NOTE DE COMMENTAIRES

Commentaires sur la Norme d'interopérabilité CT/EP, version 0.6

Remarques et propositions en vue de la version 1.0

Stefane Fermigier (Abilian SAS) · 11 novembre 2026 · DOCUMENT DE TRAVAIL

Version	**0.1**
Objet	**Norme d'interopérabilité CT/EP, version 0.6 du 6 novembre 2026**
Destinataires	**GT Collectivités, atelier Norme technique**
Licence	**CC BY 4.0**

Objet et bases

Cette note commente la *Norme d'interopérabilité — Collectivités territoriales et établissements publics*, version 0.6 du 6 novembre 2026, en vue de la version 1.0. Elle s'appuie sur l'état du dépôt public https://gitlab.adullact.net/csf-lsnc/norme-technique au 9 novembre 2026 (commit `8ad3354`) : la spécification, le compte rendu du 6 novembre, les schémas `common.schema.json` et `audit-log-event.schema.json`, les règles Spectral et leur documentation.

Chaque commentaire indique sa base. Il y en a trois :

- **les standards et référentiels publiés** (RFC de l'IETF, recommandations du W3C, spécifications OpenAPI et JSON Schema, textes et guides de l'ANSSI, du SGDSN et de la CNIL), cités avec leur numéro ;
- **la** proposition de doctrine publiée sur ce site, soumise aux participants d'Open Interop et qui n'engage que son auteur, pour les principes de conformité et de preuve ;
- **l'expérience du GT Cloud** avec le CTK S4, le kit de test de conformité du stockage objet, pour la vérification des comportements.

Les commentaires sont classés en trois niveaux : **à traiter avant la v1.0** (le point change le sens d'une exigence obligatoire ou rend la norme difficile à appliquer), **à traiter** (amélioration de fond, qui peut suivre la v1.0) et **rédactionnel**.

Le travail accompli est considérable : décisions motivées, processus RFC, intégration continue et outillage de vérification des contrats. Peu de démarches de filière en disposent. Les commentaires ci-dessous visent à consolider ce socle avant qu'il ne soit implémenté par plusieurs éditeurs.

Synthèse

N°	Section	Sujet	Niveau
1	§4.1	Authentification : distinguer service et utilisateur, préciser la confiance entre systèmes	Avant la v1.0
2	§3.4	Erreurs : adopter la RFC 9457	Avant la v1.0
3	§7.2.1	Niveaux de sensibilité : la référence à l'ANSSI et au SGDSN est inexacte	Avant la v1.0
4	§3.1, §4.2	HTTP/1.1 et TLS 1.3 : formuler des minimums	Avant la v1.0
5	§8.1	Version de l'API et version de la norme	Avant la v1.0
6	§3.5	Quotas : en-têtes et `/.well-known/interop-pub`	À traiter
7	§3.3	JSON Schema Draft-07 et OpenAPI 3.1	À traiter
8	§7	Enveloppe commune et formats métier existants (FHIR, PES, schémas publics)	À traiter
9	§6.2	Journal d'audit : bases de la rétention et données personnelles	À traiter
10	§11.2, annexe A	Conformité : des contrats aux comportements	À traiter
11	Page de titre, §9	Statut, licences et gouvernance	À traiter
12	Divers	Corrections rédactionnelles	Rédactionnel

1. Authentification entre systèmes (§4.1, avant la v1.0)

Constat. La norme impose « OAuth 2.0 + OIDC pour tous les échanges inter-systèmes » et des claims d'utilisateur obligatoires (`preferred_username`, `given_name`, `family_name`, `email`, `zoneinfo`). Elle impose aussi à chaque système un point de découverte `/.well-known/openid-configuration`.

Trois difficultés :

