الكبسولة السيادية

مرونة كاملة دون اتصال — صفر اعتماد على الإنترنت

Hadda TIKIJJA

مختبر 0DATA، فرنسا

ملخص

كل بنية تحتية متصلة تعتمد على رابط إنترنت. هذا الرابط هو **نقطة فشل وحيدة**: قطع ألياف، عطل مشغّل، تشبع، رقابة، هجوم حجب خدمة DDoS. الكبسولة السيادية هي بنية مرونة كاملة يواصل فيها كائن 0DATA أي اتصال خارجي — دون العمل — الصوت والتصوّر والختم والتخزين والاتصال. تتكون الطبقات الخمس لهذه البنية: **تطبيق PWA دون اتصال** مع عامل الخدمة وIndexedDB، و**محلي NOVA جهاز هولوسكوب** في رف 4U مع وحدة معالجة رسوميات وFreeSWITCH، و**شبكة** HMAC-SHA256، و**الإصدار SPINA 2** مع ختم محلي للتصوّر ثلاثي الأبعاد، و**دون اتصال** إعادة SPINA eIDAS RFC 3161 بمدى 5 كم تعمل بألواح شمسية. تضمن **متداخلة خارج الشبكة** المزامنة التلقائية عند عودة الشبكة. توثّق حالة ملموسة انقطاع الإنترنت عند الساعة 14:32، المحلي عند 14:33، والمزامنة الكاملة عند 16:10. تُثبت الكبسولة NOVA والتحويل التلقائي إلى قابلة للتحقق، تُكتسب بإزالة **خاصية معمارية** السيادية أن السيادة الرقمية ليست تجريدًا قانونيًا: إنها الاعتماد على الشبكة الخارجية كشرط للتشغيل.

في جملة واحدة

يوثّق هذا البحث بناء كبسولة مستقلة تبقى فيها جميع الوظائف الحيوية لـ 0DATA — الصوت والبصري والختم والإشراف والاتصال — قائمة دون إنترنت، وقد تحقّق ذلك بانقطاع حقيقي في 23 يوليو 2026.

1. المشكلة — الاعتماد على الإنترنت كنقطة فشل وحيدة

تقوم البنية الرقمية المعاصرة على افتراض ضمني: أن الإنترنت متاح دائمًا. هذا الافتراض خاطئ.

كل عام عدة آلاف من انقطاعات الألياف البصرية — حوادث أشغال ARCEP في فرنسا القارية، تسجّل هيئة، عواصف، أعطال معدات. يستمر الانقطاع المتوسط بين 4 و48 ساعة. وفي المناطق الريفية قد يمتد هذا الأجل إلى عدة أيام. وعلى الصعيد العالمي، تضيف حالات الفصل المتعمّد (رقابة الدولة، النزاعات المسلحة، العقوبات) طبقة من المخاطر المنهجية.

بالنسبة إلى بنية تحتية حرجة — مستشفى، موقع صناعي، مركز بيانات، مزرعة متصلة — لا يُعد انقطاع الإنترنت مجرد إزعاج. إنه توقف قلبي. تنطفئ أنظمة الإشراف. وتتوقف التنبيهات عن الصدور. وتتوقف البيانات عن الحصول على ختم زمني. ولا يُوجَّه الصوت. ولا يعود التصوّر ثلاثي الأبعاد يُحمَّل. ويدخل الكائن بأكمله في فشل متعدد الأعضاء.

أبدًا. الاعتماد ليس عرضيًا — إنه من دونه الإنترنت، لا مع السبب الجذري معماري: الخدمات مصمَّمة للعمل هو خيط إذا Google Fonts وكل تحقق من شهادة، وكل تحميل لخط API، وكل نداء DNS، بنيوي. كل طلب قُطع شلَّ المجموعة بأكملها.

> **مبدأ الكبسولة.** الكائن السيادي هو كائن يحافظ على جميع وظائفه الحيوية في ظل غياب كامل للاتصال شرط لا إثراء الخارجي. الاتصال.

