DURCHD8 Certification Practice Statement (CPS)

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

> This CPS implements the DURCHD8 Certificate Policy and describes the operational, technical, and organisational controls in place on the PKI host `dehgdo-pki.durchd8.com`.

---

1. Introduction

1.1 Purpose

This CPS defines how DURCHD8 implements the Certificate Policy for issuing detached CMS signatures and RFC 3161 timestamps. It documents the processes, scripts, controls, and evidence required to operate the private PKI and TSA infrastructure.

1.2 Relationship to the CP

The CP specifies policy requirements and certificate classes; this CPS provides the concrete practices. Where conflicts arise, CP requirements prevail and this CPS must be amended.

1.3 Document management

- Policy artefacts are stored in `/var/pki/www/` as Markdown/PDF pairs with accompanying SHA256 sums and change-ticket references; published copies are mirrored to the public repository.

- Revisions and approvals are logged in `/var/log/pkilog/change.log` and in the System Change Record.

1.4 References and related documents

- DURCHD8 CP v1.0 (OID 1.3.6.1.4.1.59713.8.0)
- SSOT documents (L0 System Core, L1 Schnittstelle, L2 Policy, L3 Admin)
- System Change Record OpenBSD PKI (2025-10-27)
- Work packages A-1 … A-13 (Phase A)

---

2. Publication and repository responsibilities

2.1 Repository content

All public artefacts are hosted at `https://durchd8.com/.well-known/pki/` via a read-only mirror of `/var/pki/www/`. Published files include: - CA and EE certificates (`root-ca.cer`, `signing-ca.cer`, `signing-ee.cer`, `tsa-ca.cer`, `tsa-signer.cer`) - CRLs (`root.crl`, `signing-ca.crl`, `tsa-ca.crl`) - Policy documents (`DURCHD8_Certificate_Policy.pdf`, `DURCHD8_Certification_Practice_Statement.pdf`) - Evidence manifests (`*.manifest.json`), SHA256 sums (`SHA256SUMS`) - Timestamp responses copied to `/var/pki/log/tsa_audit/` (internal retention)

2.2 Publication process

1. Signing/TSA operations create receipts in `/var/pki/log/receipts/`.
2. `pki_preflight.ksh` (daily 04:05) runs chain validation, status report, manifest rebuild, and publish.
3. `pki_www_manifest.ksh` writes `SHA256SUMS`; `pki_sync_www.sh` rsyncs to the web host (`xfer` user, forced rrsync).
4. Sync success is verified by hashing the remote `SHA256SUMS`; failures trigger alerts and block publication.

2.3 Integrity and retention

- Every artefact is accompanied by SHA256 hashes in the manifest and consolidated `SHA256SUMS`.
- Receipts and TSA audit files are retained ≥10 years in `/var/pki/log/receipts/` and `/var/pki/log/tsa_audit/`.
- Monthly evidence index (`pki_evidence_index.ksh`) records hashes of scripts, certs, CRLs, and policies under `/var/pki/archive-index/index-YYYYMMDD.sha256`.

---

3. Identification and authentication

3.1 Naming

- Subjects are fixed: `CN=DURCHD8 Root CA`, `CN=DURCHD8 Signing CA`, `CN=DURCHD8 TSA CA`, `CN=DURCHD8 Signer v1`, `CN=DURCHD8 TSA v1`.
- SAN for EE certificates includes `email:pki@durchd8.com` and `URI:https://durchd8.com/.well-known/pki/`.
- Serial numbers: 160-bit random (`-rand_serial`).

3.2 Initial identity validation

- **Root CA:** Offline ceremony executed by root and vault custodian, recorded in the change record. Vault passphrase protected (softraid CRYPTO).
- **Subordinate CAs / EEs:** Only predefined profiles exist (`sign.conf`, `tsa_ca.conf`, `pki_ee_issue.ksh`). Issuance requires:
  - Approved change ticket and runbook entry (A-2 … A-13).
  - Execution by `root` (CAs) or `sign` (EEs) using locked scripts.
  - Automatic receipts with timestamps, fingerprint, and serial.
- No external applicant authentication; all subscribers are controlled systems.

