

CHARTE D'INTEROPÉRABILITÉ DES DONNÉES

INTRODUCTION

Les infrastructures et services numériques des territoires (réseaux, objets connectés, plateformes de données, logiciels métiers, systèmes de supervision et de pilotage) sont déployés par un écosystème composé d'acteurs multiples, de technologies hétérogènes et de chaînes de valeur imbriquées. Dans ce contexte, l'interopérabilité peut être définie par la capacité à **connecter des équipements et des logiciels qui ne proviennent pas nécessairement des mêmes fournisseurs afin qu'ils puissent « opérer », fonctionner et interagir entre eux.**

Il est techniquement possible de rendre tout élément interopérable avec son écosystème. **La question n'est donc pas de savoir si l'interopérabilité est possible, mais d'en réduire la complexité.** Par ailleurs, si l'interopérabilité est nécessairement pensée à la conception d'un projet, elle est plus rarement anticipée dans l'évolution de ce projet et introduit des coûts significatifs.

Par la présente charte, les entreprises membres d'InfraNum affirment une ambition commune : **faire de l'interopérabilité un standard de fait au service des collectivités, des opérateurs et de l'ensemble des parties prenantes**, afin de réduire les coûts d'intégration, accélérer les déploiements, renforcer la résilience opérationnelle, faciliter la mutualisation et préserver la liberté de choix.

À l'échelle européenne et internationale, cette ambition s'est traduite par l'émergence de cadres structurants visant à définir des mécanismes communs d'interopérabilité. Parmi eux, les **Minimal Interoperability Mechanisms (MIMs)** constituent un socle de référence reconnu pour les territoires intelligents et durables.

L'interopérabilité suppose un effort structuré, progressif, coordonné et mesurable. Les situations de départ sont hétérogènes, les contraintes techniques et contractuelles réelles, et les maturités variables. Cette charte exprime donc un engagement volontaire, progressif et vérifiable. Chaque signataire **s'engage volontairement à se mettre en trajectoire vers l'interopérabilité telle que décrite ci-après, en tenant compte de ses contraintes et de la maturité de ses produits et services, et à rendre cette trajectoire lisible par des éléments de preuve adaptés.**

POURQUOI L'INTEROPÉRABILITÉ ?

L'interopérabilité constitue un enjeu stratégique. Elle désigne la capacité, **dans la durée, à échanger des données et des services, à les comprendre sans ambiguïté, à en maîtriser la qualité, et à faire évoluer les systèmes sans dépendance excessive** à un fournisseur, un format ou une architecture. Elle est un levier **de souveraineté, d'optimisation de coûts**, et rend les projets sur-mesure plus rapides à intégrer, plus fiables à opérer, et plus faciles à faire évoluer. Cela en fait un facteur essentiel pour **la longévité et la souveraineté** des projets.

Pour plus d'informations, voir la **Fiche interopérabilité (InfraNum)** et la **Fiche Interopérabilité (CSF IN)**

ARTICLE 1 - OBJET ET PÉRIMÈTRE

La présente charte définit un socle commun d'engagements visant à faciliter l'intégration et l'exploitation conjointe des solutions proposées par les signataires, ainsi que la circulation maîtrisée des données associées, sur des projets relatifs aux infrastructures et services numériques territoriaux (connectivité, capteurs, supervision, plateformes, applications, exploitation, maintenance, etc.).

Elle s'applique aux produits, services, API, jeux de données, connecteurs, composants logiciels et matériels mis sur le marché ou opérés par les signataires, dans la mesure où ces éléments participent à la production, au transport, au stockage ou à l'usage de données utiles aux projets territoriaux.

Elle vise une cohérence avec les cadres européens et pratiques sectorielles (voir **ANNEXE II**).

Ses signataires s'inscrivent dans une démarche volontaire d'amélioration continue. Elle est mise en œuvre dans le respect des obligations contractuelles et conditions tarifaires associées, et n'est ni un engagement contractuel, ni une certification.

ARTICLE 2 - DÉFINITION OPÉRATIONNELLE DE L'INTEROPÉRABILITÉ

Au sens de la présente charte, l'interopérabilité recouvre 4 dimensions complémentaires indissociables :

1. **Interopérabilité technique** : capacité à connecter des systèmes hétérogènes au moyen d'interfaces documentées, stables, sécurisées et testables.
2. **Interopérabilité sémantique** : capacité à échanger des données dont le sens est compris de manière identique d'un acteur à l'autre (modèles, référentiels, métadonnées, unités, conventions).
3. **Interopérabilité organisationnelle** : capacité à faire vivre l'échange dans la durée (gouvernance, responsabilités, gestion des versions, support, qualité, évolutions).
4. **Interopérabilité juridique/politique** : capacité des parties prenantes à converger vers des règles communes d'usage, de partage et de responsabilité, garantissant la confiance, la réversibilité, la souveraineté des choix et la possibilité de coopération à l'échelle d'un territoire ou d'un écosystème.

