

Digitary® Trust Network CA/ Digitary® CA

Certificate Policies and Certification Practices Statement

Version 1.1

**Digitary CA (formerly DTN CA) Certificate Practice
Statement:Version 1.1**

Table of Contents

1. INTRODUCTION

1.1. Overview

This Certification Practice Statement (CPS) describes the practices employed by Digitary (Formerly "Framework Solutions") in the issuing and management of digital certificates under the identity of the "Digitary® Trust Network".

This CPS may be used by a relying party to determine the level of trust associated with a given digital certificate.

1.2. Identification

1.2.1. Entity Names

"Framework Computer Consultants Limited" is a private company limited by shares, registered in the Republic of Ireland as company number 307503.

"Framework Solutions" is a former registered business name and registered trade mark of "Framework Computer Consultants Limited".

"Digitary" is a registered business name and registered trade mark of "Framework Computer Consultants Limited".

"Digitary Trust Network" CA (herein referred to as the "DTN CA" or "Digitary CA") is the identifier given to the Certification Authority described herein, and operated by Digitary.

1.2.1. Certificate Practice Statement Name

DigitaryTrustNetworkCACPSv1.1

1.2.2. Object Identifiers

This certificate practice statement is identified by the following unique registered Object Identifier (OID):

1.3.6.1.4.1.27691.1.1.1.1

ISO assigned 1

Organization acknowledged by ISO 3

US Department of Defense 6

Internet 1

private 4

IANA registered private enterprises 1

Framework Computer Consultants Limited *27691*

PKI 1

Certificate Practice Statement 1

Major version 1

Minor version 1

1.3. Community and Applicability

The Digitary CA issues certificates according to a number of Certificate Policies (CPs). Community and Applicability is dependent on the CP:

1.3.1. Digitary SSCD Qualified Certificate Policy

The OID for this CP is: **1.3.6.1.4.1.27691.1.2.1.1**

Certificates issued under this policy are issued to **natural persons** as **qualified certificates** under Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic signatures, where the associated private key is generated and stored on a **Secure Signature Creation Device (SSCD)**. A SSCD is defined as an appropriately certified cryptographic hardware token which is capable of key generation, storage, and digital signature operations.

Certificates issued under this policy are **not** issued to members of the general public. Certificates are issued under this policy to authorised officials of organisations which which Digitary conducts business. For example, Digitary issues certificates under this policy to officers of Higher Education Institutions so that they may digitally sign electronic documents using the Digitary secure electronic document system.

Certificate subjects and their affiliated organisations are required to undergo authentication checks outlined in section 3.1 of this document.

1.3.2. Digitary Qualified Certificate Policy

The OID for this CP is: **1.3.6.1.4.1.27691.1.2.2.1**

Certificates issued under this policy are issued to **natural persons** as **qualified certificates** under Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic signatures. The associated private key **may or may not** be generated and stored on a **Secure Signature Creation Device (SSCD)**.

Certificates issued under this policy are **not** issued to members of the general public. Certificates are issued under this policy to authorised officials of organisations which which Digitary conducts business.

Certificate subjects and their affiliated organisations are required to undergo authentication checks outlined in section 3.1 of this document.

1.3.3. Digitary General Certificate Policy

The OID for this CP is: **1.3.6.1.4.1.27691.1.2.3.1**

Certificates issued under this policy are issued to entities that **may or may not be natural persons**. For example, a certificate issued under this policy may be issued to an automated system component for the purposes of encryption and/or digital signature. The associated private key **may or may not** be generated and stored on a **Secure Signature Creation Device (SSCD)**.

Certificates issued under this policy are **not** issued to members of the general public. Certificates are issued under this policy to organisations which which Digitary conducts business.

Certificate subjects and their affiliated organisations are required to undergo authentication checks outlined in section 3.1 of this document.

1.3.1. Certification Authorities

Digitary CA is operated by Framework Computer Consultants Limited, registered in the Republic of Ireland as company number 307503, and trading under the registered business name Framework Solutions.

Digitary CA is physically managed by Geotrust Inc., having its registered office at 117 Kendrick Street, Suite 350, Needham, MA 02494.

Digitary CA digital certificates are issued under the exclusive control of trusted Digitary officers.