يوثّق هذا البحث بناء كبسولة من هذا النوع — البنية والمكوّنات والبروتوكولات والتحقق التجريبي.

2. البنية دون اتصال — الخلية المستقلة

تعتمد الكبسولة السيادية على بنية من خمس طبقات، منظّمة وفق المبدأ البيولوجي للاستقلالية الخلوية: تستطيع كل طبقة أن تعمل بمعزل عن غيرها، ويشكّل المجموع كائنًا متسقًا دون اعتماد خارجي.



الشكل 1: الطبقات الخمس للكبسولة السيادية. تعمل كل طبقة دون إنترنت. ويشكّل التكديس كائنًا مستقلًا مكتملًا.

2.1 جهاز NOVA المحلي

القلب المادي للكبسولة هو رف 4U يضم:

- **الحوسبة.** معالج Intel Core i5-12600H (12 خيطًا، 16 نواة)، وذاكرة 32 جيجابايت DDR5.
- **الاستدلال المحلي.** وحدة معالجة رسوميات Intel Arc A380 (6 جيجابايت VRAM) — تشغيل نماذج اللغة والصوت والتحليل محليًا.
- **الهاتفية.** FreeSWITCH — بدالة هاتفية كاملة (SIP، البريد الصوتي، توجيه المكالمات).
- **التخزين.** 2 تيرابايت NVMe — قاعدة المعرفة والسجلات والتسجيلات وبيانات القياس عن بُعد.
- **الأمان.** TPM 2.0 — ختم تشفيري عتادي.

لا يتطلب الجهاز أي اتصال بالإنترنت ليعمل. تشغّل وحدة معالجة الرسوميات المحلية نماذج النسخ الصوتي والتوليف. ويختم FreeSWITCH المكالمات محليًا. يبلغ إجمالي TPM البيانات دون أي سلطة خارجية. ويوجّه استهلاك الطاقة 85 واط في الوضع الاسمي — ويمكن تغذيته بلوح شمسي بقدرة 200 واط.

2.2 مبدأ السبات

تقدم الطبيعة نموذجًا للمرونة القصوى: السبات. يخفض الكائن السابتّ أيضه إلى الحد الأدنى الحيوي مع الحفاظ على سلامة أنسجته. وعند الاستيقاظ تستأنف جميع الوظائف دون ضرر.

تطبّق الكبسولة السيادية هذا المبدأ على العالم الرقمي:

- **الوضع الاسمي.** متصل بالإنترنت. مزامنة مستمرة وتحديثات واتصال خارجي. يعمل الكائن بكامل طاقته.
- **وضع الكبسولة.** انقطع الإنترنت. يتحول الكائن تلقائيًا إلى موارده المحلية. تُحافظ جميع الوظائف الحيوية. وتوضع الوظائف غير الأساسية (التحديثات، المزامنة الخارجية، المكالمات الصادرة إلى الخارج) في سبات.
- **وضع الاستيقاظ.** عاد الإنترنت. يعيد الكائن تلقائيًا مزامنة البيانات المتراكمة أثناء الانقطاع. ختم زمني لا تُفقد أي بيانات. بأثر رجعي عبر SPINA eIDAS.

زمن التحويل بين الوضع الاسمي ووضع الكبسولة أقل من ثانية واحدة. الانتقال غير مؤلم للمستخدم: تواصل كنزة الرد، ويواصل الهولوسكوب العرض، وتستمر البيانات في الحصول على أختامها.

3. تطبيق PWA — التطبيق بلا شبكة دون اتصال

الطبقة الأولى من السيادة هي واجهة المستخدم. يتوقف التطبيق الويب التقليدي عن العمل بمجرد سقوط الشبكة: يعرض المتصفح صفحة خطأ، وتتوقف البيانات عن التحميل، وتصبح الشاشة بيضاء.

يعكس تطبيق 0 DATA من نوع PWA (تطبيق الويب التقدمي) هذا المنطق: فهو مصمَّم للعمل أولًا دون اتصال، ثم المزامنة لاحقًا عندما تتوفر الشبكة.