- **Beaucoup d'échanges n'ont pas d'utilisateur.** Un traitement de nuit, une synchronisation entre un SIRH et un logiciel de finances ou un export de masse n'agissent au nom de personne. OAuth 2.0 prévoit pour ce cas le flux *client credentials* (RFC 6749, §4.4), où le jeton ne contient que l'identité du client. Les claims d'utilisateur obligatoires y sont inapplicables.
- **Les claims OIDC appartiennent au jeton d'identité, pas au jeton d'accès.** OpenID Connect Core définit `given_name`, `family_name` ou `email` comme des informations sur l'utilisateur, remises au client dans l'ID Token ou par le point UserInfo. Le jeton d'accès présenté à une API suit un autre profil : la RFC 9068 (*JWT Profile for OAuth 2.0 Access Tokens*) y exige `iss`, `exp`, `aud`, `sub`, `client_id`, `iat` et `jti`. Placer nom et courriel dans chaque jeton d'accès multiplie aussi les copies de données personnelles, contrairement au principe de minimisation du RGPD (article 5.1.c).
- **Le modèle de confiance n'est pas dit.** Entre deux logiciels d'une même collectivité, édités par deux éditeurs, la norme ne précise pas qui émet les jetons (le fournisseur d'identité de la collectivité, celui d'un des éditeurs, ProConnect), comment le service appelé connaît la clé de l'émetteur, ni comment il vérifie que le jeton lui est destiné (`aud`). Exiger un point de découverte OIDC de *chaque* système suppose que chacun est fournisseur d'identité, ce qui n'est sans doute pas l'intention.

Base. RFC 6749 (OAuth 2.0), §4.4 ; OpenID Connect Core 1.0, §2 et §5.1 ; RFC 9068 ; RFC 9700 (BCP 240, *Best Current Practice for OAuth 2.0 Security*) ; RGPD, article 5.1.c.

Proposition.

- Distinguer deux cas. **Service à service** : flux *client credentials*, jeton d'accès au profil RFC 9068, sans claim d'utilisateur. **Au nom d'un utilisateur** : jeton d'accès au profil RFC 9068 avec `sub` ; les attributs de l'utilisateur, si l'API en a besoin, s'obtiennent par le point UserInfo ou par des claims limités au besoin.
- Pour un service qui en appelle un autre au nom d'un utilisateur, retenir l'échange de jetons (RFC 8693) plutôt que la retransmission du jeton reçu. La Suite numérique de l'État l'emploie déjà entre ses services (serveur d'autorisation Menshen, code libre).
- Décrire le modèle de confiance : émetteur des jetons, publication des clés (JWKS, RFC 7517), contrôle de l'audience. Réserver l'exigence de `/.well-known/openid-configuration` (ou de `/.well-known/oauth-authorization-server`, RFC 8414) au serveur d'autorisation.
- Admettre ES256 et PS256 à côté de RS256 : la RFC 7518 classe ES256 parmi les algorithmes « Recommended+ ».

Ce point rejoint le chantier T1 (profil d'identité) de la fiche transverse et le chantier C1 du GT Collaboratif ; un profil commun éviterait des choix divergents entre domaines.

2. Format des erreurs (§3.4, avant la v1.0)

Constat. Le format est « inspiré de la RFC 7807 ». Cette RFC est remplacée depuis juillet 2023 par la RFC 9457, qui reprend le même modèle. La norme ne mentionne pas le type de média `application/problem+json`. Son exemple donne `"status": "400"` en chaîne, alors que la RFC définit `status` comme un nombre. Le champ `instance` est rendu obligatoire, alors que la RFC le laisse facultatif.

Base. RFC 9457, *Problem Details for HTTP APIs*, §3 et §6.

Proposition.

- Adopter la RFC 9457 telle quelle, avec le type de média `application/problem+json`, en la citant comme référence normative.
- Garder le référentiel des types d'erreur du GT, en documentant chaque type à son URI, comme le recommande la RFC (§3.1.1). Les URN `urn:csf:open-interop:errors:…` ne sont pas déréférençables ; une URI HTTPS pointant vers la documentation du type serait plus utile.
- Corriger l'exemple (`"status": 400`, « Erreur de validation »).
- Garder `errors` comme extension du GT, ce que la RFC permet (§3.2).

Les règles Spectral `error-format` sont à aligner en conséquence.

3. Niveaux de sensibilité (§7.2.1, avant la v1.0)

Constat. La norme présente les niveaux `public`, `interne`, `confidentiel` et `restreint` comme ceux de « la doctrine ANSSI/SGDSN ». L'instruction générale interministérielle n° 1300 du 9 août 2021 ne connaît que deux niveaux de classification, *Secret* et *Très secret*, auxquels s'ajoute la mention de protection *Diffusion restreinte*, qui n'est pas une classification. Les quatre niveaux de la norme ressemblent plutôt aux échelles de classification internes des politiques de sécurité, sans être tirés d'un texte de l'ANSSI ou du SGDSN.

Base. IGI n° 1300/SGDSN/PSE/PSD du 9 août 2021, présentée sur https://cyber.gouv.fr/instruction-generale-interministerielle-n1300.