1.3.2. Registration Authorities

The Digitary Registration Authority performs all RA duties on behalf of the Digitary CA. In some cases, the Digitary CA may appoint additional RAs as may be required from time to time. The appointment of additional RA are subject to RA authentication and a written contract. All appointed RAs are required to operate in line with strict operational procedures defined by the Digitary CA in order to issue certificates under the policies defined herein.

1.3.3. End entities

The targeted end entities (i.e. users of digital certificates issued by the Digitary CA) are the users of Digitary® products and services, and any organizations cooperating with these entities in the practice of business. For example, officials of Higher Education Institutions are typical end entities.

Subscribers that are the subject of the issued certificates may be:

1. Any natural person which can be uniquely identified.
2. Any legal person or entity which can be uniquely identified (e.g. a computerised system component acting on behalf of an organisation, such as a higher education institution).

1.3.4. Applicability

Certificates issued by the Digitary CA can facilitate:

- Authentication
- Authorization
- Confidentiality
- Integrity
- Non-repudiation

Applicable key usage is indicated in the “Key Usage” extension of the certificate. Any usage other than the one(s) indicated in this extension is at the risk of the relying party.

1.4. Contact Details

1.4.1. Specification administration organization

This CPS is maintained by the Digitary CPS Maintenance Body, which is appointed by Digitary senior management. This CPS is available online from the Digitary CA website: <https://trust.digitary.eu>

1.4.2. Contact details

This CPS is kept updated by the Digitary CPS Maintenance Body:

Chairperson
Digitary CA CPS Maintenance Body
Invent Building
Dublin City University
Glasnevin
Dublin 9,
Ireland.

E-mail: ca-cps@digitary.net

1.4.3. Person determining CPS suitability for the policy

The person determining CPS suitability for the policies outlined herein is:

Chairperson
Digitary CA CPS Maintenance Body
Digitary
Dublin City University
Glasnevin
Dublin 9,
Ireland.

E-mail: ca-cps@digitary.net

2. GENERAL PROVISIONS

2.1. Obligations

2.1.1. CA obligations

2.1.1.1. Compliance

The Digitary CA has published this CPS describing the practices employed in issuing the digital certificates. The Digitary CA operates in accordance with this CPS and the laws of the Republic of Ireland.

2.1.1.2. Assurance of cross certification compliance

No stipulation.

2.1.1.3. Certificate requests

The Digitary CA:

- accepts certification requests from entities requesting a certificate according to the agreed procedures contained in this CPS
- authenticates entities requesting a certificate, possibly by the help of separately designated RAs
- issues certificates based on requests from authenticated entities
- sends notification of issued certificates to requesters
- makes issued certificates publicly available

2.1.1.4. Certificate revocation

The Digitary CA:

- accepts revocation requests from entities requesting a certificate to be revoked according to the agreed procedures contained in this CPS
- authenticates entities requesting a certificate to be revoked
- issues and periodically updates a CRL
- makes CRLs publicly available

2.1.1.5. Data privacy

The Digitary CA is authorized to collect the information related to personal data that is necessary to perform its services. These personal data can only be used in the context of the certification services provision. The subscriber has the right to access and request correction of these data.

2.1.1.6. Protection of issuing CA's private key

The Digitary CA is obliged to protect its private key in accordance with this CPS.

2.1.1.7. Restriction on issuing CA's private key use

The Digitary CA's private key used for issuing certificates in accordance with this CPS may be used only for signing certificates and CRLs, and other adequate information consistent with the certificate issuance.

2.1.2. RA obligations

All RAs appointed by the Digitary CA are obliged to operate RA services and have the following specific obligations:

2.1.2.1. Compliance

The RA MUST operate in accordance with its CPS and the laws of the country in which the RA resides. The default Digitary RA MUST operate in accordance with the laws of the Republic of Ireland.

2.1.2.2. Authentication of the subject's identity

The RA is obliged to authenticate the identity of the subject to be certified using procedures specified in Section 3.1.

2.1.2.3. Validation of the connection between a public key and the requester identity

The RA is obliged to verify that the requester is in possession of the private key corresponding to the public key contained in the certificate request using procedures specified in Section 3.1.7.

2.1.2.4. Maintain certificate application information

The RA is obliged to keep supporting evidence for any certificate request made to the Digitary CA (e. g. certificate request forms, subject identity documentation) in accordance with this CPS.

2.1.2.5. Protection of RA's private key

The RA may be issued with a private key and certificate by the Digitary CA. In this event, the RA is obliged to protect its private key in accordance with this CPS.

