

Vers un RGI v3 : évaluation et propositions

Stefane Fermigier (Abilian SAS) · 31 octobre 2026 · DRAFT

Version 0.1
Licence CC BY 4.0

Le référentiel général d'interopérabilité (RGI) fixe les normes et les standards que doivent utiliser les autorités administratives pour échanger entre elles et avec les usagers. Sa version 2.0, datée de décembre 2015 et approuvée par arrêté du 20 avril 2016, n'a pas été mise à jour depuis. La commission d'enquête de l'Assemblée nationale sur les dépendances structurelles dans le numérique propose de l'actualiser et de le rendre obligatoire dans les marchés publics (rapport n° 3054, juillet 2026, proposition n° 12).

Cette note évalue les changements qu'appelle une version 3. Elle examine d'abord la démarche du référentiel, à la lumière de la [doctrine](#) proposée pour OpenInterop, puis son contenu : standards obsolètes, versions à actualiser, standards à ajouter, standards émergents à placer en observation, profils à refondre. Elle s'appuie sur l'[état de l'art](#) et les fiches de domaine d'OpenInterop.

Synthèse

- **Le RGI v2 avait de bonnes idées** : des critères d'adoption explicites, quatre statuts qui organisent le cycle de vie des standards, des profils d'interopérabilité par usage, une préférence pour les standards mis en œuvre par des logiciels libres. Une V3 doit les conserver.
- **Il est resté une liste**. Aucun critère n'est éliminatoire, aucune conformité n'est vérifiée, le guide de conformité et l'outil d'autodiagnostic annoncés n'ont pas été publiés à notre connaissance ; le comité d'évolution trimestriel n'a produit aucune révision en dix ans. Aucun dispositif ne permet à un usager ou à une entreprise de faire respecter le référentiel : des administrations exigent encore des formats bureautiques propriétaires, contrairement à ses recommandations.
- **Son contenu a vieilli** : SSL, FTP en clair, UDDI, WS-CDL, RAML ou la liste des navigateurs (Internet Explorer 10) côtoient l'absence d'OpenAPI, de SCIM, de WebAuthn, de la sécurité de la messagerie, de la facturation électronique ou du portefeuille d'identité européen. Le document comporte aussi des incohérences internes.
- **Sept orientations pour une V3** : passer de la liste au profil vérifiable (suite de tests, implémentation de référence, déclaration de conformité) ; rendre le critère d'ouverture éliminatoire, avec des dérogations motivées et datées ; couvrir les cinq niveaux d'interopérabilité ; inscrire la réversibilité et la portabilité des données ; appliquer les mêmes exigences aux plateformes publiques ; n'imposer aucun produit aux usagers et leur ouvrir un recours ; faire du RGI un référentiel vivant, versionné, publié sous forme exploitable par machine et révisé chaque année.
- **Une refonte des profils** autour des usages de 2026 : fondations API, identité, messagerie et collaboration, archivage, géomatique, échanges B2G, signature et confiance, données ouvertes

et de référence, facturation électronique, cloud et réversibilité, sécurité opérationnelle. Les profils SOAP et orchestration passent en fin de vie ou sont retirés.

1. Le RGI v2 en bref

Base juridique. Le RGI découle de l'ordonnance n° 2005-1516 du 8 décembre 2005 (article 11) et du décret n° 2007-284 du 2 mars 2007. Il s'impose aux autorités administratives : administrations de l'État, collectivités territoriales, établissements publics administratifs, organismes de protection sociale. Les systèmes existants disposaient de trois ans pour s'y conformer.

Périmètre. Le RGI v2 se concentre sur les échanges « aux frontières » des systèmes d'information : entre administrations (A2A), avec les entreprises (A2B) et avec les citoyens (A2C). L'interopérabilité interne relève des cadres de cohérence technique de chaque ministère. Le référentiel traite surtout des niveaux technique et syntaxique ; le chapitre sémantique se limite à des définitions et à un format pivot, l'identité pivot d'une personne (IdpPERS).

Méthode. Six critères d'adoption, inspirés de la méthode européenne CAMSS : ouvert, pertinent, mature, indépendant, facile à déployer, soutenu par l'industrie. Le texte précise que « la non satisfaction d'un critère n'est pas éliminatoire ». Chaque standard reçoit l'un de quatre statuts : en observation, recommandé, en fin de vie, retiré. Les standards non listés ne doivent pas être utilisés dans les échanges du périmètre.

Contenu. 150 standards, classés par niveau (technique, syntaxique) et par catégorie, chacun décrit par un résumé tiré de Wikipédia et un lien vers sa spécification. Neuf profils regroupent des standards par usage : fondations État plateforme (P1), web services SOAP (P2), communication interpersonnelle et bureautique (P3), archivage (P4), géomatique (P5), protection sociale (P6), orchestration (P7), conception de système (P8), signature électronique (P9).

Conformité et gouvernance. Les autorités administratives devaient publier un bilan de conformité et une trajectoire dans les six mois. Un guide de conformité et un outil d'autodiagnostic étaient annoncés. Un « comité interministériel d'évolution du RGI » devait se réunir chaque trimestre pour examiner les propositions reçues par courriel.

