Certificate Policy (CP)

DDSign: Electronic Certification Service Provider.

Document Reference: DD-CP-001
Version: 1.0
Status: PUBLISHED
Effective Date: 1st April 2026
Owner: DDSign Operations
Review Cycle: Annual, or on material change to PKI architecture or applicable law

Governing Law: Republic of Kenya: KICA CAP411A; Electronic Certification and Domain Name Administration Regulations 2010; Electronic Transactions Act; Kenya Data Protection Act 2019

Table Of Contents.

1. Introduction

1.1 Overview

This Certificate Policy (CP) defines the rules and requirements that govern the issuance, management, use, suspension, renewal, and revocation of digital certificates by DDSign in its capacity as an Electronic Certification Service Provider (E-CSP) and Timestamp Authority (TSA) under Kenyan law.

This CP is structured in accordance with RFC 3647 (Internet X.509 Public Key Infrastructure — Certificate Policy and Certification Practices Framework). It states **what** is required of all PKI participants. The **how** — the operational procedures implementing each requirement — is documented in the companion Certification Practice Statement (`CPS`) and the following operative policy documents:

Document	Reference	Purpose
Certification Practice Statement	DD-CPS-001	Operational implementation of this CP
Key Management Policy	DD-KMP-001	Cryptographic key lifecycle controls
HSM Security Policy	DD-HSP-001	Hardware Security Module configuration and controls
Certificate Lifecycle Procedures	DD-CLP-001	Step-by-step certificate issuance, renewal, revocation, CRL

In the event of a conflict between this CP and any of the above documents, this CP takes precedence in matters of policy. The implementing document takes precedence in matters of operational procedure.

1.2 Document Name and Identification

Document: DDSign Certificate Policy
URL: `https://web.ddsign.ae/resource-center/certificate_policy.pdf`

1.3 PKI Participants

1.3.1 Certification Authority (CA)

DDSign operates a single-tier CA hierarchy:

- **Root CA:** DDSign Certification Authority. The root CA private key is held exclusively in AWS KMS as a Customer Managed Key (CMK, RSA_4096, SIGN_VERIFY). The root CA is not publicly trusted (it is not embedded in browser or OS trust stores). Relying parties must explicitly install the DDSign CA certificate to verify DDSign-issued certificates.
- **TSA (Subordinate function):** The Timestamp Authority certificate is issued by the Root CA and carries the sole extended key usage with embedded OID.

1.3.2 Registration Authority (RA)

DDSign currently acts as its own RA. There are no delegated or third-party RAs. All identity verification and key ceremony authorisation is performed by DDSign Operations staff.

1.3.3 Subscribers

A Subscriber is any legal entity or individual who:

- Has been issued an API authentication key by DDSign; and
- Submits documents to DDSign services for timestamping or digital signature workflows.

The DDSign TSA certificates are **internal operational certificates** — they are not issued to external subscribers. Subscribers interact with the DDSign service via authenticated API calls; they do not themselves receive X.509 certificates from this CA hierarchy.

1.3.4 Relying Parties

A Relying Party is any entity that verifies a DDSign timestamp token, digital signature, or certificate. Relying parties must:

- Import the DDSign CA certificate into their trust store.
- Check the DDSign CRL before relying on any certificate (`CLP` Section 8).
- Accept responsibility for verification outcomes resulting from failure to check revocation status.

1.3.5 Accreditation Authority

The Accreditation Authority is the Kenya ICT Authority (`confirm authority and contact under Electronic Certification Regulations 2010 Regulation 4`).

1.4 Certificate Usage

1.4.1 Permitted Uses

Certificate	Permitted Uses
CA certificate	Sign TSA certificates and CRLs only
TSA certificate	RFC 3161 timestamp token signing only

The TSA certificate MUST NOT be used for TLS server authentication, S/MIME email signing, code signing, or any entity authentication purpose outside RFC 3161 timestamping.

1.4.2 Prohibited Uses

- Any use of a DDSign certificate in a manner inconsistent with its Extended Key Usage extension.
- Use of a revoked or suspended certificate.
- Use of a certificate by any party other than DDSign (the CA and TSA certificates are internal; they are not subscriber-held certificates).

2. Publication and Repository Responsibilities

2.1 Repositories

DDSign MUST maintain the following public repositories:

Repository	Contents	URL
CA certificate repository	Current and historical CA certificates (PEM)	`https://crl.ddsign.ae/ca.pem`
CRL Distribution Point (CDP)	Current CRL (DER)	`https://crl.ddsign.ae/current.crl`
CP/CPS repository	This CP, the CPS, and all referenced policy documents	`https://cps.ddsign.ae/`

2.2 Publication Obligations

- The CA certificate MUST be published at the CA repository URL within 24 hours of issuance or renewal.
- The CRL MUST be published within 24 hours of any revocation or suspension event, and MUST be refreshed at least every 24 hours regardless of revocation activity.
- The CP and CPS MUST be available at their published URLs at all times. Planned maintenance windows must not exceed 4 hours.
- All published materials MUST be served over HTTPS (TLS 1.2 minimum) from a server with a valid, non-revoked certificate.

2.3 Access Controls on Repositories

Repository contents are public and read-only. Write access is restricted to DDSign Operations through authenticated internal tooling. No anonymous write access is permitted.

3. Identification and Authentication

3.1 Naming

All DDSign-issued certificates MUST carry distinguished names (DNs) in accordance with ITU-T X.500 and RFC 5280:

Certificate	Subject Distinguished Name
Root CA	`C=KE, O=DDSign, CN=DDSign Certification Authority`
TSA	`C=KE, O=DDSign, CN=DDSign Timestamp Authority, emailAddress=timestamp@ddsign.local`

Subject names MUST NOT be empty. All fields MUST use UTF-8 encoding.

3.2 Initial Identity Verification

3.2.1 TSA and CA Certificates (Internal Operational)

The TSA and CA certificates are issued internally by DDSign Operations staff and do not require third-party identity verification — the CA signs its own subordinate TSA certificate following the procedures in `CLP` Section 3.