2.1.2.6. Restriction on RA private key use

The private key used by a RA for secure communication by the RA with the Digitary CA.

2.1.3. Subscriber obligations

2.1.3.1. Accuracy of representations in certificate applications

Subscribers MUST accurately represent the information required of them in a certificate request process.

2.1.3.2. Key pair generation

Subscriber key pairs may be generated either by the Subscriber or by the Digitary CA. In the event that a Subscriber generates their own key pair, the Subscriber MUST generate their key pair using a trustworthy method. The Digitary CA will define acceptable methods of key generation to Subscribers upon request.

2.1.3.3. Protection of entity's private key

Subscribers MUST properly protect their private key at all times, against loss, disclosure to any other party, modification and unauthorized use, in accordance with this CPS and the relevant CP. From the creation of their private and public key pair, subscribers are personally and solely responsible of the confidentiality and integrity of their private keys. Every usage of their private key is assumed to be the act of its owner.

2.1.3.4. Notification of CA upon private key compromise

Upon suspicion that their private keys are compromised subscribers MUST notify the Digitary CA (or the RA that enrolled the subscriber) immediately by sending a certificate revocation request.

2.1.3.5. Notification of CA upon any change in their certificate content

Upon any change in the content of their certificates subscribers MUST notify the Digitary CA that issued their certificates (or the RA that enrolled the subscriber) by sending a certificate revocation request.

2.1.3.6. Restrictions on private key and certificate use

Subscribers MUST use the keys and certificates only for the purposes authorized by the Digitary CA.

2.1.3.7. Personal data

By submitting a certificate request, the subscriber authorizes the Digitary CA to process and archive their personal data in compliance with this CPS.

2.1.4. Relying party obligations

2.1.4.1. CPS

A relying party MUST be familiar with this CPS before drawing any conclusion on how much trust he/she can put in the use of a certificate issued from the Digitary CA.

2.1.4.2. Purposes for which certificate is used

The relying party MUST only use the certificate for the prescribed applications and MUST NOT use the certificates for forbidden applications

2.1.4.3. Digital signature verification responsibilities

Relying parties MUST verify the digital signature of a received digitally signed message and to verify the digital signature of the Digitary CA who issued the certificate used for the verification purpose.

2.1.4.4. Revocation and suspension checking responsibilities

When validating a certificate a relying party MUST check it for its validity, revocation, or suspension.

2.1.5. Repository obligations

The Digitary CA uses a publicly accessible repository to store certificates and Certificate Revocation Lists (CRLs). See section 2.6 for details.

2.2 Liability

Digitary's liability to subscribers or relying parties is strictly capped at an amount equal to the fee paid for the issue of the certificate or €50, whichever is the greater.

2.2.1. CA liability

The Digitary CA warrants that all certificates issued were issued in accordance with this CPS.

2.2.2. RA liability

RA warrants that subscriber's identity has been verified and that the identities in the certificate were valid to the knowledge of the RA at the time of issuance.

2.3. Financial responsibility

No financial responsibility is accepted for certificates issued under this CPS.

2.3.1. Indemnification by relying parties

The Digitary CA assumes no financial responsibility for improperly used certificates.

2.3.2. Fiduciary relationships

Issuance of certificates in accordance with this CPS does not make the Digitary CA, or any RA within the Digitary CA infrastructure an agent, fiduciary, trustee, or other representative of subscribers or relying parties.

2.3.3. Administrative processes

Not applicable.

2.4. Interpretation and Enforcement

2.4.1. Governing law

This CPS is governed by the laws of the Republic of Ireland.

2.4.2. Severability, survival, merger, notice

Should it be determined that one section of this CPS is incorrect or invalid, the other sections shall remain in effect until the CPS is updated as indicated in Chapter 8

2.4.3. Dispute resolution procedures

In case of a dispute based on the contents of this CPS, the dispute must be brought to the attention of the Dispute Resolution Manager of the Digitary CA:

Dispute Resolution Manager
Digitary CA
Digitary
Dublin City University
Glasnevin
Dublin 9,
Ireland.

E-mail: ca-disputes@digitary.net

2.5. Fees

2.5.1. Certificate issuance or renewal fees

Fees are charged by Digitary for issuing certificates and these fees are subject to revision from time to time.