2. Diagnostic : le bilan de dix ans

2.1 Les acquis

- **Les statuts.** Les quatre statuts donnent un vocabulaire simple pour faire entrer un standard, le recommander, annoncer son remplacement et organiser son retrait. Le statut « retiré » impose un plan de décommissionnement public.
- **Les profils.** Le RGI v2 a introduit l'idée qu'un usage appelle un ensemble limité de standards. L'idée rejoint la notion de profil d'application de la doctrine OpenInterop ; elle n'a simplement pas été poussée jusqu'aux options, aux versions et aux tests.
- **Les critères.** La définition du critère « ouvert » est proche de celle de l'article 4 de la LCEN et du Cadre européen d'interopérabilité de 2004 : spécification complète, publique, sans restriction d'accès ni de mise en œuvre, maintenue par un organisme sans but lucratif, compatible avec les logiciels libres et propriétaires.

- **Le logiciel libre comme instrument de test.** Le RGI v2 demande que les standards retenus soient mis en œuvre par des logiciels libres, « pour faciliter les tests, l'appropriation, et ne pas imposer de fait l'acquisition de solutions propriétaires ».
- **La définition de l'interopérabilité réelle :** interfaces fondées sur des standards ouverts, respect d'un profil, test vis-à-vis d'une implémentation de référence, documentation des écarts. Le texte posait donc déjà les quatre éléments de la doctrine OpenInterop, sans se donner les moyens de les vérifier.

2.2 Un référentiel figé

Le RGI v2 annonçait qu'il « doit pouvoir évoluer fréquemment » et prévoyait un comité d'évolution trimestriel. Aucune version n'a suivi. Les liens du document renvoient aux sites de l'ancien SGMAR, réorganisés depuis ; l'adresse de contact relève d'une direction qui n'existe plus sous ce nom. Le référentiel a cessé d'être un outil de travail pour devenir une référence citée de loin. Le CNLL le qualifie « en friche » ; les acheteurs publics s'y réfèrent peu. La Cour des comptes rappelle en octobre 2026 qu'il est « toujours en vigueur » et que son profil P3 recommande ODF et PDF plutôt qu'OOXML, alors que la suite Microsoft Office « demeure le standard prédominant » dans les ministères.

La cause principale tient à la forme du document : un PDF de 84 pages, sans dépôt public, sans format exploitable par machine, sans calendrier de révision ni responsable nommé. Une révision demandait de reprendre tout le document et de relancer un arrêté.

2.3 Une liste plus qu'un référentiel opposable

Le RGI v2 désigne des standards ; il ne dit pas comment vérifier qu'une solution les respecte. Aucun profil ne fixe de version, d'options obligatoires ni de comportements attendus. Aucune suite de tests n'accompagne les profils. La conformité repose sur un bilan déclaratif ; le guide et l'outil d'autodiagnostic annoncés n'ont pas été publiés, à notre connaissance.

Cette lacune vide l'obligation de sa portée. Une administration ou un fournisseur peut se dire conforme parce qu'il « supporte » OpenID Connect ou ODF, sans qu'on sache sur quel périmètre ni avec quel résultat. C'est la conformité apparente que la doctrine OpenInterop (principe 1) entend remplacer par une preuve reproductible.

L'absence de contrôle laisse aussi les usagers sans recours. Le RGI s'applique aux échanges avec les citoyens et les entreprises (A2C, A2B), mais aucun dispositif ne permet de signaler un manquement ni d'obtenir qu'il cesse. Des administrations ont ainsi exigé de leurs usagers des documents au format .docx de Microsoft Office, alors que le RGI recommande ODF et place OOXML en observation ; le CNLL l'a relevé publiquement en 2019. L'usager doit alors acquérir ou utiliser un produit déterminé pour accomplir une démarche, situation que le référentiel visait à éviter.

2.4 Une ouverture affaiblie en pratique

Le critère « ouvert » est exigeant sur le papier, mais sa non-satisfaction « n'est pas éliminatoire ». Plusieurs standards retenus ne le satisfont pas :

- **H.264, H.265 et AAC**, recommandés ou en observation, sont couverts par des brevets licenciés par des groupements (*patent pools*) ; leur mise en œuvre sous licence libre n'est pas assurée partout.
- **OOXML** est conservé en observation, avec un commentaire qui relève lui-même « son manque d'ouverture (notamment dans la gouvernance de la norme) ». Seule la variante « stricte » est concernée ; la variante « transitionnelle », que produisent par défaut les suites de Microsoft, n'est pas recommandée.
- **Shapefile** est une description technique publiée par un éditeur, sans organisme de normalisation.
- **7z et RAML** relèvent d'un auteur ou d'un éditeur plus que d'une organisation de standardisation.

Le texte cite par ailleurs la définition de l'interopérabilité de l'AFUL et de Wikipédia, plus exigeante que celle de la Commission, sans en tirer de conséquence opérationnelle.