3.1 عامل الخدمة — الذاكرة المؤقتة التنبؤية

عامل الخدمة (Service Worker) هو سكربت JavaScript ينفّذه المتصفح في الخلفية، باستقلال عن صفحة الويب. يعترض جميع طلبات الشبكة ويستطيع الرد عليها من ذاكرة مؤقتة محلية.



الشكل 2: دورة حياة عامل الخدمة في 0DATA. تضمن استراتيجية cache-first عملًا دون زمن انتقال للشبكة.

يخزّن عامل الخدمة مسبقًا جميع الأصول اللازمة لعمل الواجهة: التطبيق الكامل في أقل من 4 ميجابايت، يُحمَّل مرة واحدة ويُشغَّل إلى ما لا نهاية دون طلب جديد.

3.2 قاعدة البيانات المحلية IndexedDB

تُخزَّن البيانات الديناميكية (حالة الأعضاء والسجلات والمقاييس والتنبيهات) في IndexedDB، وهي قاعدة بيانات علائقية مدمجة في المتصفح. وعلى خلاف localStorage (المحدودة بـ 5 ميجابايت والمتزامنة وذات بنية مفتاح-قيمة)، تقدّم IndexedDB:

- **تخزينًا كبيرًا.** حتى عدة جيجابايت وفق المتصفح.
- **استعلامات معقدة.** فهارس ومؤشرات ومعاملات.
- **وضعًا غير متزامن.** دون أي حجب لواجهة المستخدم.
- **استمرارية.** تبقى البيانات بعد إعادة تشغيل المتصفح.

وإذا كانت local-first). تُكتب كل إجراءات المستخدم في IndexedDB (استراتيجية قبل إرسالها إلى الخادم الشبكة غائبة تبقى البيانات في طابور محلي. وعند عودة الشبكة تُزامَن تلقائيًا.

3.3 WebRTC — الاتصال من نظير إلى نظير المحلي

يتيح بروتوكول WebRTC اتصالًا مباشرًا بين المتصفحات دون خادم وسيط. وفي الكبسولة السيادية يُستخدم WebRTC من أجل:

- نقل الصوت/الفيديو بين المحطات المحلية (مؤتمرات فيديو داخلية).
- مشاركة البيانات بين الأجهزة على الشبكة المتداخلة نفسها.

• بث الهولوسكوب من محطة إلى أخرى.

خارجي: توفر الشبكة المتداخلة المحلية (القسم 5) طبقة الاكتشاف TURN/STUN لا حاجة إلى أي خادم والتوجيه.

4. SPINA دون اتصال — الختم بلا شبكة

SPINA (بروتوكول الختم التشفيري للقطع الأثرية غير القابلة للتغيير وغير القابلة للإنكار) هو بروتوكول الختم الزمني RFC 3161 — اعتمد الإصدار 1 على سلطة ثقة خارجية (خادم TSA) إذ كان DATA. لدى 0 أن تصادق على كل بصمة.

يقدّم الإصدار 2 الختم دون اتصال: لم تعد هناك حاجة إلى أي سلطة خارجية لإنتاج ختم قابل للتحقق.

4.1 ختم HMAC-SHA256 المحلي

الآلية المركزية هي HMAC-SHA256 يُحسب محليًا بمفتاح مخزَّن في TPM الخاص بالجهاز:

```
دالة الختم دون اتصال:

ختم(بيانات، مفتاح_TPM):
  1. ساعة_النظام ← ختم_زمني()
  2. nonce       ← عشوائي(256 بت)
  3. payload     ← ختم_زمني || بيانات || nonce
  4. ختم         ← HMAC-SHA256(مفتاح_TPM، payload)
  5. إرجاع {payload، معرف_المفتاح، ختم}

تحقق(payload، معرف_المفتاح، ختم):
  1. مفتاح_عام ← TPM.قراءة_المفتاح_العام(معرف_المفتاح)
  2. ختم'      ← HMAC-SHA256(مفتاح_عام، payload)
  3. إرجاع (ختم == ختم')
```

الشكل 3: خوارزمية الختم دون اتصال. لا يغادر المفتاح الخاص جهاز TPM أبدًا.