2.5.2. Certificate access fees

Access to certificates on the Digitary CA Certificate Repository is free of charge.

2.5.3. Revocation or status information access fees

Access to Certificate Revocation Lists on the Digitary CA Certificate Registry is free of charge.

2.5.4. Fees for other services such as policy information

No fees are charged for allowing policy and CPS information access.

2.5.5. Refund policy

No stipulation.

2.6. Publication and Repository

2.6.1. Publication of CA information

The Digitary CA has made the following information publicly available in its repositories:

1. The Digitary CA Certificate Practice Statement in <http://www.digitary.net/ca.html>
2. All issued certificates including CA-certificates <http://www.digitary.net/ca.html>
3. Signed Certificate Revocation Lists in <http://www.digitary.net/ca.html>

2.6.2. Frequency of publication

CRL publication is in accordance with Section 4.4.9 of this CPS.

CPS publication is in accordance with Chapter 8 of this CPS.

2.6.3. Access controls

There is no access control on reading the CPS.

There is no access control on reading the certificates.

The certificates, CRLs, CPs and CPS in the electronic repository are protected against any unauthorized modification.

2.6.4. Repositories

The Digitary CA has made the following information publicly available in its repositories:

1. The Digitary CA Certificate Practice Statement in <http://www.digitary.net/ca.html>
2. All issued certificates including CA-certificates <http://www.digitary.net/ca.html>
3. Signed Certificate Revocation Lists in <http://www.digitary.net/ca.html>

2.7. Compliance audit

The Digitary CA declares that their practices fully comply with this CPS.

2.7.1. Frequency of entity compliance audit

No stipulation

2.7.2. Identity/qualifications of auditor

No stipulation

2.7.3. Auditor's relationship to audited party

No stipulation

2.7.4. Topics covered by audit

No stipulation

2.7.5. Actions taken as a result of deficiency

No stipulation

2.7.6. Communication of results

No stipulation

2.8. Confidentiality

The Digitary CA collects personal information about the subscribers (including, but not limited to full name, organization, job title, e-mail address, passport and/or driver's licence details). These data are collected with the express written permission of the subscribers, and are processed in line with Data Protection legislation and ensuring privacy protection according to the laws of the Republic of Ireland.

2.8.1. Types of information to be kept confidential

All subscriber information that is not present in the certificate and CRL issued by the Digitary CA is considered confidential and is not released to third parties without express written permission of the subscriber, except where required by law.

2.8.2. Types of information not considered confidential

Information included in public certificates and CRLs issued by the Digitary CA are not considered confidential.

2.8.3. Disclosure of certificate revocation/suspension information

When a certificate is revoked, a reason code MAY be included in the CRL entry for the action. This reason code is not considered confidential and may be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed.

2.8.4. Release to law enforcement officials

The Digitary CA does not disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

2.8.5. Release as part of civil discovery

The Digitary CA does not disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

2.8.6. Disclosure upon owner's request

The Digitary CA will release information about a subscriber upon the request of the subscriber.

2.8.7. Other information release circumstances

No stipulation

2.9. Intellectual Property Rights

The Digitary CA claims no intellectual property rights on issued certificates.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1. Types of names

The Digitary CA assigns each entity a X.501 Distinguished Name (DN, see X.501) which serves as a unique identifier of the entity. The DN is inserted in the subject field of the certificate(s) issued to the entity to bind the entity to the certificate(s). The DN is a non-empty `printableString`.

All end-entity DNs conform to the following format:

Attribute	Value	Optional
C (Country)	Two-letter country code (i.e. "IE" for Ireland) stating the country of residence of the subscriber.	NO
S (State or Province)	The state/province of residence of the subscriber (i.e. "Leinster")	NO
L (Locality or City)	The locality of residence of the subscriber. (i.e. Limerick)	NO
O (Organization)	(Name of organization with which the subscriber is affiliated – i.e. University of Limerick)	NO
OU (Organizational Unit) 1	Optional department (i.e. "Student Records Office")	YES
OU (Organizational Unit) 2		YES
OU (Organizational Unit) 3		YES
OU (Organizational Unit) 4		YES
CN (Common Name)	Full name of person as is appears on identity documents (and, if applicable, official job title within the Organisation)	NO
E (E-mail)	Optional email address of individual	YES

The end-entity DNs contain information that depends on the Certificate Policy under which the certificate was issued:

