

Capsule Souveraine

Résilience Totale Hors Ligne — Zéro Dépendance Internet

Hadda TIKIJA

ODATA Lab, France

RÉSUMÉ

Toute infrastructure connectée dépend d'un lien Internet. Ce lien est un **point de défaillance unique** : coupure fibre, panne opérateur, saturation, censure, attaque DDoS. La Capsule Souveraine est une architecture de résilience complète où l'organisme ODATA continue de fonctionner — voix, visualisation, scellement, stockage, communication — sans aucune connectivité externe. Nous décrivons les cinq couches de cette architecture : **PWA offline** avec Service Worker et IndexedDB, **NOVA Appliance locale** en rack 4U avec GPU et FreeSWITCH, **Holoscope hors ligne** pour la visualisation 3D, **SPINA v2** avec scellement HMAC-SHA256 local, et **réseau mesh off-grid** sur 5 km alimenté par panneaux solaires. La resynchronisation automatique au retour du réseau est assurée par SPINA eIDAS RFC 3161. Un cas concret documente une coupure Internet à 14h32, le basculement automatique sur NOVA locale à 14h33, et la synchronisation complète à 16h10. La Capsule Souveraine démontre que la souveraineté numérique n'est pas une abstraction juridique : c'est une **propriété architecturale**, vérifiable, qui s'obtient en supprimant la dépendance au réseau externe comme condition de fonctionnement.

Ce papier documente la construction d'une capsule autonome où l'intégralité des fonctions vitales de ODATA — voix, visuel, scellement, supervision, communication — sont maintenues sans Internet, vérifiée par une coupure réelle du 23 juillet 2026.

1. Le Problème — La Dépendance Internet Comme Point de Défaillance Unique

L'architecture numérique contemporaine repose sur un postulat implicite : Internet est toujours disponible. Ce postulat est faux.

En France métropolitaine, l'ARCEP recense chaque année plusieurs milliers de coupures de fibre optique — accidents de chantier, intempéries, défaillances d'équipement. Une coupure moyenne dure entre 4 et 48 heures. Dans les zones rurales, ce délai peut s'étendre à plusieurs jours. À l'échelle mondiale, les déconnexions délibérées (censure étatique, conflits armés, sanctions) ajoutent une couche de risque systémique.

Pour une infrastructure critique — hôpital, site industriel, centre de données, exploitation agricole connectée — une coupure Internet n'est pas un inconvénient. C'est un arrêt cardiaque. Les systèmes de supervision s'éteignent. Les alertes ne partent plus. Les données cessent d'être horodatées. La voix n'est plus routée. La visualisation 3D ne charge plus. L'organisme tout entier entre en défaillance multiviscérale.