3.3 Renewal and re-key authentication

- EE autorotation scripts re-issue certificates with identical subject/usage; rotation is driven by Cron and receipts (no external request).
- Intermediate CA re-issue requires staging (`pki_intermediate_stage_publish.ksh`), freeze marker, root approval, and chain validation.
- Root re-issue/rekey requires ceremony with updated work instructions and sign-off in the change record.

3.4 Revocation requests

- Initiated by root or sign roles upon detection of compromise, misconfiguration, or decommissioning.
- Requests documented in change log and receipts; revocation reason `keyCompromise` or `cessationOfOperation`.

---

4. Certificate life-cycle operational requirements

4.1 Root CA

- Generated offline using `pki_root_ca_wizard.ksh` with `REKEY/REISSUE_CERT` flags as needed.
- Stored in `/var/pki/root-vault/` (encrypted volume). Vault is unmounted when idle; `vault_maybe_umount` helper enforces unmount post-operation.
- Root CRL refreshed manually when subordinate re-issuance occurs (default 30-day `nextUpdate`).

4.2 Signing CA

- Created or renewed using `pki_signing_ca_reissue.ksh`.
- Policy OID 1.3.6.1.4.1.59713.8.2; pathLen constraint 1.
- CRL renewal via `pki_crl_roll.ksh` (Cron 03:12 daily). NextUpdate = issueDate + 7 days.
- Publication of `signing-ca.cer` and `signing-ca.crl` to `/var/pki/www/`.

4.3 TSA CA

- Generated with `pki_tsa_ca_wizard.ksh`; policy OID 1.3.6.1.4.1.59713.8.3.
- CRL refresh: `pki_crl_roll_tsa.ksh` (Cron 03:17 daily). NextUpdate = issueDate + 30 days.
- TSA CA CRL and certificate exported to `/var/pki/www/`.

4.4 End-Entity certificates

- **Signing EE (`CN=DURCHD8 Signer v1`):** Rotated via `pki_sign_ee_autorotate.ksh` (Cron 03:17). Overlap ≥30 days guaranteed. Certificates stored under `/var/pki/active/signing-ee/`.
- **TSA EE (`CN=DURCHD8 TSA v1`):** Rotated via `pki_tsa_ee_autorotate.ksh` (Cron 03:22). Same overlap policy.
- Manual issuance fallback: `EE_CN="Subject" /bin/ksh /var/pki/bin/pki_ee_issue.ksh`.
- Receipts include subject, serial, fingerprint, and rotation metadata.

4.5 Acceptance and deployment

- `pki_preflight.ksh` performs chain validation (`pki_chain_validate.ksh`), status report (`pki_status_report.ksh`), manifest rebuild, and web publish.

- Preflight receipts stored as `*_preflight.log`; alerts sent via mail/logger on failure.

4.6 Revocation

- Executed with `pki_crl_roll*.ksh` after updating `index.txt` entries. Reason codes recorded.
- Revoked certificates remain in `index.txt` with status "R" and reason.
- CRLs published promptly; `pki_status_report.ksh` exposes current `nextUpdate` values.

4.7 Archive and evidence

- Superseded certs and CRLs archived in `/var/pki/archive/<class>/`.
- Receipts, manifests, TSA audit copies retained ≥10 years.
- Monthly evidence index lists hashes of scripts, policies, certs, CRLs.

---

5. Facility, management, and operational controls

5.1 Physical and environmental security

- The PKI host `dehgdo-pki` runs OpenBSD 7.7 as a dedicated, hardened VM. The hypervisor provides encrypted memory; the guest operates entirely on an OpenBSD softraid volume with disk encryption. Boot credentials are stored in an external password safe and require change-ticket release.
- The server resides in a controlled rack; console ports are locked. Physical access alone does not grant shell access (login requires key-based authentication and approval).
- The encrypted mini root-vault partition remains offline unless a CA ceremony is in progress; unlocking requires a documented four-eyes procedure (root operator + vault custodian).