جهاز TPM (وحدة النظام الأساسي الموثوقة) هو معالج تشفيري مساعد عتادي. يُولَّد مفتاح HMAC داخل TPM ولا يخرج منه أبدًا. حتى الوصول الجذري إلى نظام التشغيل لا يسمح باستخراج هذا المفتاح. وعند محاولة اقتحام مادي يكتشف TPM فتح الهيكل ويمحو أسراره تلقائيًا.

4.2 سلسلة الأختام المحلية

يتضمّن كل ختم جديد بصمة الختم السابق، ليشكّل سلسلة غير قابلة للتغيير:

```
الكتلة₁ ← [بيانات₁، t₁، HMAC(مفتاح، بيانات₁‖t₁‖0x00)]
الكتلة₂ ← [بيانات₂، t₂، HMAC(مفتاح، بيانات₂‖t₂‖ختم₁)]
الكتلة₃ ← [بيانات₃، t₃، HMAC(مفتاح، بيانات₃‖t₃‖ختم₂)]
...
```

سلسلة الأختام: تتضمّن كل كتلة بصمة الكتلة السابقة.

تضمن هذه البنية ما يلي:

- لا يمكن إدراج أي كتلة بأثر رجعي (لأن ذلك يكسر السلسلة).
- لا يمكن تعديل أي كتلة (لأن HMAC لن يتطابق بعد ذلك).
- يمكن التحقق رياضيًا من ترتيب الكتل.

4.3 ساعة الثقة

يعتمد الختم دون اتصال على ساعة النظام. ولضمان موثوقية هذه الساعة في غياب بروتوكول وقت NTP (الشبكة)، يستخدم الجهاز:

- **ساعة RTC دقيقة.** ساعة وقت حقيقي بانحراف أقصى ±2 جزء في المليون (±1 ثانية كل 5.7 أيام).
- **نظام GPS مدمج.** وحدة GNSS للمزامنة مع مجموعتي GPS/Galileo، مستقلة تمامًا عن الإنترنت.
- **انحراف موثَّق.** يُسجَّل الفارق بين ساعة GPS ووقت RTC باستمرار. وعند عودة الشبكة يأتي الختم الزمني RFC 3161 ليصادق على السلسلة ويصحح أي انحراف.

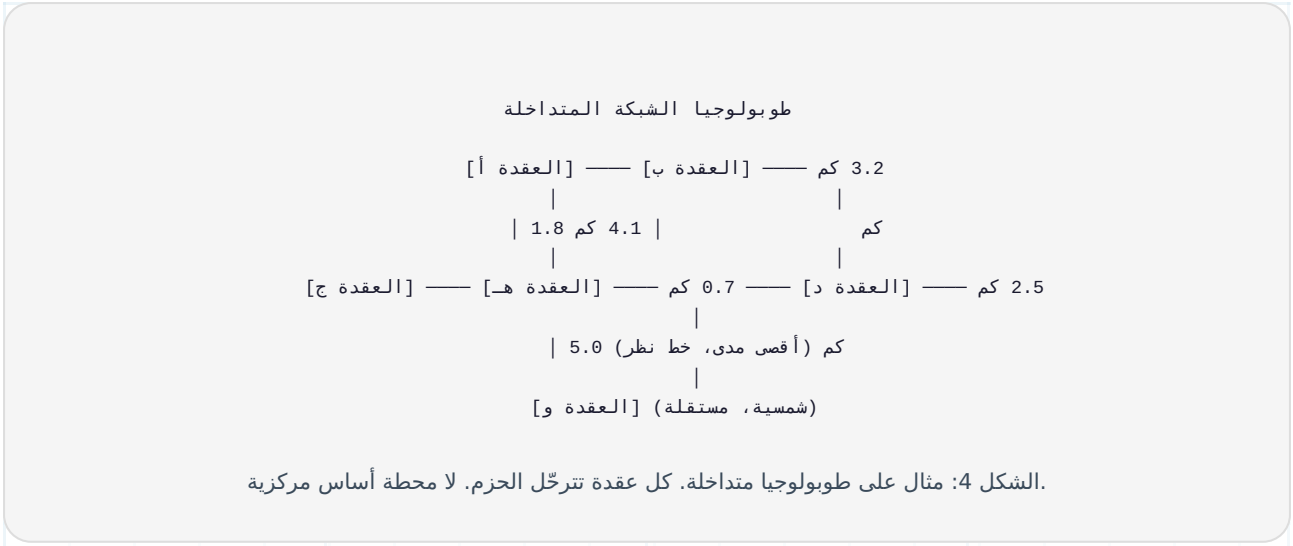
> شرط لا تأكيد عند عودة الشبكة RFC 3161 الختم المنتج دون اتصال ختمٌ صحيح. والتصديق.