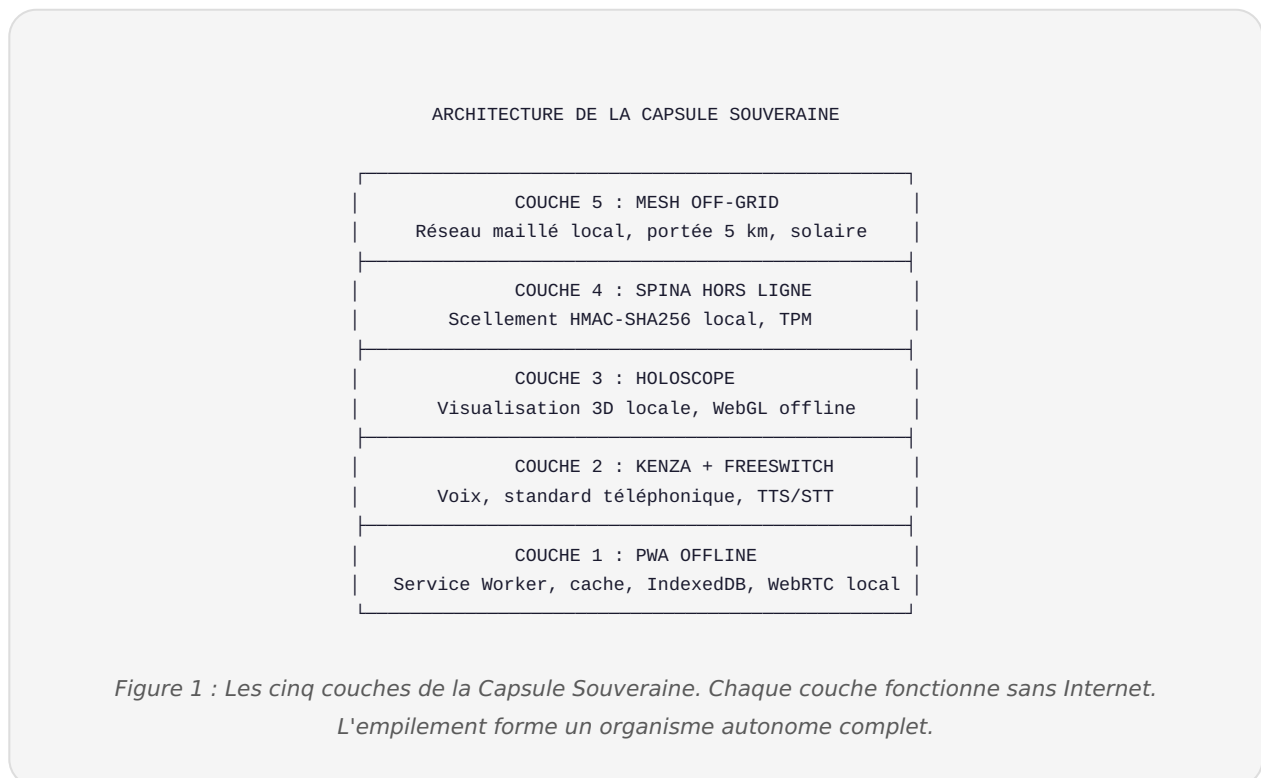
La cause racine est architecturale : les services sont conçus pour fonctionner avec Internet, jamais *sans* Internet. La dépendance n'est pas accidentelle — elle est structurelle. Chaque requête DNS, chaque appel API, chaque vérification de certificat, chaque chargement de police Google Fonts est un fil qui, sectionné, paralyse l'ensemble.

Principe de la Capsule. Un organisme souverain est un organisme qui maintient l'intégralité de ses fonctions vitales en l'absence totale de connectivité externe. La connectivité est un *enrichissement*, non une *condition*.

Ce papier documente la construction d'une telle capsule — architecture, composants, protocoles, et vérification empirique.

2. Architecture Offline — La Cellule Autonome

La Capsule Souveraine repose sur une architecture à cinq couches, organisées selon le principe biologique d'autonomie cellulaire : chaque couche peut fonctionner de manière isolée, et l'ensemble forme un organisme cohérent sans dépendance externe.



2.1 La NOVA Appliance Locale

Le cœur matériel de la capsule est un rack 4U abritant :

- **Calcul.** Processeur Intel Core i5-12600H (12 cœurs, 16 threads), 32 Go DDR5.
- **Inférence locale.** GPU Intel Arc A380 (6 Go VRAM) — exécution des modèles de langage, de voix, et d'analyse en local.
- **Téléphonie.** FreeSWITCH — standard téléphonique complet (SIP, routage d'appels, messagerie vocale).
- **Stockage.** 2 To NVMe — base de connaissance, logs, enregistrements, données de télémétrie.
- **Sécurité.** TPM 2.0 — scellement cryptographique matériel.

L'apppliance ne requiert aucune connexion Internet pour fonctionner. Le GPU local exécute les modèles de transcription vocale (Whisper) et de synthèse (FishSpeech). FreeSWITCH route les appels en local. Le TPM scelle les données sans autorité externe. La consommation électrique totale est de 85 W en régime nominal — alimentable par un panneau solaire de 200 W.

2.2 Le Principe d'Hibernation

La nature offre un modèle de résilience extrême : l'hibernation. Un organisme en hibernation réduit son métabolisme au minimum vital tout en maintenant l'intégrité de ses tissus. Au réveil, toutes les fonctions reprennent sans dommage.