Attribute	Policy	Value
CN	Digitary CA SSCD Qualified Certificate Policy	Full name of person as is appears on identity documents (and, if applicable, official job title within the Organisation) Example: "John Doe - Registrar"
	Digitary CA Qualified Certificate Policy	Full name of person as is appears on identity documents (and, if applicable, official job title within the Organisation) Example: "John Doe - Registrar"
	Digitary CA General Certificate Policy	Identity of the person or system as identified within the identified Organisation. Example: "Secure Document System" Example: "Secure Document System Automailer"
E	Digitary CA SSCD Qualified Certificate Policy	Optional email address of individual Example: "johndoe@nowhere.com"
	Digitary CA Qualified Certificate Policy	Optional email address of individual Example: "johndoe@nowhere.com"
	Digitary CA General Certificate Policy	Optional email address of individual or system Example: "johndoe@nowhere.com" Example: "digitary-noreply@nowhere.com"

3.1.1.1. Alternate names

No alternate names are used

3.1.2. Need for names to be meaningful

The Subject names contained in a certificate issued by the Digitary CA are meaningful in the sense that the issuing Digitary CA has proper evidence of the existent association between these names and the entities to which they belong. The `CommonName` DN attribute WILL contain either a) the legal name as presented in a government issued photo identification, b) a legally recognised alias to that legal name. The `CommonName` DN attribute MAY also contain the subject's job title where applicable.

3.1.3. Rules for interpreting various name forms

See Section 3.1.1 and Section 3.1.2.

3.1.4. Uniqueness of names

The Digitary CA guarantees the uniqueness of the subject names. In case of name collision when two or more persons use the same name, other elements of the DN can be used to distinguish the persons from each other.

3.1.5. Name claim dispute resolution procedure

Name disputes are managed according to the laws of the Republic of Ireland.

3.1.6. Recognition, authentication and role of trademarks

The Digitary CA does not guarantee that the names issued will contain the requested trademarks.

3.1.7. Method to prove possession of private key

The Digitary CA verifies that the certificate applicant is in possession of the private key that corresponds to the public key that is to be certified.

For all Certificate Policies, Certificate Signing Requests (CSR)s are accepted in PKCS#10 format and are accepted in a secure manner by Digitary CA from the appropriate RA. The Digitary CA verifies proof of possession of private key by verifying the signature on the PKCS#10 file.

3.1.8. Authentication of organization identity

The Digitary CA only issues certificates to organisations with which it does business. This means that there is always an existing contractual relationship between the organisation and Digitary, and that the organisation has been validated to some extent.

For Qualified Certificates, the Digitary CA requires that RA's enrol users at the organisation's official address, and may also require proof of organisation documentation before a Qualified Certificate will be issued.

3.1.9. Authentication of individual identity

For non-Qualified Certificates (that is, certificates issued under the Digitary General Certificate Policy), the identity of the individual entity is authenticated by way of an existing business contract between Digitary CA and the organisation under which the individual entity represents itself. In these cases, Digitary will be responsible for the maintenance of the system component(s) and will have authenticated the system components during the normal course of business.

For Qualified Certificates, the Digitary CA requires that RA's enrol the individual at the address of the organisation that they claim to represent. The individual will also require valid, photographic proof of identity, which must be validated by the RA in person before a Qualified Certificate will be issued. The following procedure is used for Qualified Certificates:

The RA meets the applicant in person in order to authenticate the identity of the applicant. The following procedure takes place:

- The RA verifies the applicant's identity documentation (passport or drivers licence), and takes a note of the applicant's authenticated identity
- The RA verifies the applicant's position within the applicant's organization. This may be done by obtaining and verifying the necessary organization identification and/or documentation (for example, an appropriate staff identity card showing the applicant's job title, or a letter printed on organizational letterhead and signed by the head of the relevant department within the organization will be sufficient)
- The RA photocopies the applicant's identity documentation, and witnesses the signature of the applicant being applied to the photocopy. The RA countersigns and dates the photocopy.
- The RA verifies that the signature on the photocopy matches that of the original identity document
- The RA witnesses the applicant's completion of and signature to a User Subscriber Agreement document.
- In cases where the applicant generate's their own key pair, the RA obtains applicant's Certificate Signing Request through a secure system

Once all of the RA's requirements have been met, the RA will forward the CSR to the Digitary CA for certification. The Digitary CA will issue the certificate once it is satisfied that the RA has carried out all of its authentication obligations.

