

Fiche détaillée : standards transverses

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

Version 0.3
Licence CC BY 4.0

Les standards transverses sont les fondations sur lesquelles reposent tous les domaines d'OpenInterop (collaboratif, cloud, cybersécurité, outils métier, collectivités, santé). Ils couvrent l'identité, les APIs, les formats de données, les documents et la sémantique. Un travail sur ces couches bénéficie à tous les groupes de travail. Les définitions (profil d'application, suite de tests de conformité, déclaration et rapport de conformité) et les règles de preuve employées ici sont celles de la doctrine OpenInterop ([doctrine](#)).

1. État de l'art : adoption FR et manques identifiés

Le **panorama complet** des standards transverses (fonctions, maturité, références) figure dans l'[état de l'art](#), §1. Cette fiche se concentre sur leur **adoption dans la filière française** et les **manques** qui en font des chantiers candidats pour OpenInterop.

1.1 Identité, authentification et autorisation

C'est la couche la plus mature et la plus structurante. Sans identité interopérable, aucune autre interopérabilité n'est possible.

Pour le détail des standards (OIDC, OAuth 2.0 et le projet OAuth 2.1, SAML 2.0, SCIM 2.0, WebAuthn, LDAP, eIDAS 2.0/ARF, OpenID4VP, Verifiable Credentials, DID), cf. l'[état de l'art](#), §1.1.

Standard	Statut FR	Manque identifié
OIDC + OAuth 2.0 (OAuth 2.1 en projet)	Bon (FranceConnect, ProConnect)	Identité professionnelle inter-organisations encore artisanale. OAuth 2.1 reste un Internet-Draft de l'IETF : toute exigence formelle s'appuie pour l'instant sur OAuth 2.0 et la RFC 9700 (BCP 240)
SCIM 2.0	Faible	Maillon manquant critique : provisioning et deprovisioning manuels entre éditeurs
SAML 2.0	Très répandu dans l'existant (éducation, santé, administration)	Compatibilité legacy à maintenir

Standard	Statut FR	Manque identifié
WebAuthn	En croissance (passkeys) ; Level 3 est une Recommandation W3C depuis août 2026	Adoption inégale
eIDAS 2.0 / EUDI Wallet	En cours de déploiement : chaque État membre doit proposer un portefeuille avant le 24 décembre 2026	Outillage open source insuffisant pour les PME

Initiatives françaises et européennes :

- **FranceConnect** authentifie les citoyens (OIDC). L'identité professionnelle et le provisioning sortent de son périmètre.
- **ProConnect** (DINUM) a absorbé AgentConnect en 2024 : un même service OIDC fédère l'identité des agents publics et celle des professionnels du secteur privé. Il ne traite pas le provisioning des comptes.
- **France Identité** (ministère de l'Intérieur), adossée à la carte nationale d'identité électronique, sert de base au portefeuille EUDI français. Le règlement eIDAS 2 fixe l'échéance à la fin de 2026 ; la DINUM annonce une disponibilité dans le courant de 2027.
- **IPSIE** (*Interoperability Profiling for Secure Identity in the Enterprise*), groupe de travail de l'OpenID Foundation créé en octobre 2024, rédige des profils d'OIDC, d'OAuth et de SCIM pour l'identité en entreprise ; son profil SCIM 2.0 est encore à l'état de projet. Ces travaux sont le point de départ du chantier T1 (cf. [doctrine](#), principe 3).
- **EuroID Connect** (européen) vise à fournir les outils open source manquants pour eIDAS 2.0 : stacks turnkey émetteurs/vérificateurs, SDKs OpenID4VP, bibliothèques SCIM pour provisioning consenti, identifiants pseudonymisés par défaut. Le cadre réglementaire EUDIW définit le *quoi* sans dire le *comment* ; EuroID Connect veut combler ce manque.

Constat : le socle est solide. Les verrous français sont l'absence de profil commun d'implémentation SCIM, la fragmentation des mises en œuvre du portefeuille EUDI et l'absence de fédération inter-organisations généralisée. L'approche **data-centric** de l'identité (l'utilisateur contrôle ses données, divulgation sélective) reste rare dans la pratique courante.

1.2 APIs et communication inter-services

Le panorama complet figure dans l'[état de l'art](#), §1.2 (OpenAPI, REST, GraphQL, AsyncAPI, JSON:API, HAL, OData, AMQP, MQTT, WebSocket, webhooks) et §3.4 (CloudEvents).

Standard	Statut FR	Manque identifié
OpenAPI 3.1 / 3.2	Bon (exigé par DINUM pour api.gouv.fr) ; la version 3.2 est publiée depuis septembre 2025	Spécifications publiques souvent incomplètes ou non maintenues côté éditeurs
AsyncAPI 3.x	Très faible	Quasi-inconnu alors que les architectures événementielles se multiplient
Conventions REST (JSON:API, HAL...)	Faible	Pas de convention commune entre éditeurs (pagination, filtrage, erreurs, versioning)
CloudEvents	Faible	Pas de profil partagé pour les notifications inter-applications

Standard	Statut FR	Manque identifié
Webhooks	De fait	Aucun standard formel : chaque éditeur a son propre format

Constat : OpenAPI + REST est le socle adopté, mais sans **convention commune de filière** chaque intégration de N éditeurs reste un travail spécifique. AsyncAPI et CloudEvents sont des opportunités sous-exploitées.