Issuance of internal operational certificates REQUIRES:

- Dual-operator authentication (two distinct named admin principals).
- A formal key ceremony record signed by both operators.
- Recording of the KMS CA Key ARN in the ceremony record.

3.2.2 API Key Subscribers (System-Level Authentication)

Any external system requesting access to DDSign services MUST be verified through the following identity check before an API key is activated:

1. Written request from a named technical contact identifying the organisation, intended use, and authorised contact.
2. DDSign Operations review confirming a legitimate business purpose.
3. Execution of a subscriber agreement (`attach subscriber agreement template`).
4. Admin-scoped key issuance only after additional written justification.

3.3 Renewal Identity Requirements

TSA certificate renewal (key rotation) does not require re-verification of subscriber identity — it is an internal operational procedure. Two distinct admin operators MUST authenticate the renewal action (`CLP` Section 5.2).

API key renewal requires re-confirmation of the subscriber agreement if more than 24 months have elapsed since the last agreement execution.

3.4 Revocation Request Authentication

A revocation request MUST be authenticated by two distinct admin-scoped principals before it is processed. Anonymous or unauthenticated revocation requests are rejected.

4. Certificate Lifecycle Operational Requirements

4.1 Certificate Application

Internal certificate applications (CA and TSA certificates) are initiated by DDSign Operations through the key ceremony process. No external certificate application form is required for internal operational certificates.

For future subscriber-facing certificate types, an application form process MUST be defined before such certificate types are introduced.

4.2 Certificate Issuance Requirements

A certificate MUST NOT be issued unless all of the following conditions are satisfied:

1. Dual-operator authentication has been confirmed (`RequireDualOperator` — `pkg/auth/dual_control.go`).
2. A key ceremony record has been created.
3. The CA key ARN (`KMS_CA_KEY_ARN`) is available and accessible.
4. The target key material has been generated (TSA key via CSPRNG; CA key via AWS KMS).
5. The certificate profile fields comply with Section 7.1 of this CP.
6. `KEY_GENERATION_REQUIRE_APPROVAL=true` is set in the production environment.

4.3 Certificate Acceptance

A certificate is considered accepted when it has been loaded into the running `TSAServer` instance via `TSAServer.Reload` and the audit log records a successful `key_rotation` entry with the certificate fingerprint.

4.4 Certificate Suspension Requirements

A certificate MUST be suspended when one or more of the following conditions applies and the compromise is not yet confirmed:

- A key compromise is suspected but unconfirmed.
- A subscriber's entitlement to the certificate is under active review.
- An operational anomaly requires temporary withdrawal from reliance.

Suspension MUST:

- Be authorised by two distinct admin-scoped operators.
- Result in a CRL update within **4 hours** of the suspension decision.
- Be reviewed within **5 business days**.
- Be escalated to full revocation or lifted within **30 calendar days**.
- Result in notification of suspension to the subscriber through a secure primary communication channel.

4.5 Certificate Revocation Requirements

A certificate MUST be revoked when one or more of the following conditions applies:

- Private key compromise is confirmed or determined to be highly probable.
- The CA key is compromised.
- The certificate was issued in error or in violation of this CP.
- The subscriber ceases to operate.
- An instruction to revoke is received from the Accreditation Authority.
- The certificate subject's name or affiliation has changed in a way that renders the certificate misleading.

Revocation MUST:

- Be authorised by two distinct admin-scoped operators.
- Record the correct RFC 5280 reason code (see Section 7.3 of this CP).
- Result in a published CRL update within **24 hours** of the revocation decision.
- Be permanent and irreversible.

A CA key compromise MUST additionally trigger:

- Bulk revocation of all certificates issued by the compromised CA
- Immediate notification to the Accreditation Authority via `AuthorityNotifier` and direct written notice within 24 hours (per KICA CAP411A requirements).
- Invocation of the Incident Management Plan (`IMP`).

4.6 Certificate Renewal Requirements

Certificate renewal (key rotation) MUST:

- Be initiated by two distinct admin-scoped operators.
- Generate a new RSA 4096-bit key pair using CSPRNG.
- Produce a new certificate signed by the CA via `kms:Sign` with `KMS_CA_KEY_ARN`.
- Complete atomically — the old key and new key MUST NOT both be live simultaneously.
- Result in a backup of the new key material immediately after rotation.
- Be completed before the certificate expiry date; DDSign MUST initiate renewal no later than 30 days before the expiry of the current TSA certificate.

Renewal does not require re-issuance of the CA certificate unless the CA certificate itself is approaching expiry .

4.7 Certificate Expiry

- **CA certificate:** Maximum validity 10 years from issuance. Renewal MUST be initiated on or before the 5-year mark.
- **TSA certificate:** Maximum validity 10 years from issuance. Renewal MUST be initiated before the 90-day warning threshold.

These validity periods represent maximums. The CA may issue certificates with shorter validity at its discretion. No certificate validity period may exceed 10 years.

4.8 Key Escrow and Recovery

DDSign does NOT operate a key escrow service. Private key material held in AWS KMS is non-exportable by design. TSA private keys held in a PKCS#11 HSM are non-exportable by policy (`CKA_EXTRACTABLE=false`).

In the event of a TSA HSM failure, a new TSA key is generated on a replacement HSM and a new TSA certificate is issued by signing a CSR with the KMS CA key. No key escrow or recovery of the original TSA key is attempted. See `HSP` Section 8.2.

5. Facility, Management, and Operational Controls

5.1 Physical Security Requirements

The servers hosting the DDSign service MUST be located in a facility that provides:

- Locked physical access with access logging.
- Dual-person access control for server room entry `confirm facility meets this requirement`.
- CCTV coverage with minimum 90-day recording retention.
- Uninterruptible power supply (UPS) with minimum 4-hour runtime.
- Fire suppression that does not damage electronic equipment (clean agent or FM-200).

The AWS KMS CA key is subject to AWS physical security controls (AWS compliance reports: SOC 2 Type II, ISO 27001, FIPS 140-2 Level 3). DDSign is not required to provide independent physical security for the CA key beyond the AWS KMS service boundary.