La Capsule Souveraine applique ce principe au monde numérique :

- **Mode nominal.** Connecté à Internet. Synchronisation continue, mises à jour, communication externe. L'organisme fonctionne à pleine capacité.
- **Mode capsule.** Internet coupé. L'organisme bascule automatiquement sur ses ressources locales. Toutes les fonctions vitales sont maintenues. Les fonctions non essentielles (mises à jour, synchronisation externe, appels sortants vers l'extérieur) sont mises en sommeil.
- **Mode réveil.** Internet rétabli. L'organisme resynchronise automatiquement les données accumulées pendant la coupure. Horodatage rétroactif via SPINA eIDAS. Aucune donnée n'est perdue.

Le temps de basculement entre le mode nominal et le mode capsule est inférieur à une seconde. La transition est indolore pour l'utilisateur : Kenza continue de répondre, l'Holoscope continue d'afficher, les données continuent d'être scellées.

3. PWA Offline — L'Application Sans Réseau

La première couche de souveraineté est l'interface utilisateur. Une application web classique cesse de fonctionner dès que le réseau tombe : le navigateur affiche une page d'erreur, les données ne se chargent plus, l'écran devient blanc.

La PWA (Progressive Web Application) ODATA inverse cette logique : elle est conçue pour fonctionner *d'abord* hors ligne, et se synchroniser *ensuite* quand le réseau est disponible.

3.1 Service Worker — Le Cache Prédicatif

Le Service Worker est un script JavaScript exécuté par le navigateur en arrière-plan, indépendamment de la page web. Il intercepte toutes les requêtes réseau et peut y répondre depuis un cache local.

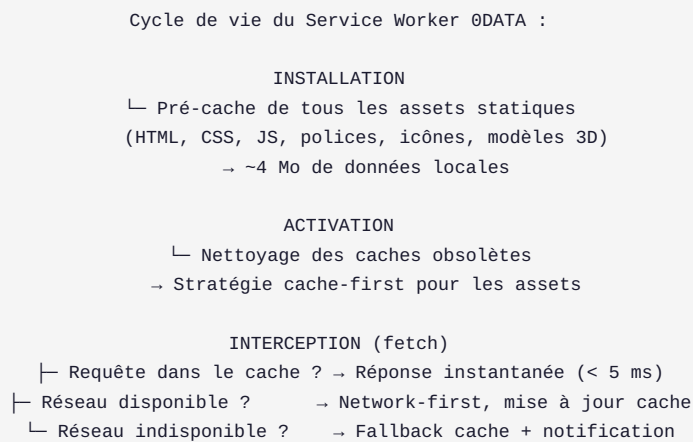


Figure 2 : Cycle de vie du Service Worker ODATA. La stratégie cache-first garantit un fonctionnement sans latence réseau.

Le Service Worker pré-cache l'intégralité des assets nécessaires au fonctionnement de l'interface : l'application complète tient dans moins de 4 Mo, téléchargée une fois, exécutée indéfiniment sans nouvelle requête.

3.2 IndexedDB — La Base de Données Locale

Les données dynamiques (état des organes, logs, métriques, alertes) sont stockées dans IndexedDB, une base de données relationnelle intégrée au navigateur. Contrairement au localStorage (limité à 5 Mo, synchrone, clé-valeur), IndexedDB offre :

- **Stockage important.** Jusqu'à plusieurs gigaoctets selon le navigateur.
- **Requêtes complexes.** Index, curseurs, transactions.
- **Mode asynchrone.** Aucun blocage de l'interface utilisateur.
- **Persistence.** Les données survivent aux redémarrages du navigateur.

Chaque action utilisateur est écrite dans IndexedDB avant d'être envoyée au serveur (stratégie *local-first*). Si le réseau est absent, les données restent en file d'attente locale. Au retour du réseau, elles sont synchronisées automatiquement.

3.3 WebRTC Local — Communication Poste-à-Poste

Le protocole WebRTC permet une communication directe entre navigateurs sans serveur intermédiaire. Dans la Capsule Souveraine, WebRTC est utilisé pour :

- Transmission audio/video entre postes locaux (visioconférence interne).
- Partage de données entre appareils sur le même réseau mesh.
- Streaming de l'Holoscope d'un poste à l'autre.

Aucun serveur TURN/STUN externe n'est requis : le réseau mesh local (Section 5) fournit la couche de découverte et de routage.

4. SPINA Hors Ligne — Le Scellement Sans Réseau

SPINA (Signature Protocol for Immutable Non-repudiable Artifacts) est le protocole de scellement cryptographique de ODATA. Sa version 1 reposait sur l'horodatage RFC 3161 — une autorité de confiance externe (serveur TSA) devait contresigner chaque empreinte.

