des délais et à des coûts maîtrisés, en récupérant ses données, leurs métadonnées et leur structure dans un état directement utilisable par la solution d'arrivée.
- **Standard ouvert** : spécification publiée, librement accessible, sans restriction juridique ni financière à son usage, qui permet des mises en œuvre concurrentes et relève d'une gouvernance indépendante et transparente. Cette définition reprend celle du Cadre européen d'interopérabilité de 2004 ; elle est conforme à l'article 4 de la loi pour la confiance dans l'économie numérique (LCEN), selon lequel les spécifications techniques d'un standard ouvert sont « publiques et sans restriction d'accès ni de mise en œuvre ».
- **Profil d'application** : document qui précise, pour un usage donné, les standards retenus, les options et les extensions obligatoires, ainsi que les comportements attendus.
- **Contrat sémantique** : description des comportements qu'une solution garantit au-delà de la forme de ses interfaces, par exemple la réaction d'un service de stockage à un export massif.
- **Implémentation de référence** : logiciel qui met en œuvre un profil, publié sous licence libre, qui enlève les ambiguïtés et sert d'étalon aux autres mises en œuvre.
- **Suite de tests de conformité** : ensemble versionné de scénarios, de jeux de données et de verdicts, publié sous licence libre, qui vérifie qu'une mise en œuvre respecte un profil.
- **Déclaration de conformité** : document par lequel un fournisseur indique le profil, la version et les fonctions qu'il revendique, selon un modèle commun inspiré des déclarations ICS et IFS de l'ETSI.
- **Rapport de conformité** : résultat d'une exécution de la suite de tests sur une solution, assez complet pour que l'exécution puisse être reproduite par un tiers.

3. Fondements

3.1. La souveraineté passe par la composition. La dépendance des organisations françaises et européennes aux grandes plateformes extra-européennes tient d'abord à l'intégration de leurs offres : une suite dont les éléments ne communiquent bien qu'entre eux rend coûteux le remplacement de chacun. L'offre européenne réunit des milliers d'éditeurs, d'hébergeurs et d'intégrateurs, le plus souvent des PME, dont chacun excelle sur une partie du besoin. L'interopérabilité leur permet de composer une offre complète que le client assemble et dont il remplace chaque élément sans toucher aux autres. Elle conditionne l'existence d'une offre européenne à l'échelle des besoins, dans le secteur public comme dans le secteur privé.

3.2. L'interopérabilité sert la concurrence. Le droit européen l'a reconnu à plusieurs reprises. Le Data Act impose aux fournisseurs de services de traitement de données de faciliter le changement de fournisseur. Le règlement sur les marchés numériques impose des obligations d'interopérabilité aux contrôleurs d'accès. La Cour de justice a jugé, dans l'arrêt *Alphabet e.a.* (C-233/23), qu'une entreprise dominante qui n'assure pas l'interopérabilité de sa plateforme avec l'application d'un tiers peut abuser de sa position, faute de justification objective.

3.3. Les déclarations ne suffisent pas. Un fournisseur peut annoncer qu'il « supporte » un standard tout en n'en mettant en œuvre qu'une partie, ou en ajoutant des extensions qui recréent l'enfermement. Cette

conformité apparente est le principal obstacle que rencontrent les acheteurs. Seuls des tests reproductibles permettent de la distinguer d'une interopérabilité réelle.

3.4. Le logiciel libre renforce l'interopérabilité et la réversibilité. L'accès au code rend visibles les formats et les comportements ; des tiers peuvent s'y connecter sans dépendre de la documentation que l'éditeur choisit de publier. Le client d'un logiciel libre qui entre en conflit avec son fournisseur peut reprendre le code et le faire maintenir par un autre prestataire. Une implémentation de référence et une suite de tests libres permettent enfin à chaque éditeur, à chaque acheteur et à chaque arbitre de vérifier la conformité dans les mêmes conditions.

4. Principes

Principe 1. L'interopérabilité se prouve par un résultat. Une solution est interopérable avec un profil si un rapport de conformité reproductible l'établit, sur le périmètre qu'elle revendique. Une déclaration « compatible » sans périmètre ni rapport n'a pas de valeur au regard de la doctrine. OpenInterop exige un résultat (échanger, exporter, migrer) et ne prescrit aucune technologie au-delà des standards retenus.