ARTICLE 3 - PRINCIPES DIRECTEURS

Les signataires se reconnaissent dans les principes suivants :

1. **Ouverture maîtrisée** : favoriser l'usage de standards et de spécifications publiées, sans fragiliser la sécurité ni les obligations contractuelles.
2. **Réversibilité et pérennité** : permettre l'évolution des systèmes et la reprise des données sans dépendance injustifiée.
3. **Transparence** : documenter ce qui est nécessaire à l'intégration, à l'exploitation et à l'audit et les conditions tarifaires associées.
4. **Proportionnalité** : adapter l'effort au risque, à l'usage et au contexte.
5. **Progressivité** : s'inscrire dans une trajectoire d'amélioration continue et objectivable.

ARTICLE 4 - ENGAGEMENTS DES SIGNATAIRES

Les signataires reconnaissent que l'interopérabilité résulte d'un ensemble cohérent de pratiques techniques, organisationnelles et documentaires. Ils s'engagent à faire évoluer leurs pratiques en s'insérant dans une trajectoire (**article 4.5**) qui répond dispositions suivantes :

4.1 Des solutions reproductibles et évolutives

L'interopérabilité technique repose sur l'existence d'interfaces documentées, stables et sécurisées. Elle vise à permettre l'intégration reproductible de solutions hétérogènes, sans dépendance excessive à des développements spécifiques.

Les signataires s'engagent à mettre à disposition, lorsque cela est pertinent pour les collectivités, **des interfaces applicatives** :

- Dont les **spécifications sont suffisamment détaillées** pour permettre leur implémentation par des tiers autorisés et la réutilisation des données ;
- En adoptant des **pratiques reconnues en matière de conception d'API** ;
- En garantissant **l'accès uniforme aux données de contexte** par ces API.

L'ouverture des interfaces ne saurait toutefois compromettre les exigences de sécurité (**article 4.6**) ou les obligations contractuelles ; elle doit s'inscrire dans un **cadre maîtrisé, proportionné et documenté**.

4.2 Des données compréhensibles, découvrables et réutilisables

L'interopérabilité sémantique constitue la condition première d'un échange de données réellement exploitable. Elle implique que les objets, événements, mesures et états décrits par un système puissent être interprétés de manière identique par un autre, indépendamment des technologies employées. Elle suppose en particulier que les concepts métier soient définis de manière explicite, que les unités et conventions soient stabilisées, et que les référentiels associés (temps, localisation, périmètres, statuts) soient compris sans ambiguïté.

Les signataires s'engagent à **structurer leurs données selon des modèles explicites, documentés et accessibles** :

- Ils conviennent de privilégier des **extensions maîtrisées ou à des modèles sectoriels ouverts**, en veillant à préserver **la compatibilité et la compréhension par des tiers**.
- Lorsque des modèles internes ou propriétaires sont utilisés, les signataires s'engagent à fournir un alignement formalisé vers un modèle ouvert, sous la forme de **dictionnaires de données, de schémas, et de règles de correspondance maintenues dans le temps**. Cet alignement doit permettre à un tiers autorisé de comprendre le sens, le format et les transformations nécessaires sans dépendre d'une connaissance implicite ou d'accords ad hoc.
- Les signataires veillent à **explicitement les métadonnées nécessaires pour découvrir et interpréter les données** de manière systématique sur un périmètre pertinent, et à associer aux données mises à disposition **les informations nécessaires à leur compréhension et à leur usage responsable**.

L'ensemble des modèles ouverts et des standards communément utilisés par le secteur sont répertoriés en **Annexe II**.

4.3 Des données de qualité et traçables

La circulation des données ne peut produire de valeur que si leur qualité est connue et maîtrisée. Les signataires reconnaissent que l'interopérabilité implique **la traçabilité et la transparence sur l'origine, la transformation et les limites des données échangées**.

Les signataires s'engagent :

- À mettre en place des **identifiants stables et traçables** permettant de relier les données aux objets qu'elles décrivent par un adressage **bout-en-bout** ;
- À assurer une **traçabilité et une historisation robustes**, proportionnée aux usages ;

- À définir des **mécanismes internes de suivi** de la qualité des données et à définir des indicateurs pertinents, adaptés à la nature des services concernés ;
- À procurer un **suivi dans le temps**, y compris en cas d'évolution, de remplacement d'équipement ou de changement de périmètre ;
- À faciliter **l'export de données** en proposant des exports complets et des procédés de migrations testés.

4.4 Gouvernance et cycle de vie

L'interopérabilité s'inscrit dans le temps long : il s'agit de **l'interopérabilité organisationnelle**. Elle suppose une gouvernance claire, des responsabilités identifiées et une gestion maîtrisée des évolutions pour garantir la stabilité, la prévisibilité et la confiance dans les relations d'intégration.

Chaque signataire s'engage à :

- **Organiser en interne la responsabilité de l'interopérabilité de ses offres**, par exemple par la désignation d'un référent ou d'une fonction identifiée.
- Encadrer les évolutions affectant les modèles de données, les interfaces ou les modalités d'échange par des **procédures de gestion de version explicites**.
- Annoncer, dans des délais raisonnables, les **modifications substantielles** susceptibles d'impacter les partenaires ou les clients, afin de permettre l'adaptation des systèmes interconnectés.