5.2 Procedural Controls

5.2.1 Trusted Roles

Role	Minimum Headcount	Responsibilities
Operations Lead	1	End-to-end CA operations, policy owner
Operator (Primary / Secondary)	3 (minimum)	Key ceremonies, rotation, revocation — must have ≥2 active at all times

Security Auditor	1 (independent of Operations)	Log review, compliance assessment, ceremony record audit
Key Ceremony Officer	1 (may be the Operations Lead)	Conducts key ceremonies, signs ceremony records

A minimum of **three** named operator key holders MUST be maintained at all times. If headcount falls below three, the shortfall MUST be remediated before the next key operation.

5.2.2 Dual-Operator Enforcement

Every sensitive operation MUST satisfy the following conditions, which are enforced programmatically by `RequireDualOperator` (`pkg/auth/dual_control.go`):

- Both `x-api-key` and `x-operator2-key` gRPC metadata headers are present.
- Both keys validate against stored SHA-256 hashed credentials with `admin_scope: true`.
- The `name` field of both keys differs — the same individual may not authorise both sides of a dual-control action.

Policy prohibits any attempt to circumvent the dual-operator requirement by sharing API key credentials between individuals.

5.2.3 Key Ceremony Requirements

All production key material MUST be generated through a formal key ceremony that:

- Is attended and authenticated by two named operators.
- Records the KMS CA Key ARN, certificate fingerprints, serial numbers, operator names, and UTC date/time in a signed ceremony record stored in `ceremony-records/`.
- Results in an immediate backup of non-KMS key material.

See `KMP` Section 4.2 and `CLP` Section 3.1 for ceremony procedures.

5.3 Personnel Security Requirements

All personnel with access to DDSign key material or operational systems MUST:

- Have a background check on record
- Have signed a Non-Disclosure Agreement (NDA) covering PKI operations and key material.
- Complete annual security awareness training covering topics relevant to their role.
- Be subject to access review every 12 months — administrator credentials MUST be revoked within 24 hours of role change or termination.

Personnel holding admin-scoped API keys are subject to the additional requirements:

- Named credentials only — team or shared accounts are prohibited.
- Key rotation every 12 months.
- Immediate revocation on departure or role change.

5.4 Audit and Accountability

5.4.1 Audit Log Requirements

All certificate lifecycle events MUST be recorded in the DDSign audit log. The audit log MUST:

- Use an HMAC-SHA256 forward-linked integrity chain (each entry commits to the HMAC of the preceding entry).
- Be stored with access control — only the service process has write access; the Security Auditor has read access.
- Be retained for a minimum of 13 months (configurable via `AUDIT_LOG_MAX_AGE_DAYS`).
- Produce gzip-compressed rotated archives on size or age limits.

5.4.2 AWS CloudTrail Requirements

Because the CA private key resides in AWS KMS, all `kms:Sign` and `kms:GetPublicKey` API calls on the CA CMK MUST be logged to AWS CloudTrail and reviewed in the monthly security report. Any unexplained `kms:Sign` invocation is a P1 security incident.

5.4.3 Events That MUST Be Logged

The following events MUST appear in the audit log:

- CA certificate issuance (key ceremony start and completion)
- TSA certificate issuance
- TSA key rotation (emergency and scheduled)
- Certificate suspension and unsuspension
- Certificate revocation (individual and bulk)
- API key issuance and revocation
- Key backup creation and verification
- Key destruction
- Any failed dual-operator authentication attempt

5.4.4 Audit Log Review

The Security Auditor MUST review the audit log:

- Monthly, as part of the standing security review.
- Immediately following any revocation or key rotation event.
- Immediately following any security incident.
- Annually as part of the compliance audit (see Section 8).

5.5 Records Retention

Record Type	Minimum Retention	Storage
Audit log (active)	13 months	Service host
Audit log archives	7 years	Encrypted object storage
Key ceremony records	Indefinitely	Physical signed copy + encrypted digital copy
Backup custody log	7 years	Encrypted object storage
Certificates of destruction	7 years	Physical and digital
Revocation records	7 years after certificate expiry	Revocation store + audit log

5.6 Business Continuity

CA certificate re-issuance after a catastrophic failure is possible using the AWS KMS CA key, which survives independent of DDSign's on-premises infrastructure. Key operational continuity scenarios are documented in the `Business Continuity Plan`.

6. Technical Security Controls

6.1 Key Generation Requirements

Key	Required Method	Key Spec
CA root private key	Generated in AWS KMS — `CreateKey` API; key origin `AWS_KMS` (non-exportable)	RSA_4096, SIGN_VERIFY
TSA signing private key	OS CSPRNG (`crypto/rand`, `getrandom`)	RSA 4096-bit
Timestamp token serial numbers	OS CSPRNG (`crypto/rand`)	64-bit random integer
Certificate serial numbers	OS CSPRNG (`crypto/rand`)	Random 128-bit integer (RFC 5280 4.1.2.2)
API keys	OS CSPRNG (`scripts/generate-api-key.sh`)	256-bit entropy minimum
HMAC audit key	OS CSPRNG	256-bit (32 bytes)

Keys MUST NOT be generated outside an approved source of entropy. Use of deprecated or predictable PRNGs is prohibited.

6.2 Private Key Protection Requirements

Key	Production Requirement	Development Allowance
CA root private key	Exclusively in AWS KMS (FIPS 140-2 Level 3); non-exportable; no plaintext key ever written to disk	Local PEM `chmod 0600` for bootstrap testing only
TSA signing private key	PKCS#11 HSM with `CKA_EXTRACTABLE=false`; FIPS 140-2 Level 3 minimum	PEM `chmod 0600` at `TSA_KEY_PATH`

The following MUST hold in all environments:

- No private key material may be committed to version control (`.gitignore` enforces exclusion of `*.pem` and `certs/`).
- Key files MUST be owned by the service user with mode `0600`; the containing directory MUST be mode `0700`.
- No private key MUST be transmitted over an unencrypted channel.
- All Certificates, Keys, and password hashes are fully managed on secure transit and stationery DDSign platform components. And non exportable.

