

RDEM Time Evidence — Référentiel méthodologique de mesure et de preuve

Constitution, qualification et conservation d'une preuve temporelle continue · document normatif

RDEM Time Evidence est un système de preuve continue de conformité temporelle, fondé sur la séparation entre la mesure, son interprétation et la qualification de la preuve.

Statut : ☒ Stable ☒ Applicable ☒ Document normatif · **En résumé (lecture non technique) :** ce référentiel définit comment RDEM Systems mesure l'heure d'une organisation, comment il qualifie ces mesures, et comment il en conserve une preuve vérifiable dans le temps. Il sépare trois questions distinctes : « l'heure est-elle juste ? », « l'appareil de mesure est-il crédible ? » et « la preuve est-elle complète ? ».

Référence : RDEM-TEM-001 · **Version :** 1.5 · **Date :** 2026-07-17 · **Éditeur :** RDEM Systems

Disponible publiquement : <https://pkg.rdem-systems.com/time-evidence/RDEM-TEM-001-v1.5.pdf>

Ce référentiel décrit la méthode, les politiques, les règles, les hypothèses et les limites appliquées pour produire les dossiers de preuve « RDEM Time Evidence ». Chaque rapport généré référence l'identifiant, la version et l'empreinte SHA-256 de ce document. Il est stable et versionné : toute évolution incrémente la version et produit une nouvelle empreinte.

1. Objet et portée

RDEM Time Evidence produit des **dossiers de preuve de conformité temporelle** destinés à être versés à l'audit d'une organisation tierce (l'« audité »). RDEM Systems intervient comme **mesureur indépendant** : le rapport **constate** la conformité de l'heure de l'audit, telle qu'observée par l'instrument de mesure RDEM. Le référentiel du rapport est donc l'**audité** ; un défaut imputable à un tiers (RDEM lui-même, un fournisseur amont) est **tracé et distingué**, jamais imputé à tort à l'audité.

La méthode ne se prononce que sur ce qui est **mesuré**. Elle sépare explicitement le fait mesuré de son interprétation, et n'affirme jamais au-delà des données collectées.

Un dossier RDEM Time Evidence répond à **trois questions distinctes**, chacune établie par sa propre chaîne de mesure :

1. **L'instrument de mesure est-il fiable ?** — établi par la déviance de la sonde par rapport à une pluralité d'**ancres publiques hétérogènes** (§5, §7).
2. **Les serveurs de temps de l'audité sont-ils conformes ?** — établi par l'offset mesuré des serveurs internes déclarés, contre la politique appliquée (§4, §6).
3. **Ces serveurs sont-ils effectivement utilisés ?** — établi par l'observation du trafic entrant : quelles adresses ont **effectivement interrogé** le serveur pendant la période (annexe parc). Ceci constate un **usage observé**, non une configuration déclarée ni une appartenance au parc de l'audité — ce rapprochement relève de l'inventaire de l'audité (CMDB, pages détenues), au titre de la séparation des responsabilités (§12).

1bis. Registre de langage (normatif)

La méthode **constate** et **établit** ; elle n'affirme pas. Tout énoncé produit sous ce référentiel est **attribué** : « **selon RDEM-TEM-001**, ... ». Un rapport ne dit jamais « le serveur est conforme » mais « RDEM-TEM-001 **constate** que X % des mesures sont dans la tolérance de la **politique appliquée** ». La distinction n'est pas cosmétique : RDEM mesure et constate, il ne

certifie pas — la qualification finale appartient à l'audité et à son auditeur, dans leur propre référentiel (§12).

2. Principe fondateur — séparation des preuves

Ce rapport distingue trois propriétés **indépendantes**. Une insuffisance sur l'un de ces axes n'implique pas automatiquement une insuffisance sur les deux autres.

C'est le fondement de la méthode, davantage que la mesure NTP elle-même. La plupart des systèmes de supervision ramènent tout à un **indicateur unique de disponibilité** ; TEM-001 refuse cette réduction et permet des verdicts nuancés — par exemple « *heure conforme, instrument qualifié, preuve incomplète mais justifiée* », ou « *heure non conforme, instrument parfaitement qualifié, preuve complète* ». Cette séparation rend le raisonnement d'audit rigoureux : chaque axe se lit et se conteste séparément.