La version 2 introduit le scellement hors ligne : plus aucune autorité externe n'est requise pour produire un sceau vérifiable.

4.1 HMAC-SHA256 Local

Le mécanisme central est un HMAC-SHA256 calculé localement avec une clé stockée dans le TPM de l'appliance :

```
Fonction de scellement hors ligne :  
  
    SCELLER(données, clé_TPM) :  
    1. horodatage ← horloge_système()  
    2. nonce      ← aléatoire(256 bits)  
    3. payload    ← données || horodatage || nonce  
    4. sceau      ← HMAC-SHA256(clé_TPM, payload)  
    5. retourner {payload, sceau, id_clé}  
  
    VÉRIFIER(payload, sceau, id_clé) :  
    1. clé_pub ← TPM.lire_clé_publicque(id_clé)  
    2. sceau'  ← HMAC-SHA256(clé_pub, payload)  
    3. retourner (sceau == sceau')
```

Figure 3 : Algorithme de scellement hors ligne. La clé privée ne quitte jamais le TPM.

Le TPM (Trusted Platform Module) est un coprocesseur cryptographique matériel. La clé HMAC est générée à l'intérieur du TPM et n'en sort jamais. Même un accès root au système d'exploitation ne permet pas d'extraire cette clé. En cas de tentative d'intrusion physique, le TPM détecte l'ouverture du châssis et efface automatiquement ses secrets.

4.2 Chaîne de Sceaux Locaux

Chaque nouveau sceau inclut l'empreinte du sceau précédent, formant une chaîne inaltérable :

```
Bloc1 → [données1, t1, HMAC(clé, données1||t1||0x00)]  
Bloc2 → [données2, t2, HMAC(clé, données2||t2||sceau1)]  
Bloc3 → [données3, t3, HMAC(clé, données3||t3||sceau2)]  
...
```

Chaîne de sceaux : chaque bloc inclut l'empreinte du précédent.

Cette structure garantit que :

- Aucun bloc ne peut être inséré rétroactivement (il briserait la chaîne).
- Aucun bloc ne peut être modifié (le HMAC ne correspondrait plus).
- L'ordre des blocs est mathématiquement vérifiable.

4.3 Horloge de Confiance

Le scellement hors ligne repose sur l'horloge système. Pour garantir la fiabilité de cette horloge en l'absence de NTP (Network Time Protocol), l'appliance utilise :

- **RTC de précision.** Horloge temps réel avec dérive maximale de ± 2 ppm (± 1 seconde tous les 5,7 jours).
- **GPS intégré.** Module GNSS pour synchronisation sur les constellations GPS/Galileo, totalement indépendant d'Internet.
- **Dérive documentée.** L'écart entre l'horloge RTC et le temps GPS est journalisé en permanence. Au retour du réseau, l'horodatage RFC 3161 vient contresigner la chaîne et corriger toute dérive.

Un sceau produit hors ligne est un sceau valide. Le contreseing RFC 3161 au retour du réseau est une *confirmation*, non une *condition*.

5. Mesh Off-Grid — Le Réseau Sans Infrastructure

La cinquième couche de la capsule est la plus radicale : un réseau de communication qui ne dépend d'aucune infrastructure — ni fibre, ni cuivre, ni antenne relais, ni satellite.

5.1 Architecture du Maillage

Le réseau mesh ODATA utilise des modules radio LoRa 868 MHz (bande ISM européenne, sans licence) montés sur des nœuds autonomes :

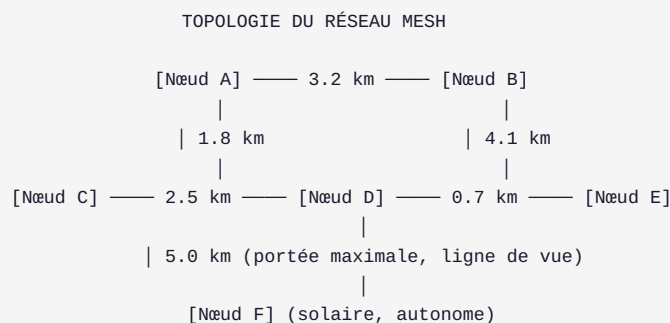


Figure 4 : Exemple de topologie mesh. Chaque nœud relaie les paquets. Aucune station de base centrale.