1.3 Formats de données

Le panorama complet figure dans [l'état de l'art](#), §1.3 (JSON, JSON Schema, JSON-LD, XML/XSD, CSV, Avro, Parquet, Protobuf, UTF-8).

Standard	Statut FR	Manque identifié
JSON + JSON Schema	Universelle ; JSON Schema en croissance (schema.data.gouv.fr)	Pas de schémas partagés entre éditeurs pour les concepts métier communs
XML + XSD	Forte dans l'existant (administration, santé)	Legacy à maintenir
CSV	Très répandu	Souvent mal formé (séparateurs, encodages, en-têtes)
JSON-LD	Faible hors open data	Sous-exploité pour les données liées en entreprise

Constat : le problème tient à l'absence de **schémas partagés** : chaque éditeur modélise les mêmes concepts (utilisateur, document, événement, tâche) avec des structures différentes.

1.4 Formats documentaires

Le panorama complet figure dans [l'état de l'art](#), §1.4 (ODF, OOXML, PDF 2.0, PDF/A-4, Markdown, HTML5).

Standard	Statut FR	Manque identifié
ODF 1.4 (OASIS Standard depuis octobre 2025)	Faible malgré la recommandation du RGI (v2.0, arrêté du 20 avril 2016)	Adoption marginale face à OOXML
OOXML	Dominante de fait	Hors de la définition du standard ouvert retenue : admissible par dérogation seulement (doctrine §6.1)
PDF / PDF/A-4	Très forte (échanges, archivage, marchés publics)	Aucun
Markdown	Forte chez les développeurs	Peu utilisé hors-tech

Constat : l'enjeu principal est la **fidélité des conversions** ODF ↔ OOXML et la capacité d'import/export sans perte de métadonnées.

1.5 Sémantique et données liées

Le panorama complet figure dans [l'état de l'art](#), §1.5 (RDF, SPARQL, OWL, DCAT-AP, Core Vocabularies).

Standard	Statut FR	Manque identifié
DCAT-AP v3.0	Bonne (data.gouv.fr)	Restreint à l'open data
Schema.org	Croissante (SEO, web sémantique)	Peu utilisé en B2B
Core Vocabularies (UE)	Faible hors projets européens	Sous-exploité par la filière française
RDF / SPARQL	Niche (recherche, open data)	Aucun

Constat : L'open data français utilise bien DCAT-AP. En revanche, il n'existe pas de **vocabulaires métier partagés** entre éditeurs de la filière pour décrire les concepts communs (utilisateur, organisation, rôle, permission, document, espace de travail, etc.).

1.6 Réseau et transport

Le panorama complet figure dans l'[état de l'art](#), §1.6 (TLS 1.3, HTTP/2-3, IPv6, DNSSEC, SFTP, QUIC).

Constat : la couche est bien standardisée. L'adoption française varie (IPv6 lente, DNSSEC marginal hors DNS publics) sans créer d'enjeu spécifique pour OpenInterop.

1.7 Méthodologie de validation et de tests d'interopérabilité

« 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.

Cette couche est transverse aux six autres : elle conditionne la **vérifiabilité effective** des standards OpenInterop, sans laquelle aucune « interopérabilité opposable » n'est possible. OpenInterop reste indépendante d'ETSI sur le plan institutionnel mais s'appuie sur son corpus méthodologique mature (30+ ans, 150+ événements Plugtests™ organisés). ETSI opère généralement à un niveau plus bas (protocoles, télécoms, IoT, smart cards, eIDAS) que les domaines applicatifs OpenInterop ; les overlaps réels (identité eIDAS, SIP/IMS, sécurité) justifient une articulation, pas une fusion.

Démarche top-down (ITU-T I.130, adoptée par ETSI)

Toute spécification OpenInterop distingue trois stades :

1. **System Objectives** : les capacités attendues du système standardisé, en termes larges.
2. **Functional Requirements** : comment l'objectif est atteint au niveau fonctionnel.
3. **Detailed Requirements** : caractéristiques atomiques, testables, exprimables à une interface de communication.

Critères de validation d'un objectif (RAMR)

Un objectif valide est :

- **Realistic** : n'exige pas l'inatteignable.
- **Achievable** : implémentable avec les technologies actuelles ou émergentes à coût raisonnable.
- **Measurable** : observable et testable, directement ou indirectement.
- **Relevant** : directement lié à la fonctionnalité attendue.

Ces quatre critères mettent en œuvre le principe 1 de la [doctrine](#) (§4) : l'interopérabilité se prouve par un résultat reproductible, conformément à la notion d'interopérabilité opposable posée dans la [note de vision](#).