2.5 Des incohérences internes

Une V3 devra corriger des contradictions du texte actuel, qui ne facilitent ni la lecture ni la vérification. Le [catalogue du RGI v2](#) les recense toutes ; les principales sont les suivantes :

Point	Contradiction
S/MIME, DSML	« Recommandé » (S/MIME) ou « en fin de vie » (DSML) dans leur fiche, « retirés » dans le tableau des évolutions
JPEG 2000	« En fin de vie » dans sa fiche, présent dans le profil géomatique recommandé, « en observation » pour l'archivage
CSV	« En fin de vie » sauf entre application et utilisateur, mais format de conservation recommandé pour l'archivage
TLS (SSL)	Le standard recommandé inclut SSL, alors que seule la version 1.2 ou ultérieure de TLS est conforme au RGS
FTP / FTPS	FTP, qui transmet les identifiants en clair, est recommandé ; FTPS, sa version chiffrée, est retiré
WS-CDL	En observation, mais inclus dans le profil orchestration recommandé (P7)
P7	Prérequis P1 dans la synthèse, P2 dans la description
GeoJSON	Cité deux fois dans le profil P5
Profils recommandés	Seize standards « en observation » ou « en fin de vie » y figurent, dont SPARQL, RAML, WebM, VP9 et Opus dans le profil de fondation P1 et PRESTO 2.0 dans le profil SOAP P2

2.6 Une couverture trop étroite

- **Sémantique.** Le chapitre sémantique ne contient que des définitions et un format pivot d'identité. Le service public de la donnée et ses données de référence (loi pour une République numérique, octobre 2016) ne sont pas mentionnés, puisqu'ils lui sont postérieurs. Aucun vocabulaire commun, aucun schéma de données partagé n'est référencé.
- **Organisation et droit.** Les niveaux organisationnel et juridique sont décrits mais ne donnent lieu à aucune exigence : ni licences, ni conditions d'accès aux API, ni clauses d'interopérabilité.
- **Réversibilité.** Le RGI traite des échanges entre systèmes, pas de la capacité d'une administration à quitter une solution. Or la dépendance aux fournisseurs, de logiciels comme de cloud, est devenue la question centrale (cf. [fiche cloud](#)).
- **Sécurité.** Seuls IDMEF et IODEF couvrent l'échange d'informations de sécurité. La sécurité de la messagerie (SPF, DKIM, DMARC, MTA-STS), les avis de sécurité, les nomenclatures logicielles et le signalement de vulnérabilités sont absents.

2.7 Un environnement qui a changé

Depuis 2015, plusieurs évolutions ont rendu le RGI v2 partiellement obsolète :

- **Le droit européen** : Cadre européen d'interopérabilité révisé en 2017 (douze principes, quatre niveaux et une gouvernance intégrée) ; Interoperable Europe Act (règlement (UE) 2024/903), qui impose depuis le 12 janvier 2025 une évaluation d'interopérabilité avant toute exigence contraignante touchant des services publics numériques transeuropéens ; Data Act (règlement (UE) 2023/2854),

applicable depuis le 12 septembre 2025 ; eIDAS 2 (règlement (UE) 2024/1183) et le portefeuille d'identité numérique européen ; Cyber Resilience Act et NIS2.

- **Le droit français** : loi pour une République numérique (2016), service public de la donnée, circulaire du Premier ministre du 5 février 2026 sur la commande publique numérique, réforme de la facturation électronique (réception obligatoire pour toutes les entreprises à partir du 1er septembre 2026).
- **Les pratiques** : généralisation des API REST décrites en OpenAPI, abandon de SOAP pour les nouveaux projets, fédération d'identité (FranceConnect, ProConnect), cloud et conteneurs, messageries fédérées (Tchap, fondée sur Matrix), outils collaboratifs de l'État (La Suite numérique), agents d'IA qui consomment des API.

3. Orientations pour une V3

Les orientations suivantes reprennent la démarche de la [doctrine](#) OpenInterop. Elles concernent la forme et le fonctionnement du référentiel, avant son contenu.

3.1 Du catalogue au profil vérifiable

Le cœur d'une V3 devrait être ses profils, pas sa liste de standards. Chaque profil devrait comprendre, conformément au principe 4 de la doctrine :

- les standards retenus, avec leur version minimale et les options obligatoires ou interdites ;
- les comportements attendus, décrits par des contrats sémantiques quand l'usage le demande (par exemple, le contenu d'un export complet) ;
- une suite de tests de conformité publiée sous licence libre ;
- une implémentation de référence, quand il n'en existe pas déjà ;
- un modèle de déclaration de conformité, sur le modèle des déclarations ICS de l'ETSI.

La liste des standards subsiste comme catalogue : elle donne le statut de chaque standard, sa version et ses dates. Elle ne suffit plus à établir la conformité.

3.2 Un critère d'ouverture éliminatoire, des dérogations encadrées

Le critère « ouvert » devrait devenir éliminatoire, au sens de l'article 4 de la LCEN et du Cadre européen d'interopérabilité de 2004. La spécification est publique, sans restriction d'accès ni de mise en œuvre, y compris sous licence libre ; elle permet des mises en œuvre concurrentes et relève d'une gouvernance indépendante et transparente. Les conditions dites FRAND, qui admettent des redevances, ne suffisent pas (doctrine, principe 2).