5. الشبكة المتداخلة خارج الشبكة — الشبكة بلا بنية تحتية

الطبقة الخامسة من الكبسولة هي الأكثر جذرية: شبكة اتصال لا تعتمد على أي بنية تحتية — لا ألياف ولا نحاس ولا هوائي ترحيل ولا قمر صناعي.

5.1 بنية الشبكة المتداخلة

تستخدم الشبكة المتداخلة لدى 0DATA وحدات راديو LoRa (النطاق الأوروبي 868 ميجاهرتز) بتردد ISM، دون ترخيص) مركّبة على عقد مستقلة:



الشكل 4: مثال على طوبولوجيا متداخلة. كل عقدة تترحّل الحزم. لا محطة أساس مركزية.

وتشمل IP67 كل عقدة موضوعة في غلاف محكم:

- **راديو LoRa SX1276.** مدى 5 كم في خط النظر، و1–2 كم في المنطقة الحضرية الكثيفة.
- **سعة 50 واط/ساعة LiFePO4 لوح شمسي 20 واط + بطارية.** استقلالية غير محدودة في الهواء الطلق.
- **متحكم دقيق ESP32.** إدارة بروتوكول التوجيه وطابور الرسائل.
- **GPS.** مزامنة زمنية وتحديد موقع العقدة.

5.2 بروتوكول التوجيه المتحمّل للانقطاعات

بروتوكول الاتصال مشتق من شبكات التسامح مع التأخير (DTN، RFC 4838)، مكيّف مع قيود LoRa:

- **الإنتاجية.** من 0.3 إلى 37.5 كيلوبت/ثانية وفق المسافة والتضمين (LoRa SF7–SF12).
- **الحمولة المفيدة.** من 51 إلى 222 بايت لكل إطار.
- **التخزين وإعادة الإرسال.** تخزّن كل عقدة الرسائل في طابور وتعيد إرسالها فور وجود جار في المدى.
- **الأولوية.** تُقدَّم أُطر التنبيه (شذوذ حرج) على أُطر القياس عن بُعد.
- **إزالة التكرار.** لكل رسالة معرف فريد؛ وتتجاهل العقد النسخ المكررة.

متوسط زمن الانتقال من 200 إلى 800 مللي ثانية لكل قفزة. وفي شبكة من 6 عقد، تعبر رسالة التنبيه الشبكة المتداخلة في أقل من 5 ثوانٍ — وهو ما يضاهي وصلة قمر صناعي.

5.3 صفر بنية تحتية

لا تتطلب الشبكة المتداخلة لدى 0 DATA:

- أي برج اتصالات.

- أي مزوّد وصول.
- أي ترخيص طيف (نطاق ISM 868 ميجاهرتز).
- أي تغذية من الشبكة الكهربائية.

عند نشرها في موقع معزول — مزرعة أو ملجأ جبلي أو قاعدة خلفية — توفّر الشبكة المتداخلة طبقة اتصال مستقلة تمامًا، تعمل بالشمس على الدوام. وتقتصر الصيانة على التنظيف السنوي للألواح الشمسية.