Vocabulaire d'exigence (RFC 2119 / ISO Directives Part 2)

Pour la rédaction des standards OpenInterop, on utilise les verbes normatifs :

- **shall / must** : exigence obligatoire (Mandatory).
- **should** : recommandation forte (Recommended).
- **may** : option (Optional).

Verdicts et règle de conformité

Chaque critère d'une suite de tests reçoit l'un des quatre verdicts retenus par l'atelier cloud du 9 octobre 2026 : « conforme », « non conforme », « non applicable », « non concluant » (cf. [fiche cloud](#), §1.4). Une solution est conforme à un profil, sur le périmètre qu'elle revendique, quand tous les critères obligatoires de ce périmètre sont « conformes ». Aucune compensation n'est admise entre critères ; les autres mesures (performances, coûts, effort) sont publiées séparément. Une déclaration « compatible X » doit préciser les fonctions prises en charge et s'accompagner d'un rapport de conformité sur ce périmètre ([doctrine](#), principe 1).

Outillage de référence

Outil	Origine	Rôle
ICS (Implementation Conformance Statement)	ETSI EG 201 058	Proforma tabulé déclarant les fonctionnalités supportées par une implémentation, avec statut Mandatory / Optional / Conditional ; modèle de la déclaration de conformité retenue par la doctrine (§2)
IFS (Interoperable Features Statement)	ETSI	Variante de l'ICS axée sur les fonctions effectivement testées en interopérabilité
TTCN-3	ETSI ES 201 873 / ITU-T Z.160	Langage standardisé pour spécifier des suites de tests interopérables (utilisé pour LTE, SIP/IMS, IPv6, smart cards, ITS, ePassport, etc.)
TPLan	ETSI EG 202 553	Notation tabulée pour Test Purposes, vérifiable par outils
Plugtests™ (modèle)	ETSI CTI	Événements neutres où les implémentations se confrontent pour valider l'interopérabilité par construction ; modèle de l'essai croisé, seul niveau de preuve qui ouvre droit au badge (doctrine , §5.3)
IPT Framework	ETSI EG 202 568	Méthodologie et cadre pour les tests d'interopérabilité de protocoles Internet

Constat : OpenInterop dispose d'un référentiel mature à mobiliser. Le travail spécifique consiste à **adapter ce référentiel aux protocoles applicatifs** (profils OIDC, OCM, passerelles Matrix, etc.), ETSI l'ayant construit pour ses protocoles télécoms. L'indicateur d'interopérabilité de la [doctrine](#) (§5.4), qui reprend l'indicateur d'interopérabilité de la [note de vision](#) (§ « Phase 2 »), se calcule à partir des rapports de conformité selon une méthode publique ; les déclarations ICS/IFS des éditeurs en délimitent le périmètre.

2. Analyse des besoins de l'écosystème français

2.1 Pain points transverses

Les difficultés ci-dessous sont des **retours qualitatifs** issus des échanges du CSF, des discussions Cigref/TOSIT, des consultations ARCEP et de l'étude OPIIEC sur l'interopérabilité (cf. [note de vision](#) et [état de l'art](#) pour les références). Elles n'ont pas fait l'objet d'un sondage quantitatif dédié et seront à corroborer par un travail empirique ultérieur. Le cadrage stratégique général est celui de l'**interopérabilité opposable** (cf. note de positionnement Abilian, novembre 2025 : « *L'interopérabilité, clé de l'efficacité collaborative et de la souveraineté* »).

Ces problèmes reviennent dans **tous** les domaines (collaboratif, cloud, cybersécurité, etc.) :

1. « **L'annuaire n'est pas synchronisé entre nos outils** » : absence de provisioning automatique (SCIM). Il faut ajouter ou supprimer chaque utilisateur à la main dans chaque outil. Risque de sécurité (comptes orphelins) et coût opérationnel.
2. « **Chaque éditeur a sa propre API, avec ses propres conventions** » : pas de cohérence dans la manière d'exposer les APIs REST (pagination, filtrage, erreurs, versioning). L'intégration de N éditeurs nécessite N adaptations spécifiques.
3. « **On ne peut pas échanger de données structurées entre outils sans développement spécifique** » : absence de schémas de données partagés pour les concepts communs (utilisateur, document, événement, tâche). Chaque éditeur a son modèle de données propre.
4. « **Les webhooks de chaque outil sont incompatibles** » : pas de format de notification standardisé. Un orchestrateur ou un bus d'événements doit être configuré spécifiquement pour chaque source.
5. « **L'import/export de documents perd la mise en forme** » : les conversions ODF <-> OOXML sont imparfaites. Le copier-coller entre applications perd les métadonnées.
6. « **FranceConnect, c'est pour les citoyens, pas pour nos agents ni pour nos applications** » : il manque un socle d'identité professionnelle fédérée universel. ProConnect, qui a absorbé AgentConnect, progresse mais ne couvre pas tous les cas, en particulier le provisioning des comptes.

