

Digital Signature Record

This page was added by host.name.my for the digital signature. It is not part of the original document.



SECURE
SIGNATURE

DIGITALLY SIGNED
host.name.my Repository

host.name.my
Signed: 2026-09-19 01:49:25 +08
Serial: 1020

host.name.my · Trust Services

Private CA · cryptographically verifiable



Verify
host.name.my

Time-Stamping Policy and Practice Statement (TSPS)

host.name.my · Version 1.1 · 2026-09-17 · companion to the CP/CPS

1. Overview

host.name.my operates an RFC 3161 Time Stamping Authority (TSA) that issues timestamp tokens used in signatures and stored with signed documents.

2. TSA identity

- TSA certificate subject: CN=host.name.my TSA, O=host.name.my, C=MY
- Issued by: host.name.my Issuing CA
- Extended key usage: timeStamping (critical)
- Endpoint: POST <https://host.name.my/ca/tsa>

3. Timestamp policy

- Protocol: RFC 3161
- Policy OID: 2.25.328614226442479192614111317020995041098.3
- Hash algorithms: SHA-256, SHA-384, SHA-512
- Accuracy: 1 second
- Ordering: yes
- TSA name included: yes
- ESSCertID chain included: yes
- Clock source: host system clock (kept synchronised by the host)

4. Use in signatures

- PDF (PAdES): the timestamp is embedded in the signature (PAdES-B-T).
- Other files (CMS): a separate .tsr token over the original file is stored alongside the .p7s signature.
- A public TSA (FreeTSA) may be used as a fallback if the local TSA is unavailable.

5. Verification

Timestamps are verified against the host.name.my chain. A relying party can verify through the public portal.

6. Limits (honest)

- The TSA is private; tokens are not trusted outside the host.name.my root.
- The policy OID is self-assigned from an ISO/IEC 9834-8 UUID arc (2.25.328614226442479192614111317020995041098); it is globally unique without registration, but carries no third-party verification.
- Long-term validation (LTV/DSS) is not supported.
- This TSPS is not an audited ETSI EN 319 421 statement.

7. Document history

Version	Date	Change
1.0	2026-09-17	Initial

Version		Date	Change
1.1		2026-09-17	Self-assigned policy OID
			2.25.32861422644247919261411
			1317020995041098.3 (replaces
			placeholder 1.2.3.4.1)