Qualité de l'heure	Qualité de l'instrument	Complétude de la preuve
L'écart (offset) des mesures acquises vis-à-vis de l'heure de référence, sur les points effectivement collectés.	La crédibilité de l'appareil de mesure lui-même : stabilité de son horloge, cohérence avec des références externes hétérogènes.	La proportion de la période pour laquelle une preuve a effectivement été collectée (couverture), et la qualification des éventuels trous.

La plupart des outils de supervision fondent ces propriétés dans un indicateur unique de « disponibilité ». RDEM Time Evidence les **sépare** : un rapport peut être « heure conforme, couverture incomplète mais justifiée », sans que la qualité de l'horloge soit mise en cause.

3. Architecture de mesure

Trois dimensions distinctes — à ne pas confondre : le **logiciel** (un seul), le **déploiement** (où il tourne) et la **topologie** (comment la mesure est prise).

Logiciel	Déploiement	Topologie de mesure
Agent RDEM <i>binaire Go identifié, versionné, qualifié</i>	Sonde SaaS	plusieurs sondes observent le NTP de l'audité depuis des points de mesure distincts — consensus multi-sondes (une perte de sonde isolée ne crée pas de faux incident)
	Appliance	mesure locale des NTP officiels + vérification contre ≥ 5 ancres publiques hétérogènes + comptage des requêtes NTP servies au parc
	Agent client léger	mesure locale uniquement, transmise signée à l'API

Le logiciel est commun ; **les capacités changent selon le déploiement**. « Agent » désigne le logiciel ; « sonde », « appliance » et « agent léger » désignent des **points de mesure** — ce ne sont pas des synonymes.

Chaîne de preuve.

Agent RDEM (mesure) → API sécurisée → Moteur Time Evidence (qualifie, applique TEM, signe) → Rapport (conclut).

Une appliance = un instrument = un rapport. Le mono-déploiement est un point de mesure unique (mais MULTI-références : NTP internes + ancres publiques + privées de diagnostic) ; la redondance s'obtient par plusieurs déploiements indépendants (rapport consolidé), non par regroupement dans un même dossier.

3bis. Séparation des rôles et attribution des fautes

Deux principes **distincts** — à ne pas confondre :

- **Séparation des rôles de la chaîne** : l'agent **mesure**, le moteur **qualifie** (applique la méthode), le rapport **conclut**. L'instrument ne juge **jamais** lui-même la conformité de l'audité — le mesureur ne s'auto-certifie pas.
- **Attribution des fautes** : chaque défaut de collecte est **imputé à une cause** (panne RDEM · perte internet · maintenance/extinction VM déclarée par l'audité · dérive de la cible) et **jamais mélangé** aux autres. Le fait mesuré est immuable ; l'attribution vit à côté, à recouper avec le registre de l'audité.

4. Grandeur mesurée

La grandeur fondamentale est l'**offset** : l'écart, en millisecondes, entre l'heure servie par la cible et l'heure de référence de la sonde, mesuré par les protocoles **NTP** et, lorsque la cible le supporte, **NTS** (NTP sécurisé, authentifié). Chaque mesure porte son horodatage, son protocole et son résultat (succès avec offset, ou échec). Les mesures en échec (cible injoignable) ne portent pas d'offset : elles relèvent de la **couverture**, non de la qualité de l'heure.

5. Références (ancres)

RDEM ne prétend pas « prouver UTC ». Aucun système ne le fait — un laboratoire accrédité lui-même ne démontre qu'une **traçabilité** vers une référence. RDEM **constate** que l'infrastructure de l'audité est restée **cohérente avec une pluralité de références temporelles hétérogènes**, selon une politique de mesure documentée.