Proposition. Retirer la référence à l'ANSSI et au SGDSN et présenter l'échelle comme une convention du GT, définie par la norme. Préciser que les informations classifiées au sens de l'IGI 1300 sont hors du périmètre. Préciser aussi la portée du niveau : une étiquette informative, ou une obligation de traitement (chiffrement, journalisation renforcée, interdiction d'export) ? Le texte actuel (« traitement technique associé à cette propriété ») ne le dit pas.

4. HTTP/1.1 et TLS 1.3 (§3.1, §4.2, avant la v1.0)

Constat. « HTTP/1.1 obligatoire comme protocole de transport » peut se lire comme une interdiction de HTTP/2 ou HTTP/3. « TLS 1.3 obligatoire » va au-delà des recommandations en vigueur, qui admettent TLS 1.2.

Base. RFC 9110 (*HTTP Semantics*), qui définit la sémantique de HTTP indépendamment de la version ; RFC 9325 (BCP 195), qui demande la prise en charge de TLS 1.2 et recommande TLS 1.3 ; guide de l'ANSSI *Recommandations de sécurité relatives à TLS* (v1.2, 2020), qui fixe TLS 1.2 comme minimum et recommande de privilégier TLS 1.3.

Proposition. « La sémantique HTTP (RFC 9110) est obligatoire ; HTTP/1.1 est le minimum, HTTP/2 et HTTP/3 sont admis. » « TLS 1.2 au minimum, TLS 1.3 recommandé, configuration conforme au guide TLS de l'ANSSI ; TLS 1.0 et 1.1 interdits. » Des infrastructures de collectivités (passerelles, équipements de sécurité) ne permettent pas toujours TLS 1.3 ; une exigence trop stricte serait contournée ou ignorée.

5. Version de l'API et version de la norme (§8.1, avant la v1.0)

Constat. Le §8 s'intitule « Versionnement de la norme », mais ses règles visent tantôt la norme (`X-Interop-Version`), tantôt l'API de l'éditeur (`/api/v{MAJOR}`, support de la version N-1, en-têtes de dépréciation). Un lecteur ne sait pas si `/api/v1` désigne la version 1 de la norme ou de l'API de l'éditeur. Le support de la version précédente (12 mois) vaut-il pour la norme, pour les API, ou pour les deux ?

Base. Semantic Versioning 2.0.0.

Proposition. Séparer deux sous-sections : le versionnement de la norme (SemVer, `X-Interop-Version`, durée de coexistence) et le versionnement des API des éditeurs (préfixe de route, dépréciation, durée de support). Préciser que le préfixe `/api/v{MAJOR}` désigne la version de l'API de l'éditeur. Préciser aussi à quoi s'applique la durée de support.

6. Quotas (§3.5, à traiter)

Constat. Les en-têtes `X-RateLimit-Limit`, `X-RateLimit-Remaining` et `X-RateLimit-Reset` sont une convention répandue mais non normalisée. L'IETF normalise des en-têtes `RateLimit` et `RateLimit-Policy` (Internet-Draft du groupe httpapi, révision −11 de mai 2026, pas encore publié en RFC). Les règles Spectral exigent les trois en-têtes sur toute réponse 2xx de toute opération, ce qui alourdit chaque contrat. Les seuils doivent être « signalés dans `/.well-known/interop-pub` », un chemin qui n'est ni défini par la norme (format, contenu) ni enregistré auprès de l'IANA.

Base. draft-ietf-httpapi-ratelimit-headers-11 ; RFC 6585 (code 429) ; RFC 8615 (*Well-Known URIs*), qui prévoit l'enregistrement des chemins `/.well-known/`.

Proposition.

- Garder le 429 avec `Retry-After` obligatoire, qui suffit au client pour se réguler.

- Rendre les en-têtes de quota recommandés ; annoncer l'adoption des en-têtes de l'IETF à leur publication en RFC.
- Soit spécifier le document `/.well-known/interop-pub` (format JSON, schéma, contenu), soit le remplacer par une extension du contrat OpenAPI de l'éditeur (`x-rate-limit`), qui a l'avantage d'être déjà publié et vérifiable par Spectral.

7. JSON Schema et OpenAPI (§3.3, à traiter)

Constat. La norme impose JSON Schema Draft-07 (2018) et OpenAPI 3.x. Depuis OpenAPI 3.1 (2021), le dialecte de schéma d'OpenAPI est JSON Schema 2020-12. Un éditeur qui écrit ses contrats en OpenAPI 3.1 produit des schémas 2020-12, différents de ceux que publie la norme.