6.3 Approved Cryptographic Algorithms

This CP adopts the algorithm requirements of `KMP` Section 3, and ETSI TS 119 312.

Algorithm	Use	Status
RSA-4096	CA signing (via AWS KMS)	**REQUIRED**

RSA-4096	TSA signing	**REQUIRED**
SHA-256	All certificate digests, HMAC, fingerprints	**REQUIRED**
AES-256-CBC	Key backup archive encryption	**REQUIRED** (backup only)
RSA-2048	Legacy PDF signer certificates	**DEPRECATED** — no new issuance after 1 January 2027
SHA-1	Any use	**PROHIBITED**
MD5	Any use	**PROHIBITED**
DES / 3DES	Any use	**PROHIBITED**
RSA < 2048-bit	Any use	**PROHIBITED**
EC curves below P-256	Any use	**PROHIBITED**

The algorithm list is reviewed annually. Any deviation from the above requires written approval from the Security Auditor and the Operations Lead, is documented in `algorithm-review-log`, and is reported to the Accreditation Authority.

6.4 Key Backup Requirements

Backups of non-KMS key material (TSA key and certificates) MUST be:

- Encrypted with AES-256-CBC using a randomly generated passphrase (minimum 48 bytes of entropy).
- Accompanied by a SHA-256 checksum file.
- Stored in at least two physically separate locations:
    - Primary: encrypted object storage (S3 or equivalent) with versioning and MFA Delete.
    - Secondary: offline encrypted removable media held in a physical safe.
- Passphrase stored separately from the archive (e.g. AWS Secrets Manager, HashiCorp Vault) under break-glass access control.

Backups MUST be tested for successful restoration at minimum once per quarter. Failed restoration tests are P2 incidents.

The CA private key (AWS KMS CMK) is NOT included in backup archives. AWS KMS provides its own durability and multi-AZ redundancy for CMK key material.

6.5 HSM Requirements

Production TSA keys MUST be held in an HSM that meets ALL of the following:

- FIPS 140-2 Level 3 (or equivalent Common Criteria EAL 4+) certified.
- Exposes a standard PKCS#11 interface.
- Enforces `CKA_EXTRACTABLE=false` on TSA key objects.
- Maintains an internal access log of all signing operations.

See `HSP` for full HSM configuration, access control, vendor certification, and decommissioning requirements.

6.6 Network Security Requirements

- All gRPC endpoints MUST run behind TLS (minimum TLS 1.2; TLS 1.3 preferred).
- The admin gRPC API MUST NOT be accessible from the public internet. Network access to the admin port MUST be restricted to operator workstations via IP allowlist or VPN.

- AWS KMS access MUST be further restricted by IAM policy to specific IAM roles (see `KMP` Section 5.2).

7. Certificate, CRL, and OCSP Profiles

7.1 CA Certificate Profile

Field	Required Value
Version	X.509 v3
Serial number	Cryptographically random 128-bit integer
Subject	`C=KE, O=DDSign, CN=DDSign Certification Authority`
Issuer	Same as Subject (root CA)
Key algorithm	RSA 4096-bit (AWS KMS CMK, non-exportable)
Signature algorithm	`sha256WithRSAEncryption`
Validity — Not Before	Date of key ceremony
Validity — Not After	Not Before + 10 years (maximum)
`BasicConstraints`	`CA:true` (critical)
`KeyUsage`	`keyCertSign`, `cRLSign` (critical)

`SubjectKeyIdentifier`	SHA-1 of the CA public key (per RFC 5280 4.2.1.2)
`CRLDistributionPoints`	`https://crl.ddsign.ae/current.crl`
Certificate Policies	This CP OID

7.2 TSA Certificate Profile

Field	**Required Value**
Version	X.509 v3
Serial number	Cryptographically random 128-bit integer
Subject	`C=KE, O=DDSign, CN=DDSign Timestamp Authority, emailAddress=timestamp@ddsign.local`
Issuer	DDSign Certification Authority
Key algorithm	RSA 4096-bit
Signature algorithm	`sha256WithRSAEncryption`
Validity — Not Before	Date of issuance

Validity — Not After	Not Before + 10 years (maximum)
`BasicConstraints`	`CA:false`
`KeyUsage`	`digitalSignature` (critical)
`ExtKeyUsage`	`OID`
`AuthorityKeyIdentifier`	Key ID of the issuing CA
`SubjectKeyIdentifier`	SHA-1 of the TSA public key
`CRLDistributionPoints`	`https://crl.ddsign.ae/current.crl`
`AuthorityInfoAccess`	`CA Issuers URI — https://crl.ddsign.ae/ca.pem; OCSP URI when operational`
Certificate Policies	This CP OID

The `id-kp-timeStamping` EKU MUST be the **sole** extended key usage on the TSA certificate. The presence of any additional EKU is a certificate issuance error.

7.3 CRL Profile

Field	**Required Value**
Version	X.509 CRL v2

Issuer	DDSign Certification Authority
Signature algorithm	`sha256WithRSAEncryption`
`thisUpdate`	Time of CRL generation
`nextUpdate`	`thisUpdate + 24 hours`
`AuthorityKeyIdentifier`	Key ID of the issuing CA
CRL entry — reasonCode	Required for all entries; MUST use RFC 5280 reason codes

Approved CRL Reason Codes

Code	Name	Permitted Use
0	`unspecified`	Only when no more specific code applies
1	`keyCompromise`	Private key of TSA suspected or confirmed compromised
2	`cACompromise`	CA key suspected or confirmed compromised

3	`affiliationChanged`	Subject's name or organisational affiliation changed
4	`superseded`	Certificate replaced by a new issuance
5	`cessationOfOperation`	Subject entity has ceased operating
6	`certificateHold`	Temporary suspension (reversible)

Use of reason code `removeFromCRL` (8) is ONLY permitted for CRL entries that accompany an unsuspension operation.

7.4 OCSP

An OCSP responder is not yet operational. This CP requires DDSign to implement a compliant OCSP service before seeking Tier 2 or higher accreditation status. Until OCSP is deployed:

- Relying parties MUST use CRL checking.
- The CPS and this CP MUST explicitly disclose the absence of an OCSP responder.