2.2 Besoins structurels

- **Un socle d'identité partagé** : OIDC + SCIM implémentés de manière homogène par tous les éditeurs, avec un profil commun documenté.
- **Des conventions API communes** : un « style guide » REST partagé par la filière, avec OpenAPI obligatoire, pour réduire le coût d'intégration.
- **Des schémas de données partagés** : un vocabulaire commun pour les entités métier transverses (utilisateur, organisation, document, espace, permission, événement).
- **Un format de notifications standardisé** : un profil CloudEvents ou équivalent pour les webhooks.
- **La conformité documentaire** : un niveau de qualité minimum pour les conversions ODF <-> OOXML, avec des tests de fidélité.

2.3 Priorisation

Besoin	Urgence	Impact	Faisabilité
Profil OIDC/SCIM commun	Haute	Très élevé	Haute
Style guide API REST + OpenAPI obligatoire	Haute	Élevé	Haute
Schémas de données partagés (entités transverses)	Haute	Élevé	Moyenne
Format de notifications (CloudEvents)	Moyenne	Moyen	Moyenne
Profil AsyncAPI pour événements inter-applications	Moyenne	Moyen	Moyenne

Besoin	Urgence	Impact	Faisabilité
Vocabulaires sémantiques (JSON-LD / Core Vocabularies)	Basse	Moyen	Faible
Fidélité conversions ODF/OOXML	Basse	Moyen	Faible

3. Propositions concrètes

Chaque chantier livre, conformément au principe 4 de la [doctrine](#) (§4), un profil, 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.

3.1 Chantier T1 : profil d'identité OpenInterop (Quick Win)

Objectif : Tout éditeur participant à OpenInterop implémente un socle commun d'identité, permettant le SSO et le provisioning automatique entre solutions.

Standards : OpenID Connect Core 1.0, OAuth 2.0 (RFC 6749, RFC 6750) avec les bonnes pratiques de sécurité de la RFC 9700 (BCP 240), SCIM 2.0 (RFC 7643, RFC 7644). Le profil reprend les exigences d'OAuth 2.1 déjà présentes dans la RFC 9700 (PKCE, abandon du flux implicite) ; il passera à OAuth 2.1 quand celui-ci sera publié en RFC. Il part des profils du groupe IPSIE de l'OpenID Foundation et les complète pour le contexte français.

Actions :

1. Rédaction du profil d'identité OpenInterop :

- Claims OIDC obligatoires : sub, email, name, given_name, family_name, preferred_username, locale, groups (claim personnalisé)
- Scopes OAuth obligatoires : openid, profile, email, groups
- Attributs SCIM obligatoires : User (userName, name, emails, groups, active), Group (displayName, members)
- Scénarios à supporter : création/modification/désactivation d'utilisateur, ajout/retrait de groupe, SSO, déconnexion (back-channel logout)
- Flux d'autorisation : Authorization Code + PKCE obligatoire, Implicit interdit

2. Suite de tests de conformité :

- Développer un outil open source (inspiré de la suite de conformité OIDC de la fondation OpenID) testant les endpoints d'un éditeur.
- Les scénarios de test couvrent le SSO, le provisioning SCIM (CRUD utilisateur, CRUD groupe), le back-channel logout et le refresh token ; chaque critère reçoit l'un des quatre verdicts (cf. §1.7).

3. POC multi-éditeurs :

- Démontrer SSO + provisioning automatique entre 3 éditeurs (ex. : solution collaborative + email + GED) avec un IdP de référence (Keycloak ou LemonLDAP::NG), qui sert d'implémentation de référence.

4. Badge de conformité :

- Publier le modèle de déclaration de conformité (fonctions revendiquées, version du profil et de la suite de tests).
- Faire délivrer le badge «OpenInterop Identity» par l'autorité technique, après un essai croisé, quand tous les critères obligatoires du périmètre revendiqué sont conformes ([doctrine](#), §5.3).

Livrables : Profil documenté (spécification), implémentation de référence, suite de tests open source, modèle de déclaration de conformité, POC, badge de conformité.

Délai : 3-6 mois. C'est le chantier fondateur : il conditionne tous les autres.

3.2 Chantier T2 : conventions API et style guide REST

Objectif : Les APIs des éditeurs OpenInterop suivent des conventions communes, réduisant le coût d'intégration.

Actions :

1. Rédaction du style guide API OpenInterop :

- **Spécification obligatoire :** toute API publique doit être décrite en OpenAPI (3.1 ou 3.2), publiée et maintenue à jour.
- **Conventions de nommage :** les chemins d'URL sont en kebab-case, les propriétés JSON en camelCase et les noms de ressources au pluriel.
- **Pagination :** le format est standardisé (offset/limit ou cursor-based) et l'enveloppe de réponse contient des champs total, next, previous.
- **Filtrage et tri :** les conventions s'inspirent de JSON:API ou d'un sous-ensemble pragmatique (?filter[field]=value, ?sort=field, -field2).
- **Gestion des erreurs :** les erreurs suivent le format RFC 9457 (Problem Details for HTTP APIs).
- **Versioning :** la version figure dans l'URL (/v1/, /v2/) ou dans un en-tête ; une politique de dépréciation l'accompagne.
- **Authentification :** les appels transmettent un jeton Bearer (OAuth 2.0, RFC 6750, selon le profil T1) ; les clés d'API restent admises pour les cas simples.
- **Hypermedia :** HAL ou JSON:API est recommandé, sans être obligatoire dans un premier temps.