Robustesse plutôt qu'indépendance absolue. RDEM Systems opère à la fois des serveurs NTP publics et les sondes de mesure ; certaines références publiques **peuvent donc être communes** avec l'infrastructure audité. La méthode ne revendique **pas** l'indépendance absolue des sources — une garantie que personne ne peut honnêtement apporter sur l'écosystème NTP public. Elle est conçue pour rester **robuste** même lorsqu'une ou plusieurs références sont communes, en s'appuyant sur : la **diversité des opérateurs**, la **pluralité des références**, le **consensus** (quorum), et l'**absence de décision fondée sur une mesure unique**. La preuve ne repose jamais sur une source isolée mais sur la convergence de plusieurs instruments et de plusieurs références.

5.1 Références publiques — diversité et consensus

La cohérence de l'instrument est établie contre un jeu d'ancres publiques **volontairement hétérogènes** (opérateurs, systèmes autonomes, infrastructures et implémentations différents) afin de **limiter le risque de dépendance commune** : à titre d'exemple Google, Cloudflare, Netnod, Apple, Microsoft. La cohérence est établie par **quorum** (≥ 5 ancres) : une ancre isolée aberrante est écartée tant que le quorum tient ; l'absence de quorum est signalée comme une déviance de l'instrument, jamais imputée aux cibles de l'audité. C'est la **diversité et le consensus** qui font la robustesse, non l'hypothèse d'une indépendance parfaite.

5.2 Références privées RDEM — diagnostic uniquement

Les serveurs de RDEM Systems (pa3/pa4/pa5) peuvent apparaître à titre de **diagnostic**. N'étant pas indépendants de l'éditeur, ils ne sont **pas** comptés comme référence de cohérence et sont présentés séparément des références publiques.

5.3 Transparence de l'infrastructure RDEM — contrôle externe

Les infrastructures opérées par RDEM Systems et utilisées comme références privées sont elles-mêmes exploitées comme **serveurs publics du projet `pool.ntp.org`**. Leur disponibilité et leur qualité de service sont **surveillées en continu par les moniteurs du pool**, et leurs scores sont **publiquement consultables** (`ntppool.org/a/rdem-systems`). Autrement dit : RDEM Systems n'est pas uniquement juge de sa propre infrastructure — une partie de sa qualité opérationnelle est également **observée par un tiers ouvert**, indépendamment de Time Evidence, et **vérifiable sans nous croire sur parole**. Cette transparence **ne remplace pas** les références publiques utilisées pour la mesure (§5.1) ; elle fournit un **contrôle externe supplémentaire** sur l'infrastructure RDEM.

5.4 Vocabulaire du consensus — quatre notions à ne pas confondre

Ces termes sont proches mais **techniquement distincts**. Un lecteur qui découvre le référentiel ne doit pas lire « consensus » en pensant toujours au même mécanisme.

Terme	Définition exacte
Quorum	nombre minimal d'ancres publiques cohérentes exigé (paramètre de la méthode).
Consensus des ancres	résultat obtenu lorsque ce quorum est atteint : une majorité d'ancres hétérogènes s'accorde.
Consensus des sondes	accord entre plusieurs sondes SaaS observant la même cible depuis des points distincts. N'existe qu'en mode multi-sondes ; en appliance mono-sonde, il n'y a pas de consensus inter-sondes.
Cohérence avec les ancres	propriété observée de l'instrument : la sonde reste alignée sur le consensus des ancres. C'est ce qui qualifie l'instrument (§7), y compris en mode mono-sonde .

En clair, selon le mode de déploiement : une **appliance mono-sonde** s'appuie sur le **consensus des ancres** (quorum) et la **cohérence** de son instrument — jamais sur un consensus des sondes, qui n'a pas de sens à une seule sonde. Une **flotte SaaS** ajoute le **consensus des sondes**. Le mode mono-sonde **n'est pas en soi une réserve** : le consensus y est porté par le **quorum d'ancres**, pas par une pluralité de sondes.