Principe 2. Seuls des standards ouverts sont retenus. Les profils d'OpenInterop ne s'appuient que sur des standards ouverts au sens de la section 2. Les conditions dites « équitables, raisonnables et non discriminatoires » (FRAND) admettent des redevances de brevet et peuvent interdire la mise en œuvre sous licence libre ; elles ne satisfont pas cette définition.

Principe 3. L'existant d'abord. Tout chantier part d'un état de l'art. OpenInterop adopte un standard existant quand il suffit, en définit un profil quand il laisse trop d'options, l'étend quand il présente un manque et ne crée un standard nouveau que sur un manque avéré. Il retient de préférence les standards déjà gouvernés par une organisation internationale ou européenne reconnue.

Principe 4. Tout livrable est complet. Un profil d'OpenInterop est publié avec une implémentation de référence libre, quand il n'en existe pas déjà une, une suite de tests de conformité libre et un modèle de déclaration de conformité. Un profil sans suite de tests reste un projet.

Principe 5. Les cinq niveaux sont couverts. Un profil traite les niveaux d'interopérabilité que son usage mobilise, sans se limiter au niveau technique. Il décrit les comportements attendus par des contrats sémantiques.

Principe 6. Les données restent exploitables hors de la solution. Toute solution conforme permet l'export complet des données qu'elle gère, avec leurs métadonnées, dans un format ouvert et selon un schéma documenté, par une interface programmable. La réversibilité concerne les données autant que les fonctions.

Principe 7. Les profils sont ouverts à toutes les mises en œuvre. Toute solution peut mettre en œuvre un profil et faire établir sa conformité, quels que soient son éditeur, sa licence et son statut public ou privé. Les livrables d'OpenInterop (spécifications, implémentations de référence, suites de tests) sont, eux, publiés sous licence libre ou ouverte.

Principe 8. Les mêmes exigences valent pour toutes les solutions. Une plateforme développée ou opérée par une administration est évaluée selon les mêmes profils et les mêmes tests qu'une offre privée. Aucune solution, publique ou privée, ne doit devenir un point de passage obligé.

Principe 9. Les travaux sont publics. Spécifications, suites de tests, rapports d'essais croisés et comptes rendus sont publiés. Les contributions et les conflits d'intérêts des participants sont déclarés.

Principe 10. Les travaux s'inscrivent dans le cadre public. Les profils qui concernent les systèmes d'information publics sont conçus pour pouvoir être versés au référentiel général d'interopérabilité (RGI). Tous les profils s'alignent sur le Cadre européen d'interopérabilité et sur les règlements européens applicables (Interoperable Europe Act, Data Act).

5. Application

5.1. Ouvrir un chantier. Un groupe de travail ouvre un chantier lorsque quatre conditions sont réunies. Des utilisateurs ont documenté le besoin. L'état de l'art confirme le manque ou l'absence de profil. Au moins deux participants indépendants s'engagent à mettre en œuvre le résultat. Ce résultat peut être vérifié par des tests. Les chantiers d'identité et de conventions d'API, dont dépendent les autres, sont traités en priorité.

5.2. Établir la conformité. La preuve de conformité comprend une déclaration de conformité et un rapport de conformité. Le rapport identifie le service et sa version, les fonctions évaluées, le profil et la version de la suite de tests, le jeu de données et les conditions d'exécution, les résultats, les écarts et les limites, ainsi que les éléments permettant de reproduire le test. Ce format reprend celui que l'atelier OpenInterop du 9 octobre 2026 a proposé pour la réversibilité du stockage objet. Un profil distingue des critères obligatoires et des mesures : la conformité exige que tous les critères obligatoires du périmètre revendiqué soient satisfaits, sans compensation entre critères ; les mesures sont publiées à part, avec leurs conditions. Aucune moyenne pondérée ne fonde un verdict de conformité.