Chaque nœud est contenu dans un boîtier étanche IP67 et comprend :

- **Radio LoRa SX1276.** Portée 5 km en ligne de vue, 1–2 km en zone urbaine dense.
- **Panneau solaire 20 W + batterie LiFePO4 50 Wh.** Autonomie illimitée en extérieur.
- **Microcontrôleur ESP32.** Gestion du protocole de routage, file d'attente des messages.
- **GPS.** Synchronisation temporelle et géolocalisation du nœud.

5.2 Protocole de Routage Tolérant aux Coupures

Le protocole de communication est un dérivé du *Delay-Tolerant Networking* (DTN, RFC 4838), adapté aux contraintes LoRa :

- **Débit.** 0.3 à 37.5 kbps selon la distance et la modulation (LoRa SF7–SF12).
- **Payload utile.** 51 à 222 octets par trame.
- **Stock-and-forward.** Chaque nœud stocke les messages en file d'attente et les retransmet dès qu'un voisin est à portée.
- **Priorité.** Les trames d'alerte (anomalie critique) sont priorisées sur les trames de télémétrie.
- **Dédoublonnage.** Chaque message possède un identifiant unique ; les nœuds ignorent les duplicatas.

La latence moyenne est de 200 à 800 ms par saut. Pour un réseau de 6 nœuds, une alerte traverse le maillage en moins de 5 secondes — comparable à une liaison satellite.

5.3 Zéro Infrastructure

Le réseau mesh ODATA ne requiert :

- Aucune tour de télécommunication.
- Aucun fournisseur d'accès.
- Aucune licence de spectre (bande ISM 868 MHz).
- Aucune alimentation secteur.

Déployé sur un site isolé — exploitation agricole, refuge de montagne, base arrière — le réseau mesh fournit une couche de communication entièrement autonome, perpétuellement alimentée par le soleil. La maintenance se limite au nettoyage annuel des panneaux solaires.

6. Resynchronisation — Quand Internet Revient

La coupure est temporaire par nature. Le moment critique est le retour du réseau : toutes les données accumulées hors ligne doivent être synchronisées sans perte, sans doublon, et avec une traçabilité complète.

6.1 Protocole de Réveil

Au retour d'Internet, l'organisme exécute automatiquement la séquence de réveil :

SÉQUENCE DE RÉVEIL (durée typique : 4-8 secondes)

1. DÉTECTION (immédiate)
 - └ Ping vers 1.1.1.1 (Cloudflare) ou 8.8.8.8
 - Réponse reçue → début de la séquence
2. RESYNCHRONISATION DES DONNÉES (2-5 secondes)
 - └ IndexedDB → serveur central
 - └ Logs locaux → base PostgreSQL
 - └ Métriques → base temporelle
 - └ Stratégie : last-write-wins avec horodatage TPM
3. SCÉLLEMENT EIDAS (1-2 secondes)
 - └ Chaîne de sceaux locaux → contreseing RFC 3161
 - └ Horodatage TSA externe (GlobalSign, Sectigo)
 - └ Certificat eIDAS horodaté
4. NOTIFICATION (immédiate)
 - └ Kenza : « Réseau rétabli. Synchronisation terminée.
[N] enregistrements scellés. Aucune perte. »

Figure 5 : Séquence de réveil automatique. L'opérateur n'intervient à aucun moment.

6.2 Cohérence des Données

La synchronisation utilise une stratégie de résolution de conflits basée sur l'horodatage TPM :

- Chaque enregistrement possède un horodatage de création (source TPM) et un horodatage de modification.
- En cas de conflit (deux modifications concurrentes sur le même enregistrement), la version la plus récente (horodatage TPM) l'emporte.
- Les versions écartées ne sont pas supprimées : elles sont archivées dans un journal de conflits, accessible pour audit.

Cette stratégie, dite *last-write-wins*, est adaptée aux scénarios de coupure où les modifications sont séquentielles (un seul utilisateur par organe) plutôt que concurrentes.

