

IIC TSA — Self-assessment against ETSI EN 319 421 V1.2.1

Publication notice. This document is published by HTTPS CARD — INTERNET IDENTITY CARD LIMITED (England and Wales, company no. 09168431) for the IIC TSA time-stamping service at <https://tsa.internetidentitycard.com/tsa>. IIC TSA is designed to RFC 3161 / RFC 5816. It is **not** a qualified trust service under eIDAS or UK eIDAS, and it is not certified, accredited or recognised by any authority. IIC TSA and VerifBox (verifbox.com) belong to the same company: for VerifBox users, IIC TSA is not an independent third party. Use of the service is subject to the [IIC TSA terms of use](#).

Version 1.0 — 11 October 2026. Published by the operator on www.internetidentitycard.com/tsa. This is a self-assessment, not a conformity assessment, a certification or a claim of conformance (see below). It is revised with every revision of the Practice Statement and published in the same lot, so that it never describes a practice other than the current one; its date and version are to be compared with those of the Practice Statement.

What this is. A clause-by-clause comparison of IIC TSA, as described in its Timestamp Policy v1.0 and Practice Statement v1.0 (both with erratum 1) and as operated since 10 October 2026, with the requirements of ETSI EN 319 421 V1.2.1 (2023-05), *Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*, read against the V1.2.1 text. Where EN 319 421 delegates to ETSI EN 319 401 (general TSP requirements), the assessment is summarised at the level of the referring clause and is less detailed.

What this is not. It is a **self-assessment by the operator**, not a conformity assessment under EN 319 403-1, not a certification, and not a claim of conformance to EN 319 421. IIC TSA does **not** claim the Best practices Time-Stamp Policy (BTSP, OID 0.4.0.2023.1.1) and does not include it in its tokens. IIC TSA is designed to RFC 3161 / RFC 5816; it is not a qualified trust service; IIC TSA and VerifBox belong to the same company. Clause 8 (qualified time-stamps) is out of scope and not assessed.

Reading the status column. *Meets* — the practice described in the Practice Statement satisfies the requirement as written. *Partial* — the intent is met by a different or weaker control, stated. *Gap, stated* — not met; the gap is known, documented in the Practice Statement or Risk Register, and accepted by the operator. *Inherited* — the control belongs to the cloud provider (Google Cloud, region europe-west1) under its own certifications, which the operator relies on but has not assessed. *N/A* — not applicable to this service.

Totals over the 76 rows below (requirements of clauses 5 to 7, grouped where the standard groups them, "shall" and "should" alike): 47 meets · 13 partial · 9 gap, stated (10 counting the ceremony environment under 7.8) · 3 inherited · 4 not applicable. The gaps all come

from three facts the operator states openly: a single operator (no dual control, no personnel separation), a software key in Cloud KMS (no Level 3 / EAL 4+ module), and no conformity assessment.

Clause 5 — Policies, identification

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-5.1-01/02	A TSA may define its own policy; if so it incorporates or constrains these requirements	N/A	Own policy OID 1.3.6.1.4.1.67100.1.1.1.1 ; it is not presented as enhancing the ETSI policy and does not claim it, so the conditional requirement does not apply
OVR-5.1-03	Accuracy better than 1 s stated in disclosure and in each token	N/A	Declared accuracy is 1 s, not better; tokens carry accuracy = 1 s
OVR-5.2-01	Policy identifier in the disclosure statement	Meets	OID on /tsa, in the Policy §1 and in iic-tsa.json
OVR-5.2-02	If own identifier, indicate the ETSI identifier supported	N/A	No ETSI policy is claimed; this is stated here and on /tsa ("designed to RFC 3161 / RFC 5816", not certified)
OVR-5.3-01	Policy usable for public or closed community	Meets	Closed community since 10 Oct 2026 (VerifBox only, public access on request)

Clause 6 — Policies and practices

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-6.1-01	Risk assessment (EN 319 401 §5)	Meets	IIC TSA — Risk Register v1.1, reviewed with the design; residual risks accepted and listed in the Practice Statement §10
OVR-6.2-01	Practice statement (EN 319 401 §6.1)	Meets	Practice Statement v1.0, approved 10 Oct 2026, published as PDF with SHA-256
OVR-6.2-02 a	Hash algorithms accepted	Meets	SHA-256, SHA-384, SHA-512 (Policy §3)
OVR-6.2-02 b	Accuracy with respect to UTC	Meets	1 s, declared in tokens and Policy §5
OVR-6.2-02 c	Limitations on use	Meets	Policy §2 and terms of use: not qualified, same company as VerifBox, no availability commitment
OVR-6.2-02 d	Subscriber obligations	Meets	Terms of use (tsa-terms.html)
OVR-6.2-02 e	Relying-party obligations	Meets	Terms of use, relying-party section; Policy §7 validation rules
OVR-6.2-02 f	How to verify, validity-period limits	Meets	Policy §7 (CRL after genTime, long-term validation), /tsa "how to verify", public verifiers, validation report on GitHub

