

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 :** 1.0 · **Date :** 2026-07-05 · **Éditeur :** RDEM Systems

Disponible publiquement : <https://pkg.rdem-systems.com/time-evidence/RDEM-TEM-001-v1.0.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 atteste la conformité de l'heure de l'audité, 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.

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.

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 indépendantes.	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

3.1 Mode SaaS (l'objet audité est le serveur NTP)

Plusieurs sondes RDEM réparties interrogent le serveur NTP de l'audité. La conformité est établie par **consensus multi-sondes** : une perte de sonde isolée ne crée pas de faux incident.

3.2 Mode Appliance (l'objet audité est l'instrument de mesure local)

Une appliance autonome est déployée sur le site de l'audité. Elle :

- mesure en permanence les serveurs NTP officiels de l'audité ;
- se vérifie en continu contre **au moins 5 ancrs publics indépendantes** ;
- peut servir de source NTP au parc de l'audité (avec comptage des requêtes servies).

Une appliance = un instrument = un rapport. Le déploiement mono-appliance constitue un point de mesure unique ; la redondance métrologique s'obtient par plusieurs appliances (rapport consolidé), non par regroupement dans un même dossier.

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)

5.1 Références publiques — preuve d'UTC

La cohérence de l'instrument avec UTC est établie contre un jeu d'ancres publiques **volontairement hétérogènes** (opérateurs, systèmes autonomes, infrastructures et implémentations différents) afin d'éviter toute dépendance commune : à titre d'exemple Google, Cloudflare, Netnod, Apple, Microsoft. L'intégrité UTC est établie par **quorum** (≥ 5 ancrs) : 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.

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** utilisés comme preuve d'UTC et sont présentés séparément des références publiques.

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

L'instrument (l'horloge de la sonde) est qualifié par : la **santé de sa synchronisation** (état chrony, âge de synchronisation, sources joignables, absence de falsetickers), sa **cohérence offset** contre les ancres 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.

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'audit sort du **dénominateur** de couverture, exactement comme il sort du décompte des pertes inexpliquées. 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'audit.
- **Déclaration de l'audit** → reproduite à l'identique, sans modification par RDEM Systems ; elle constitue un élément de preuve à **recouper avec le registre d'incidents de l'audit**. 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 une **preuve technique de mesure** — 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

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'incrmente, et un lot d'une version non supportée est rejeté plutôt qu'interprété de travers.

12. Limites et non-garanties

- Un déploiement **mono-appliance** constitue un point de mesure unique ; la redondance s'obtient par plusieurs appliances indépendantes.
- La version V1 produit des rapports **non signés** = preuve **technique** de mesure. L'opposabilité juridique renforcée (signature électronique + horodatage qualifié) est disponible dans la version de production.
- Le seuil de conformité est une **politique**, pas une norme : l'audité reste responsable du seuil applicable à son référentiel.
- Les déclarations de l'audité ne sont **pas vérifiées** par RDEM ; elles sont reproduites pour recoupement avec le référentiel de l'audité.