

# 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 01:49:20 +08  
Serial: 1020

host.name.my · Trust Services

Private CA · cryptographically verifiable



**Verify**  
host.name.my

# Certificate, CRL and OCSP Profiles

host.name.my · v1.0 · 2026-09-17 · companion to CP/CPS §7

## Root CA certificate

- Subject: CN=host.name.my Root CA, O=host.name.my, C=MY
  - Key: RSA-4096; Signature: sha256WithRSAEncryption
  - Validity: 20 years; self-signed
  - Extensions: basicConstraints CA:TRUE (critical); keyUsage keyCertSign, cRLSign;
- subjectKeyIdentifier

## Issuing CA certificate

- Subject: CN=host.name.my Issuing CA, O=host.name.my, C=MY
  - Key: RSA-4096; Signature: sha256WithRSAEncryption
  - Issuer: Root CA; Validity: 10 years
  - Extensions: basicConstraints CA:TRUE; keyUsage keyCertSign, cRLSign;
- authorityKeyIdentifier

## TSA certificate

- Subject: CN=host.name.my TSA, O=host.name.my, C=MY
- Key: RSA; Issuer: Issuing CA
- Extensions: EKU timeStamping (critical)

## Subscriber (signer) certificate

- Subject: CN=<full name>, emailAddress=<email>, O=host.name.my, C=MY
  - Key: RSA-3072; Signature: sha256WithRSAEncryption
  - Issuer: Issuing CA; Validity: 730 days
  - Extensions:
  - basicConstraints: CA:FALSE
  - keyUsage (critical): digitalSignature, nonRepudiation
  - extendedKeyUsage: emailProtection, clientAuth, id-kp-documentSigning
- (1.3.6.1.5.5.7.3.36, RFC 9336)
- subjectKeyIdentifier: hash
  - authorityKeyIdentifier: keyid,issuer
  - crlDistributionPoints: URI:https://host.name.my/ca/issuing-ca.crl
  - authorityInfoAccess: OCSP;URI:https://host.name.my/ca/ocsp,
- caIssuers;URI:https://host.name.my/ca/issuing-ca.crt

## CRL

- X.509 v2; Issuer: Issuing CA; Signature: SHA-256
- Published: https://host.name.my/ca/issuing-ca.crl
- Regenerated at least daily and on every revocation.

## OCSP

- RFC 6960; endpoint: POST https://host.name.my/ca/ocsp
- Response signed by the Issuing CA; statuses: good / revoked.

## Signature formats

- PDF: PAdES, embedded; RFC 3161 timestamp embedded (PAdES-B-T)
- Other files: detached CMS / PKCS#7 (.p7s); separate RFC 3161 .tsr for the original
- Not supported: PAdES-B-LT/LTA (LTV/DSS), qualified signatures