2. Linter OpenAPI :

- Configurer un linter (Spectral ou équivalent) avec les règles du style guide, distribuable aux éditeurs pour auto-validation.

3. Catalogue d'APIs :

- Publier un catalogue centralisé des APIs OpenInterop (sur le modèle d'api.gouv.fr), permettant la découverte des APIs des éditeurs participants.

Livrables : Style guide documenté, configuration linter, catalogue d'APIs.

Délai : 3-6 mois.

3.3 Chantier T3 : schémas de données transverses

Objectif : Définir des schémas JSON partagés pour les entités métier communes à tous les domaines OpenInterop.

Actions :

1. Identification des entités transverses :

- **Utilisateur (User) :** identité, attributs, rôles
- **Organisation (Organization) :** structure, hiérarchie
- **Groupe (Group) :** regroupement d'utilisateurs
- **Document (Document) :** fichier + métadonnées
- **Espace de travail (Workspace) :** conteneur logique
- **Événement (Event) :** action horodatée (création, modification, partage, etc.)
- **Permission (Permission) :** droit d'accès sur une ressource
- **Tâche (Task) :** unité de travail assignable

2. Rédaction des schémas JSON Schema :

- Pour chaque entité, définir un schéma JSON Schema (Draft 2020-12) avec les champs obligatoires et optionnels, ainsi que leurs formats.

- S'inspirer des Core Vocabularies européens (Person, Business, Location) et de Schema.org pour la compatibilité sémantique.
- Prévoir des mécanismes d'extension (x- ou namespaces) pour les champs spécifiques à un domaine.

3. Mapping avec les modèles existants :

- Pour chaque éditeur fondateur, documenter le mapping entre le modèle de données natif et les schémas OpenInterop.
- Identifier les divergences et les résoudre par consensus.

4. Publication et gouvernance :

- Publier les schémas sur un dépôt Git (hébergé OW2), avec un processus de contribution et de versioning.

Livrables : Schémas JSON Schema pour 6-8 entités transverses, documentation de mapping, dépôt Git.

Délai : 6-9 mois.

3.4 Chantier T4 : format de notifications standardisé

Objectif : Les événements et notifications émis par les applications OpenInterop suivent un format commun, permettant l'orchestration inter-applications.

Standard : CloudEvents 1.0 (CNCF)

Actions :

1. Profil CloudEvents OpenInterop :

- Définir les types d'événements communs (document.created, user.added, task.completed, etc.) en s'appuyant sur les entités du chantier T3.
- Spécifier les attributs CloudEvents obligatoires (source, type, subject, time, datacontenttype).
- Définir le format du payload (JSON, référençant les schémas T3).

2. Mécanisme d'inscription aux événements :

- Spécifier une API d'inscription/désinscription aux webhooks (OpenAPI), reprenant le pattern de CloudEvents Subscriptions API ou un sous-ensemble pragmatique.

3. POC d'orchestration :

- Démontrer un scénario inter-applications : un document créé dans l'application A déclenche une notification CloudEvents, captée par l'application B qui crée automatiquement une tâche de revue.

4. Passerelle AsyncAPI :

- Pour les cas de communication asynchrone (files d'attente, event streaming), publier une spécification AsyncAPI 3.x décrivant les canaux d'événements OpenInterop.

Livrables : Profil CloudEvents, spécification d'inscription webhooks, POC, spec AsyncAPI.

Délai : 6-9 mois (après la rédaction des schémas de T3, car les notifications référencent les entités).

3.5 Chantier T5 : portail de documentation, outillage et méthodologie de tests

Objectif : Fournir aux éditeurs et intégrateurs un point d'entrée unique pour les spécifications, outils, tests et processus de validation OpenInterop.

Méthodologie de référence : la chaîne validation/tests s'appuie sur le cadre décrit en §1.7 : démarche top-down ITU-T I.130, critères RAMR, proformas ICS/IFS, langage TTCN-3 le cas échéant, modèle Plug-tests™ pour les sessions inter-éditeurs. OpenInterop reste indépendante d'ETSI et réutilise ce vocabulaire et ces outils sans en créer de nouveaux.

Actions :**1. Site de documentation :**

- Publier toutes les spécifications (profils d'identité, style guide API, schémas de données, profils CloudEvents) sur un site unique, versionné, avec historique des changements.
- Hébergé sous le chapeau OW2.

2. Boîte à outils de l'éditeur :

- Réunir la suite de tests d'identité (T1, exprimable en TTCN-3 ou dans un équivalent léger), le linter API (T2), le validateur de schémas (T3) et le validateur CloudEvents (T4).
- Fournir les **modèles de déclaration de conformité** (proformas tabulés inspirés des ICS/IFS) que remplissent les éditeurs.
- Publier tous ces outils en open source, installables en local ou en CI/CD.