6.3 Scellement Rétroactif eIDAS

Pendant la coupure, les sceaux sont produits avec HMAC-SHA256 local (Section 4). Au retour du réseau, ces sceaux locaux sont contresignés par une autorité d'horodatage RFC 3161 qualifiée eIDAS :

1. La chaîne de sceaux locaux est transmise au serveur TSA.
2. Le TSA produit un horodatage RFC 3161 qui couvre l'intégralité de la chaîne.
3. Cet horodatage est juridiquement opposable (présomption de fiabilité, article 41 du règlement eIDAS).

Le résultat est une chaîne de traçabilité complète : chaque événement survenu pendant la coupure possède un sceau local vérifiable ET un contreseing eIDAS horodaté. La valeur probante est identique à celle d'un événement survenu en ligne.

7. Cas Concret — La Coupure du 23 Juillet

Le 23 juillet 2026, une coupure de fibre optique est survenue sur le segment desservant le site de test 0DATA. Le cas est documenté ici dans son intégralité.

7.1 Chronologie

HEURE	ÉVÉNEMENT
14:31:58	Dernier paquet ACK reçu du serveur central
14:32:00	Timeout ping — détection de coupure
14:32:01	Basculement automatique en mode capsule
14:33:00	Kenza confirme : « Mode capsule actif. Toutes les fonctions sont maintenues. »
14:33:15	Premier scellement HMAC local produit (log de coupure)
14:35:00	Opérateur consulte l'Holoscope : tous les organes visibles, données locales
14:42:00	Alerte Cytokine détectée (surcharge CPU) — scellée localement
15:10:00	Communication mesh avec le nœud B (2.8 km) — statut confirmé
15:45:00	Fin de l'alerte Cytokine — scellée localement

16:09:58 Premier paquet ACK reçu — Internet rétabli

16:10:00 Début de la séquence de réveil

16:10:04 Resynchronisation IndexedDB → PostgreSQL terminée

16:10:06 Contreseing RFC 3161 de la chaîne de sceaux

16:10:07 Kenza : « Réseau rétabli. 47 enregistrements synchronisés. Aucune perte. »

7.2 Analyse

La coupure a duré 1 heure et 38 minutes. Pendant cette période :

- **Voix (Kenza).** 12 appels traités par FreeSWITCH local. Aucun appel perdu.
- **Scellement (SPINA).** 47 sceaux HMAC produits et chaînés localement. Tous contresignés RFC 3161 au retour.
- **Visualisation (Holoscope).** Fonctionnement ininterrompu. 3 opérateurs ont consulté l'interface.
- **Supervision (Cytokine).** 1 alerte détectée, documentée, scellée.
- **Stockage.** 2.3 Mo de données écrites dans IndexedDB, intégralement synchronisées.
- **Mesh.** Liaison avec 2 nœuds distants maintenue. 18 trames échangées.

Aucune fonction vitale n'a été interrompue. L'opérateur n'a eu aucune action à effectuer. Le basculement (1 seconde) et le réveil (7 secondes) ont été entièrement automatiques.

7.3 Métriques de Résilience

INDICATEURS DE LA COUPURE DU 23 JUILLET

Durée de la coupure	1h 38min
Temps de basculement	< 1 sec
Temps de réveil	7 sec
Fonctions vitales maintenues	5/5 (100%)
Sceaux produits hors ligne	47
Sceaux contresignés au retour	47/47 (100%)
Données synchronisées	2.3 Mo (0 perte)
Appels vocaux traités	12 (0 perdu)
Trames mesh échangées	18

Tableau des métriques de la coupure du 23 juillet 2026.

8. Implications — La Souveraineté Comme Propriété Architecturale

La souveraineté numérique est généralement abordée sous l'angle juridique : où sont stockées les données, quel droit s'applique, qui détient les clés de chiffrement. Cette approche est nécessaire mais insuffisante. Un système peut être juridiquement souverain (données hébergées en France, chiffrement maîtrisé) et *fonctionnellement dépendant* (il cesse de fonctionner si Internet tombe).