When OCSP is deployed it MUST:

- Comply with RFC 6960.
- Reflect revocation status within **15 minutes** of a revocation event.
- Sign responses with a dedicated OCSP responder certificate or delegated signing using the CA key.
- Assert a `nextUpdate` value no greater than 24 hours from response generation.

8. Compliance Audit and Other Assessments

8.1 Frequency and Scope

An independent compliance audit MUST be conducted at least annually. The audit MUST assess:

- Conformance of DDSign operations with this CP and the CPS.
- Accuracy and completeness of the certificate inventory.
- Correct implementation of dual-operator control.
- Completeness of the CRL (all revoked serials present).
- Timely CRL publication (within 24 hours of every revocation event).
- Compliance of key generation, storage, and destruction with Section 6 of this CP.
- AWS KMS CloudTrail log review — all `kms:Sign` operations on the CA CMK are accounted for.
- Accuracy of quarterly Accreditation Authority returns.
- Algorithm compliance against approved list (Section 6.3).

8.2 Auditor Independence

The Security Auditor role MUST be held by a person who is:

- Not in the operational chain of command for the CA or TSA functions.
- Not a holder of an admin-scoped API key.
- Free from conflicts of interest with DDSign Operations.

8.3 Actions on Findings

Finding Severity	**Required Response Time**	**Escalation**
Critical (active compromise or policy violation)	Immediate — incident response plan invoked	Accreditation Authority within 24 hours
High (gap in controls, near-miss)	Within 5 business days	Reported in next quarterly return
Medium (documentation gap, process weakness)	Within 30 days	Internal tracking only
Low (observation, recommendation)	Next annual review cycle	Internal tracking only

All compliance findings MUST be recorded in the incident management system and tracked to resolution.

8.4 Quarterly Accreditation Authority Returns

DDSign MUST submit quarterly operational returns to the Accreditation Authority by the **15th day after each quarter end**, covering:

- New certificates issued in the quarter
- Currently valid certificates
- Currently suspended certificates
- Certificates renewed in the quarter
- Certificates revoked in the quarter
- Cyber incidents declared in the quarter

These counters are maintained automatically by `QuarterlyReportManager` and retrieved via `AdminService.GetQuarterlyReport`.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Fee Schedule and Subscription Model

The DdSign E-CSP operates a subscription-based fee model. The following sub-sections define the fee schedule, plan structure, included services, usage limits, trial terms, fee change procedures, refund policy, and payment terms.

9.1.1.1 Fee Schedule Overview

The DdSign E-CSP operates a subscription-based fee model. All certification services, including digital certificate issuance, digital signature execution, timestamping, certificate status checking (CRL/OCSP), and document storage are bundled into the subscription plan. There are no separate per-certificate or per-transaction fees for these services. Fees are denominated in United States Dollars (USD), with Kenya Shilling (KES) equivalents charged at the prevailing exchange rate at the time of billing.

9.1.1.2 Subscription Plans

The E-CSP offers the following subscription tiers:

Plan	Monthly Fee (USD)	Monthly Fee (KES)	Trial Period
Free	$0	KES 0	N/A
Starter	$15.00	KES equivalent at prevailing rate	14 days
Business	$49.00	KES equivalent at prevailing rate	14 days
Enterprise	Custom pricing	Custom pricing	14 days

The Enterprise plan is available on a negotiated basis. Organisations requiring Enterprise services shall contact Centric Limited directly for a custom quotation.

9.1.1.3 Services Included in Subscription

Each subscription plan includes the following services at no additional per-transaction cost:

- Digital certificate issuance: Subscriber certificates are issued under the DDSign Issuing CA as part of the subscription. No separate certificate application or issuance fee applies.

- Digital signature execution: Document signing via envelopes is included up to the plan's per-period envelope limit.

- Timestamping: RFC 3161-compliant timestamps are applied to all signed documents as a bundled benefit of the subscription. There is no separate timestamping fee.

- Certificate status services: Access to CRL distribution points and OCSP responders is provided free of charge to all Subscribers and Relying Parties.

- Document storage: Signed documents are stored up to the plan's storage limit.

- Templates: Reusable signing templates are available up to the plan's template limit.

- API access: Programmatic access to the ddsign platform is available on Starter, Business, and Enterprise plans, subject to daily API request limits.

9.1.1.4 Plan Limits

Each plan enforces the following usage limits per billing period:

Feature	Free	Starter	Business	Enterprise
Envelopes per period	5	50	500	Unlimited
Organisation members	3	10	50	Unlimited
Stored documents	10	100	1,000	Unlimited
Storage capacity	100 MB	1 GB	10 GB	Unlimited
Templates	2	20	Unlimited	Unlimited
API requests per day	100	1,000	10,000	Unlimited

When a Subscriber approaches or exceeds a usage limit, the platform provides a grace period (typically three days with a small additional allowance) before access to the exceeded feature is restricted. Subscribers are notified via in-application alerts and are encouraged to upgrade their plan to restore access.

9.1.1.5 Plan Features

Access to advanced platform features varies by plan:

Feature	Free	Starter	Business	Enterprise
Basic templates	Yes	Yes	Yes	Yes
Advanced templates	No	Yes	Yes	Yes
API access	No	Yes	Yes	Yes
Webhooks	No	Yes	Yes	Yes
Audit logs	No	Yes	Yes	Yes
Custom branding	No	No	Yes	Yes
Power Forms	No	No	Yes	Yes
Cloud storage integration	No	No	Yes	Yes
Reports and analytics	No	No	Yes	Yes
Priority support	No	No	No	Yes

9.1.1.6 Free Trial

Paid subscription plans (Starter, Business, and Enterprise) include a fourteen (14) day free trial. During the trial period, the Subscriber has full access to all features and limits of the selected plan. If the Subscriber does not subscribe before the trial expires, the subscription reverts to the Free plan. Usage accrued during the trial period is retained.