6. Politique de conformité

La conformité de l'heure est évaluée contre un **offset maximal autorisé** :

Paramètre	Valeur par défaut	Origine
Offset maximal autorisé	± 50 ms	Politique RDEM Systems par défaut — configurable par le client

Ce seuil est un **choix de politique RDEM Systems**, non une norme universelle. Il est calibré pour être suffisamment strict pour la plupart des métiers, tout en restant assez large pour ne pas déclencher sur le bruit réseau des sondes SaaS. Il n'est pas dérivé d'une exigence réglementaire particulière : selon le référentiel applicable (MiFID II RTS 25, PCI-DSS, ISO 27001...), l'audité définit son propre seuil, que la politique RDEM permet de configurer. La valeur appliquée est indiquée sur chaque rapport.

7. Qualité de l'instrument

Définition. L'instrument de mesure est constitué de l'**Agent RDEM** (le logiciel de collecte — composant identifié, versionné et qualifié : il interroge l'environnement temporel local via `chronyc`, effectue des requêtes NTP/NTS actives, signe ses lots et les transmet au moteur) **et de l'environnement temporel local qu'il interroge**. Son **identité** — id d'agent, version/commit, empreinte de clé publique — est portée par le rapport : l'instrument n'est pas un logiciel anonyme.

L'instrument est qualifié par : la **santé de sa synchronisation** (état chrony, âge de synchronisation, sources joignables, absence de falsetickers), sa **cohérence offset** contre les ancrs publiques, et l'**intégrité UTC** par quorum d'ancres. Les phases de démarrage (bootstrap de la synchronisation) sont **tracées et exclues** du verdict de l'instrument, car non représentatives du régime établi.

7bis. Défendabilité de la mesure — badge de confiance

Défendabilité — niveau de **confiance qu'un tiers (auditeur) peut accorder AU DOSSIER**. Elle répond à une question **distincte du verdict de conformité** : le verdict dit « l'heure était-elle juste ? » ; la défendabilité dit « a-t-on assez observé, l'instrument était-il fiable ? ». **Un rapport peut être CONFORME et porter une défendabilité inférieure à « Élevée »** : l'heure était bonne, mais le dossier comporte une réserve (couverture ou instrument). Ce n'est **pas** une contradiction. La défendabilité qualifie **le dossier de preuve**, pas l'audité.

Elle se calcule sur **trois axes**, chacun classé en trois bandes :

Axe	Bandes
Couverture (complétude de la collecte, brute — §8)	mauvais : < 50 %
Données (qualité temporelle : mesures dans la tolérance — §6)	moyen : [50 % ; seuil[
Instrument (§7) : qualifié→bon · indéterminé→moyen · dégradé→mauvais	bon : ≥ seuil

Le **seuil « bon »** est un **paramètre de politique, par défaut 99 %**. L'audité peut le **durcir** (le porter plus haut) via son contrat ; il ne peut **jamais** l'abaisser sous 99 %. Le **plancher « mauvais » à 50 %** est **fixe** : au-delà de la moitié de la période sans donnée, le dossier est indéfendable, quel que soit le reste.

Le niveau résulte du **compte des axes par bande** :

Niveau	Condition	Lecture
Élevée (vert)	les 3 axes bons	rien à signaler — dossier pleinement opposable.
Satisfaisante (jaune)	exactement 1 axe moyen	un axe légèrement en retrait, le dossier reste solide.
Modérée (orange)	≥ 2 axes moyens	plusieurs réserves, sans rupture — dossier à lire avec les axes.
Insuffisante (rouge)	≥ 1 axe mauvais (dont instrument dégradé, ou > 50 % de trou)	on ne peut pas se fier au dossier — cause tracée.

Un rapport **sans aucune donnée** (période antérieure à la mise en service, 0 mesure) a couverture et données en « mauvais » → défendabilité **Insuffisante** : la méthode **refuse de conclure** en l'absence de preuve, plutôt que d'afficher un résultat positif sur une période vide.

Les **trois axes restent lisibles séparément** dans le corps du rapport — le badge les **résume** en page de synthèse, il ne les **fond pas**. Le rapport porte le badge global **et** une pastille par axe, plus le **seuil appliqué**.