Base. OpenAPI Specification 3.1.0 et 3.2.0 ; JSON Schema 2020-12.

Proposition. Retenir OpenAPI 3.1 au minimum et JSON Schema 2020-12 pour les schémas publiés, en version majeure suivante si le changement est jugé cassant. La fiche transverse publiée sur ce site fait le même choix (chantier T2).

8. Enveloppe commune et formats métier existants (§7, à traiter)

Constat. Toute ressource échangée doit contenir l'enveloppe (`id` en UUID v7, `sensitivityLevel`, `createdAt`, `updatedAt`, `producerId`). Or les ateliers métier s'orientent vers des formats qui ont leur propre structure : HL7 FHIR pour l'action sociale (identifiant, `meta.lastUpdated`, `meta.security`), le PES de la DGFiP pour les finances (XML). La norme exclut par ailleurs « les échanges avec des systèmes d'État (DGFiP, DINUM, etc.) ». Elle ne cite pas non plus les schémas de données déjà publiés pour les collectivités : le socle commun des données locales sur schema.data.gouv.fr couvre notamment les délibérations, l'exemple même du §7.2.2.

Base. Proposition de doctrine, principe 3 (« l'existant d'abord ») ; HL7 FHIR R4, ressource `Meta` ; RFC 9562 (UUID, dont la version 7) ; schema.data.gouv.fr.

Proposition.

- Préciser le périmètre de l'enveloppe : les API REST conçues selon la norme. Pour un format qui a déjà ses métadonnées (FHIR, PES, SEDA), publier une table de correspondance plutôt qu'imposer une double enveloppe.
- Citer la RFC 9562 pour l'UUID v7.
- Ajouter au §11.3 les schémas de schema.data.gouv.fr et, pour l'action sociale, les travaux de l'Agence du numérique en santé (FHIR, profil FR Core).
- Préciser la place du PES, que l'atelier Finances envisage comme socle, au regard de l'exclusion des échanges avec l'État.

9. Journal d'audit (§6.2, à traiter)

Constat. Le journal enregistre l'adresse IP, l'en-tête `X-Forwarded-For` et, en recommandé, l'identifiant et le nom d'utilisateur, avec une rétention de 6 mois minimum. Ce sont des données personnelles. La rétention a été fixée « au plus petit commun des pratiques des éditeurs ».

Base. CNIL, recommandation relative aux mesures de journalisation (délibération n° 2021-122 du 14 octobre 2021), qui retient une conservation de six mois à un an, une durée plus longue devant être justifiée ; RGPD, article 5.1.e (limitation de la conservation).

Proposition. Citer la recommandation de la CNIL comme base de la durée retenue. Ajouter une durée maximale (un an, sauf obligation particulière). Pour le format, signaler la convergence possible avec le modèle de journaux d'OpenTelemetry, déjà cohérent avec `traceparent` ; la fiche cloud en propose un chantier (CL1).

10. Conformité (§11.2, annexe A, à traiter)

Constat. L'outillage vérifie les contrats OpenAPI et les exports de journal. Il ne vérifie pas qu'une API se comporte comme son contrat l'annonce (en-têtes réellement renvoyés, format des erreurs, pagination, propagation de `traceparent`), ni que deux implémentations échangent effectivement. La norme renvoie à plus tard les niveaux de conformité et la question de l'autodéclaration.

Base. Proposition de doctrine, principe 1 et §5 (déclaration et rapport de conformité, trois niveaux de preuve) ; méthode des déclarations ICS de l'ETSI ; expérience du CTK S4 du GT Cloud, dont les premiers essais ont révélé des écarts qu'aucune déclaration ne signalait.

Proposition.

- Rédiger un modèle de déclaration de conformité : version de la norme, exigences recommandées et optionnelles revendiquées, extensions, limites.
- Écrire une première suite de tests de comportement, qui interroge une API réelle à partir de son contrat : en-têtes, erreurs, pagination, `traceparent`, enveloppe.
- Organiser un essai croisé pour la démonstration prévue par l'atelier Finances début 2027, avec des rapports reproductibles.

Les règles Spectral actuelles en sont la première brique.