4.5. Evaluation et trajectoires

Conformément aux principes de **l'article 3**, les signataires visent à mettre en place une trajectoire progressive et proportionnelle pour répondre aux dispositions des articles de la charte.

Les éditeurs et fabricants de solutions IoT s'engagent à :

- Dans les 12 mois suivants la signature de cette charte, mettre en place une démarche de **transparence**, par **la désignation d'une personne référente** sur l'interopérabilité au sein de l'organisation, et par **la publication des actions dès à présent mises en œuvre** concernant le périmètre de la charte ;
- Dans un second temps, entrer dans une démarche **d'alignement** en formulant **une feuille de route individuelle** volontaire établissant **les actions à mettre en place pour s'aligner** sur les éléments de cette charte. Ce plan d'action, ou certains de ses modules, sera rendu public, dans le respect du secret des affaires et des droits de propriété intellectuelle.

Les intégrateurs s'engagent à :

- **Promouvoir et diffuser les principes d'interopérabilité** de cette charte auprès de leur écosystème
- **Privilégier les solutions alignées avec les articles** de la charte dans leur activité.

Chaque article de la charte est traduit en modules, avec différents éléments de preuves, que les signataires peuvent intégrer à leur plan d'action respectif selon leurs priorités et actions (voir **ANNEXE I**).

4.6 Sécurité, conformité réglementaire et confiance

L'interopérabilité ne peut se concevoir au détriment de la sécurité des systèmes ou de la protection des données. Elle doit également s'inscrire en cohérence avec les cadres réglementaires et normatifs applicables, et leurs **exigences liées à l'interopérabilité, la portabilité et la transparence des échanges de données**.

L'ouverture maîtrisée des systèmes doit renforcer la confiance entre acteurs et non créer de nouvelles vulnérabilités. Les signataires s'engagent à **mettre en œuvre des mécanismes appropriés d'authentification, d'autorisation et de traçabilité des accès aux interfaces et aux données**, dans le respect des cadres réglementaires et normatifs.

Les signataires prennent en compte, dans leurs engagements d'interopérabilité, les dispositions pertinentes des **règlements européens**. Ils s'appuient, lorsque pertinent, sur les **référentiels normatifs** encadrant la sécurité des interfaces et des échanges de données dans un contexte multi-acteurs. L'ensemble des cadres reconnus par les signataires se retrouve en **ANNEXE III**.

ANNEXE I

BOÎTE À OUTILS

Indicateurs et livrables techniques par thématique

Les modules ci-dessous sont des exemples de bonnes pratiques pour les plans d'actions des entreprises et pour les appels d'offre des collectivités territoriales. Ils ne sont pas des exigences systématiques, et leur adoption dépend de la trajectoire individuelle et volontaire de chaque signataire.

ARTICLE 4.1 : INTERFACES

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Politique d'API ouvertes	Garantir l'accès uniforme aux données de contexte	% d'API documentées ; MTTR d'intégration ; disponibilité >99,5 %	MIM1 Context Information ; pour les bâtiments voir R2S Connect (SBA)	Specs OpenAPI/AsyncAPI publiées ; portail/sandbox ; changelog + policy de versioning ; tests d'API (contract tests) & rapports.

ARTICLE 4.2 : MODÈLES DE DONNÉES

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Modèles de données harmonisés	Parler le même langage métier	% d'entités au format de référence ; défauts de mapping/sprint	MIM2 Data Models; NGSI-LD	Catalogue de schémas (JSON Schema/SHACL) ; dictionnaire métier ; guide d'extension ; tests de validation de payloads ; matrice de mapping.
Catalogue et métadonnées	Rendre les jeux de données découvrables et réutilisables	% catalogué ; fraîcheur ; taux de réutilisation	DCAT	Catalogue (export) ; fiches datasets complètes (owner, licence, sensibilité...) ; workflow de validation ; API/endpoint de découverte.

ARTICLE 4.3 : TRAÇABILITÉ DES DONNÉES

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Qualité, traçabilité et lignée des données	Instaurer la confiance par la preuve, permettre l'historisation et un suivi fiable sans rupture	Taux d'anomalies ; complétude ; traçabilité end-to-end	Qualité de données	DQ ruleset ; rapports de contrôles ; backlog anomalies ; lineage (runs, versions, sources) ; tableau de bord qualité.
Référentiels et identifiants des objets	Adresser et suivre chaque objet de bout en bout	Taux d'objets non résolus ; doublons détectés/corrigés	Référentiels IoT	Politique d'identification ; référentiel "maître" ; règles de dédoublonnage ; journal de fusion/retrait ; table de correspondances.
Réversibilité et portabilité	Éviter le verrouillage et faciliter les migrations	Durée réelle de sortie ; % export sans perte ; coûts de migration	Réversibilité contractuelle	"Exit plan" + clauses ; scripts d'export ; laC repo ; PV de tests de restauration ; PV de tests de migration ; inventaire dépendances.