Lorsqu'aucune alternative ouverte n'existe, notamment pour la compatibilité avec des systèmes existants, un standard non ouvert peut être admis par dérogation. Celle-ci est motivée, signalée dans le profil, limitée dans le temps et accompagnée d'un plan de sortie (doctrine, §6). Les codecs audio et vidéo brevetés et OOXML relèveraient de ce régime.

Les autres critères (pertinence, maturité, soutien) restent des critères d'appréciation, à documenter pour chaque standard selon la méthode CAMSS, qui reste maintenue au niveau européen.

3.3 Les cinq niveaux

Une V3 devrait couvrir les cinq niveaux d'interopérabilité, au-delà des niveaux technique et syntaxique :

- **sémantique** : référencer les données de référence du service public de la donnée et leurs identifiants (SIREN et SIRET, code officiel géographique, Base adresse nationale...), les vocabulaires communs

européens (SEMIC Core Vocabularies), les schémas publiés sur schema.data.gouv.fr ; aligner le format pivot d'identité sur les données d'identification personnelle d'eIDAS 2 ;

- **organisationnel** : décrire, pour chaque profil, les rôles (fournisseur de données, fournisseur de service, intermédiaire) et les engagements de service attendus des API publiques ;
- **juridique** : fixer les exigences de licence des spécifications et des implémentations de référence, les conditions d'accès aux API et les clauses types d'interopérabilité et de réversibilité.

3.4 La réversibilité et la portabilité des données

Le RGI v2 traite des échanges ; une V3 devrait aussi traiter de la sortie. Toute solution utilisée par une autorité administrative devrait permettre l'export complet des données qu'elle gère, avec leurs métadonnées, dans un format ouvert, selon un schéma documenté, par une interface programmable (doctrine, principe 6). Cette exigence prolonge le Data Act, qui impose le changement de fournisseur de services cloud. Elle vaut au-delà du cloud : suites collaboratives, gestion documentaire, logiciels métier.

Le référentiel devrait donc s'étendre des échanges « aux frontières » aux solutions acquises par les administrations, au moins pour leurs interfaces d'export et d'administration. Les profils de réversibilité que prépare OpenInterop, à commencer par celui du stockage objet (cf. [fiche cloud](#), §1.4), peuvent fournir cette matière.

3.5 Les mêmes exigences pour les plateformes publiques

Les plateformes que l'État développe ou opère (FranceConnect, ProConnect, La Suite numérique, API de l'État) occupent une place centrale. Elles devraient mettre en œuvre les profils du RGI et passer les mêmes tests que les offres privées (doctrine, principe 8). Une plateforme publique doit pouvoir être remplacée, ou en remplacer une autre, sans réécriture des intégrations.

3.6 Aucun produit imposé aux usagers

Une autorité administrative ne devrait jamais imposer à un usager, une entreprise ou une association l'usage d'un produit déterminé pour échanger avec elle. Une V3 devrait le dire explicitement et en tirer trois règles :

- tout téléservice et toute procédure de dépôt acceptent les formats pivots du RGI (ODF pour les documents modifiables, PDF pour les documents figés), à côté des autres formats qu'ils admettent ;
- les documents que diffuse l'administration le sont au moins dans un format ouvert ;
- un format admis par dérogation, comme OOXML, peut être accepté en plus des formats pivots, jamais exigé seul.

Les usagers devraient disposer d'un point de signalement des manquements. L'autorité chargée du RGI publierait les signalements, les réponses des administrations concernées et leurs délais de mise en conformité. Ce mécanisme simple rendrait le référentiel opposable par les usagers qu'il protège, sans attendre la vérification des solutions.

3.7 Une conformité prouvée et opposable

La conformité au RGI devrait se prouver selon les trois niveaux de la doctrine (§5.3) : autoévaluation publiée par le fournisseur, vérification par un acheteur ou un tiers, essai croisé organisé entre plusieurs mises en œuvre. Elle devrait pouvoir être exigée dans les marchés publics, sur un périmètre défini, comme le propose la commission d'enquête de l'Assemblée nationale. Le rapport de conformité apporte la preuve technique ; les clauses du marché en tirent les conséquences contractuelles, avec leur rédaction propre.

Les autorités administratives devraient publier l'état de conformité de leurs principaux services, à partir des rapports de tests plutôt que de bilans déclaratifs. Un différend sur l'interprétation d'un profil devrait pouvoir être porté devant une instance technique, qui décide de façon motivée et publique.

3.8 Un référentiel vivant

La forme du référentiel conditionne sa mise à jour. Une V3 devrait être :

- **versionnée** : publiée sur un dépôt public, avec des versions datées, un journal des modifications et des identifiants stables pour chaque standard et chaque profil ;
- **exploitable par machine** : catalogue des standards en format structuré (statut, version minimale, dates d'entrée et de fin de vie, lien vers la spécification, profils concernés), d'où la version lisible est générée ;
- **datée** : chaque statut « en fin de vie » comporte une date de retrait prévue, chaque statut « en observation » une date de réexamen ;
- **révisée chaque année**, après une consultation publique d'au moins un mois, avec publication des réponses aux principales observations (doctrine, §8) ;
- **réglementairement souple** : l'arrêté approuve le cadre (critères, statuts, procédure de révision) et renvoie au catalogue et aux profils, dont les révisions suivent une procédure plus légère.