6. إعادة المزامنة — عند عودة الإنترنت

الانقطاع مؤقت بطبيعته. واللحظة الحرجة هي عودة الشبكة: يجب مزامنة جميع البيانات المتراكمة دون اتصال دون فقدان ودون تكرار ومع تتبع كامل.

6.1 بروتوكول الاستيقاظ

عند عودة الإنترنت ينفّذ الكائن تلقائيًا تسلسل الاستيقاظ:

```
تسلسل الاستيقاظ (المدة النموذجية: 4–8 ثوانٍ)

1. الاكتشاف (فوري)
└ ping 1.1.1.1 (Cloudflare) أو 8.8.8.8
استلام الرد ← بداية التسلسل ←

2. إعادة مزامنة البيانات (2–5 ثوانٍ)
└ الخادم المركزي ← IndexedDB
└ السجلات المحلية ← قاعدة PostgreSQL
└ المقاييس ← القاعدة الزمنية
└ الاستراتيجية: last-write-wins مع ختم زمني TPM

3. الختم eIDAS (ثانية 1–2)
└ سلسلة الأختام المحلية ← تصديق RFC 3161
└ ختم زمني خارجي TSA (GlobalSign، Sectigo)
└ شهادة eIDAS بختم زمني

4. الإشعار (فوري)
└ كنزة: «عادت الشبكة. اكتملت المزامنة.
سجلًا مختومًا. لا فقدان [N]».
```

الشكل 5: تسلسل استيقاظ تلقائي. لا يتدخل المشغّل في أي لحظة.

6.2 اتساق البيانات

تستخدم المزامنة استراتيجية لحل التعارضات تستند إلى الختم الزمني TPM:

- ختم زمني للتعديل (مصدر TPM) لكل سجل ختم زمني للإنشاء.
- عند التعارض (تعديلان متزامنان على السجل نفسه) يغلب الإصدار الأحدث (الختم الزمني TPM).
- لا تُحذف الإصدارات المستبعدة: بل تُؤرشف في سجل التعارضات المتاح للتدقيق.

هذه الاستراتيجية المسماة last-write-wins مناسبة لسيناريوهات الانقطاع حيث تكون التعديلات تسلسلية (مستخدم واحد لكل عضو) لا متزامنة.

6.3 الختم بأثر رجعي eIDAS

أثناء الانقطاع تُنتج الأختام باستخدام HMAC-SHA256 المحلي (القسم 4). وعند عودة الشبكة تصادق سلطة الختم الزمني RFC 3161 المؤهلة وفق eIDAS على هذه الأختام المحلية:

1. تُرسَل سلسلة الأختام المحلية إلى خادم TSA.
2. ينتج TSA ختمًا زمنيًا RFC 3161 يغطي السلسلة بأكملها.
3. هذا الختم الزمني قابل للاحتجاج به قانونيًا (eIDAS، المادة 41 من لائحة قرينة الموثوقية).

النتيجة سلسلة تتبع كاملة: لكل حدث وقع أثناء الانقطاع ختم محلي قابل للتحقق وتصديق eIDAS بختم زمني. القيمة الإثباتية مطابقة لقيمة حدث وقع أثناء الاتصال.

7. حالة ملموسة — انقطاع 23 يوليو

وقع انقطاع في الألياف البصرية على المقطع الذي يخدم موقع اختبار 0 في 23 يوليو 2026DATA. تُوثَّق الحالة هنا بالكامل.

7.1 التسلسل الزمني

الوقت	الحدث
14:31:58	آخر حزمة ACK مستلمة من الخادم المركزي
14:32:00	انتهاء مهلة ping — كشف الانقطاع
14:32:01	تحويل تلقائي إلى وضع الكبسولة
14:33:00	تؤكد كنزة: «وضع الكبسولة نشط. جميع الوظائف قائمة.»