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-6.2-02g	Claim under national law	Meets	None claimed; stated as non-qualified under eIDAS and UK eIDAS
OVR-6.2-03	Availability in the disclosure statement (should)	Partial	No commitment by design; measured availability published on /tsa-status from November 2026
OVR-6.2-04/05/06	Disclosure statement form (may)	Meets	Disclosure spread over /tsa, the Policy §1-2 and the terms; conspicuous
OVR-6.3-01	Terms and conditions (EN 319 401 §6.2)	Meets	tsa-terms.html, dated, governed by the laws of England and Wales
OVR-6.4-01	Information security policy (EN 319 401 §6.3)	Partial	Security controls are described in the Practice Statement §9; there is no separate, approved information security policy document
OVR-6.5-01	TSA adheres to obligations indicated in the token	Meets	Policy OID in every token; no extension or additional obligation
OVR-6.6-01 a-c	Relying party must verify signature and non-compromise, respect limitations	Meets	Terms of use and Policy §7: CRL check, chain to root R1, limitations

Clause 7 — TSA management and operation

7.2-7.5 Organisation, personnel, assets, access

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-7.2-01	Internal organisation (EN 319 401 §7.1)	Partial	Legal entity, responsibilities documented; no separation of roles
OVR-7.2-02	TSA is a legal entity	Meets	HTTPS CARD — INTERNET IDENTITY CARD LIMITED, no. 09168431
OVR-7.2-03	Quality and information security management system	Partial	Documented procedures (Policy, Practice Statement, ceremony script, acceptance tests, nightly batch checks); no formal ISMS
OVR-7.2-04	Sufficient personnel with the necessary skills	Gap, stated	Single operator; stated in Practice Statement §3 with compensating controls (KMS audit logs, least privilege, append-only journal, daily third-party anchoring)
OVR-7.3-01	Personnel security (EN 319 401 §7.2): trusted roles, screening, separation	Gap, stated	One person holds every role; no separation of duties, no two-person control
OVR-7.4-01	Asset management (EN 319 401 §7.3)	Partial	Assets listed in the Practice Statement (projects, keys, buckets, USB backups); no formal asset register with owners and classification

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-7.5-01	Access control (EN 319 401 §7.4)	Meets	IAM least privilege; private service callable by VerifBox's service account only; KMS Data Access logging on every key use

7.6 Cryptographic controls

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-7.6-01	Cryptographic controls (EN 319 401 §7.5)	Partial	Algorithms, key sizes, lifetimes documented; see gaps below
TIS-7.6.2-01	TSU key generated in a physically secured environment, trusted roles, dual control	Gap, stated	Key generated in Cloud KMS by the single operator; no dual control
TIS-7.6.2-02	Personnel limited to those required	Meets	One person; IAM restricts key administration to the owner
TIS-7.6.2-03/04	Generation in a device at EAL 4+ or FIPS 140-2/-3 Level 3	Gap, stated	Cloud KMS SOFTWARE protection level: per Google's documentation, software keys use the FIPS 140-3 Level 1-validated BoringCrypto module; Level 3 (FIPS 140-2 Level 3 validated HSMs, per the same page) is the HSM protection level, planned for the next key generation
TIS-7.6.2-05	Algorithms per TS 119 312 (should)	Meets	ECDSA P-256 with SHA-256 for tokens; root P-384 with SHA-384; both within TS 119 312 recommendations
TIS-7.6.2-06/07	Key not imported into other modules	Meets	KMS key is non-exportable; one module
TIS-7.6.2-08	Single signing key active per TSU	Meets	One key version active (tsa-2026-a)
TIS-7.6.3-01/02/03	Private key held and used in an EAL 4+ or Level 3 module	Gap, stated	As TIS-7.6.2-03; key never leaves KMS, but the module level is Level 1
TIS-7.6.3-04/05/06	Backups of the private key under dual control, encrypted by the module	N/A	No backup of the TSU key by design ("losing it means a new generation, not a restoration"). Outside the TSU scope of this clause: the offline root key has two encrypted USB copies held by a single custodian, without dual control — stated in record R1
TIS-7.6.4-01/02	Public key available in a certificate	Meets	TSU certificate returned in every token (certReq) and published
TIS-7.6.4-03	TSU certificate issued by a CA under EN 319 411-1 (should)	Gap, stated	Issued by the operator's own offline root "IIC TSA Root R1", not an EN 319 411-1 CA
TIS-7.6.4-04	No token before the certificate is loaded	Meets	Service starts with the certificate installed; acceptance test checks the chain