Les résumés tirés de Wikipédia peuvent disparaître : le lien vers la spécification et une phrase d'usage suffisent.

3.9 L'alignement européen

Le RGI est le cadre national d'interopérabilité de la France au sens du Cadre européen. Une V3 devrait reprendre la structure du Cadre européen de 2017 et ses principes, puis ceux de sa nouvelle version, attendue au premier semestre 2027 selon la Cour des comptes. Elle devrait s'articuler avec les obligations d'évaluation de l'Interoperable Europe Act et réutiliser les solutions publiées sur le portail Interoperable Europe (vocabulaires SEMIC, DCAT-AP, eDelivery). Elle devrait aussi alimenter l'observatoire européen des cadres nationaux (NIFO), qui permet de comparer les États membres.

3.10 Une gouvernance ouverte

L'État reste seul compétent pour les normes qui s'imposent à ses systèmes d'information. Mais la co-construction annoncée en 2015 devrait s'étendre au-delà des architectes des ministères : éditeurs, hébergeurs, intégrateurs, collectivités, associations et utilisateurs. Le comité d'évolution devrait être ouvert, se réunir réellement et rendre compte de ses travaux. OpenInterop peut fournir la matière d'une partie des profils avec leurs suites de tests, puis organiser les essais croisés (doctrine, §7).

3.11 L'articulation avec les autres référentiels

Le RGI s'articule avec le référentiel général de sécurité (RGS), le référentiel général d'amélioration de l'accessibilité (RGAA), le référentiel général de gestion des archives et le socle interministériel de logiciels libres (SILL). Le RGS v2 date de 2014 ; sa révision devrait être coordonnée avec celle du RGI, notamment pour les versions de TLS, les algorithmes post-quantiques et les signatures électroniques. Le SILL pourrait signaler, pour chaque logiciel, les profils du RGI qu'il met en œuvre.

4. Revue des standards

Les tableaux suivants proposent des évolutions de statut. Le [catalogue du RGI v2](#) reprend ces propositions standard par standard, sous forme de tableau et de fichier YAML. Ils ne prétendent pas à l'exhaustivité ; chaque proposition devra être instruite selon les critères de la V3 et soumise à consultation.

4.1 À retirer ou à passer en fin de vie

Standard	Statut v2	Proposition v3	Motif
SSL, TLS 1.0 et 1.1	Inclus dans « TLS (SSL) »	Retiré	Abandonnés par l'IETF (RFC 8996, 2021) ; vulnérables
FTP	Recommandé	Retiré	Identifiants et données en clair ; SFTP le remplace
POP3, POP3S	Recommandé	Fin de vie	IMAP et JMAP couvrent l'usage ; synchronisation entre terminaux impossible
H.323, MGCP	Recommandé	Fin de vie	Remplacés par SIP et WebRTC dans les systèmes de visioconférence actuels
UDDI	Recommandé	Retiré	Abandonné depuis le milieu des années 2000
WS-CDL	En observation	Retiré	Jamais finalisé par le W3C ni mis en œuvre
WS-BPEL	Recommandé	Fin de vie	Peu utilisé ; BPMN couvre la modélisation, les moteurs ne sont plus interopérables
SOAP, WSDL, MTOM, XOP, WS-Security, WS-Addressing	Recommandé	Fin de vie pour les nouveaux projets	Maintenus pour les échanges existants (sphère sociale) ; REST et OpenAPI pour les nouveaux
RAML	En observation	Retiré	Abandonné par son écosystème au profit d'OpenAPI
ATOM, AtomPub	Recommandé	Fin de vie, hors usages existants	Remplacés par des API REST et des webhooks ; maintenus pour les flux INSPIRE
CMIS	Recommandé (dans P1)	Fin de vie	Adoption en baisse ; à retirer du profil de fondation
DSML, PeSIT, PRESTO 2.0	Fin de vie	Retiré	Fin de vie déjà prononcée en 2015
IDMEF	Recommandé	Fin de vie	RFC expérimentale peu adoptée ; remplacée par STIX et OCSF
GIF	Fin de vie	Retiré	PNG, WebP et SVG couvrent les usages

Standard	Statut v2	Proposition v3	Motif
Shapefile	Recommandé	Fin de vie	Description publiée par un éditeur, sans organisme de normalisation ; GeoPackage et GeoJSON le remplacent
7z	Recommandé	Fin de vie	Format d'un auteur, sans organisme de normalisation ; ZIP et TAR suffisent
Liste de navigateurs (Chrome 35, IE 10, Firefox 31, Safari 7)	Recommandé	Remplacée	Politique de compatibilité avec les navigateurs à jour, sans liste de versions
XMPP	Recommandé	À réexaminer	Toujours utilisé, mais la messagerie instantanée de l'État (Tchap) repose sur Matrix

