

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 01:49:18 +08
Serial: 1020

host.name.my · Trust Services

Private CA · cryptographically verifiable



Verify
host.name.my

Certificate Policy / Certification Practice Statement (CP/CPS)

host.name.my · Version 2.5 · 19 September 2026

Document OID: 2.25.328614226442479192614111317020995041098.1

RFC 3647 framework · Private (non-public) certificate authority

Scope. This CP/CPS covers the private certificate authority and document

signing service operated at host.name.my. It is published in the CA repository

(see §2). It is **not** a qualified or publicly-trusted CA.

1. INTRODUCTION

1.1 Overview

host.name.my operates a private two-tier certificate authority and a document signing/verification service. It issues X.509 certificates to registered subscribers and produces PAdES (PDF) signatures with an embedded RFC 3161 timestamp, and detached CMS (PKCS#7) signatures accompanied by a separate RFC 3161 timestamp token over the original file. Timestamping depends on the availability of the time-stamping service; if no TSA can be reached, the signature is still produced, without a timestamp. Trust is scoped to relying parties that choose to trust the host.name.my root.

1.2 Document name and identification

- Title: host.name.my Certificate Policy / Certification Practice Statement
- Version: 2.5 (2026-09-19); Document OID: 2.25.328614226442479192614111317020995041098.1
- Private OID arc: 2.25.328614226442479192614111317020995041098 (ISO/IEC 9834-8 UUID arc; CP/CPS = .1, TSPS = .2, TSA policy = .3)
- This document combines CP and CPS.

1.3 PKI participants

- **CA operator:** host.name.my administrator (Super Admin / CA Admin).
- **Subscribers (signers):** registered users issued certificates.
- **Relying parties:** document recipients verifying via the public portal, or with Adobe Acrobat / OpenSSL after importing the root.
- **Registration authority:** the CA administrator (no separate RA).

1.4 Certificate usage

Signing (PAdES/CMS) and client authentication. Not for TLS server authentication and not accepted by public trust stores. Key usages in §7.

1.5 Policy administration

The CA administrator owns this CP/CPS. Changes are recorded in §9.5 and published.

1.6 Definitions and acronyms

CA, CP, CPS, CRL, OCSP, PAdES, CMS/PKCS#7, RFC 3161, TSA, X.509, RA, RPA.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Public repository at <https://host.name.my/ca/>:

- Root certificate /ca/root-ca.crt
- Issuing certificate /ca/issuing-ca.crt
- Chain /ca/ca-chain.crt
- CRLs /ca/issuing-ca.crl, /ca/root-ca.crl
- This CP/CPS, certificate profiles, Time-Stamping Policy (TSPS),

Subscriber Agreement, Relying Party Agreement, and the Subscriber Registration Form

2.2 Publication of certificate information

A public subscriber directory is published at <https://host.name.my/directory>. It

lists, for each issued certificate: subscriber name, organisation, serial number,

issue date, expiry and status (active / revoked / expired). Email addresses are not

displayed. Each signed document also has a public record reachable only via a random token (/d/<token>).

2.3 Time or frequency of publication

CP/CPS on issue and on change. CRLs at least daily and on every revocation. OCSP

answers live status.

2.4 Access controls on repositories

Repository files are public and read-only. Operational records are not public.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

- Root CA: CN=host.name.my Root CA, O=host.name.my, C=MY
- Issuing CA: CN=host.name.my Issuing CA, O=host.name.my, C=MY
- Subscribers: CN=<full name>, emailAddress=<email>, O=host.name.my, C=MY
- TSA: CN=host.name.my TSA, O=host.name.my, C=MY

3.2 Initial identity validation

Subscribers are created by a CA administrator, who validates the subscriber identity

before a certificate is issued. The identity recorded is the subscriber name and

email address (the organisational record). No government-ID verification is

performed.

By issuing a certificate, host.name.my **asserts** that the public key belongs to the

identified subscriber — i.e. that the subscriber is registered and its identity was

checked as described above. The assertion reflects the registration process and the

CA records; it does not by itself prove that the subscriber personally operated a

signing device (see §9.4). A relying party can confirm registration and current

status in the public subscriber directory (§2.2).

3.3 Identification and authentication for re-key

Not applicable; renewal is by re-issuance (§4.6–4.7).

3.4 Identification and authentication for revocation

Revocation requests are accepted from a CA administrator; the reason is recorded.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate application

A CA administrator issues a certificate for a registered, active user via the console.

4.2 Certificate application processing

The CA verifies the user is active. No automated approval.

4.3 Certificate issuance

Key pair generated on the CA host (RSA-3072); certificate signed by the Issuing CA (RSA-4096, SHA-256); validity **730 days**. The private key is stored AES-256 encrypted; its passphrase is encrypted with the application key.

4.4 Certificate acceptance

Deemed accepted on first use.

4.5 Key pair and certificate usage

Used to sign documents; relying parties verify signatures. Credentials must not be shared.

4.6 Certificate renewal

By re-issuance (new key pair + certificate). No automatic renewal.

4.7 Certificate re-key

Same as renewal.