14:33:15	إنتاج أول ختم HMAC (سجل الانقطاع) محلي
14:35:00	يستشير المشغّل الهولوسكوب: جميع الأعضاء مرئية، بيانات محلية
14:42:00	كشف تنبيه سيتوكين (إجهاد وحدة المعالجة) — مختوم محليًا
15:10:00	اتصال متداخل مع العقدة ب (2.8 كم) — تأكدت الحالة
15:45:00	انتهاء تنبيه سيتوكين — مختوم محليًا
16:09:58	عاد الإنترنت — استلام أول حزمة ACK
16:10:00	بداية تسلسل الاستيقاظ
16:10:04	اكتمال إعادة مزامنة IndexedDB ← PostgreSQL
16:10:06	تصديق RFC 3161 على سلسلة الأختام
16:10:07	كنزة: «عادت الشبكة. تمت مزامنة 47 سجلًا. لا فقدان.»

7.2 التحليل

استمر الانقطاع ساعة واحدة و38 دقيقة. خلال هذه الفترة:

- **الصوت (كنزة).** عالجها 12 مكالمة FreeSWITCH المحلي. لم تُفقد أي مكالمة.
- **الختم (SPINA).** أُنتجت وسُلسلت محليًا 47 ختم HMAC. صودق عليها جميعًا بـ RFC 3161 عند العودة.
- **التصوّر (الهولوسكوب).** استشار 3 مشغّلين الواجهة. تشغيل متواصل.
- **الإشراف (سيتوكين).** كُشف تنبيه واحد ووُثّق وخُتم.
- **التخزين.** ميجابايت من البيانات كُتبت في 2.3 IndexedDB، ومُزامَنة بالكامل.
- **الشبكة المتداخلة.** جرى تبادل 18 إطارًا. حوفظ على الاتصال بعقدتين بعيدتين.

لم تنقطع أي وظيفة حيوية. ولم يكن على المشغّل القيام بأي إجراء. كان التحويل (ثانية واحدة) والاستيقاظ (7 ثوانٍ) تلقائيين بالكامل.

7.3 مقاييس المرونة

```
مؤشرات انقطاع 23 يوليو

مدة الانقطاع ..... 1س 38د
زمن التحويل ..... < 1 ث
زمن الاستيقاظ ..... 7 ث
الوظائف الحيوية القائمة ..... 5/5 (100%)
الأختام المنتَجة دون اتصال ..... 47
الأختام المصدّق عليها عند العودة .. 47/47 (100%)
البيانات المُزامَنة ..... 2.3 ميجابايت (0 فقدان)
المكالمات الصوتية المعالَجة ..... 12 (0 مفقودة)
أُطر الشبكة المتبادلة ..... 18
```

جدول مقاييس انقطاع 23 يوليو 2026.

8. الآثار — السيادة كخاصية معمارية

تُعالَج السيادة الرقمية عمومًا من الزاوية القانونية: أين تُخزَّن البيانات، وأي قانون يسري، ومن يملك مفاتيح التشفير. هذا المقارَب ضروري لكنه غير كافٍ. قد يكون النظام سياديًا قانونيًا (بيانات مستضافة في فرنسا، وتشفير مُتقن) و تابعًا وظيفيًا (يتوقف عن العمل إذا سقط الإنترنت).

تنقل الكبسولة السيادية مسألة السيادة من المستوى القانوني إلى المستوى المعماري. الكائن السيادي هو كائن:

1. **يحافظ على وظائفه الحيوية دون اتصال خارجي.** الصوت والإشراف والختم والتصوّر والتخزين مضمونة محليًا.
2. **لا يفقد أي بيانات أثناء الانقطاع.** تضمن الكتابة المحلية (IndexedDB والسجلات والأختام) استمرارية التسجيل.
3. **يعيد المزامنة تلقائيًا عند عودة الشبكة.** الانتقال شفاف. دون أي تدخل بشري.
4. **ينتج أدلة قابلة للتحقق حتى دون اتصال.** يوفر الختم المحلي HMAC + التصديق الرجعي RFC 3161 تتبعًا كاملًا.
5. **يتواصل دون بنية تحتية خارجية.** تضمن الشبكة المتداخلة خارج الشبكة اتصال الملاذ الأخير، دون مشغّل.