5.2 Personnel controls

- Roles: root (administrator), sign (operator), audit (read-only), vault custodian (ceremony oversight).
- SSH is key-based only. The signing interface is restricted by ForceCommand (`pki_sigsvc_wrapper.ksh`), no PTY, no port/agent forwarding; all other access paths are disabled.
- Change management adheres to dual approval with ticket references; manual interventions (vault mount, cron changes) require role pairing and receipts.

5.3 Procedural controls

- Scripts under `/var/pki/bin/` follow `set -eu`, structured logging, and locking (`with_lock`) to prevent concurrent runs.
- Cron jobs (UTC) ensuring continuous operation: | Schedule | Task | |———-|——| | `12 3 * * *` | Signing CRL roll (`/var/pki/bin/pki_crl_roll.ksh`) | | `17 3 * * *` | TSA CRL roll (`/var/pki/bin/pki_crl_roll_tsa.ksh`) | | `17 3 * * *` | Signing EE autorotate (`/var/pki/bin/pki_sign_ee_autorotate.ksh`) | | `22 3 * * *` | TSA EE autorotate (`/var/pki/bin/pki_tsa_ee_autorotate.ksh`) | | `45 3 * * *` | Chain validation (`/var/pki/bin/pki_chain_validate.ksh`) | | `0 4 * * *` | Status report (`/var/pki/bin/pki_status_report.ksh`) → `/var/pki/log/status-YYYYMMDD.json` | | `5 4 * * *` | Manifest rebuild (`/var/pki/bin/pki_www_manifest.ksh`) | | `6 4 * * *` | Web sync + HTTPS verification (`/var/pki/bin/pki_sync_www.sh`) | | `@daily` | Preflight orchestration (`/var/pki/bin/pki_preflight.ksh`) | | `30 5 1 * *` | Monthly evidence index (`/var/pki/bin/pki_evidence_index.ksh`) | | `@weekly` (optional) | Weekly digest mail (`/var/pki/bin/pki_weekly_digest.ksh`) |

5.4 Logging and monitoring

- Syslog: `local5.info` → `/var/pki/log/admin.log`; `receipts/` captures JSON action logs; TSA audit logs under `/var/pki/log/tsa_audit/`.
- Rate-limited alerts (`PKI_ALERT_RATE_SECS`, default 1800s) for incidents only (preflight failure, CRL roll failure, TSA drift, HTTPS verification failure).
- Hash verification script (adm_hashcheck) quarantines mismatches in `/var/pki/quarantine/`.

5.5 Records retention

- Policy documents, receipts, CRLs, manifests retained ≥10 years (per Standards v4.2).
- Logs rotated daily via newsyslog (`/var/pki/log/*.log root:sign 640 7 * $D0 Z`).
- Archived copies stored under `/var/pki/archive/` and `/var/pki/archive-index/`.

---

6. Technical security controls

6.1 Key pair generation and installation

- Root CA keys are generated offline within the root-vault using OpenSSL 3.5.4 and `/dev/random`.
- Subordinate CA/EE keys are generated on the hardened PKI host (no internet access, default-deny firewall). Keys never

leave the system except the encrypted root backup (root-ca.key.gpg).

- No PEM passphrases are used; security derives from the air-gapped deployment, disk encryption, restricted access, and strict role separation.

6.2 Key protection and storage

- /var/pki/active/ contains CA and EE keys with permissions 0640 root:sign.
- /var/pki/root-vault/ contains root material; volume mounted only during ceremonies; helper vault_maybe_umount unmounts after operations.
- Backups: encrypted root key stored offline; CA/EE keys not exported.
- Signing service temporary workspace /var/pki/sigsvc/ uses per-run directories (run.XXXXXX) cleaned on exit.

6.3 Other aspects of key management

- EE autorotation ensures overlapping validity, preventing gaps.
- Intermediates staged with freeze/backout markers; failover instructions in SSOT A-5.
- TSA serial allocation locked to prevent concurrency; tsa.conf ensures accuracy secs:1 and tsa_name=yes.