3. Programme de conformité :

- Appliquer les trois niveaux de preuve de la [doctrine](#) (§5.3) : autoévaluation par l'éditeur, vérification par un acheteur ou un tiers, essai croisé organisé par OpenInterop.
- Établir la conformité profil par profil, selon la règle du §1.7 : tous les critères obligatoires du périmètre revendiqué sont conformes, sans compensation.
- Faire délivrer par l'autorité technique, après essai croisé, un badge par profil. Les niveaux envisagés (1 : identité ; 2 : APIs et schémas ; 3 : événements et réversibilité) se définissent comme des ensembles de profils tous conformes ; aucun ne résulte d'une moyenne pondérée.
- Publier une matrice de conformité des éditeurs participants, qui alimente l'indicateur d'interopérabilité ([doctrine](#), §5.4) dont la méthode de calcul est publique.
- Rédiger avec les acheteurs des clauses types ([doctrine](#), §5.6). Le rapport de conformité apporte une preuve technique ; sa portée contractuelle dépend de la clause qui y renvoie.

4. Événements de validation croisée :

- Organiser des sessions périodiques d'essais croisés multi-éditeurs (modèle Plugtests™ : environnement neutre, supervision dédiée, rapports publics).
- Articuler avec les plugfests sectoriels (C2 CalDAV, C3 Matrix, C6 OCM) et avec les essais croisés du profil de stockage objet issu de l'atelier cloud du 9 octobre 2026.

Livrables : Site de documentation, boîte à outils, programme de conformité, modèle de déclaration de conformité OpenInterop (inspiré des ICS/IFS), protocole de session d'essais croisés.

Délai : 9-12 mois (consolidation progressive des livrables des autres chantiers).

3.6 Chantier T6 : outillage EUDI Wallet / eIDAS 2.0 (moyen terme)

Objectif : Fournir aux éditeurs français les briques open source pour intégrer le portefeuille d'identité numérique européen (EUDI Wallet) dans leurs solutions.

Contexte : Le règlement eIDAS 2.0 (UE) 2024/1183 et l'Architecture de Référence (ARF) définissent le *quoi* ; chaque État membre doit proposer au moins un portefeuille avant le 24 décembre 2026. Les protocoles se sont stabilisés en 2025 : l'OpenID Foundation a publié en version finale OpenID4VP 1.0 (juillet 2025) et OpenID4VCI 1.0. L'écosystème manque encore d'outils open source accessibles aux PME pour les mettre en œuvre. Le projet européen EuroID Connect vise à combler ce manque ; OpenInterop peut se positionner comme relais français.

Standards : eIDAS 2.0 ARF, OpenID4VP 1.0, OpenID4VCI 1.0, formats SD-JWT VC et ISO/IEC 18013-5 (mdoc) retenus par l'ARF, Verifiable Credentials 2.0 (Recommandation W3C depuis mai 2025), DIDs

Actions :

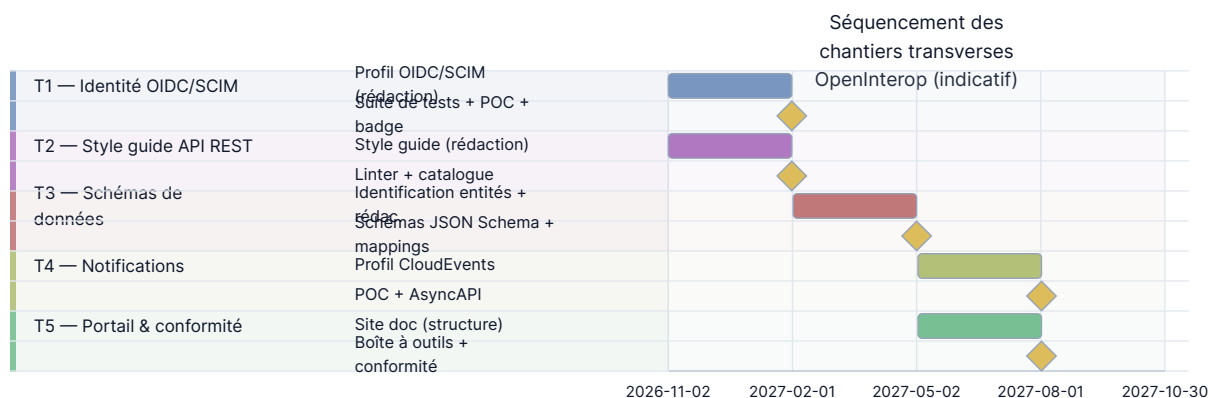
1. **Veille et participation à EuroID Connect** : suivre le projet, contribuer le cas échéant, relayer les outils produits vers la filière française.
2. **SDKs d'intégration OpenID4VP** : adapter ou développer des bibliothèques « developer-friendly » permettant aux éditeurs d'accepter des présentations d'attestations via OpenID4VP.
3. **Bibliothèques SCIM pour provisioning consenti** : étendre le profil SCIM du chantier T1 pour supporter le provisioning fondé sur le consentement utilisateur (modèle EUDI).
4. **Pilote sectoriel** : tester l'intégration EUDI Wallet dans un cas d'usage concret (ex. : authentification d'un agent public dans une suite collaborative avec présentation sélective d'attributs).