Le **mode appliance mono-sonde n'est pas en soi une réserve** : l'instrument unique est **multi-références** (ancres publiques hétérogènes + cibles internes déclarées), et une appliance à collecte complète et heure conforme atteint **Élevée**. Le « consensus » y est porté par le **quorum d'ancres** (§5), non par une flotte de sondes.

8. Complétude de la preuve (couverture)

La couverture mesure la proportion de la période pour laquelle une preuve a effectivement été collectée. Elle repose sur une **cadence d'engagement** (par défaut 1 point toutes les 10 minutes) : au-delà de ce délai sans mesure, un **trou** est

constaté. La couverture est calculée sur la **présence de données** de la sonde, distinctement de la réussite des cibles.

Ajustement des trous justifiés. Un trou **excusé** (cause attribuée à un tiers par constat RDEM), **résolu** (données finalement reçues en différé — retard de livraison, 0 impact) ou **justifié** par l'audité sort du **dénominateur** de couverture, exactement comme il sort du décompte des pertes inexplicables. Le trou reste **montré** (bornes, durée) : il n'est jamais effacé, seulement qualifié. Seul un trou **injustifié** abaisse la couverture sous le seuil et rend le verdict de couverture non conforme.

9. Gestion des incidents

Un incident est un **fait mesuré, immuable** (« N mesures en échec de T1 à T2 »). Son **attribution** et sa **justification** vivent dans des annotations distinctes, à côté du fait — jamais en écrasement. Trois sources d'annotation, hiérarchisées par niveau de confiance :

Type	Signification
offset_drift	Dérive d'offset au-delà du seuil (axe qualité de l'heure).
target_gap	Cible injoignable : mesures en échec sur une cible (axe couverture).
vantage_gap / sonde muette	Perte de données de la SONDE elle-même (toutes cibles), pas un échec des cibles.

- **Constat RDEM** (cause attribuée à RDEM ou à un tiers amont) → l'incident est **excusé** : hors faute de l'audité.
- **Déclaration de l'audité** → reproduite à l'identique, sans modification par RDEM Systems ; elle constitue un élément de preuve à **recouper avec le registre d'incidents de l'audité**. RDEM ne valide pas la cause déclarée.
- **Résolution automatique** (retard de livraison) → un trou comblé par des données arrivées en différé, complètes et dans l'ordre, est **clos** avec 0 impact conformité, en restant tracé.

10. Chaîne de preuve et intégrité

L'intégrité des données mesurées repose sur un **journal d'intégrité append-only** (`evidence_log`) : chaque lot de mesures est signé par l'agent de la sonde et chaîné par empreinte (`prev_hash` → `chain_hash`), rendant toute altération ou réordonnancement détectable. Chaque rapport porte une empreinte **SHA-256 de son instantané de synthèse** (`report_hash`), le liant à un jeu de données exact et vérifiable.

Chaque entrée du journal d'intégrité contient :

- `timestamp` — l'instant du lot de mesures ;
- `payload` — le lot de mesures lui-même ;
- `prev_hash` — l'empreinte de l'entrée précédente (chaînage) ;
- `chain_hash` — l'empreinte cumulée de la chaîne jusqu'à cette entrée ;
- `signature_agent` — la signature du lot par l'agent de la sonde émettrice.

Toute modification, suppression ou réordonnancement rompt la chaîne d'empreintes et devient donc détectable.

Preuve technique vs preuve juridique (feuille de route signature). La version actuelle produit des rapports **non signés** (mention explicite en première page). Un tel rapport constitue un **élément de preuve technique** — un fait démontré et vérifiable ; l'**opposabilité juridique renforcée** (signature électronique **PADES** + horodatage qualifié **RFC 3161** par un tiers de confiance) sera disponible dans la **version de production**. « Preuve technique » et « preuve juridique » (pièce opposable) sont deux niveaux distincts : ce référentiel documente et outille le premier, et prépare le second.

11. Versionnement et référence

Historique : v1.4 — chapitre modèle de menaces (§12), gel/scellement (§11bis), registre de langage (§1bis). v1.4-b — glossaire du consensus (§5.4) et mise en avant de la séparation des axes (§2). **Une version publiée est immuable** : son empreinte SHA-256 fait foi ; toute évolution du contenu produit une nouvelle version et une nouvelle empreinte, jamais une réécriture de la précédente.