5.3. Qui établit la preuve. La doctrine reconnaît trois niveaux de preuve.

- **l'autoévaluation** : le fournisseur exécute la suite de tests et publie son rapport ;
- **la vérification** : un acheteur ou un tiers reproduit l'exécution à partir des éléments du rapport ;
- **l'essai croisé** : plusieurs solutions sont testées ensemble lors d'une session organisée par OpenInterop, sur le modèle des *Plugtests* de l'ETSI ; seul ce niveau ouvre droit au badge de conformité délivré par l'autorité technique.

5.4. Mesurer. OpenInterop publie, pour chaque solution évaluée, un indicateur d'interopérabilité calculé à partir des rapports de conformité. L'indicateur mesure la facilité de sortie et de transfert des données ; sa méthode de calcul est publique.

5.5. Trancher un différend. Un différend sur l'interprétation d'un profil ou sur un résultat de test est porté devant l'autorité technique. Elle statue par une décision motivée et publiée ; si le différend révèle une ambiguïté du profil, celui-ci est corrigé dans sa version suivante.

5.6. Usage par les acheteurs. OpenInterop publie des clauses types d'interopérabilité et de réversibilité. Elles permettent à un acheteur, public ou privé, d'exiger une déclaration et un rapport de conformité sur un périmètre défini, puis de faire vérifier le rapport.

6. Dérogations

6.1. Un profil peut s'appuyer sur un standard qui ne satisfait pas la définition du standard ouvert lorsqu'aucune alternative ouverte n'existe pour l'usage visé, en particulier pour la compatibilité avec des systèmes existants. La dérogation est signalée dans le profil, motivée et limitée dans le temps ; le groupe de travail indique comment en sortir.

6.2. Une exigence de sécurité peut justifier qu'un profil restreigne une fonction d'interopérabilité. La restriction est motivée, proportionnée et documentée ; la sécurité ne peut pas servir de prétexte à fermer une interface.

6.3. Les dérogations sont accordées par l'autorité technique, sur proposition du groupe de travail concerné. Elles sont publiées. Chaque révision du profil les réexamine.

7. Rôles

- **Le Comité stratégique de filière** pilote l'initiative et en assure la représentation auprès des pouvoirs publics.
- **OW2**, communauté européenne de logiciels libres indépendante et à but non lucratif, héberge l'initiative, ses dépôts et ses outils ; elle garantit la pérennité de ses livrables.
- **Les groupes de travail**, organisés par domaine et pour les standards transverses, sont ouverts à tout participant. Chacun avance au rythme de ses membres : ceux qui veulent avancer avancent, sans attendre le consensus de tous. Ils proposent les chantiers, rédigent les profils, développent les implémentations de référence et les suites de tests.
- **L'autorité technique**, instance experte et indépendante des fournisseurs, valide les profils et les suites de tests, délivre les badges de conformité, accorde les dérogations et tranche les différends. Elle pourrait être constituée avec le laboratoire commun I4C (*Interoperability 4 Cloud*) de l'IMT et de partenaires industriels.
- **Les utilisateurs**, publics et privés, documentent les besoins, participent aux essais et vérifient l'utilité des livrables.
- **L'État** reste seul compétent pour les normes qui s'imposent aux systèmes d'information publics. OpenInterop met ses profils à sa disposition pour la mise à jour du RGI, que la commission d'enquête de l'Assemblée nationale sur les dépendances structurelles dans le numérique propose ensuite de rendre obligatoire dans les marchés (rapport n° 3054, juillet 2026, proposition n° 12). Pour ces normes, la concertation au sein d'OpenInterop éclaire la décision de l'État, à qui elle revient.

8. Révision

8.1. La doctrine est réexaminée au moins une fois par an, ou à la demande d'un groupe de travail ou de l'autorité technique.

8.2. Tout projet de révision est soumis aux participants pendant une période de consultation d'au moins un mois. La version adoptée est datée, numérotée et publiée avec la liste des modifications et les réponses aux principales observations.