11. Statut, licences et gouvernance (à traiter)

Constat. La page de titre est marquée « CONFIDENTIEL – DRAFT » et les comptes rendus « diffusion restreinte », alors que le dépôt est public. Le dépôt applique CeCILL-B au livrable et la Licence Ouverte 2.0 aux schémas ; les notes de travail de ce site sont publiées sous CC BY 4.0 et le CTK S4 sous Apache 2.0. Le §9.1 réserve le vote au comité technique, un représentant par éditeur, à la majorité des deux tiers : les collectivités, premières utilisatrices de la norme, n'y ont pas de voix.

Base. Proposition de doctrine, §7 (rôles : groupes de travail ouverts à tout participant, utilisateurs qui documentent les besoins et vérifient l'utilité des livrables, autorité technique indépendante des fournisseurs).

Proposition. Retirer la mention « confidentiel » de la norme publiée. Expliciter le choix des licences ; CeCILL-B et la Licence Ouverte 2.0 se défendent, mais une licence commune avec les autres groupes d'Open Interop, si elle était retenue, faciliterait la réutilisation croisée. Donner une voix aux collectivités dans l'adoption des spécifications qui les concernent.

12. Corrections rédactionnelles

- Avant-propos : « version initiale (draft 0.1) » et renvoi au « processus RFC défini en section 6 », devenu la section 9.
- §2 : « header traceparent requis et muté à chaque passage » ; préférer « propagé, avec un nouveau `parent-id` à chaque service », comme au §6.1.
- §3.2 : la langue des attributs reste marquée « À valider par le GT », alors que le compte rendu du 6 novembre l'a actée.
- §3.4 : l'exemple d'erreur (voir commentaire 2).
- §5.3 : la taille maximale de page est « Obligatoire » alors que le style de pagination n'est que « Recommandé » ; préciser l'articulation.
- §6.2.1 : « suiveront ».
- §7.2 : « Traitement technique associé à cette. propriété ».
- §9.2 : les objectifs de calendrier (« version finale du socle d'ici septembre 2026 ») sont dépassés.
- Annexe A : la référence à OpenRTB, standard de la publicité en ligne, semble sans rapport avec la norme.
- Annexe B : la ligne 0.6 est à compléter.

Références

- RFC 6585, *Additional HTTP Status Codes*, 2012.
- RFC 6749, *The OAuth 2.0 Authorization Framework*, 2012.
- RFC 7517, *JSON Web Key*, et RFC 7518, *JSON Web Algorithms*, 2015.
- RFC 8414, *OAuth 2.0 Authorization Server Metadata*, 2018.
- RFC 8594, *The Sunset HTTP Header Field*, 2019.
- RFC 8615, *Well-Known Uniform Resource Identifiers*, 2019.
- RFC 8693, *OAuth 2.0 Token Exchange*, 2020.
- RFC 9068, *JWT Profile for OAuth 2.0 Access Tokens*, 2021.
- RFC 9110, *HTTP Semantics*, 2022.
- RFC 9325 (BCP 195), *Recommendations for Secure Use of TLS and DTLS*, 2022.
- RFC 9457, *Problem Details for HTTP APIs*, 2023.
- RFC 9562, *Universally Unique IDentifiers (UUIDs)*, 2024.
- RFC 9700 (BCP 240), *Best Current Practice for OAuth 2.0 Security*, 2025.
- RFC 9745, *The Deprecation HTTP Response Header Field*, 2025.
- draft-ietf-httpapi-ratelimit-headers-11, *RateLimit header fields for HTTP*, mai 2026. https://datatracker.ietf.org/doc/draft-ietf-httpapi-ratelimit-headers/
- OpenID Connect Core 1.0.
- OpenAPI Specification 3.1.0 ; JSON Schema 2020-12.
- W3C, *Trace Context*, Recommandation.
- HL7 FHIR R4 ; Agence du numérique en santé, profils FR Core.
- ANSSI, *Recommandations de sécurité relatives à TLS*, v1.2, 2020.
- SGDSN, IGI n° 1300 sur la protection du secret de la défense nationale, 9 août 2021.
- CNIL, délibération n° 2021-122 du 14 octobre 2021 portant recommandation relative à la journalisation.
- Règlement (UE) 2016/679 (RGPD), article 5.
- schema.data.gouv.fr, socle commun des données locales.
- Proposition de doctrine pour Open Interop : https://open-interop.lab.abilian.com/doctrine/ ; CTK S4 : https://open-interop.lab.abilian.com/gt/cloud/s4/ctk/.