DURCHD8 Certificate Policy (CP)

Document title: DURCHD8 Certificate Policy
Version: 1.0
Effective date: 2025-10-31
Policy OID: 1.3.6.1.4.1.59713.8.0
Supersedes: initial release (new)
Related CPS: DURCHD8 Certification Practice Statement (PDF)
CPS OID: 1.3.6.1.4.1.59713.8.0.1
Policy authority: DURCHD8 Root Certification Authority (PKI Steering Team)
Contact: pki@durchd8.com
Repository: https://durchd8.com/.well-known/pki/

> This Certificate Policy follows the structure of RFC 3647. It defines the trust model, certificate classes, and high-level requirements for the DURCHD8 PKI. Operational details are provided in the CPS.

---

1. Introduction

1.1 Overview

The DURCHD8 PKI provides detached CMS signatures (CAdES-BES/T) and RFC 3161 timestamps for internal documents, evidence artefacts, and audit deliveries. The PKI is operated on the hardened host `dehgdo-pki.durchd8.com` (OpenBSD 7.7) and consists of a Root CA, a Signing CA, a TSA CA, and their operational End-Entity certificates. This CP governs all certificates issued within this hierarchy.

1.2 Document name and identification

- Certificate Policy (CP) name: “DURCHD8 Certificate Policy”
- Policy OID: 1.3.6.1.4.1.59713.8.0
- CPS reference: DURCHD8 Certification Practice Statement (CPS) v1.0, OID 1.3.6.1.4.1.59713.8.0.1

1.3 PKI participants

- **Policy Authority / Certification Authority (CA):** DURCHD8 Root CA, operating the signing hierarchy and supervising subordinate CAs.
- **Subordinate CAs:** DURCHD8 Signing CA, DURCHD8 TSA CA.
- **Registration Authority (RA):** Functions performed by the same staff as the CA (root and sign operators); no delegated RAs.
- **Subscribers:** Internal DURCHD8 systems (signing service, TSA service) and designated audit users. No external subscribers.
- **Relying parties:** Internal DURCHD8 staff, appointed auditors, and automated verification systems consuming the published artefacts.

1.4 Certificate usage

Certificate class	Policy OID	Intended use	Prohibited use
DURCHD8 Root CA	1.3.6.1.4.1.59713.8.1	Trust anchor for the hierarchy	Any direct end-user use; issuing non-DURCHD8 certificates
DURCHD8 Signing CA	1.3.6.1.4.1.59713.8.2	Issuing CMS signing EEs	TLS, VPN, code signing for third parties
DURCHD8 TSA CA	1.3.6.1.4.1.59713.8.3	Issuing TSA EEs	Non-TSA usage
DURCHD8 Signer EE	1.3.6.1.4.1.59713.8.10.1	Detached CMS signatures for DURCHD8 artefacts	Public trust, end-user authentication
DURCHD8 TSA EE	1.3.6.1.4.1.59713.8.10.3	RFC 3161 time-stamp tokens	Non-TSA signing

Certificates may only be relied upon within the DURCHD8 business context. Third-party reliance is not supported.

1.5 Policy administration

- **Organisation:** DURCHD8 GmbH, PKI Steering Team

- **Change control:** All amendments require a PKI change ticket, dual approval (root + audit), and publication of a revised CP/CPS pair in the repository. Document history is archived in `/var/pki/www/` together with the associated change records.
- **Contact:** pki@durchd8.com

1.6 Definitions and acronyms

- **CA:** Certification Authority
- **CP/CPS:** Certificate Policy / Certification Practice Statement
- **EE:** End-Entity certificate
- **TSA:** Time-Stamping Authority (RFC 3161)
- **PKI:** Public Key Infrastructure
- **SA:** Security Authority (root/sign operators)

---

2. Publication and repository responsibilities

- All certificates, CRLs, policy documents, manifests, and SHA256 sums are published at https://durchd8.com/.well-known/pki/.
- Publication occurs automatically after each successful signing preflight via `pki_www_manifest.ksh` and `pki_sync_www.sh`. Releases include:
  - `root-ca.cer`, `signing-ca.cer`, `tsa-ca.cer`, `tsa-ca.crl`, `signing-ca.crl`, `root.crl`
  - Detached manifests (`*.manifest.json`) and consolidated `SHA256SUMS`
  - CP/CPS PDFs (`DURCHD8_Certificate_Policy.pdf`, `DURCHD8_Certification_Practice_Statement.pdf`)
- Availability is ensured through HTTPS with pinned certificate hashes (per manifest) and daily sync verification. Integrity is additionally verifiable via SHA256 checksums and receipts stored under `/var/pki/log/receipts/`.