3.2. Routine Rekey

The identification and authentication for routine rekey may be accomplished either with the same procedure as for Section 3.1 or using digitally signed requests sent to the CA before certificate expiration.

In case where the certificate to be reissued contains the name of a certain organization, the new affiliation verification procedure as described in Section 3.1.8 will be performed before rekeying.

3.3. Rekey after Revocation

A public key whose certificate has been revoked for private key compromise will NOT be re-certified.

3.4. Revocation Request

Revocation requests are authenticated either contacting the authenticated Subscriber in section 3.1.9, or by verifying the digital signature of the revocation request made by a valid certificate.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application

The Digitary CA issues certificates according to a number of Certificate Policies (CPs). Certificate Application is dependent on the CP:

4.1.1. Digitary SSCD Qualified Certificate Policy

Certificates issued under this policy are **not** issued to members of the general public. Certificates are issued under this policy to authorised officials of organisations which which Digitary conducts business. For example, Digitary issues certificates under this policy to officers of Higher Education Institutions so that they may digitally sign electronic documents using the Digitary secure electronic document system.

4.1.2. Digitary Qualified Certificate Policy

Certificates issued under this policy are **not** issued to members of the general public. Certificates are issued under this policy to authorised officials of organisations which which Digitary conducts business.

4.1.3. Digitary General Certificate Policy

Certificates issued under this policy are **not** issued to members of the general public. Certificates are issued under this policy to organisations which which Digitary conducts business.

4.2. Certificate Issuance

In order to issue a certificate, the following steps need to be undertaken:

1. RA verifies all identity information using procedures from Section 3.1
2. RA verifies whether the requester qualifies for the certificate
3. RA verifies the identity of the requester as indicated in Section 3.1 and accepts the request
4. RA retrieves the certificate request in a secure manner and passes the certificate request over a secure connection to the Digitary CA operator. The Digitary CA operator passes the certificate over a secure connection to the Digitary CA certificate issuing system. The Digitary CA issues the certificate, which is securely passed back to the RA.
5. RA places the digital certificate into a secure repository for retrieval by the subscriber
6. The subscriber retrieves the certificate from the secure repository.

4.3. Certificate Acceptance

The certificate is assumed to be accepted unless its requester explicitly rejects it in an authenticated communication with the Digitary CA.

4.4. Certificate Suspension and Revocation

4.4.1. Circumstances for revocation

A certificate will be revoked when the information in the certificate is known to be suspected or compromised or at the request of the authorized entity. It includes following situations:

1. The associated private key is known to be compromised or misused
2. The associated private key is suspected to be compromised or misused.
3. The subscriber's information in the certificate has changed.
4. The subscriber is known to have violated his/her obligations.
5. An authorized requester requested the certificate revocation.

4.4.2. Who can request revocation

1. The following entities can request the revocation of a certificate:
2. The entity who originally made the certificate request, or a delegate appointed by them when the certificate request was made
3. The entity which can prove its current responsibility for a certified machine or service.
4. Any entity which demonstrates the compromise of the private key or misuse of the certificate.
5. Any entity which demonstrates the change of subscriber's data.
6. The Digitary CA or it's associated RA(s).

4.4.3. Procedure for revocation request

In case where the Digitary CA can independently confirm that the certificate has been compromised or misused, the Digitary CA will revoke the certificate, even if the request to do so comes from an unauthenticated source and/or the holder of the certificate is unreachable.

In all other cases the Digitary CA will authenticate the revocation request and try to contact the subscriber before revoking the certificate.

4.4.4. Revocation request grace period

The Digitary CA will respond within one day (excluding weekends and public holidays) to revocation requests. It will, however, handle revocation requests with priority as soon as the request is recognized as such.

4.4.5. Circumstances for suspension

The Digitary CA does not offer a certificate suspension service.

4.4.6. Who can request suspension

Not applicable

4.4.7. Procedure for suspension request

Not applicable

4.4.8. Limits on suspension period

Not applicable

4.4.9. CRL issuance frequency

CRLs issued by Digitary CA are renewed whenever any certificate is revoked or when any CRL is more than 1 day old.

4.4.10. CRL checking requirements

The CRLs are checked at the certificate relying party responsibility. Relying parties should update their local copies of CRLs at least once per day.