ARTICLE 4.4 : GOUVERNANCE

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Gouvernance de l'interopérabilité	Établir responsabilités, rôles et règles du jeu	Décisions tracées ; taux de conformité ; délais d'arbitrage	4 couches d'interopérabilité, guide juridique Cerema	Charte/RACI signés ; compte-rendus de comité ; registre des décisions ; politique versioning/dépréciation.
Interopérabilité intégrale	Traiter simultanément les 4 couches de l'interopérabilité	Couverture par couche ; risques résiduels ; jalons atteints	Cadre européen d'interopérabilité et RGI	Dossier "interopérabilité par cas d'usage" ; matrice 4 couches ; décisions d'arbitrage ; preuves (contrats, schémas, tests, sécu).

ARTICLE 4.5 : TRAJECTOIRES ET ÉVALUATION

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Alignement MIMs et MIM meter	Objectiver la conformité aux MIMs	Score MIM global ; progression/ semestre ; écarts critiques	MIM1/2/3/4/6 ; MIM meter	Grille d'évaluation ; score par MIM ; "evidence pack" ; rapports d'audit ; plan d'actions daté.
Paliers d'exigence et trajectoires	Proposer un chemin de maturité	Modules au palier cible ; délais tenus ; budget d'intégration	Gestion de maturité	Référentiel de paliers ; roadmap ; engagements contractuels ; tableaux de bord de progression ; revues de jalons.
Évaluation par cas d'usage	Fixer les exigences d'interopérabilité par domaine	% cas d'usage couverts ; incidents par domaine ; coût d'intégration	Cadres métiers (eau, déchets, énergie...)	Spécifications par cas ; jeux de tests ; PV de recette ; métriques (latence, fraîcheur, qualité) ; REX formalisé.
Tests et conformité	Prouver l'interopérabilité avant production	Taux de succès ; défauts bloquants ; non-régressions	Cadre ?	Suite de tests (CI) ; rapports charge ; rapports contract tests ; rapports sécu ; critères de conformité publiés.

ARTICLE 4.6 : SÉCURITÉ

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Sécurité by design	Sécuriser objets, flux et plateformes	Vulnérabilités corrigées ; MTDD/ MTTR sécu ; taux de chiffrement	MIM6 Security	Modèles de menace ; politiques IAM ; preuves chiffrement ; rapports scans CI/CD ; SBOM ; pentest / audit ; runbooks sécurité.
Protection des données sensibles	Conformité RGPD et transparence	Incidents privacy ; demandes d'accès ; délais d'effacement	MIM4 Trust ; RGPD	Registre des traitements ; DPIA ; politique de conservation ; procédures droits (accès/ effacement) ; preuves masquage/ pseudo ; logs d'accès.
Cybersécurité IoT terrain	Maîtriser le risque du capteur à la plateforme	Taux de correctifs ; incidents terrain ; dérives non conformes	Guide Cybersécurité de l'IoT CSF IN	Procédure provision+B2:G28ing ; PKI/certificats ; politique OTA + signatures ; inventaire objets ; tests sécu IoT ; playbooks incident.

AUTRES INDICATEURS

INTITULÉ	OBJECTIF	INDICATEURS	CADRES	EXEMPLE PREUVES / LIVRABLES
Connectivité et réseaux	Garantir l'interopérabilité du transport et de l'applicatif	Pertes de paquets ; disponibilité ; temps d'activation	Normes radio	Schémas réseau ; preuves mTLS/VPN ; tests QoS ; monitoring liens ; procédures bascule.
Compatibilité plateforme avec les équipements et les systèmes	Fiabiliser le parc objet	% capteurs certifiés ; retours terrain ; pannes prématurées	Qualification produit IoT	Procès-verbal de qualification ; fiches capteurs ; résultats de tests interop ; politique firmware/OTA ; liste capteurs "approuvés".
Interopérabilité des plateformes IoT	Accueillir capteurs/plateformes hétérogènes	Temps d'onboarding équipement ; % connecteurs réutilisables	Protocoles normalisés IoT	Matrice protocoles supportés ; connecteurs certifiés ; tests d'intégration par constructeur/LNS ; exemples payloads validés ; rapports de non-régression.
Souveraineté et localisation des données	Maîtriser hébergement, dépendances et réversibilité	% data en UE ; audits fournisseurs ; coûts de sortie maîtrisés	Souveraineté numérique	Attestations localisation ; SBOM ; KMS/gestion clés ; audits fournisseurs ; PV tests réversibilité ; registre dépendances critiques.
Support multi-acteurs	Contractualiser la qualité de service bout-en-bout	Respect SLA ; temps d'escalade ; satisfaction client	ITSM/SLM; OLA/SLA	Catalogue de services ; SLA/OLA ; tickets & métriques ; procédure escalade ; comités de suivi.
Maintenance logicielle	Maintenir un parc sécurisé et à jour	Taux de réussite OTA ; dérives de version ; incidents post-maj	Gestion du cycle de vie	Calendrier patching ; rapports vuln ; PV upgrades ; SBOM ; SLA MCO + reporting mensuel.
Documentation et kits d'intégration	Réduire le coût d'onboarding partenaires	Délais d'intégration ; tickets support ; NPS développeurs	Catalogue API	Portail + docs versionnées ; kits (repo) ; exemples validés ; changelog ; temps d'onboarding mesuré.
Supervision et observabilité	Détecter, diagnostiquer, expliquer	Disponibilité ; MTTR/MTTD ; incidents évités	Observabilité et OpenTelemetry	Portail + docs versionnées ; kits (repo) ; exemples validés ; changelog ; temps d'onboarding mesuré.
Formation et acculturation	Aligner compétences et pratiques d'interopérabilité	Taux de certification ; autonomie ; tickets N1	Catalogues de formation interopérabilité	Plan de formation ; supports ; taux de complétion ; évaluations ; playbook versionné ; sessions REX.
Ouverture et partage (Open Data)	Publier ce qui peut l'être pour innover	Jeux ouverts ; téléchargements ; réutilisations	Open Data ; licences ouvertes	Jeux publiés + métadonnées ; licence ; preuve anonymisation ; pipeline/release notes ; stats d'usage.