4.2 À actualiser

Standard	Référence v2	Proposition v3
TLS	RFC 5246 (TLS 1.2), « SSL » inclus	TLS 1.3 (RFC 8446) recommandé, TLS 1.2 toléré selon le RGS
HTTP	HTTP/1.1 (version 2014) ; HTTP/2 « en cours de mise en place »	Sémantique HTTP (RFC 9110), HTTP/2 (RFC 9113), HTTP/3 (RFC 9114)
OAuth 2.0	RFC 6749	OAuth 2.0 avec ses extensions de sécurité (RFC 9700, BCP 240) ; OAuth 2.1 en observation tant qu'il reste un projet de l'IETF
OpenPGP	RFC 4880	RFC 9580 (2024)
S/MIME	RFC 5750	S/MIME 4.0 (RFC 8551), statut à clarifier
IODEF	RFC 5070	IODEF v2 (RFC 7970)
ODF	ODF 1.2	ODF 1.4 (OASIS, octobre 2025)
PDF, PDF/A	ISO 32000-1 ; PDF/A-1 et 2 (ISO 19005-1 et 2)	PDF 2.0 (ISO 32000-2), PDF/A-4 (ISO 19005-4)
EPUB	EPUB 3 (IDPF)	EPUB 3.3 (recommandation du W3C, 2023)
JSON	RFC 7159	RFC 8259
HTML	HTML5 (W3C), HTML 5.1 en observation	HTML, standard évolutif du WHATWG
Signatures PAdES, XAdES, CAdES, ASiC	Profils <i>Baseline</i> de l'ETSI	Normes ETSI EN 319 1xx, ajout de JAdES (signatures JSON, ETSI TS

Standard	Référence v2	Proposition v3
		119 182-1) ; alignement sur eIDAS 2
SEDA	SEDA, NF Z 44-022 (MEDONA)	SEDA 2.3, ou version ultérieure publiée par le SIAF
SIARD	Observation	SIARD 2 (eCH-0165), à passer en recommandé pour l'archivage des bases de données
WebRTC	En observation	Recommandé : recommandation du W3C et RFC 8825 et suivantes
WebM, VP9, Opus	En observation	Recommandés : libres de redevances, largement mis en œuvre
AMQP	En observation	AMQP 1.0 (OASIS, ISO/IEC 19464) recommandé
YAML	En observation	YAML 1.2.2 recommandé, comme format de description d'API
JPEG 2000	Statut contradictoire	Statut unique, à fixer avec le SIAF et le CNIG
CSV	Fin de vie (sauf usage humain)	Recommandé avec un profil : RFC 4180, UTF-8, schéma de table publié

4.3 À ajouter : standards mûrs absents du RGI v2

Domaine	Standards	Usage
Description d'API	OpenAPI 3.1 et 3.2, JSON Schema, AsyncAPI	Description des API synchrones et événementielles, validation des données
Conventions d'API	Problem Details (RFC 9457), ISO 8601 et RFC 3339 pour les dates	Erreurs et formats communs aux API publiques
Événements	CloudEvents (CNCF), MQTT 5 (OASIS), webhooks signés	Notifications entre systèmes
Identité	SCIM 2.0 (RFC 7643, 7644), WebAuthn et FIDO2	Provisionnement des comptes, authentification sans mot de passe
Identité numérique européenne	OpenID4VP 1.0, OpenID4VCI 1.0, SD-JWT VC, ISO/IEC 18013-5 (mdoc)	Portefeuille d'identité numérique européen (eIDAS 2)
Sécurité de la messagerie	SPF, DKIM, DMARC, MTA-STS (RFC 8461), DANE pour SMTP (RFC 7672)	Authentification de l'expéditeur, chiffrement entre serveurs
Messagerie et agenda	JMAP (RFC 8620, 8621), CalDAV (RFC 4791), CardDAV (RFC 6352), WebDAV (RFC 4918)	Accès aux courriels, agendas, contacts et fichiers
Messagerie instantanée	Matrix	Messagerie fédérée (Tchap)

Domaine	Standards	Usage
Partage de fichiers fédéré	OCM (Open Cloud Mesh, en cours de normalisation à l'IETF)	Partage entre services de fichiers de fournisseurs différents
Certificats	ACME (RFC 8555)	Émission et renouvellement automatiques de certificats
Temps	NTS (RFC 8915)	Synchronisation horaire authentifiée
Échanges B2G	AS4 (OASIS ebMS 3.0, profil eDelivery), Peppol	Échanges de documents sécurisés, notamment marchés et factures
Facturation	EN 16931, UBL 2.1, UN/CEFACT CII, Factur-X	Facturation électronique (Chorus Pro, réforme de 2026)
Données ouvertes	DCAT-AP 3, Table Schema (schema.data.gouv.fr), Apache Parquet	Catalogues, schémas de données tabulaires, diffusion de gros volumes
Web sémantique	JSON-LD 1.1, SKOS, SHACL, DCAT 3	Données liées, vocabulaires contrôlés, validation
Géomatique	OGC API (Features, Tiles, Maps, Records), GeoPackage, Cloud Optimized GeoTIFF	Services géographiques modernes, échange de jeux de données
Images et patrimoine	WebP (RFC 9649), AVIF, IIIF	Images web, diffusion d'images patrimoniales
Vidéo	AV1 (Alliance for Open Media)	Codec vidéo libre de redevances
Cloud	Images de conteneurs OCI, API S3 sous profil de réversibilité, OpenTelemetry (OTLP)	Portabilité des charges, stockage objet, observabilité
Sécurité opérationnelle	CSAF 2.0 (OASIS), STIX et TAXII 2.1, SPDX (ISO/IEC 5962), CycloneDX (ECMA-424), security.txt (RFC 9116)	Avis de sécurité, renseignement sur les menaces, nomenclatures logicielles (Cyber Resilience Act), signalement de vulnérabilités
Santé	Renvoi au cadre d'interopérabilité des systèmes d'information de santé (CI-SIS) de l'ANS, fondé notamment sur HL7 FHIR	Éviter de dupliquer le cadre sectoriel
Texte	CommonMark	Documents textuels structurés légers, déjà évoqués par le RGI v2