8.1 التطبيقات القطاعية

الصحة. يتعرض مستشفى في منطقة ريفية لقطع الألياف. يبقى ملف المريض متاحًا محليًا (PWA + IndexedDB). وتُختم قراءات الشاشات دون انقطاع FreeSWITCH وتُوجَّه مكالمات التمريض عبر المحلي. وعند عودة الشبكة يُزامَن الملف مع الخادم المركزي.

الصناعة. يفقد مصنع متصل الإنترنت لمدة 6 ساعات. يستمر الإشراف (الهولوسكوب المحلي). وتُكشف وتتواصل الفرق عبر الشبكة المتداخلة (دون الحاجة إلى شبكة .(دون اتصال SPINA) تنبيهات الآلات وتُختم هاتف محمول). وعند إعادة المزامنة يكون تقرير الإنتاج مكتملًا وبختم زمني eIDAS.

الزراعة. تستخدم مزرعة معزولة (بلا ألياف، وبتغطية خلوية متقطعة) الشبكة المتداخلة لربط LoRa مستشعرات الرطوبة ومحطات الطقس ومضخات الري. تعمل الشبكة على الدوام بالطاقة الشمسية. وتُجمَّع البيانات محليًا وتُزامَن أثناء المرور الدوري لمركبة متصلة.

8.2 الفرضية المعكوسة

تطرح المعلوماتية التقليدية: «كل شيء يعمل مع الإنترنت. فماذا نفعل عند العطل؟»

تعكس الكبسولة السيادية الفرضية: «كل شيء يعمل دون إنترنت. والإنترنت يجلب إثراءً.»

هذا الانقلاب ليس بلاغيًا. إنه معماري. كل مكوّن مصمَّم ومطوَّر ومختبر ليعمل أولًا في عزلة. الاتصال طبقة إضافية لا أساس. وكما يحافظ الكائن الحي على استتبابه الداخلي باستقلال عن الظروف الخارجية، تحافظ الكبسولة على سلامتها الوظيفية مهما كانت ظروف الشبكة.

> المرونة ليست ميزة. إنها خاصية ناشئة عن بنية لا يكون فيها الاتصال الخارجي شرطًا للتشغيل أبدًا.

المراجع

[1] TIKIJJA, Hadda. «0 مختبر .«الانضباطIDATA، 2026 يوليو 001، البحث.

[2] TIKIJJA, Hadda. «0 مختبر .«الجهاز العصبيIDATA، 10.5281 :زينودو. 2026 يوليو 003، البحث/ zenodo.21342768.

[3] TIKIJJA, Hadda. «0 مختبر .«الجهاز المناعيIDATA، 2026 يوليو 005، البحث.

[4] TIKIJJA, Hadda. «SPINA — 0 مختبر .«بروتوكول الختمDATA، 2026 يوليو 008، البحث.

[5] TIKIJJA, Hadda. «0 مختبر .«أول طُعمIDATA، 2026 يوليو 010، البحث.

[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] 910/2014 رقم (الاتحاد الأوروبي) اللائحة — eIDAS. 2014 ،البرلمان الأوروبي.

[10] LoRa Alliance. «LoRaWAN Specification 1.1». 2017.

[11] Trusted Computing Group. «TPM 2.0 Library Specification». 2019.

[12] ARCEP. «مرصد جودة الشبكات الثابتة». التقرير السنوي، 2025.

شكر وتقدير.

إلى فرق الاختبار التي قبلت فصل الألياف البصرية طوعًا للتحقق من بروتوكول التحويل. وإلى على الأعمال التأسيسية حول الشبكات DTN ميجاهرتز. وإلى مجتمع ISM 868 لتحرير النطاق LoRa مشروع المتحملة للتأخير. هذا البحث مهدى إلى جميع البنى التحتية التي تعمل في ظل اتصال غير مؤكد — المناطق الريفية والمواقع المعزولة والبيئات العدائية.

لم تعد بحاجة إلى الإنترنت لتوجد.

«المرونة ليست ميزة. إنها خاصية ناشئة عن بنية لا يكون فيها الإنترنت شرطًا أبدًا».