---

3. Identification and authentication

- **Identity vetting:** Only predefined internal system identities (subjects and SANs) are allowed. Identity proofing consists of Change Ticket verification, approval by the Security Authority, and cross-checks against the system inventory.
- **Key ownership:** Root CA ceremonies require dual control (root operator + vault custodian). Subordinate CA/EE issuance requires authenticated access by `sign` within controlled scripts.
- **Re-key and re-issue:** Keys are regenerated only under scheduled rotations or incident response. Re-issuance uses the

same subject distinguished name; approval and receipts are mandatory.
- **Revocation requests:** Initiated by SA personnel (root or sign). Any detection of compromise, misuse, or decommissioning triggers a revocation ticket.

---

4. Certificate life-cycle operational requirements

- **Application:** No self-service enrollment. Requests originate from the PKI team based on approved work packages (A-1… A-13 in the SSOT).
- **Issuance:** Executed via controlled scripts (`pki_root_ca_wizard.ksh`, `pki_signing_ca_reissue.ksh`, `pki_tsa_ca_wizard.ksh`, `pki_ee_issue.ksh`). Outputs (certificates, CRLs, receipts) are archived and mirrored to `/var/pki/www/`.
- **Acceptance:** Certificates become valid once the preflight run passes (chain validation, status report, manifest, publish) and receipts are countersigned (A-12 sign-off).
- **Renewal/Re-key:** EE autorotation runs daily (03:17/03:22) ensuring overlap of at least 30 days. Intermediates are renewed manually with staging (A-5) and dual publication. Root renewal requires a documented ceremony.
- **Revocation:** Reasons include keyCompromise, CA key change, cessation. CRLs are generated daily (03:12 for Signing CA, 03:17 for TSA CA, Root on demand) with `default_crl_days` of 30 (root, TSA) and 7 (signing). OCSP is not provided; CRL-only policy applies.
- **Status checking:** Relying parties consume CRLs via HTTPS. The preflight script (`pki_preflight.ksh`) aborts and raises alerts on any failure (chain, CRL, manifest, publish).

---

5. Facility, management, and operational controls

- **Host environment:** The PKI runs on a dedicated, fully patched OpenBSD 7.7 virtual machine. The hypervisor provides encrypted memory; the guest boots from an OpenBSD softraid volume with disk encryption. Boot credentials are stored in a separate password safe and released only under change control.
- **Vault handling:** CA private keys reside on an encrypted mini root-vault partition that remains unmounted during normal operation. Unlocking the vault requires a documented four-eyes procedure (root operator + vault custodian) and is performed only for CA re-issuance.

- **Network isolation:** Apart from the forced-command SSH interface for the signing service (public-key only, no PTY, no port forwarding), the system has no inbound access. Physical console access is protected and audited; direct access alone does not grant shell control without credentials and change approval.
- **Personnel controls:** Roles are segregated (root, sign, audit, vault custodian). Every sensitive action demands dual approval and is logged by script receipts.
- **Logging and retention:** Receipts, TSA artefacts, admin/change/hashverify logs, and evidence indexes are retained for at least ten years. Daily log rotation and monthly evidence indexing ensure integrity.
- **Archival & incident handling:** Superseded certificates/CRLs are archived under `/var/pki/archive/`. Incident triggers (hash mismatch, TSA drift, CRL failure) follow the runbooks defined in L3, including quarantine and alerting.