ANNEXE II

MODÈLES ET STANDARDS

COUCHE 1 - CADRES RÉGLEMENTAIRES ET POLITIQUES

Le «pourquoi» : ce qui encadre, oriente ou impose l'interopérabilité. Du contraignant au volontaire.

INITIATIVE / STANDARD	PORTEUR(S)	STATUT	PÉRIMÈTRE ET FONCTION	ADOPTION
Interoperable Europe Act (2024)	Commission européenne ; Parlement et Conseil de l'UE	Règlement UE (contraignant)	Rend obligatoires les évaluations d'interopérabilité pour les services publics numériques européens. Crée le Comité Interoperable Europe et un portail de solutions réutilisables.	En vigueur depuis janvier 2025. Applicable à toutes les administrations publiques de l'UE.
Data Act (2024) / Data Governance Act (2022)	Commission européenne ; Parlement et Conseil de l'UE	Règlement UE (contraignant)	Data Act : droit d'accès aux données générées par les objets connectés ; exigences d'interopérabilité des espaces de données. DGA : cadre de confiance pour le partage de données.	Data Act applicable à partir de septembre 2025. DGA en vigueur depuis septembre 2023. Structurent juridiquement l'économie de la donnée en UE.
Directive INSPIRE (2007/2/CE)	Commission européenne (DG ENV) ; transposée par les États membres	Directive UE (contraignante)	Interopérabilité des données géospatiales des autorités publiques. 34 thèmes de données, services de découverte, visualisation, téléchargement, transformation.	En vigueur depuis 2007. Transposée dans les 27 États membres. Infrastructure opérationnelle.
EIF4SCC (European Interoperability Framework for Smart Cities & Communities)	Commission européenne (DG DIGIT + DG CONNECT) ; Deloitte, KU Leuven	Recommandation officielle (CE)	Cadre global englobant : 5 principes, 7 éléments d'interopérabilité (technique, sémantique, organisationnelle, culturelle, juridique), modèle de gouvernance intégrée. Positionne les MIMs comme composant opérationnel.	Staff Working Document (2021). Disponible dans toutes les langues UE. Cas d'usage : Lyon, Flanders, etc. Cadre le plus englobant.
Living-in.EU / MIMs Plus	Eurocities, OASC, ENoLL, ERRIN, CEMR ; soutenu par la CE	Engagement volontaire (politique)	Déclaration « Join, Boost, Sustain ». Déclinaison européenne des MIMs (MIMs Plus) avec contexte réglementaire UE. Groupes de travail thématiques (jumeaux numériques, espaces de données, plateformes).	217 signataires (villes, régions, États membres), 230 supporters. Initiative politique la plus large pour les villes intelligentes en UE.
Guide pour la souveraineté et l'interopérabilité des données pour les collectivités territoriales et leurs fournisseurs	Cerema	Guide de recommandations	Panorama des enjeux de l'interopérabilité, des solutions techniques d'interopérabilité, des types de plateformes existantes, des initiatives européennes, des dispositions juridiques à mettre en place, et un outil d'auto-évaluation	Sortie en septembre 2026, rédigé avec un consortium de collectivités et d'entreprises

COUCHE 2 - NORMALISATION ET MÉCANISMES D'INTEROPÉRABILITÉ

Le « cadre de jeu » : normes officielles et mécanismes minimaux qui structurent l'interopérabilité entre acteurs.