4.8 Certificate modification

A certificate is never modified; a new one is issued.

4.9 Certificate revocation and suspension

Revocation with a standard reason (keyCompromise, cessationOfOperation, superseded, etc.). Suspension is not supported. CRL and OCSP reflect revocation. Documents can be **withdrawn**; the verifier reports them as revoked.

4.10 Certificate status services

- CRL per §2.1
- OCSP: POST <https://host.name.my/ca/ocsp> (RFC 6960)

4.11 End of subscription

On deactivation, outstanding certificates are revoked.

4.12 Key escrow and recovery

No key escrow. The encrypted key remains on the CA host; a lost passphrase is only recoverable from backup.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Hosted virtual server; physical security delegated to the hosting provider.

5.2 Procedural controls

Roles: Super Admin, CA Admin, Auditor, Signer, Verifier. CA operations run through an isolated helper executed as a low-privilege user (pki).

5.3 Personnel controls

CA administration limited to authorised administrators.

5.4 Audit logging procedures

Every action is recorded in a SHA-256 hash-chained audit log.

5.5 Records archival

CA database (openssl index/serials), audit log, backups and document artefacts are retained per the operational records policy.

5.6 Key changeover

The Issuing CA can be re-issued under the Root CA; the Root CA key is kept offline-capable.

5.7 Compromise and disaster recovery

Encrypted backups daily (CA + DB + env) and document artefacts separately. Restore is documented; a formal restore test is pending (§9.4).

5.8 CA termination

Subscribers and relying parties are notified; the root is revoked if applicable.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

CA keys RSA-4096 with OpenSSL, passphrase-protected. Subscriber keys RSA-3072, generated on the CA host.

6.2 Private key protection

- CA keys passphrase-encrypted, unreadable by the web tier.
- Subscriber keys AES-256 encrypted; passphrases encrypted with APP_KEY.
- **Note:** keys and passphrases are service-held, so the service can sign on the

subscriber's behalf; this limits non-repudiation (§9.4).

6.3 Other aspects of key pair management

Key usage and validity per §7; subscriber validity 730 days.

6.4 Activation data

Account passwords (hashed) and key passphrases (encrypted).

6.5 Computer security controls

Least-privilege OS users, restricted PHP-FPM pool, single sudoers rule, strict argument/path validation.

6.6 Life cycle technical controls

Versioned deployment (git) with an internal changelog.

6.7 Network security controls

HTTPS (TLS 1.2/1.3); repository and OCSP/TSA endpoints public; CA keys never exposed.

6.8 Time-stamping

RFC 3161 timestamps by the host.name.my TSA, embedded in PAdES (B-T) when the TSA is available; a public TSA is used as a fallback. If no TSA can be reached the signature is produced without a timestamp. LTV/DSS is **not** supported.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Detailed profiles in docs/CERT-PROFILES.md. Summary:

- **Subscriber:** X.509v3, RSA-3072, SHA-256, 730 days, KeyUsage digitalSignature, nonRepudiation; EKU emailProtection, clientAuth, documentSigning (1.3.6.1.5.5.7.3.36, RFC 9336); CDP /ca/issuing-ca.crl; AIA OCSP /ca/ocsp, caIssuers /ca/issuing-ca.crt.
 - **CA:** basicConstraints CA:TRUE; KeyUsage keyCertSign, cRLSign.
 - **TSA:** EKU timeStamping.
 - **CRL:** X.509 v2, SHA-256, published daily/on revocation.
 - **OCSP:** RFC 6960, good/revoked.
-

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

A private CA; no WebTrust/ETSI audit. This CP/CPS and the repository are maintained so an internal or third-party audit can be performed against RFC 3647. A self-assessment checklist is maintained internally.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

No fees; internal service.

9.2 Liability

Provided "as is"; liability limited as permitted by law. See Terms of Service.

9.3 Confidentiality

Documents and keys are not sold or shared with third-party signing services.

9.4 Known limitations

- Not a publicly-trusted or licensed CA; not a qualified digital signature.
- LTV/DSS (PAdES-B-LT/LTA) is **not** supported.
- Keys/passphrases are service-held, limiting non-repudiation.
- Root CA is currently on the same server; offline storage available but not enforced.
- A formal restore test is pending.

9.5 Document history

Version	Date	Change
1.0	2026-09-17	Initial short CP/CPS
2.0	2026-09-17	RFC 3647 structure; repository, profiles, limits
2.1	2026-09-17	Assign private OID arc 2.25.32861422644247919261411 1317020995041098 (document OID .1); replace placeholder OIDs Registration/identity assertion (§3.2); public subscriber directory (§2.2); certificatePolicies OID in issued certificates
2.2	2026-09-17	Correct §1.1: CMS signature carries no embedded timestamp; a separate RFC 3161 token is produced. Subscribers, not just signers
2.3	2026-09-17	Clarify timestamping depends on TSA availability (§1.1, §6.8)
2.4	2026-09-17	Add id-kp-documentSigning (1.3.6.1.5.5.7.3.36, RFC 9336) to subscriber EKU
2.5	2026-09-19	