Req.	Requirement (short)	Status	IIC TSA evidence or gap
TIS-7.6.4-05	TSA verifies the certificate chain	Meets	<code>openssl verify -x509_strict -purpose ti mestampsign</code> at the ceremony (record R1)
TIS-7.6.5-01	Certificate validity not longer than algorithm fitness	Meets	135 months, P-256/SHA-256, within TS 119 312 horizons
TIS-7.6.6-01/02	Signing hardware not tampered with in shipment or storage	Inherited	Google Cloud KMS; no hardware handled by the operator for the TSU key
TIS-7.6.6-03	Installation/activation of signing keys under dual control in a secure environment	Gap, stated	Single operator; key activation in KMS by one person
TIS-7.6.6-04	Keys erased on device retirement	Inherited	KMS key destruction (scheduled destruction, non-recoverable after the delay)
TIS-7.6.7-01/02	Expiration date for TSU keys, not beyond the certificate	Meets	Signing limited to 15 months; certificate 135 months
TIS-7.6.7-03	Lifetime per TS 119 312 (should)	Meets	As above
TIS-7.6.7-04/05	Signing period shorter than certificate validity (should)	Partial	15 months signing vs 135 months validity is documented and enforced by procedure (new generation certified before month 15); the certificate carries no <code>privateKeyUsagePeriod</code> extension
TIS-7.6.7-06	Key not used beyond its validity	Partial	Enforced by operator procedure and the rotation calendar; not enforced in code by a hard stop at month 15
TIS-7.6.7-07	Procedure to put a new key in place on expiry	Meets	Key generations <code>tsa-YYYY-x</code> , ceremony <code>leaf</code> command, documented in Practice Statement §5 and record R1
TIS-7.6.7-08	Private keys destroyed so they cannot be retrieved	Meets	KMS key version destruction after retirement; root key: USB copies destroyed at termination (Practice Statement §10)

7.7 Time-stamping

Req.	Requirement (short)	Status	IIC TSA evidence or gap
TIS-7.7.1-01	Tokens conform to EN 319 422 profile	Partial	RFC 3161 tokens with SHA-256/384/512 imprints, accuracy, TSA name, ESSCertIDv2; full EN 319 422 profile conformance (every mandatory field and constraint) has not been checked item by item

Req.	Requirement (short)	Status	IIC TSA evidence or gap
TIS-7.7.1-02	Tokens issued securely	Meets	HTTPS only; private service under IAM; KMS signing; journal entry written before the token is returned
TIS-7.7.1-03/04	Correct time, traceable to a UTC(k) laboratory	Meets	Every token gated by a live measurement against four sources including PTB's web clock (PTB is a UTC(k) laboratory; traceability of its web service is as PTB documents it)
TIS-7.7.1-05/06	Time synchronised within the declared accuracy	Meets	SYNC only if ≥ 3 usable sources incl. PTB, spread ≤ 250 ms, median offset within ± 100 ms; declared accuracy 1 s
TIS-7.7.1-07	No token when the clock is out of accuracy	Meets	Fail-closed: FAIL state $\rightarrow$ <code>timeNotAvailable</code>
TIS-7.7.1-08	Key generated exclusively for time-stamping	Meets	<code>ttsa-2026-a</code> used for nothing else; ECU timeStamping critical
TIS-7.7.1-09	Reject issuance after the key's validity end	Partial	Certificate validity enforced; the 15-month signing limit is procedural (see TIS-7.6.7-06)
TIS-7.7.2-01/02	Clock synchronised and calibrated within accuracy	Meets	Measured at every lease (≤ 30 s), not trusted between measurements
TIS-7.7.2-03	Declared accuracy 1 s or better	Meets	1 s
TIS-7.7.2-04	Clock protected against undetected change	Meets	Monotonic/wall-clock comparison; a step > 1 s is detected and requires manual readmission
TIS-7.7.2-05/06	Drift or jump detected; issuance stopped	Meets	SYNC/FAIL state machine; lease withdrawn on FAIL
TIS-7.7.2-07/08/09	Leap seconds handled in the last minute of the day, recorded	Gap, stated	Practice Statement §6: the hosting infrastructure smears the leap second over 24 hours while some sources step it; the guardian then moves to FAIL and issuance pauses (fail-closed). Accuracy stays within 1 s but the change is not a last-minute step and the record of TIS-7.7.2-09 would be the guardian log, not a dedicated record

7.8-7.15 Physical, operations, network, incidents, evidence, continuity, termination, compliance

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-7.8-01 to -12	Physical and environmental security of TSU and management facilities (secure perimeter, logged and overseen entry, utilities, disaster)	Inherited	TSU runs in Google Cloud (europe-west1) under Google's physical controls and certifications, not assessed by the operator. Gap, stated for the root-key ceremony: performed on the operator's own computer, offline, with no secure area, no independent oversight and no entry log (record R1 §7)