INITIATIVE / STANDARD	PORTEUR(S)	STATUT	PÉRIMÈTRE ET FONCTION	ADOPTION
ISO/TC 268 / ISO 37100 series	ISO (Organisation internationale de normalisation)	Norme officielle (internationale)	Normes pour les villes durables : ISO 37101 (système de management), ISO 37120/37122 (indicateurs smart cities), ISO 37104/37105 (mise en œuvre). Terminologie, KPI, cadre de gouvernance.	23+ normes publiées, 19+ en cours. Dizaines de pays participants. Sous-comités SC1 (infrastructures) et SC2 (mobilité).
CEN/TC 465 + SF-SSCC	CEN (organisme européen de normalisation) ; Sector Forum CEN-CENELEC-ETSI	Norme officielle (européenne)	Normalisation européenne complémentaire à l'ISO/TC 268 pour les besoins spécifiquement européens. Coordination avec ETSI et les MIMs.	Créé en octobre 2019. Articulation formelle avec ISO/TC 268, IEC SyC Smart Cities et ITU-T SG20.
ITU-T SG20 / Y.4505	UIT-T (Union internationale des télécommunications)	Norme officielle (internationale)	Groupe d'étude dédié à l'IoT et aux villes intelligentes. Recommandation Y.4505 : format standardisé des MIMs. Cadre international pour les architectures smart city.	Cadre adopté pour la formalisation internationale des MIMs. Articulation avec OASC, CEN/TC 465, ISO/TC 268.
OASC MIMs (Minimal Interoperability Mechanisms)	OASC (Open & Agile Smart Cities & Communities)	Adopté par consensus de villes	10 MIMs : contexte (MIM1/NGSI-LD), modèles de données (MIM2), écosystème (MIM3), données personnelles (MIM4), IA (MIM5), sécurité (MIM6), etc. Mécanismes minimaux et suffisants, vendor-neutral.	150+ villes dans 30+ pays (100M citoyens). Format ITU-T Y.4505. Slovaquie : 1er pays à exiger les MIMs. Ratifiés par le Council of Cities.
Grille d'évaluation du niveau d'interopérabilité	Cerema	Outil d'évaluation	Grille d'auto-évaluation de conformité avec les MIMs	Sortie en septembre 2026, développée par Kereval

COUCHE 3 - MODÈLES DE DONNÉES ET SÉMANTIQUE

Le « langage commun » : comment structurer et interpréter les données de manière uniforme entre acteurs.

INITIATIVE / STANDARD	PORTEUR(S)	STATUT	PÉRIMÈTRE ET FONCTION	ADOPTION
NGSI-LD (ETSI ISG CIM)	ETSI ISG CIM / TC DATA ; issu de la communauté FIWARE et de l'OMA	Norme officielle (ETSI)	Modèle d'information contextuelle (entités, propriétés, relations) et API associée. Format JSON-LD. Socle technique du MIM1. Cible : smart cities, jumeaux numériques, agriculture, industrie.	Spécification ETSI (850+ membres, 65 pays). Tests Plugtests : 88 % d'interopérabilité. Référencée dans Horizon Europe.
Smart Data Models	FIWARE Foundation, TM Forum, IUDX (Inde), OASC	Adopté par le marché (programme ouvert)	800+ modèles de données harmonisés compatibles NGSI-LD dans 13+ domaines. Schémas JSON, spécifications, URI, exemples. Licence libre. Implémentation de référence du MIM2.	170+ contributeurs. Utilisés dans de nombreux projets UE. Serveur MCP pour intégration IA disponible.
SAREF (ETSI TC SmartM2M)	ETSI TC SmartM2M ; initiée par la CE (étude TNO)	Norme officielle (ETSI)	Ontologie modulaire de référence pour l'IoT. Extensions sectorielles : SAREF4City, SAREF4Energy, SAREF4Building, SAREF4Water, SAREF4Agri, SAREF4Grid.	Standard ETSI officiel (TS 103 264 + extensions). Financée par la CE. Dans la feuille de route numérique européenne.
DCAT / DCAT-AP	W3C (DCAT) ; CE / ISA ² (DCAT-AP)	Norme W3C - obligatoire pour les portails UE	Vocabulaire de métadonnées pour cataloguer des jeux de données. Découvrabilité, licence, qualité, provenance. DCAT-AP : profil européen obligatoire pour les portails open data.	Recommandation W3C. DCAT-AP utilisé par data.europa.eu et des milliers de collectivités. Aligné avec MIM3.
CityGML / OGC Standards	OGC (Open Geospatial Consortium)	Norme OGC - reprise en norme ISO	Standards géospatiaux ouverts : CityGML (modèle 3D de villes), SensorThings API (capteurs), IndoorGML, 3D Tiles, WMS/WFS, OGC APIs.	500+ membres (gouvernements, industrie, recherche). Standards ISO 19100. Déploiements dans des centaines de villes.

COUCHE 4 - INTERFACES ET PROTOCOLES APPLICATIFS

Le « comment les systèmes dialoguent » : API, protocoles d'échange et interfaces normalisées.