La méthode est versionnée et publiée à une URL permanente. Chaque rapport indique la **référence (RDEM-TEM-001)**, la **version** et l'**empreinte SHA-256** du présent document, ainsi que la version du moteur de mesure (commit) ayant produit le rapport. L'auditeur peut ainsi vérifier exactement quelle méthode a été appliquée, et reproduire le raisonnement.

Chaque rapport porte l'identification du moteur ayant produit la mesure, par exemple :

Moteur	Version	Commit	Build
RDEM Collector	2.4.7 <i>(exemple)</i>	ab34fd9 <i>(exemple)</i>	2026-07-04 <i>(exemple)</i>

Gestion des mises à jour. La version de l'agent collecteur et sa version de protocole sont **scellées par lot de mesures** dans le journal d'intégrité signé (§10). Une mise à jour du binaire en cours de période fait donc apparaître **plusieurs versions** dans le rapport, avec leurs bornes temporelles : la transition est **tracée et vérifiable**, jamais silencieuse. La compatibilité agent↔moteur est garantie par la **version de protocole** — tout changement de format de lot l'incrémente, et un lot d'une version non supportée est rejeté plutôt qu'interprété de travers.

11bis. Gel, scellement et réémission

Le **gel** d'un rapport est matérialisé par sa **signature** : avant signature, rien n'est opposable. Un rapport scellé n'est **jamais réécrit**. Lorsque les données d'entrée d'une période évoluent après le gel — mesure parvenue tardivement, justification enregistrée après coup — RDEM produit une **nouvelle émission**, datée et signée à son propre instant, qui **ne remplace ni ne corrige** la précédente : celle-ci demeure valide et conservée. Chaque émission porte son **rang** et son **motif**. La **suite des émissions** constitue elle-même un élément de la piste d'audit ; l'écart entre deux émissions est un fait, non une erreur.

Le scellement associe : une **signature OpenPGP détachée** (origine et intégrité), un ou plusieurs **horodatages RFC 3161** délivrés par des autorités tierces (la redondance vise la **disponibilité à l'instant du scellement** — un horodatage ne se rattrape pas — et la **diversité des ancrs de confiance** dans la durée), et un ancrage **OpenTimestamps** indépendant de toute autorité. L'empreinte de la clé de signature est **imprimée dans le rapport avant scellement** ; la clé publique n'est **pas** jointe au dossier — jointe au document qu'elle certifie, elle n'établirait rien : elle se récupère hors bande.

12. Modèle de menaces — hypothèses, couverture, limites

Ce chapitre est **normatif**. Il énonce ce que la méthode **suppose**, ce qu'elle **couvre** et ce qu'elle **ne couvre pas**. Ces limites sont **énoncées par RDEM Systems**, non découvertes par un tiers : elles font partie de la méthode. Un dossier de preuve ne vaut que si l'on sait **contre quoi** il protège.

12.1 Hypothèses de confiance

- Les **ancres** retenues ne sont pas compromises simultanément (le quorum, §5, perd sinon son sens).
- La **clé de signature** RDEM n'est pas compromise.
- Le **central RDEM** et l'**agent** ne sont pas compromis (cf. 12.3).
- Les **autorités d'horodatage** attestent une date honnête (atténué : plusieurs autorités + ancrage OpenTimestamps, §10).

12.2 Menaces couvertes

- **Altération du rapport après émission** — signature OpenPGP détachée, vérifiable par l'auditeur seul.
- **Antidatage** — horodatage RFC 3161 auprès d'autorités tierces + ancrage OpenTimestamps.
- **Altération des mesures après ingestion** — journal d'intégrité append-only, chaîné et signé.
- **Sonde qui dérive** — qualification de l'instrument (§7) et cohérence avec un quorum d'ancres.
- **Usurpation NTP sur le chemin** — NTS (authentification), plancher par exécution.
- **Faux incident** issu d'une sonde isolée — consensus multi-sondes ; aucune décision mono-mesure.
- **Réécriture silencieuse d'un rapport** — impossible par construction : une donnée qui évolue produit une **nouvelle émission** signée ; l'émission antérieure demeure (§11bis).