6.4 Cryptographic module controls

- No Hardware Security Module; security achieved via softraid encryption, air gap, locked accounts, and audit trail.
- OpenSSL compiled with enable-cms enable-ts and installed to /usr/local/openssl-3.5.4/bin/openssl.

6.5 Secure communications and controls

- PF firewall operates on default deny; the only inbound rule permits SSH from the signing client 192.168.100.1 and is bound to the forced-command wrapper.
- The signing service runs via forced SSH command (no PTY, no agent or port forwarding). Optional SFTP fallback requires explicit operator action (/var/pki/etc/sigsvc_mode).
- System time is maintained via ntpd with a trusted internal peer; the TSA selftest enforces a ±2 s drift threshold.

6.6 Certificate and CRL issuance

- Certificates include policy OIDs and CPS pointers (CPS.1 extension).

- CRLs generated with `default_crl_days` (root 30, signing 7, TSA 30) and published immediately.
- No OCSP; CRL-only policy enforced (see L2).

7. Certificate, CRL, and OCSP profiles

Class	Policy OID	Key / Hash	Extensions

Root CA	1.3.6.1.4.1.59713.8.1	RSA 4096 / SHA-256	`basicConstraints CA:true pathLen:2,`
			`CRLDistributionPoints`

Signing CA	1.3.6.1.4.1.59713.8.2	RSA 3072 / SHA-256	as Root + `authorityInfoAccess (caI`
TSA CA	1.3.6.1.4.1.59713.8.3	RSA 3072 / SHA-256	as Signing CA

Signing EE	1.3.6.1.4.1.59713.8.10.1	RSA 2048 / SHA-256	`extendedKeyUsage emailProtection`, `s`
			`CRLDistributionPoints`

TSA EE	1.3.6.1.4.1.59713.8.10.3	RSA 2048 / SHA-256	`extendedKeyUsage timeStamping`, `subj`

- CRLs adhere to RFC 5280; reasons limited to `keyCompromise`, `cessationOfOperation`, `superseded`.
- TSA tokens follow RFC 3161 with policy OID 1.3.6.1.4.1.59713.8.10.3, accuracy `secs:1`, ordering `no`, TSA name included.

8. Compliance audit and other assessments

8.1 Internal oversight

- Daily preflight + chain validation.
- Daily CRL roll (Signing/TSA), weekly hash verification, monthly evidence index.
- Optional weekly digest summarises status and CRL horizons.
- Receipts and admin logs reviewed by audit role; hash mismatches quarantined.

8.2 External audit

- Annual independent review against ETSI EN 319 421/422 and RFC 3161; scope includes key management, publication availability, script integrity.
- Audit findings recorded in change log, with remediation tracked via tickets and subsequent receipts.

8.3 Incident response

- Documented in L3: CRL/manifest/publish errors raise immediate alerts, block sync, and require manual intervention.
- For key compromise: isolate host, unmount vault, revoke affected certificates, reissue chain, update repository, notify internal stakeholders.

---

9. Business, legal, and liability

- **Usage limitations:** Certificates are for internal DURCHD8 operations; no warranties for external relying parties.
- **Liability:** DURCHD8 assumes no liability for third-party reliance or misuse beyond documented procedures.
- **Fees:** None (internal service).
- **Confidentiality:** Private keys, vault data, change tickets, and audit logs are confidential. Published artefacts are open.
- **Privacy:** Subscriber data is limited to functional identifiers; no personal data beyond duty contacts (pki@durchd8.com).
- **Dispute resolution:** Managed by the PKI Steering Team; escalations follow DURCHD8’s governance process.

---

10. References

1. DURCHD8 Certificate Policy v1.0 (OID 1.3.6.1.4.1.59713.8.0)
2. RFC 3647, RFC 5280, RFC 5652, RFC 3161
3. ETSI EN 319 421 & 319 422
4. DURCHD8 SSOT documents (L0–L3) dated 2025-10-24
5. System Change Record OpenBSD PKI 2025-10-27

End of document — DURCHD8 CPS v1.0.