INITIATIVE / STANDARD	PORTEUR(S)	STATUT	PÉRIMÈTRE ET FONCTION	ADOPTION
NGSI-LD API	ETSI ISG CIM	Norme officielle (ETSI)	API RESTful pour publier, requêter, souscrire aux informations de contexte. Implémentée par les Context Brokers (Orion-LD, Scorpio, Stellio). Socle du MIM1.	Plusieurs implémentations open source certifiées. Intégrée dans des dizaines de plateformes urbaines en UE.
TM Forum Open APIs	TM Forum	Adopté par le marché (consortium industriel)	Suite de 60+ API standardisées pour les services numériques (catalogue, commande, facturation, gestion de ressources). Compatibles REST/JSON. Complémentaires de NGSI-LD pour la couche service.	900+ membres (opérateurs, éditeurs, intégrateurs). Adoptées par les principaux opérateurs télécoms mondiaux.
TALQ Smart City Protocol	TALQ Consortium (fondé 2012 : Signify, Zumtobel, Schréder, Itron...)	Adopté par le marché (consortium industriel)	Protocole OpenAPI/REST pour l'interopérabilité CMS - ODN (réseaux d'équipements terrain). Éclairage, déchets, parking, trafic, environnement, armoires électriques. Modèle de données JSON.	50+ membres. V2.7.0 (avril 2026). Programme de certification. Spécification publique sur GitHub. 100+ villes ciblées.
MQTT (OASIS) / CoAP (IETF)	OASIS (MQTT) ; IETF (CoAP)	Norme internet (OASIS/IETF)	MQTT : protocole publish/subscribe léger, largement adopté pour l'IoT. CoAP : protocole requête/réponse pour réseaux contraints (UDP). Complémentaires : MQTT pour le temps réel, CoAP pour les capteurs légers.	MQTT : utilisé par AWS IoT, Azure IoT, Google Cloud IoT. CoAP : intégré dans LwM2M (OMA). Omniprésents dans les déploiements smart city.
oneM2M	Partenariat mondial : ETSI, ARIB, ATIS, CCSA, TTA, TSDSI, TTA	Norme officielle (partenariat mondial)	Couche de services communs IoT : enregistrement, découverte, gestion de données, sécurité, interfonctionnement entre plateformes hétérogènes. Indépendante du transport réseau. Intégration avec SAREF.	7 organismes de normalisation (Europe, Amériques, Asie). Release 4 publiée. Déploiements en smart cities, e-santé, industrie.

COUCHE 5 - CONNECTIVITÉ ET TRANSPORT IoT

Le « tuyau » : technologies LPWAN et réseaux de communication des capteurs et objets connectés.

INITIATIVE / STANDARD	PORTEUR(S)	STATUT	PÉRIMÈTRE ET FONCTION	ADOPTION
LoRaWAN	LoRa Alliance (association ouverte, fondée 2015)	Adopté par le marché - bande libre ISM	LPWAN longue portée (2-15 km), très basse consommation, bande ISM libre (868 MHz EU). Réseaux publics (opérateurs), privés ou communautaires. Bidirectionnel. Certification LoRaWAN.	125M+ équipements déployés (déc. 2025, CAGR 25 %). 170+ opérateurs. 625+ devices certifiés. Top marchés : comptage, bâtiment, villes. Réseau déployable sans licence.
NB-IoT (3GPP)	3GPP (normalisé Release 13+)	Norme télécom (3GPP) - spectre licencié	LPWAN cellulaire étroite bande (180 kHz) sur infrastructure 4G/5G existante. Pénétration indoor forte. Pas de mobilité. Intégré à la feuille de route 5G (partie du 5G mMTC).	137 réseaux dans 69 pays (GSMA, 2025). ~90 % des connexions en Chine. Adoption limitée hors Asie. AT&T a arrêté le NB-IoT en 2025 (migration LTE-M).
LTE-M / Cat-M1 (3GPP)	3GPP (normalisé Release 13+)	Norme télécom (3GPP) - spectre licencié	LPWAN cellulaire 1,4 MHz sur LTE existant. Mobilité, voix (VoLTE), débit plus élevé que NB-IoT. Compatible handover. Intégré à la feuille de route 5G.	115 réseaux dans 35+ pays (GSMA, 2025). Forte adoption en Amérique du Nord et Australie. Préféré par les opérateurs pour le remplacement du 2G/3G.
Sigfox 0G (UnaBiz)	UnaBiz (repreneur de Sigfox en 2022)	Protocole propriétaire - bande libre ISM	LPWAN ultra-basse consommation, ultra-bas coût. 140 messages/jour, 12 octets. Réseau opéré centralement. Programme Sub0G pour tracking logistique à très bas coût.	15M devices connectés. 70+ pays, 1 500 antennes en France. Redressement judiciaire en France (sept. 2025). Pérennité à surveiller.
Wi-SUN	Wi-SUN Alliance	Adopté par le marché - bande libre ISM	Réseau mesh IPv6 auto-cicatrisant pour smart grid, éclairage, comptage. Portée longue, haut débit relatif. Basé sur IEEE 802.15.4g. Interopérable IP natif.	Wi-SUN Alliance : 300+ membres. Utilisé par les utilities (compteurs électriques) et éclairage public. Fort au Japon et Amérique du Nord.

ANNEXE III

NORMES ET CADRES DE CYBERSÉCURITÉ

CADRES RÉGLEMENTAIRES EUROPÉENS CONCERNANT LES DONNÉES

- **Règlement européen sur les données (Data Act, règlement 2023/2854)** : obligations de portabilité des données générées par les objets connectés, droit d'accès pour les utilisateurs et les tiers autorisés, interdiction des barrières injustifiées au changement de fournisseur de services de traitement de données, exigences d'interopérabilité des espaces de données (chapitres III, IV et VIII).
- **Règlement général sur la protection des données (RGPD, règlement 2016/679)** : texte concernant les données personnelles, reconnaissant un droit à la portabilité des données personnelles dans un format structuré, couramment utilisé et lisible par machine (article 20) ; droit d'accès impliquant la capacité technique d'extraction des données sur demande (article 15).
- **Règlement sur l'intelligence artificielle (AI Act, règlement 2024/1689)** : exigences de traçabilité et de documentation des données d'entraînement pour les systèmes à haut risque, obligation d'interopérabilité avec les dispositifs de supervision humaine (articles 12 et 14).