8.3. Les annexes sont mises à jour par les groupes de travail au fil des travaux, sans révision de la doctrine.

Annexe A. État de l'art : synthèse

Le recensement mené par domaine (note d'état de l'art, v0.3) montre que l'essentiel des fondations existe :

- **standards suffisants**, à adopter tels quels : OpenID Connect, OAuth et SCIM pour l'identité ; OpenAPI pour la description des API ; OCI pour les conteneurs ; ODF et PDF pour les documents ; FHIR pour la santé ; Factur-X et EN 16931 pour la facturation ; TLS 1.3 pour le transport ;
- **standards mûrs mais peu adoptés en France**, à promouvoir : SCIM pour la synchronisation des annuaires, CalDAV et CardDAV pour les agendas et les contacts, Matrix pour la messagerie, OpenTe-

lemetry pour l'observabilité, SPDX et CycloneDX pour la nomenclature logicielle, CloudEvents pour les notifications, OCSF et Sigma pour la sécurité ;

- **manques avérés**, qui justifient des chantiers : une API commune de gestion d'infrastructure cloud, la portabilité des services managés, des schémas de données partagés pour les entités transverses (utilisateur, document, événement), des contrats sémantiques et un indicateur d'interopérabilité.

Annexe B. Premiers chantiers

Cette liste reprend les fiches de domaine rédigées en avril 2026 et révisées le 30 octobre 2026 ; les fiches font foi.

Domaine	Besoin	Chantier	Résultat vérifiable
Transverse	Les comptes se créent et se suppriment à la main dans chaque outil	Profil commun OpenID Connect et SCIM	Suite de tests, badge de conformité
Transverse	Chaque éditeur a ses propres conventions d'API	Guide de style REST, description OpenAPI obligatoire, schémas de données partagés	Valideur automatique, catalogue d'API
Outils collaboratifs	Partager un fichier ou un agenda entre deux suites	Fédération de fichiers (OCM, CS3 APIs), CalDAV et CardDAV, passerelle Matrix ; un profil par sous-domaine	Essais croisés entre éditeurs
Outils collaboratifs	Quitter une suite sans perdre ses données	Format de réversibilité pour l'export et l'import	Migration réussie entre deux solutions
Cloud	Changer de fournisseur de stockage objet	Profil de réversibilité du stockage objet (atelier du 9 octobre 2026)	Six scénarios de test, dont un à affiner ; rapport reproductible
Cloud	Chaque fournisseur a sa propre API d'infrastructure	Adoption et extension de SECA ; standards de journaux et de gestion des secrets	Indicateur d'interopérabilité cloud
Cybersécurité	Les alertes et les journaux ne circulent pas entre outils	OCSF, Sigma, playbooks CACAO, nomenclatures logicielles	Règles et journaux échangés entre produits
Santé, collectivités, outils métier	Formats d'échange propres à chaque éditeur	Fiches à établir avec les acteurs de ces domaines	À définir par chaque groupe

Références

- Appel fondateur OpenInterop (CSF), et note de vision OpenInterop, v0.3, octobre 2026.
- État de l'art des standards d'interopérabilité, v0.3, octobre 2026 ; [fiche transverse](#), [fiche collaboratif](#), [fiche cloud](#) et [fiche cybersécurité](#).
- Atelier OpenInterop du 9 octobre 2026, réversibilité du stockage objet : déroulé et compte rendu.
- Projet « Éléments de base pour la constitution de la doctrine OpenInterop », 29 octobre 2026.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 4.

- Ordonnance n° 2005-1516 du 8 décembre 2005 ; RGI version 2.0, approuvé par arrêté du 20 avril 2016.
- Assemblée nationale, rapport n° 3054 de la commission d'enquête sur les dépendances structurelles et les vulnérabilités systémiques dans le secteur du numérique, juillet 2026.
- Commission européenne, *European Interoperability Framework*, version 1.0 (2004) ; règlement (UE) 2024/903 (Interoperable Europe Act) ; règlement (UE) 2023/2854 (Data Act) ; règlement (UE) 2022/1925 (Digital Markets Act).
- CJUE, 25 février 2025, *Alphabet e.a.*, C-233/23.
- ETSI, *Interoperability Best Practices* ; ETSI White Paper n° 3, *Achieving Technical Interoperability: the ETSI Approach*.
- Stefane Fermigier, « L'interopérabilité, clé de l'efficacité collaborative et de la souveraineté », Abilian, novembre 2025 : <https://abilian.com/fr/news/interopabilite-efficacite-collaborative-souverainete/>