4.4.11. On-line revocation/status checking availability

The on-line revocation/status checking service is not currently available.

4.4.12. On-line revocation checking requirements

Not currently applicable.

4.4.13. Other forms of revocation advertisements available

The subscriber, where possible, will be notified of the revocation of his/her certificate by email.

4.4.14. Checking requirements for other forms of revocation advertisements

Not applicable

4.4.15. Special requirements re key compromise

No stipulation

4.5. Security Audit Procedures

4.5.1. Types of event recorded

4.5.1.1. RA

The following types of events are recorded by authorised RAs:

1. Identity verification procedures

4.5.1.2. CA

The following types of events are recorded by the Digitary CA:

1. Boots of the equipment
2. Login and logouts to the issuing machine
3. Account management
4. Use of the Digitary CA software
5. Unauthorized attempts to access the Digitary CA system
6. Requests for certificates
7. Certificate issuing
8. Requests for revocation
9. CRL issuing

4.5.2. Frequency of processing log

The log files are analyzed at least once every month.

4.5.3. Retention period for audit log

Audit logs are be retained as archive records. The audit logs are be kept on Digitary CA equipment until moved to the archive.

4.5.4. Protection of audit log

Only authorized and trusted Digitary CA personnel are allowed to view and process audit log files.

4.5.5. Audit log backup procedures

A backup of the audit logs on physically removable, optical media is performed periodically. The backup media are saved in safe storage.

4.5.6. Audit collection system (internal vs external)

The audit collection system runs separately from the CA software. The audit collection system is internal to the Digitary CA.

4.5.7. Notification to event-causing subject

The subjects causing an audit event are not notified of the audit action.

4.5.8. Vulnerability assessments

The Digitary CA personnel pay attention to any sign of an attempt to violate the integrity of the PKI system. Any deficiency is followed by a vulnerability assessment revision.

4.6. Records Archival

4.6.1. Types of event recorded

The following types of events are recorded:

1. Certificate requests and related messages exchanged between the subscriber and the RA and Digitary CA
2. Subject identity and organisation verification documentation
3. Issued certificates
4. Revocation requests and related messages exchanged with the requester and/or the subscriber
5. Issued CRLs
6. Audit data as described in Section 4.5.1.

4.6.2. Retention period for archive

The minimum retention period for information pertaining to the issuance of certificates is fifty years following the issuance of the applicable certificates, or the maximum retention period permitted by Irish law, whichever is the lesser.

4.6.3. Protection of archive

Digitally stored records are stored in a logically and physically secure manner in multiple locations, accessible only to Digitary CA personnel.

4.6.4. Archive backup procedures

Archive records are regularly backed up and stored. See Section 4.6.3.

4.6.5. Requirements for time-stamping of records

No stipulation.

4.6.6. Archive collection system (internal or external)

The archive collection system is internal to the Digitary CA.

4.6.7. Procedures to obtain and verify archive information

Archived audit logs are available only to the Digitary CA personnel.

4.7. Key changeover

The Digitary CA's keys are changed while sufficient validity time remains on the existing keys to allow uninterrupted validity of all subordinate keys.

4.8. Compromise and Disaster Recovery

4.8.1. Computing resources, software, and/or data are corrupted

In the case where the Digitary CA computing resource, software and/or data have been corrupted, the responsible personnel will immediately:

1. start recovery procedures
2. identify the cause of corruption
3. take necessary steps to prevent reoccurrence
4. notify users where applicable

4.8.2. Entity public key is revoked

4.8.2.1. Subscriber's public key

See sections 3.2, 3.3, and 3.4.

4.8.2.2. CA public key

1. The key is revoked.
2. The CRL is updated and published
3. The CA system is brought down
4. New CA keys pair is generated as indicated in Section 6.1
5. Users are notified

4.8.3. Entity key is compromised

4.8.3.1. Subscriber's key

Whenever the subscriber's key is compromised, the subscriber is obliged to notify Digitary CA or the RA that enrolled the user as soon as possible. The revocation procedure will follow according to Section 3.3, Section 3.4.

4.8.3.2. CA key

In case that the Digitary CA private key is compromised, the following actions will be undertaken:

1. The key is revoked
2. The CRL is updated and published
3. The CA system is brought down
4. The cause of the compromising is analyzed and the necessary steps are taken to minimize the risk in future
5. New CA keys pair is generated as indicated in Section 6.1
6. Users are notified

4.8.4. Secure facility after a natural or other type of disaster

In the case of a natural or other type of disaster the Digitary CA will start the recovery as soon as possible using off-site stored backups.