9.1.1.7 Fee Changes

Centric Limited reserves the right to modify the fee schedule. Any changes to subscription fees shall be communicated to existing Subscribers in writing (via email and in-application notification) at least ninety (90) days before the new fees take effect. Fee changes do not apply retroactively to the current billing period. Subscribers who do not accept the revised fees may cancel their subscription before the new fees take effect.

9.1.1.8 Refund Policy

All subscription fees are non-refundable once paid. Subscribers who cancel their subscription retain access to the paid plan's features and limits for the remainder of the current billing period (grace period). Upon expiry of the grace period, the subscription reverts to the Free plan. No pro-rata refunds are issued for partial billing periods, downgrades, or early cancellation.

9.1.1.9 Payment Terms

Subscription fees are billed monthly in advance. Payment is due at the start of each billing period. If payment fails, the subscription enters a past-due state. Centric Limited shall notify the Subscriber of the failed payment and provide a reasonable opportunity to remedy the payment before downgrading the subscription to the Free plan.

9.2 Financial Responsibility

9.2.1 Liability and Insurance Framework

The following sub-sections define the liability limitations, insurance provisions, indemnification obligations, and relying party conditions applicable to the ddsign E-CSP.

9.2.1.1 Limitation of Liability

The liability of Centric Limited, as the operator of the ddsign E-CSP, is governed by the Kenya Information and Communications Act (KICA), CAP 411A, Section 14. Centric Limited reserves the right to set a maximum aggregate liability cap in its Subscriber Agreement and Relying Party terms, subject to the statutory framework.

Centric Limited shall not be liable for:

- Losses arising from the misuse of a certificate by a Subscriber, including use beyond the scope of the certificate's stated purpose or the Subscriber Agreement.
- Losses arising from a Relying Party's failure to check the revocation status of a certificate via CRL or OCSP before reliance.
- Losses arising from a Relying Party's reliance on a certificate for a transaction value exceeding any stated reliance limit.
- Losses caused by events beyond the reasonable control of Centric Limited, including force majeure events (natural disasters, war, government action, power failure, telecommunications failure).
- Indirect, consequential, incidental, special, or punitive damages, including loss of profits, loss of data, or business interruption, even if Centric Limited has been advised of the possibility of such damages.

9.2.1.2 Insurance

Centric Limited maintains appropriate insurance coverage to support its obligations as an E-CSP. The insurance programme is designed to provide financial backing for potential liabilities arising from the operation of the ddsign certification services. Details of the insurance coverage are documented separately and are available for review by the Communications Authority of Kenya upon request.

9.2.1.3 Indemnification

The following mutual indemnification obligations apply:

Centric Limited's Indemnification of Subscribers: Centric Limited shall indemnify and hold harmless Subscribers against direct losses, damages, and reasonable legal costs arising from:

(a.) Centric Limited's negligence in the issuance, management, or revocation of certificates;

(b.) A failure by Centric Limited to comply with the representations made in the Certificate Policy or Certification Practice Statement; or

(c.) A breach of the Kenya Data Protection Act, 2019, by Centric Limited in its handling of Subscriber personal data. This indemnification is subject to the liability cap established by Centric Limited.

Subscriber Indemnification of Centric Limited: Subscribers shall indemnify and hold harmless Centric Limited against direct losses, damages, and reasonable legal costs arising from:

(a.) the Subscriber's misuse of a certificate or private key, including use for purposes not permitted by the Certificate Policy or Subscriber Agreement;

(b.) the Subscriber's failure to protect their private key or to notify the E-CSP promptly of a known or suspected key compromise;

(c.) the Subscriber's provision of false, inaccurate, or misleading information during the certificate application or identity verification process; or

(d.) the Subscriber's breach of the Subscriber Agreement.

9.2.1.4 Relying Party Obligations

Relying Parties who rely on certificates issued by the ddsign E-CSP do so subject to the following conditions:

1. The Relying Party must verify the certificate's revocation status via CRL or OCSP before reliance.
2. The Relying Party must not rely on a certificate that has been revoked, expired, or suspended.
3. The Relying Party must not rely on a certificate for a purpose inconsistent with the certificate's stated key usage or the Certificate Policy.
4. Failure to comply with these obligations releases Centric Limited from liability to the Relying Party.

9.3 Confidentiality

The following information is considered confidential and MUST NOT be disclosed outside DDSign without legal authorisation:

- Private key material (CA CMK, TSA key, HMAC secrets, API keys).
- Ceremony records (except to the Accreditation Authority).
- Audit logs (except to the Security Auditor, the Accreditation Authority, or pursuant to a lawful order).

The CA certificate, TSA certificate, this CP, the CPS, and the current CRL are public documents.

9.4 Intellectual Property

All DDSign certificates are the intellectual property of DDSign. Subscribers and relying parties are granted a non-exclusive, non-transferable licence to use DDSign certificates solely for the purposes described in Section 1.4.

9.5 Representations and Warranties

DDSign warrants that:

- Private key material protected under this CP has not been intentionally disclosed to any unauthorised party.
- All certificates issued comply with the profiles in Section 7 of this CP.
- The CRL is published within 24 hours of any revocation event.
- DDSign operations are conducted in accordance with this CP and its implementing documents.

DDSign makes no guarantee that timestamps issued under this CP will be accepted by any particular jurisdiction's courts or regulatory bodies without additionally satisfying applicable local procedural requirements.

9.6 Disclaimer of Warranties

9.6 Disclaimer of Warranties

This section sets out the warranty disclaimers applicable to the DDSign Electronic Certification Service Provider (E-CSP), operated by Centric Limited. These disclaimers define the boundaries of the representations and warranties made by the E-CSP to Subscribers, Relying Parties, and other participants in the DDSign trust framework, and should be read together with the express warranties in Section 9.5 and the liability limitations in Section 9.2.

9.6.1 General Warranty Disclaimers

The following sub-sections establish the general warranty disclaimers that apply across all DDSign E-CSP services, including certificate issuance, digital signature execution, timestamping, certificate status services, and the DDSign platform.