Les identifiants des API publiques et des services de l'État devraient aussi être référencés : catalogue api.gouv.fr, identifiants SIREN et SIRET, codes INSEE, identifiants d'adresse de la Base adresse nationale.

4.4 À placer en observation : standards émergents

Standard	Organisme	Motif de l'observation
OAuth 2.1	IETF (projet)	Consolidation d'OAuth 2.0 ; à recommander une fois publié en RFC
IPSIE	OpenID Foundation	Profils d'identité pour l'entreprise (OIDC, SCIM, gestion des sessions)

Standard	Organisme	Motif de l'observation
OpenID Federation	OpenID Foundation	Fédération d'identité à grande échelle, utile au-delà de France-Connect et ProConnect
Algorithmes post-quantiques (ML-KEM, ML-DSA) et TLS hybride	NIST (FIPS 203, 204), IETF	Transition recommandée par l'ANSSI en mode hybride ; à suivre avec le RGS
MLS (RFC 9420) et MIMI	IETF	Chiffrement de bout en bout des messageries de groupe, interopérabilité entre messageries
JMAP Calendars	IETF (projet)	Accès moderne aux agendas
RDF 1.2, SPARQL 1.2	W3C (projets)	Évolution du web sémantique
SECA	Aruba, IONOS, Dynamo	API ouverte de gestion d'infrastructure cloud, encore peu adoptée
OCSF	Linux Foundation	Schéma commun des journaux de sécurité
JPEG XL	ISO/IEC 18181	Image à haute efficacité ; prise en charge inégale par les navigateurs
DNS chiffré (DoT, DoH)	IETF (RFC 7858, 8484)	Confidentialité des requêtes DNS
Dataspace Protocol	Eclipse Foundation (issu de l'IDSA)	Échanges de données dans les espaces de données européens
Model Context Protocol, A2A	Linux Foundation	Accès des agents d'IA aux API et coopération entre agents ; trop récents pour être recommandés

4.5 Questions à trancher

- **Codecs brevetés.** H.264 et H.265 pour la vidéo, AAC pour l'audio restent très répandus. Une V3 peut les admettre par dérogation datée pour la compatibilité, tout en recommandant AV1, VP9 et Opus pour les nouveaux services.
- **OOXML.** Les administrations reçoivent et produisent des documents OOXML. Le RGI peut admettre leur lecture, par dérogation, tout en maintenant ODF et PDF comme formats pivots, comme le faisait le profil P3. La dérogation exclurait la variante transitionnelle et ne permettrait jamais d'exiger OOXML d'un usager (§3.6).
- **SAML et OpenID Connect.** SAML 2.0 reste utilisé par des fédérations établies (enseignement supérieur et recherche). OpenID Connect devrait être recommandé pour tout nouveau service ; SAML 2.0, maintenu pour l'existant.
- **L'API S3.** Interface de fait du stockage objet, elle est contrôlée par un seul fournisseur. Le RGI pourrait référencer un profil ouvert et versionné de cette API, assorti d'une suite de tests, sur le modèle du profil de réversibilité qu'OpenInterop prépare.
- **Les formats de données ouvertes.** CSV reste le format le plus utilisé par les producteurs et les réutilisateurs. Plutôt que de le déclasser, une V3 devrait le profiler (encodage, séparateur, schéma de table) et recommander Parquet pour les gros volumes.