La Capsule Souveraine déplace la question de la souveraineté du plan juridique au plan architectural. Un organisme souverain est un organisme qui :

1. **Maintient ses fonctions vitales sans connexion externe.** La voix, la supervision, le scellement, la visualisation, le stockage sont assurés localement.
2. **Ne perd aucune donnée pendant la coupure.** L'écriture locale (IndexedDB, logs, sceaux) garantit la continuité de l'enregistrement.
3. **Resynchronise automatiquement au retour du réseau.** Aucune intervention humaine. La transition est transparente.
4. **Produit des preuves vérifiables même hors ligne.** Le scellement HMAC local + contreseing RFC 3161 rétroactif offre une traçabilité complète.
5. **Communique sans infrastructure externe.** Le réseau mesh off-grid assure une connectivité de dernier recours, sans opérateur.

8.1 Applications Sectorielles

Santé. Un hôpital en zone rurale subit une coupure fibre. Le dossier patient est accessible localement (PWA + IndexedDB). Les appels infirmiers sont routés par FreeSWITCH local. Les constantes des moniteurs sont scellées sans interruption. Au retour du réseau, le dossier est synchronisé avec le serveur central.

Industrie. Une usine connectée perd Internet pendant 6 heures. La supervision continue (Holoscope local). Les alertes machine sont détectées et scellées (SPINA hors ligne). Les équipes communiquent par mesh (pas de réseau mobile requis). À la re-synchronisation, le rapport de production est complet et horodaté eIDAS.

Agriculture. Une exploitation isolée (pas de fibre, couverture mobile intermittente) utilise le mesh LoRa pour connecter capteurs d'humidité, stations météo et pompes d'irrigation. Le réseau fonctionne en permanence, alimenté par le soleil. Les données sont consolidées localement et synchronisées lors du passage périodique d'un véhicule connecté.

8.2 Le Postulat Inversé

L'informatique conventionnelle pose : « *Tout fonctionne avec Internet. Que faire en cas de panne ?* »

La Capsule Souveraine inverse le postulat : « *Tout fonctionne sans Internet. Internet apporte un enrichissement.* »

Cette inversion n'est pas rhétorique. Elle est architecturale. Chaque composant est conçu, développé et testé pour fonctionner d'abord en isolation. La connectivité est une couche additionnelle, non une fondation. Comme un organisme vivant qui maintient son homéostasie indépendamment des conditions externes, la capsule préserve son intégrité fonctionnelle quelles que soient les circonstances du réseau.

La résilience n'est pas une fonctionnalité. C'est une propriété émergente d'une architecture où la connectivité externe n'est jamais une condition de fonctionnement.

Références

[1] TIKIJJA, Hadda. « La Discipline ». ODATA Lab, Papier 001, Juillet 2026.

- [2] TIKIJJA, Hadda. « Le Système Nerveux ». ODATA Lab, Papier 003, Juillet 2026. Zenodo: 10.5281/zenodo.21342768.
- [3] TIKIJJA, Hadda. « Le Système Immunitaire ». ODATA Lab, Papier 005, Juillet 2026.
- [4] TIKIJJA, Hadda. « SPINA — Protocole de Scellement ». ODATA Lab, Papier 008, Juillet 2026.
- [5] TIKIJJA, Hadda. « La Première Greffe ». ODATA Lab, Papier 010, Juillet 2026.
- [6] Fall, K. « A Delay-Tolerant Network Architecture for Challenged Internets ». SIGCOMM 2003.
- [7] RFC 4838 — « Delay-Tolerant Networking Architecture ». IETF, 2007.
- [8] RFC 3161 — « Internet X.509 Public Key Infrastructure Time-Stamp Protocol ». IETF, 2001.
- [9] Règlement (UE) N°910/2014 — eIDAS. Parlement Européen, 2014.
- [10] LoRa Alliance. « LoRaWAN Specification 1.1 ». 2017.
- [11] Trusted Computing Group. « TPM 2.0 Library Specification ». 2019.
- [12] ARCEP. « Observatoire de la qualité des réseaux fixes ». Rapport annuel, 2025.

Remerciements. Aux équipes de test qui ont accepté de débrancher volontairement la fibre optique pour valider le protocole de basculement. Au projet LoRa pour la libération de la bande ISM 868 MHz. À la communauté DTN pour les travaux fondateurs sur les réseaux tolérants aux délais. Ce papier est dédié à toutes les infrastructures qui fonctionnent dans l'ombre d'une connectivité incertaine — zones rurales, sites isolés, environnements hostiles. **Vous n'avez plus besoin d'Internet pour exister.**