12.3 Menaces NON couvertes

- **Compromission de RDEM Systems.** Les rapports produits par les outils internes de RDEM et signés automatiquement **établissent** qu'ils ont été **émis par notre plateforme**. En cas de compromission de notre infrastructure, un attaquant pourrait produire des rapports **signés en notre nom** et **horodatés par nos tiers**, exactement comme nous le faisons. **Ce constat est structurel** : une signature automatique par API — fût-elle opérée par un tiers de confiance, avec tout niveau de certification — ne fermerait pas cet écart, car l'API demanderait la signature et l'obtiendrait. La signature **établit l'origine et l'intégrité** ; elle n'établit **jamais l'indépendance** : RDEM signe ses propres rapports. Le **seul tiers** de la chaîne est l'autorité d'horodatage, qui atteste la **date** sans rien savoir du **contenu**. Des mécanismes de contrôle, notamment dans la base de séries temporelles, visent à **détecter** de telles intrusions ou modifications de données.
- **Clé de signature compromise** — permettrait de produire des rapports indiscernables des nôtres jusqu'à révocation ; propriété de toute infrastructure à clés.
- **Détournement simultané des références.** Les mesures proviennent de **5 points d'observation situés dans 5 systèmes autonomes**, dont **3 opérateurs tiers dans 3 pays** (AS1299 Arelion/SE, AS29075 IELO/FR, AS51167 Contabo/DE), **1 opéré par RDEM** (AS206014) et **1 par un client** (AS199275 — entité distincte mais **partie liée**). Un détournement BGP devrait réussir **sur l'ensemble**, et simultanément sur des ancres hétérogènes. La diversité **réellement indépendante de RDEM** est donc de **3 systèmes autonomes** ; face à une compromission de RDEM (ci-dessus), elle est nulle sur AS206014.
- **Déclarations de l'audité** — justifications et qualifications sont **client-déclarées et non vérifiées**. RDEM les reproduit **à côté** du fait mesuré, ne les valide pas et ne masque jamais la mesure.
- **Portée juridique** — les horodatages **ne sont pas qualifiés** au sens eIDAS : **aucune présomption légale**. Preuve **technique** de date. Un horodatage qualifié peut être fourni en option.
- **Durée** — RDEM s'engage sur **3 ans** (rétention). La vérifiabilité au-delà est **recherchée, non garantie**.
- **Heure légale** — RDEM ne prouve **pas** UTC ; il **établit la cohérence** avec une pluralité de références hétérogènes, selon une politique documentée.
- **Seuil de conformité** — c'est une **politique**, pas une norme : l'audité reste responsable du seuil applicable à son référentiel.
- **Mono-appliance** — un déploiement mono-appliance constitue un point de mesure unique ; la redondance s'obtient par plusieurs appliances.
- **Indépendance des ancres** — le jeu d'ancres publiques (issu notamment de `pool.ntp.org`) est dynamique et peut, par construction, inclure des serveurs opérés par RDEM. La méthode ne s'appuie donc pas sur une hypothèse d'indépendance mais sur la **robustesse par diversité et consensus** (§5) ; en contrepartie l'infrastructure RDEM est soumise à un **contrôle externe public** (§5.3).

RDEM-TEM-001 v1.5 — © RDEM Systems, 2026-07-17. Document méthodologique référencé par les dossiers de preuve RDEM Time Evidence.

Versionné et publié : chaque version est **figée** par l'empreinte SHA-256 imprimée dans le rapport qui la référence, et publiée à l'adresse ci-dessous. Le **contenu** de la méthode est reproductible depuis les sources ; le fichier PDF publié, lui, est identifié par son empreinte — c'est elle, et non une reconstruction octet-à-octet, qui fait foi. <https://pkg.rdem-systems.com/time-evidence/RDEM-TEM-001-v1.5.pdf>