5. Profils proposés pour une V3

N°	Profil	Contenu principal	Évolution par rapport au v2
P1	Fondations des API et du web	HTTP, TLS 1.3, IPv6, URI, UTF-8, JSON, JSON Schema, OpenAPI, Problem Details, ISO 8601, HTML, CSS	Refonte de P1 : retrait de CMIS, ATOM, RAML, SPARQL, des formats multimédias ; ajout des conventions d'API
P2	Identité et annuaires	OpenID Connect, OAuth 2.0 avec RFC 9700, SCIM 2.0, WebAuthn, LDAP, SAML 2.0 pour l'existant, portefeuille européen	Nouveau ; reprend la partie identité de P1 et P2
P3	Messagerie et collaboration	SMTP avec STARTTLS, MTA-STS, SPF, DKIM, DMARC ; IMAP, JMAP ; CalDAV, CardDAV, iCalendar, vCard ; Matrix ; WebRTC, SIP ; WebDAV, OCM ; ODF, PDF	Refonte de P3 : retrait de H.323, MGCP, POP3 ; ajout de la sécurité de la messagerie, de Matrix, de la fédération de fichiers
P4	Archivage	SEDA 2.3, OAIS, PDF/A, ODF, SIARD 2, CSV, JSON, XML, FLAC, TIFF	Actualisation des versions ; statuts cohérents
P5	Géomatique	Profils du CNIG et d'INSPIRE ; OGC API, WMS, WMTS, WFS, GeoPackage, GeoJSON, GML, Cloud Optimized GeoTIFF	Ajout des OGC API et de GeoPackage ; Shapefile en fin de vie
P6	Protection sociale	InterOPS	À réexaminer avec le GIP MDS
P7	Échanges de documents B2G	SFTP, AS2, AS4 (eDelivery), AMQP 1.0, MQTT 5, CloudEvents	Nouveau ; remplace le profil orchestration
P8	Conception de système	UML, BPMN, XMI, OpenAPI, AsyncAPI	Ajout de la description d'API
P9	Signature et confiance	PADES, XAdES, CAdES, JAdES, ASiC (ETSI EN 319 1xx), eIDAS 2	Actualisation ; ajout de JAdES
P10	Données ouvertes et données de référence	DCAT-AP 3, CSV profilé, Table Schema, Parquet, JSON-LD, RDF, SPARQL ; identifiants des données de référence	Nouveau
P11	Facturation électronique	EN 16931, UBL 2.1, UN/CEFACT CII, Factur-X, Peppol	Nouveau ; aligné sur la réforme de 2026
P12	Cloud et réversibilité	OCI, API S3 profilée, OpenTelemetry, formats d'export ouverts	Nouveau ; reprend les travaux d'OpenInterop sur la réversibilité
P13	Sécurité opérationnelle	CSAF 2.0, STIX et TAXII 2.1, IO-DEF v2, SPDX, CycloneDX, security.txt	Nouveau ; remplace IDMEF

N°	Profil	Contenu principal	Évolution par rapport au v2
ex-P2	Web services SOAP	SOAP, WSDL, WS-Security...	Fin de vie pour les nouveaux projets
ex-P7	Orchestration	WS-BPEL, WS-CDL	Retiré

Chaque profil serait publié avec ses versions et options, sa suite de tests et son modèle de déclaration de conformité (cf. §3.1). Les profils sectoriels qui relèvent d'autres cadres (santé, justice, défense) seraient référencés plutôt que dupliqués.

6. Démarche proposée

- 1. Inventaire.** Établir le catalogue des standards du RGI v2 sous forme structurée, avec leur statut actuel ; corriger les incohérences relevées au §2.5. Ce travail ne demande aucun arbitrage. OpenInterop en publie une première version : le [catalogue du RGI v2](#), en tableau et en YAML.
- 2. Cadre.** Fixer les critères (dont le critère d'ouverture éliminatoire), les statuts datés, la procédure de dérogation et la procédure de révision. C'est la partie qui relève de l'arrêté.
- 3. Profils prioritaires.** Commencer par les profils dont dépendent les autres et dont les standards existent : fondations des API (P1) et identité (P2). Publier pour chacun une suite de tests et organiser un premier essai croisé.
- 4. Consultation.** Soumettre le cadre, le catalogue révisé et les premiers profils à une consultation publique d'au moins un mois ; publier les réponses.
- 5. Révision annuelle.** Ajouter chaque année de nouveaux profils et réexaminer les statuts, selon un calendrier public.

OpenInterop peut contribuer à chacune de ces étapes : état de l'art par domaine, profils et suites de tests, essais croisés entre éditeurs, propositions de statut.

Références

- Référentiel général d'interopérabilité, version 2.0, DINSIC, décembre 2015 ; approuvé par arrêté du 20 avril 2016.
- Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ; décret n° 2007-284 du 2 mars 2007.
- Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, article 4.
- Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.
- CNLL, Ploss Auvergne-Rhône-Alpes, La Mouette, « Le CNLL demande à l'INPI de respecter le RGI version 2 afin de permettre l'utilisation de l'Open Document Format (ODF) pour les dépôts des brevets en France », communiqué du 26 juin 2019.
- Cour des comptes, *Les outils bureautiques et collaboratifs au sein de l'État*, rapport d'initiative citoyenne, octobre 2026.
- 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, *New European Interoperability Framework*, 2017 ; *European Interoperability Framework*, version 1.0, 2004 ; méthode CAMSS.
- Règlement (UE) 2024/903 (Interoperable Europe Act) ; règlement (UE) 2023/2854 (Data Act) ; règlement (UE) 2024/1183 (eIDAS 2).

-
- OpenInterop : [doctrine](#), [état de l'art](#), [fiche transverse](#), [fiche collaboratif](#), [fiche cloud](#), [fiche cybersécurité](#).