Req.	Requirement (short)	Status	IIC TSA evidence or gap
OVR-7.9-01	Operation security (EN 319 401 §7.7)	Partial	Pinned container images, acceptance tests before production, change log in the documents' history; no formal change-management procedure
OVR-7.9-02	Capacity monitored and projected	Partial	Rate limits (60/min public, 600/min private); Cloud Run scales; no capacity projection documented
OVR-7.10-01 to -04	Network security: TSU in a secure zone, hardened, trusted roles only	Meets	Cloud Run services with no inbound access except HTTPS; private service IAM-only; minimal container; KMS reachable only by the service account
OVR-7.11-01	Incident management (EN 319 401 §7.9)	Meets	Incident definition, recording within seven days and publication on /tsa-status; Practice Statement §10
OVR-7.12-01	Collection of evidence (EN 319 401 §7.10)	Meets	Append-only issuance log (12 years, create-only objects), daily batches time-stamped by DigiCert and anchored in Bitcoin, archive copy in another region
OVR-7.12-02/03	Key and certificate life-cycle events logged	Meets	KMS Admin and Data Access audit logs; ceremony records (R1); CRL history
OVR-7.12-04/05/06	Clock synchronisation events logged, incl. loss of sync	Meets	Guardian logs every measurement cycle: source, offset, uncertainty, state and state changes
OVR-7.13-01	Business continuity (EN 319 401 §7.11)	Partial	Recovery is "new key generation", documented; no tested continuity plan with recovery objectives
OVR-7.13-02	Disaster plan addresses key compromise and loss of calibration	Meets	Practice Statement §10: revocation with invalidity date, journal evidence, new generation
OVR-7.13-03/04/05	On compromise: inform, stop issuing, identify affected tokens	Meets	Fail-closed; publication on /tsa-status and /tsa; journal of serial numbers and signature digests allows identification of affected tokens; daily third-party anchoring dates the journal
OVR-7.14-01	Termination plan (EN 319 401 §7.12)	Meets	Three months' notice, final CRL, key destruction, deposit with Software Heritage (Practice Statement §10)
OVR-7.14-02	On termination, revoke all non-expired TSU certificates	Meets	Practice Statement §10, erratum 2 of 11 October 2026: every TSA certificate not yet expired is revoked in the final root CRL, whose validity reaches the end of the longest remaining certificate validity
OVR-7.15-01	Compliance (EN 319 401 §7.13): conformity assessment	Gap, stated	No conformity assessment by an independent body; this self-assessment only

Summary of gaps and what would close them

Gap	Clauses	What would close it	Operator's position
Single operator, no dual control, no personnel separation	7.2-04, 7.3, 7.6.2-01, 7.6.6-03	A second trusted person with real duties (ceremony witness, backup holder, second approval)	Stated openly; compensating controls in place; a second person only if the role is real
Software key, not a Level 3 / EAL 4+ module	7.6.2-03, 7.6.3-02	Next key generation at the Cloud KMS HSM protection level (FIPS 140-2 Level 3), new ceremony record	Planned for the next generation, subject to the (small) recurring cost
TSU certificate from own root, not an EN 319 411-1 CA	7.6.4-03	A certificate from a CA operating under EN 319 411-1	Not planned; own root published with fingerprints and ceremony record
No conformity assessment	7.15	Assessment under EN 319 403-1 by a CAB	Not planned at zero budget; self-assessment published instead
Ceremony environment	7.8	Secure area, two people, entry log	Not planned; stated in record R1

Minor items to fix at the next document revision (no architecture change)

- Add to the Policy §5 the leap-second behaviour already stated in the Practice Statement §6 (smearing, fail-closed), so that the deviation from TIS-7.7.2-08 is visible in the policy too.
- Add a formal asset list with owners (EN 319 401 §7.3).
- Consider a privateKeyUsagePeriod extension, or a hard stop in the service at month 15, for the next generation (TIS-7.6.7-04/06, TIS-7.7.1-09).
- Check the EN 319 422 token profile field by field and record the result (TIS-7.7.1-01).

Sources

- ETSI EN 319 421 V1.2.1 (2023-05), clauses 5-7 — https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.02.01_60/en_319421v010201p.pdf
- ETSI EN 319 401 (referenced for general requirements; assessed only at the referring-clause level here)
- IIC TSA Timestamp Policy v1.0 and Practice Statement v1.0 (erratum 1), Risk Register v1.1, Technical Specification v1.0, Key Ceremony Record R1, /tsa, /tsa-terms, /tsa-status

History

Version	Date	Change
1.0	2026-10-11	First published version

© 2026 Htts Card — Internet Identity Card Ltd, 124 City Road, London EC1V 2NX, United Kingdom. UK Company No. 09168431. Governed by the laws of England and Wales.