OTSPI

OPEN TRUSTED SERVICE PROVIDER INITIATIVE

CHARTE

Charte d'éthique, de déontologie et de transparence publique

Open Trusted Service Provider Initiative (OTSPI)
Association en cours de constitution
Version du 20 octobre 2026

Licence Creative Commons Attribution 4.0 International · contact@otspi.org

Sommaire

1. Vision et raison d'être : la confiance numérique comme bien commun 3

2. Principes directeurs d'ordre public interne 3

3. Déclaration publique d'engagement 4

Association « Open Trusted Service Provider Initiative » (OTSPI)
Organisation d'Intérêt Général et à Gestion Désintéressée

1. Vision et raison d'être : la confiance numérique comme bien commun

L'association **« Open Trusted Service Provider Initiative » (OTSPI)** a pour but d'intérêt général de lever les barrières économiques, techniques, administratives et éducatives à la sécurité, à la confidentialité et à la confiance numérique dans les communications électroniques mondiales.

À l'instar du modèle d'infrastructure d'intérêt général à but non lucratif développé pour le chiffrement du web par l'**ISRG (*Let's Encrypt*)**, OTSPI conçoit, opère et pérennise des infrastructures critiques de confiance numérique ouvertes, souveraines, transparentes et universellement accessibles (notamment sous les règlements européens eIDAS / eIDAS 2.0 et les référentiels internationaux ETSI et WebTrust).

L'association est régie par les principes d'**intérêt général**, de **gestion désintéressée** au sens de la législation fiscale (articles 200 et 238 bis du CGI), et de service public pour l'ensemble de la collectivité.

2. Principes directeurs d'ordre public interne

A. Redevabilité publique intégrale (*Full Public Accountability*)

- **Transparence des processus** : Toutes les réunions statutaires, délibérations du Conseil d'Administration, résolutions normatives, documents de cadrage, feuilles de route (*roadmaps*), budgets prévisionnels et comptes financiers sont publiés en libre accès public (*open access*).
- **Code source et spécifications ouvertes** : Tous les logiciels d'infrastructure sont sous licence libre ou ouverte. Les rapports d'évaluation d'audit de conformité (normes ETSI EN 319 401, EN 319 411 / 421 / 422, WebTrust, eIDAS) sont rendus publics.
- **Les deux seules réserves protégées** :
- **Protection stricte de la vie privée et conformité RGPD** : Anonymisation ou pseudonymisation préalable des données personnelles des membres, votants, donateurs et contributeurs avant publication (Règlement UE 2016/679).
- **Sécurité opérationnelle et divulgation coordonnée de vulnérabilités (*Coordinated Vulnerability Disclosure*)** : Confidentialité temporaire sous embargo des rapports de vulnérabilités le temps de la correction et du déploiement, et secret technique absolu des clés privées et secrets matériels protégés au sein des modules HSM qualifiés.

B. Gestion strictement désintéressée et inaliénabilité

- **Bénévolat intégral des mandats** : Conformément à l'Article 12 des Statuts, les fonctions d'administrateurs au Conseil d'Administration et de membres du Bureau sont exercées à titre strictement bénévole. Aucun membre ne perçoit de rémunération, dividende ou avantage matériel direct ou indirect.

- **Séparation étanche avec les salariés** : Les éventuels salariés ou prestataires techniques de l'association ne peuvent siéger ni au Bureau ni au Conseil d'Administration.
- **Inaliénabilité perpétuelle (Article 13 des Statuts)** : L'association s'interdit perpétuellement toute transformation lucrative. Ses dépôts logiciels libres, marques et infrastructures sont inaliénables. En cas de dissolution, l'actif net subsistant après exécution complète du plan de terminaison d'activité (*Termination Plan*) est obligatoirement dévolu à un organisme d'intérêt général ou d'utilité publique poursuivant des missions analogues.

C. Ségrégation des fonctions et intégrité normative

- **Indépendance de l'autorité normative (Article 8 bis des Statuts)** : Le Comité des Politiques de Confiance (CPC / PMA) assure la garantie normative et cryptographique en toute indépendance de la gestion administrative ou des pressions commerciales.
- **Incompatibilité de gouvernance** : L'appartenance au Bureau exécutif est strictement incompatible avec les fonctions de membre du CPC ou d'auditeur interne.
- **Prévention des conflits d'intérêts** : Tout administrateur, membre du CPC ou Officier d'Autorité déclare publiquement ses liens d'intérêt et s'abstient de prendre part au vote en cas de délibération susceptible de créer un conflit d'intérêts.

D. Neutralité, égalité d'accès et souveraineté

- **Universalité et non-discrimination (Article 12 quater des Statuts)** : L'accès aux services de confiance et briques logicielles édités par l'association est universel, neutre et non discriminatoire, dans le respect strict des sanctions légales et embargos applicables.
- **Indépendance technologique** : L'association veille à la neutralité et à l'interopérabilité de ses infrastructures, face aux risques d'enfermement propriétaire (*vendor lock-in*) et de dépendance vis-à-vis de juridictions extraterritoriales intrusives.
- **Minimisation des données (*Privacy by Design*)** : L'architecture privilégie systématiquement la protection de la vie privée, le traitement d'empreintes cryptographiques (*hashes*) et le refus absolu de tout profilage ou exploitation commerciale des métadonnées des utilisateurs.

3. Déclaration publique d'engagement

Tout administrateur, membre du Bureau, membre du CPC et Officier d'Autorité souscrit formellement à cette charte dès sa prise de fonction et s'engage à œuvrer au service exclusif de l'intérêt général et de la confiance numérique collective.