9.6.1.1 As-Is and As-Available Basis

Except as expressly stated in the Certificate Policy (CP), the Certification Practice Statement (CPS), and the Subscriber Agreement, all services provided by the DDSign E-CSP are delivered on an "as is" and "as available" basis. Centric Limited makes no representations or warranties of any kind, whether express, implied, or statutory, beyond those explicitly set out in the governing documents.

9.6.1.2 Exclusion of Implied Warranties

To the maximum extent permitted by applicable law, including the laws of the Republic of Kenya, Centric Limited expressly disclaims all implied warranties, including but not limited to:

- **Merchantability:** No warranty that the E-CSP services are of merchantable quality or suitable for commercial use in all circumstances.
- **Fitness for a particular purpose:** No warranty that the E-CSP services will meet the specific requirements of any individual Subscriber or Relying Party beyond the purposes described in the Certificate Policy.
- **Non-infringement:** No warranty that the use of the DDSign platform or certificates issued by the E-CSP will not infringe the intellectual property rights of any third party.
- **Accuracy or completeness:** No warranty that information contained in certificates is accurate beyond the identity verification procedures described in the CPS. The

E-CSP verifies Subscriber identity in accordance with its documented procedures but does not guarantee the absolute accuracy of Subscriber-provided information.

9.6.1.3 No Warranty of Uninterrupted Service

Centric Limited does not warrant that the DDSign platform, including the certificate issuance system, the OCSP responder, CRL distribution points, the signing interface, or any supporting infrastructure, will operate without interruption, delay, or error. The E-CSP may experience planned maintenance windows and unplanned service disruptions. Procedures for handling service disruptions are defined in the Incident Response Action Plan (CENT-ECSP-IRP-001) and the Business Continuity Plan.

Specifically, Centric Limited does not warrant:

- Continuous, uninterrupted availability of the DDSign platform or any component thereof.
- That certificate issuance requests will be processed within any guaranteed timeframe.
- OCSP responses or CRL updates will be delivered within any guaranteed latency, although the E-CSP makes commercially reasonable efforts to publish CRL updates within one (1) hour of a revocation event.
- That the platform will be free from software defects, bugs, or vulnerabilities at all times.

9.6.1.4 No Warranty of Error-Free Operation

While Centric Limited employs commercially reasonable security measures and quality assurance practices, the E-CSP does not warrant that the DDSign platform or its certification services will be entirely free from errors. Software systems inherently carry the possibility of defects. The E-CSP maintains monitoring via its self-hosted Sentry instance (sentry.centricltd.co.ke) to detect and address errors promptly, but does not guarantee that all errors will be detected or resolved before they affect Subscribers or Relying Parties.

9.6.2 Certificate-Specific Disclaimers

The following disclaimers apply specifically to digital certificates issued by the DDSign Issuing CA and to the trust relationships established through those certificates.

9.6.2.1 Certificate Content Accuracy

The E-CSP verifies Subscriber identity using the procedures described in the Certification Practice Statement. However, Centric Limited does not warrant the absolute accuracy, completeness, or truthfulness of information contained in a certificate beyond the scope of its documented verification procedures. The E-CSP relies on information provided by the Subscriber during the application process. If a Subscriber provides false, inaccurate, or misleading information, the resulting certificate may contain inaccurate data despite the E-CSP's verification efforts.

9.6.2.2 Certificate Fitness for Specific Transactions

Certificates issued by the DDSign E-CSP are intended for the purposes described in the Certificate Policy. Centric Limited does not warrant that a certificate is suitable for any particular transaction, regulatory requirement, or legal proceeding beyond the scope defined in the CP. Relying Parties and Subscribers are responsible for determining whether a DDSign certificate is appropriate for their intended use.

9.6.2.3 Reliance Limits

Centric Limited does not warrant that reliance on a certificate is appropriate for transactions of any value. Relying Parties rely on certificates at their own risk and must exercise their own judgement regarding the level of trust to place in a certificate. The E-CSP's liability for any single certificate is subject to the liability cap established by Centric Limited in accordance with Section 9.2.

9.6.2.4 No Warranty Regarding Subscriber Conduct

Centric Limited does not warrant, represent, or guarantee the conduct, financial standing, creditworthiness, or trustworthiness of any Subscriber. The issuance of a certificate confirms only that the E-CSP has verified the Subscriber's identity in accordance with its documented procedures. It does not constitute an endorsement of the Subscriber or a guarantee of the Subscriber's future behaviour or compliance with any agreement.

9.6.3 Third-Party and Infrastructure Disclaimers

The ddsign E-CSP operates within a broader technology and trust ecosystem. The following disclaimers address the boundaries of Centric Limited's warranties in relation to third-party systems, infrastructure dependencies, and external services.

9.6.3.1 Third-Party Software and Services

The ddsign platform incorporates third-party software libraries, cryptographic modules, and infrastructure services. Centric Limited does not warrant the performance, security, or availability of any third-party component beyond the E-CSP's own commercially reasonable selection, configuration, and monitoring practices. Any warranties provided by third-party vendors are between the vendor and the applicable party and do not extend through Centric Limited.

9.6.3.2 Network and Internet Infrastructure

Centric Limited does not warrant the availability, reliability, or security of the internet or any network infrastructure outside its direct control. The delivery of certificates, CRL updates, OCSP responses, and platform access depends on network connectivity that is subject to disruption by third-party telecommunications providers, internet service providers, or force majeure events.

9.6.3.3 Subscriber Systems and Key Storage

Centric Limited does not warrant the security of the Subscriber's own systems, devices, or private key storage. The E-CSP generates and issues certificates, but the Subscriber is solely responsible for the protection of their private key and the security of the environment in which the private key is stored and used. The E-CSP does not hold Subscriber private keys and has no ability to monitor or enforce the Subscriber's key protection practices.

9.6.3.4 Cross-Certified and Hierarchical Trust

Where the ddsign Issuing CA is cross-signed by the Kenya Root CA (KE-RCA / ICTA) or participates in a hierarchical trust chain, Centric Limited does not warrant the continued availability, policies, or practices of the root CA or any other CA in the trust chain. Changes to root CA policies, trust store inclusion, or cross-certificate status are outside the control of Centric Limited.