---

6. Technical security controls

- **Key generation:** Performed on the air-gapped host using OpenSSL 3.5.4 (`/usr/local/openssl-3.5.4/bin/openssl`) with `/dev/random`. Root ceremonies occur offline in the vault.
- **Key sizes and algorithms:**
  - Root: RSA 4096, SHA-256
  - Signing CA & TSA CA: RSA 3072, SHA-256
  - EE (signing, TSA): RSA 2048, SHA-256
  - Timestamp accuracy: 1 second; hashing algorithm SHA-256
- **Key protection:**
  - Root key stored in encrypted mini-vault (`/var/pki/root-vault`, read-only when not mounted).
  - CA/EE keys stored under `/var/pki/active/` with permissions 0640 (root:sign); backups none except encrypted root key (`root-ca.key.gpg`).
  - No PEM passphrases (air-gapped system).
- **Multi-person control:** Root vault operations require two operators. Staging and activation of intermediates demand explicit freeze/backout markers (`pki_intermediate_stage_publish.ksh`).
- **Time synchronisation:** Internal `ntpd` locked to 192.168.100.1; TSA selftest enforces ±2s drift threshold.
- **Software controls:** PF firewall default deny; ForceCommand for SSH signing service; scripts run with `set -eu` and locking to prevent concurrency.

---

7. Certificate, CRL, and OCSP profiles

Level	Key/ Hash	Critical extensions	Polic OID
Root CA	RSA 4096 / SHA-256	`basicConstraints CA:true pathLen:2`, `keyUsage keyCertSign,cRLSign`, `certificatePolicies 1.3.6.1.4.1.59713.8.1`	20 ye
Signing CA	RSA 3072 / SHA-256	`basicConstraints CA:true pathLen:1`, `keyUsage keyCertSign,cRLSign`, `authorityInfoAccess (caIssuers)`, `CRLDistributionPoints`, `certificatePolicies 1.3.6.1.4.1.59713.8.2`	10 ye
TSA CA	RSA 3072 / SHA-256	as Signing CA but policy 1.3.6.1.4.1.59713.8.3	10 ye
Signing EE	RSA 2048 / SHA-256	`extendedKeyUsage emailProtection`, `subjectAltName=email:copy,URI:https://durchd8.com/.well-known/pki/`, `certificatePolicies 1.3.6.1.4.1.59713.8.10.1`	≤ 18 days (rota
TSA EE	RSA 2048 / SHA-256	`extendedKeyUsage timeStamping`, policy 1.3.6.1.4.1.59713.8.10.3	≤ 18 days

OCSP is not operated. Relying parties must consult the CRL URLs included in every certificate.

---

8. Compliance audit and other assessments

- **Internal checks:** Daily preflight (chain, status, manifest, publish), daily chain validation, daily CRL generation, weekly hash verification, monthly evidence index, optional weekly digest.
- **External audit:** Annual independent assessment aligned with ETSI EN 319 421/422 and RFC 3161 requirements. Outcomes documented in `/var/pki/log/change.log` and the change record.
- **Remediation:** Non-conformities trigger incident handling, quarantine of affected artefacts, and reissue/revocation. Policy revisions follow the change management process.

---

9. Other business and legal provisions

- **Jurisdiction:** Germany / EU law.

- **Liability:** Certificates are for internal DURCHD8 use only; there is no liability towards third parties or public relying parties.
- **Confidentiality:** Private keys, vault contents, and audit artefacts are confidential. Published certificates, CRLs, manifests, and policy documents are public.
- **Privacy:** Subscriber data limited to technical contact (pki@durchd8.com) and service identifiers; no personal data beyond duty contacts.
- **Intellectual property:** Certificates, scripts, and documentation remain property of DURCHD8.
- **Fees:** None (internal service).
- **Dispute resolution:** Managed by the DURCHD8 Security Authority; escalations handled by the executive board.

---

10. Document management

- Version 1.0 – initial publication (2025-10-31).
- Updated versions are archived under `/var/pki/www/` (and mirrored to the public repository) together with their change tickets and SHA256 checksums. Superseded versions remain archived for at least ten years.
- Change requests reference a ticket ID and require joint approval by root and audit roles prior to publication.

---

11. References

1. RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
2. RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile
3. RFC 5652 – Cryptographic Message Syntax (CMS)
4. RFC 3161 – Time-Stamp Protocol (TSP)
5. ETSI EN 319 421 & EN 319 422 – Policy Requirements and TSP Profiles
6. DURCHD8 SSOT documents L0–L3 (2025-10-24) and System Change Record (2025-10-27)