

# 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 01:49:23 +08  
Serial: 1020

**Verify**  
host.name.my

host.name.my · Trust Services

Private CA · cryptographically verifiable

# Relying Party Agreement

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

Before relying on a host.name.my signature, the relying party agrees:

1. **Trust decision.** You must decide whether to trust the host.name.my root. Import <https://host.name.my/ca/root-ca.crt> into your trust store to validate independently in Adobe Acrobat or OpenSSL.
1. **Verification.** Verify the signature and its status (CRL at [/ca/issuing-ca.crl](#), OCSP at [/ca/ocsp](#)) before relying on it.
1. **Scope.** Certificates are for document signing and client authentication only, not for TLS server authentication.
1. **No qualified signature.** This is a private CA; signatures are not qualified digital signatures and have no presumed legal effect beyond what the parties agree.
1. **Revocation.** A signature may be invalid if the certificate was revoked or the document was withdrawn; the portal reports this.
1. **Limits.** LTV/DSS is not supported; long-term validity depends on the embedded timestamp and continued availability of the trusted root.
1. **No warranty.** The service is provided "as is"; see the CP/CPS §9.2.