Livrables : SDKs, bibliothèques SCIM étendues, pilote.

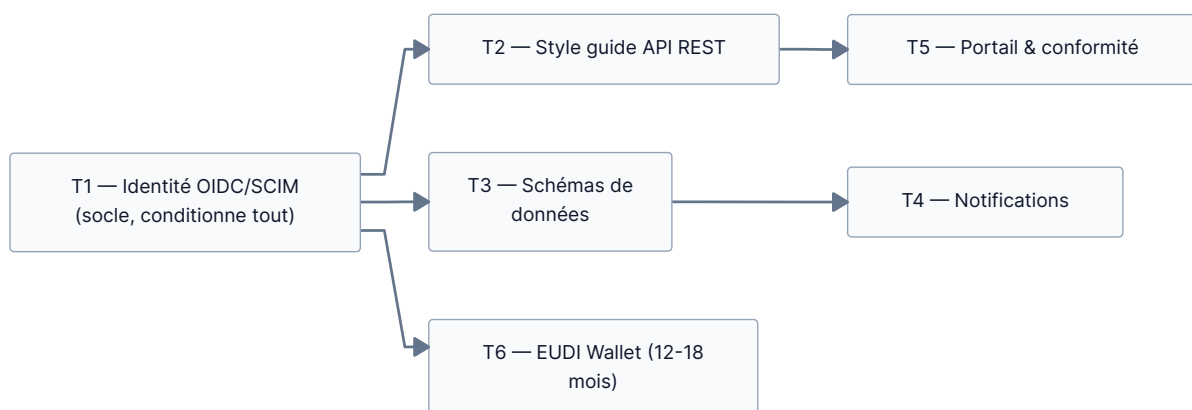
Délai : 12-18 mois (dépend de la maturité de l'écosystème EUDI, dont les premiers portefeuilles nationaux arrivent fin 2026).

4. Vue d'ensemble et séquencement

Le calendrier ci-dessous est indicatif ; il part de novembre 2026.



Dépendances



T1 est le chantier fondateur. Sans un socle d'identité interopérable, aucune autre interopérabilité n'est viable. T2 et T3 sont parallélisables une fois T1 lancé. T4 dépend de T3 (les notifications référencent les schémas d'entités). T5 consolide l'ensemble. T6 (EUDI Wallet) est un chantier à horizon 12-18 mois, hors du périmètre des 12 premiers mois, qui démarre une fois le socle T1 stabilisé.

5. Articulation avec les domaines sectoriels

Les standards transverses sont conçus pour être **étendus** par les domaines sectoriels :

Chantier transverse	Extension collaboratif	Extension cloud	Extension cybersécurité
T1 (Identité OIDC/SCIM)	Profil collaboratif (C1)	Identité cloud (JWT pour SECA)	Identité SOC (SPIFFE)
T2 (Style guide API)	APIs de partage de documents, calendrier	APIs de control plane	APIs de threat intelligence
T3 (Schémas de données)	Document, Workspace, Task	Instance, Network, Volume	Alert, Incident, Rule
T4 (Notifications)	document.created, task.assigned	instance.provisioned	alert.fired, incident.opened
T5 (Conformité)	Badges des profils collaboratifs	Badges des profils cloud	Badges des profils cybersécurité

Le profil d'identité T1 et le style guide API T2 sont les **prérequis communs** à tous les chantiers sectoriels. Les groupes de travail sectoriels consomment et étendent les livrables transverses ; ils n'ont pas à redéfinir ces fondations. Pour le stockage objet, l'atelier cloud du 9 octobre 2026 a distingué l'identité de l'orchestrateur de migration, qui relève de T1 (OIDC), de la signature des requêtes S3, propre à cette API et hors du périmètre de T1.