CADRES CONCERNANT LES ÉCHANGES SÉCURISÉS ENTRE SYSTÈMES

- **IEC 62443 (Sécurité des systèmes d'automatisation et de contrôle industriels)** : structuration de la sécurité par zones et conduits, définition de niveaux de sécurité (SL) aux points d'intégration entre acteurs, permettant de contractualiser les exigences de sécurité des échanges dans un écosystème hétérogène.
- **Règlement Cyber Resilience Act (CRA, règlement 2024/2847)** : obligations de mise à jour sécurisée (OTA), de documentation des composants logiciels (SBOM) et de maintien en conditions de sécurité, impactant la gestion du cycle de vie et la compatibilité des mises à jour dans un environnement multi-fournisseurs.
- **Directive NIS2 (directive 2022/2555)** : gestion des risques liés à la chaîne d'approvisionnement et notification d'incidents, supposant des interfaces d'échange d'informations de sécurité entre acteurs (alertes, escalades).

RÉFÉRENTIELS COMPLÉMENTAIRES

Les référentiels suivants sont cités à titre de bonnes pratiques pour la sécurisation des interfaces d'échange, sans constituer en eux-mêmes des exigences de la présente charte :

- Standards : ISO/IEC 27001 (système de management de la sécurité de l'information), ISO 15408 (critères d'évaluation pour la sécurité des technologies de l'information), ETSI EN 303 645 (cybersécurité pour l'IoT) ;
- OWASP Top 10 (risque de cybersécurité des applications et des API) ;
- Guides : Guide Cybersécurité IoT (CSF IN, Avicca), préconisations de l'ANSSI ;

ANNEXE IV

OPEN SOURCE

Les enjeux d'interopérabilité et de souveraineté soulèvent la question de l'Open Source, notamment à l'échelle européenne. L'open source fait communément partie du développement logiciel, y compris dans le domaine de l'IoT, et présente un relai de compétitivité intéressant pour les entreprises européennes (cf stratégie Open Source annoncée de la Commission Européenne). Il est utile de distinguer d'une part l'utilisation de l'open source et d'autre part les solutions 100% open source :

- Une solution peut intégrer des composants open source sans être intégralement open source
 - *Pour préserver le fonctionnement et l'interopérabilité de la solution, la question est alors le degré de maîtrise de l'éditeur sur les composants de sa solution*
- Une solution peut être interopérable sans être open source
 - *Par exemple, une collectivité n'a pas accès au code source du logiciel, mais elle peut transférer ses données de manière compréhensible et interprétable, selon les conditions établies par cette charte, lorsqu'elle change de fournisseur*
- Une solution intégralement open source n'est pas nativement interopérable, cela demande des développements plus ou moins importants
 - *Une documentation de qualité reste indispensable pour une solution évolutive et compatible avec les standards d'interopérabilités*
 - *Par exemple, le code source est partagé, mais la solution ne s'appuie pas sur les standards communément utilisés au sein du domaine, ou un modèle de données spécifique, ce qui génère des difficultés d'interfaçage*
- Une solution intégralement open source demande d'en structurer le modèle économique
 - *Le maintien de la solution exige des compétences et des ressources humaines afin de préserver l'interopérabilité dans le temps, qui nécessitent de s'appuyer sur une structure de mutualisation et/ou un éditeur/intégrateur*

GLOSSAIRE

DES ACRONYMES

API : Application Programming Interface - interface de programmation

CMS : Central Management Software - logiciel de gestion centralisée (ex : supervision éclairage)

DCAT-AP : Data Catalog Vocabulary - Application Profile (profil européen de métadonnées)

DGA : Data Governance Act - Règlement européen sur la gouvernance des données

ISM : Industrial, Scientific and Medical - bandes de fréquences libres (868 MHz en Europe)

JSON-LD : JavaScript Object Notation for Linked Data - format de données sémantiques

LPWAN : Low Power Wide Area Network - réseau étendu basse consommation

MIM : Minimal Interoperability Mechanism - mécanisme minimal d'interopérabilité

NGSI-LD : Next Generation Service Interfaces - Linked Data (API de contexte ETSI)

ODN : Outdoor Device Network - réseau d'équipements terrain (capteurs, contrôleurs)

OASC : Open & Agile Smart Cities & Communities

UNB : Ultra Narrow Band - modulation radio ultra-bande étroite (Sigfox)

SIGNATAIRES DE LA CHARTE

Eridanis - Synox - Ubicité - Sogetrel - Ineo Infracom - Netmore

CONTRIBUTEURS

RÉFÉRENTS DU GT : Alexis Semmama, Eridanis, David Virapin, Ubicité, Emmanuel Mouton, Synox

CONTRIBUTEURS : Ineo Infracom, Kuzzle, Lacroix, Netmore, NomoSense, Requea, Sogetrel, Watteco

COORDINATION : Astrid Voorwinden, InfraNum

MISE EN PAGE : Paola Ropele, InfraNum