9.6.4 Regulatory and Legal Disclaimers

The following disclaimers address the regulatory and legal context in which the DDSign E-CSP operates.

9.6.4.1 No Legal Advice

Nothing in the Certificate Policy, Certification Practice Statement, Subscriber Agreement, or any other document published by Centric Limited in relation to the DDSign E-CSP constitutes legal advice. Subscribers and Relying Parties are responsible for obtaining their own legal counsel regarding the legal effect, enforceability, and admissibility of digital signatures and certificates in their jurisdiction and for their intended purposes.

9.6.4.2 Jurisdictional Variations

The DDSign E-CSP is licensed and regulated under the laws of the Republic of Kenya, specifically the Kenya Information and Communications Act (KICA), CAP 411A. Centric Limited does not warrant that certificates issued by the DDSign E-CSP will be recognised, accepted, or legally valid in any jurisdiction outside Kenya. Subscribers and Relying Parties who use DDSign certificates in cross-border transactions do so at their own risk and are responsible for understanding the applicable legal framework in the relevant jurisdiction.

9.6.4.3 Regulatory Changes

Centric Limited does not warrant that the DDSign E-CSP's current practices, policies, or technical standards will remain compliant with future changes to applicable law, regulation, or industry standards. The E-CSP will make commercially reasonable efforts to adapt to regulatory changes, but does not guarantee uninterrupted compliance during transition periods following material regulatory changes.

9.6.4.4 Force Majeure

Centric Limited shall not be deemed to have breached any warranty or obligation under the CP, CPS, or Subscriber Agreement to the extent that performance is prevented, delayed, or hindered by events beyond its reasonable control, including but not limited to: natural disasters, armed conflict, terrorism, civil unrest, government action or order, pandemic, epidemic, power failure, telecommunications failure, internet outage, cyberattack by a state or state-sponsored actor, or failure of a critical third-party infrastructure provider. In the event of a force majeure, Centric Limited shall notify affected Subscribers as soon as reasonably practicable and resume normal operations as soon as the impediment is removed.

9.6.5 Preservation of Express Warranties

The following sub-sections clarify the relationship between the disclaimers in this section and the express warranties made elsewhere in the CP/CPS.

9.6.5.1 Express Warranties Unaffected

The disclaimers in this Section 9.6 do not limit, modify, or override the express representations and warranties made by Centric Limited in Section 9.5 of the CP/CPS or in the Subscriber Agreement. Where an express warranty conflicts with a disclaimer in this section, the express warranty shall prevail to the extent of the conflict.

9.6.5.2 Statutory Rights

Nothing in this section is intended to exclude or limit any warranty or right that cannot be lawfully excluded or limited under the laws of the Republic of Kenya, including any rights afforded to consumers under the Consumer Protection Act, 2012, or data subjects under the Kenya Data Protection Act, 2019. To the extent that any disclaimer in this section is held to be unenforceable, the remaining disclaimers shall continue in full force and effect.

9.6.5.3 Severability

If any provision of this Section 9.6 is found by a court of competent jurisdiction or regulatory authority to be invalid, illegal, or unenforceable, such finding shall not affect the validity or enforceability of the remaining provisions. The invalid provision shall be modified to the minimum extent necessary to make it valid and enforceable while preserving its original intent.

9.7 Limitations of Liability

The Certification Authority’s liability to Subscribers and Relying Parties in connection with the issuance, management, and use of digital certificates for document signing services is strictly limited in accordance with the Kenya Information and Communications Act (KICA) CAP411A Section 14 and as advised by legal counsel. The CA’s aggregate liability, whether in contract, tort, or otherwise, for any claim or series of related claims, shall not exceed the insurance limits prescribed by KICA CAP411A Section 14 and any additional requirements specified by legal counsel. The CA does not accept liability for any indirect, incidental, consequential, exemplary, or punitive damages arising from or related to the use of its certificates, except where such liability may not be lawfully excluded under applicable law.

9.8 Governing Law and Dispute Resolution

This CP is governed by the laws of the Republic of Kenya. Disputes arising from this CP shall be resolved in accordance with Kenyan law.

9.9 CP Amendment Procedure

Changes to this CP MUST follow the process defined in `CPS` Section 7.3:

1. Approval by DDSign Legal and Operations Lead.
2. Advance notification to the Accreditation Authority Version increment and effective-date update.
3. Notification to subscribers and relying parties.
4. Re-publication of the CP at `https://web.ddsign.ae/resource-center/certificate_policy.pdf`.

Changes that materially affect the security of the PKI hierarchy (e.g. algorithm changes, key storage changes, new certificate types) MUST be approved by the Accreditation Authority before taking effect.

10. Cross-Reference to Implementing Documents

This CP is implemented by the following documents. All implementing documents MUST be consistent with and subordinate to this CP.

CP Section	Implementing Document	Section Reference
2.2 — CRL publication	DD-CLP-001	8.1–8.3
3.2 — Identity verification	DD-CLP-001	4.1–4.3

4.2 — Certificate issuance	DD-CLP-001	3.1–3.3
4.4 — Suspension	DD-CLP-001	6
4.5 — Revocation	DD-CLP-001	7
4.6 — Renewal	DD-CLP-001	5
5.2 — Dual-operator control	DD-KMP-001	2
5.2 — Key ceremony	DD-KMP-001	4.2
5.4 — Audit logging	DD-KMP-001	11
5.5 — Records retention	DD-KMP-001	11.2
6.1 — Key generation	DD-KMP-001	4
6.2 — CA key in AWS KMS	DD-KMP-001	5.2
6.2 — TSA key in HSM	DD-HSP-001	4–6

6.4 — Key backup	DD-KMP-001	9
6.5 — HSM requirements	DD-HSP-001	3, 5, 10
7.1 — CA certificate profile	DD-CLP-001	2.1
7.2 — TSA certificate profile	DD-CLP-001	2.2
7.3 — CRL profile	DD-CLP-001	8.1
8.4 — Quarterly returns	DD-KMP-001	10