Références

Standards et spécifications

- **OpenID Connect Core 1.0** — OpenID Foundation. https://openid.net/specs/openid-connect-core-1_0.html
- **OAuth 2.0** — RFC 6749 (cadre) et RFC 6750 (jetons Bearer). <https://datatracker.ietf.org/doc/html/rfc6749> / <https://datatracker.ietf.org/doc/html/rfc6750>
- **RFC 9700 (BCP 240)** — Best Current Practice for OAuth 2.0 Security, janvier 2025. <https://datatracker.ietf.org/doc/html/rfc9700>
- **OAuth 2.1** — IETF Internet-Draft, non publié en RFC en octobre 2026. <https://datatracker.ietf.org/doc/html/draft-ietf-oauth-v2-1>
- **SCIM 2.0** — RFC 7643 (schéma) et RFC 7644 (protocole). <https://datatracker.ietf.org/doc/html/rfc7643> / <https://datatracker.ietf.org/doc/html/rfc7644>
- **IPSIE** — OpenID Foundation, groupe de travail *Interoperability Profiling for Secure Identity in the Enterprise*. <https://openid.net/wg/ipsie/>
- **WebAuthn Level 3** — W3C Recommendation, août 2026. <https://www.w3.org/TR/webauthn-3/>
- **OpenAPI 3.1 / 3.2** — OpenAPI Initiative. <https://spec.openapis.org/oas/v3.1.0> / <https://spec.openapis.org/oas/v3.2.0>
- **AsyncAPI 3.1** — AsyncAPI Initiative. <https://www.asyncapi.com/docs/reference/specification/v3.1.0>
- **JSON Schema** — Draft 2020-12. <https://json-schema.org/specification>
- **CloudEvents 1.0** — CNCF. <https://cloudevents.io/>
- **RFC 9457** — Problem Details for HTTP APIs. <https://datatracker.ietf.org/doc/html/rfc9457>
- **HAL** — Hypertext Application Language. <https://datatracker.ietf.org/doc/html/draft-kelly-json-hal>

- **JSON:API** — Spécification. <https://jsonapi.org/>
- **eIDAS 2.0** — Règlement (UE) 2024/1183. <https://eur-lex.europa.eu/eli/reg/2024/1183>
- **Verifiable Credentials Data Model 2.0** — W3C Recommendation, mai 2025. <https://www.w3.org/TR/vc-data-model-2.0/>
- **OpenID for Verifiable Presentations 1.0 (OpenID4VP)** — OpenID Foundation, version finale, juillet 2025. https://openid.net/specs/openid-4-verifiable-presentations-1_0-final.html
- **OpenID for Verifiable Credential Issuance 1.0 (OpenID4VCI)** — OpenID Foundation. https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- **Decentralized Identifiers (DIDs)** — W3C Recommendation. <https://www.w3.org/TR/did-core/>

Projets et outils

- **EuroID Connect** — Outillage open source EUDI Wallet / eIDAS 2.0. https://pad.cloud.abilian.com/s/FmVO8D_9
- **FranceConnect** — Service d'identité numérique de l'État français. <https://franceconnect.gouv.fr/>
- **ProConnect** — Identité des agents publics et des professionnels (DINUM), qui a absorbé AgentConnect en 2024. <https://proconnect.gouv.fr/>
- **France Identité** — Application d'identité numérique adossée à la CNIE, base du portefeuille EUDI français. <https://france-identite.gouv.fr/>
- **api.gouv.fr** — Catalogue des APIs de l'État français. <https://api.gouv.fr/>
- **Keycloak** — Serveur d'identité open source (implémentation de référence OIDC). <https://www.keycloak.org/>
- **LemonLDAP::NG** — WebSSO et fédération d'identité open source. <https://lemonldap-ng.org/>
- **Spectral** — Linter OpenAPI. <https://stoplight.io/open-source/spectral>

Méthodologie de validation et de tests d'interopérabilité

- **ETSI, Interoperability Best Practices**, 2011-2013 — brochure méthodologique du Centre for Testing and Interoperability. <https://www.etsi.org/>
- **ETSI White Paper N°3, Achieving Technical Interoperability — the ETSI Approach**.
- **ITU-T I.130** — Méthode top-down (objectifs / fonctionnels / détaillés) pour la spécification de standards. <https://www.itu.int/rec/T-REC-I.130/>
- **ETSI EG 201 058** — Implementation Conformance Statement (ICS) Proforma Style Guide.
- **ETSI EG 202 568** — IPT (Internet Protocol Testing) ; Methodology and Framework.
- **ETSI EG 202 553** — TPlan : a Notation for Expressing Test Purposes.
- **ETSI ES 201 873** — TTCN-3 (Testing and Test Control Notation v3), série multi-parts. <https://www.etsi.org/standards/tools-and-services/testing/ttcn-3>
- **ETSI Plugtests™** — événements de validation d'interopérabilité. <https://www.etsi.org/about/what-we-do/plugtests-testing-services>
- **RFC 2119** — Key words for use in RFCs to Indicate Requirement Levels (MUST/SHOULD/MAY). <https://datatracker.ietf.org/doc/html/rfc2119>

Documents OpenInterop

- [Note de vision OpenInterop](#)
- [État de l'art des standards d'interopérabilité](#)
- [Fiche collaboratif](#) (T1 → C1, T2-T4 → schémas Document/Workspace/Task, T4 → notifications d'activité)
- [Fiche cloud](#) (T1 → JWT pour SECA, T2 → control plane, T4 → CloudEvents pour la supervision)
- [Fiche cybersécurité](#) (T1 → identité SOC/SPIFFE, T4 → notifications d'alertes)
- [Doctrine OpenInterop](#) (définitions, principes, niveaux de preuve, autorité technique)

-
- Atelier cloud du 9 octobre 2026, compte rendu (verdicts, critères obligatoires sans compensation, distinction OIDC / signature S3)