4.9. CA Termination

4.9.1. Transfer of CA services

The Digitary CA may decide to transfer its PKI services to another organization. In that case it will inform all subscribers, higher level CAs, and relying parties with which the Digitary CA has agreements or other form of established relations about the transfer at least 3 months before the transfer date. The new organization will be required to comply with this CPS.

4.9.2. Cessation of CA services

The Digitary CA may decide to cease its services. In that case the Digitary CA Termination Plan will be executed, and the following steps will be taken:

1. The Digitary CA will inform all subscribers, higher level CAs, and relying parties with which the Digitary CA has agreements or other form of established relations about the decision at least one year before the termination date. In the event that it is not possible to provide notification one year in advance, the CA will provide the advance notice on termination as early as possible.
2. Any certificates issued after the announcement of the termination will not have an expiration date that exceeds the termination date.
3. At the termination date all the certificates issued by the CA will be revoked
4. The Digitary CA will stop distributing certificates and CRLs

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Controls

The Digital CA equipment is physically hosted managed by GeoTrust Inc., USA, and is subject to the GeoTrust CPS as follows:

5.1.1. Site location and construction

GeoTrust's CA operations are conducted within GeoTrust's facilities in Billerica, Massachusetts, USA and Suwanee, Georgia, USA which meet WebTrust for CAs audit requirements. All GeoTrust CA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration.

GeoTrust's CAs are physically located in a highly secure facility which includes the following:

- Slab to slab barriers
- Electronic control access systems
- Alarmed doors and video monitoring
- Security logging and audits
- Proximity card access for specially approved employees with defined levels of management approval required

5.1.2. Physical access

Access to the GeoTrust CA facility requires the two authentication factors of "be and have" incorporating biometrics, keys, and proximity cards. Access to the facility requires a minimum of two authorized GeoTrust employees and is checked at three independent physical locations.

5.1.3. Power and air conditioning

GeoTrust's CA facility is equipped with primary and backup:

- Power systems to ensure continuous, uninterrupted access to electric power and
- Heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4. Water exposures

The GeoTrust CA facility is located above ground on a raised floor and is not susceptible to flooding or other forms of water damage. GeoTrust has taken reasonable precautions to minimize the impact of water exposure to GeoTrust systems.

5.1.5. Fire prevention and protection

The fire detection system in GeoTrust CA facility tests air health and looks for certain signatures of possible fire conditions in the air. In addition, the GeoTrust CA facility has a pre-action water suppression system. When temperatures above 300 degrees are detected, the effected sprinkler head will release water on the area where the temperature rise is detected.

5.1.6. Media storage

All media containing production software and data, audit, archive, or backup information is stored within multiple GeoTrust facilities in TL-30 rated safes with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage.

5.1.7. Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance the manufacturers' guidance prior to disposal. Other waste is disposed of in accordance with GeoTrust's normal waste disposal requirements.

5.1.8. Off-site backup

GeoTrust performs routine backups of critical system data, audit log data, and other sensitive information. Critical CA facility backup media are stored in a physically secure manner at an offsite facility.

5.2. Procedural Controls

5.2.1. Trusted roles

Responsibilities at the Digitary CA are divided among different trusted roles:

1. *System Administrator* is responsible for:
 - a) The Digitary CA equipment maintenance and management
 - b) The security of the Digitary CA equipment
 - c) Performing regular backups
2. *System Operator* is responsible for:
 - a) SSCD preparation
 - b) Subject key generation
3. *Security Officer* is responsible for:
 - a) Certificate issuance
 - b) Certificate revocation
4. *System Auditor* is responsible for:
 - a) Auditing systems and processes
 - b) Auditing system logs
 - c) Auditing documentation and checklists completed by officers
5. *Enrolment Officer* is responsible for:
 - a) Authentication of identities
 - b) Ensuring proper archival of identity and organisational documentation
 - c) Disseminate certificates and/or SSCDs

Different roles can be occupied by one person.

Some System Administrator tasks are performed by authorised personnel of GeoTrust Inc., at the request of Digitary CA management.

All appointment to/from trusted roles is made by the Managing Director of Digitary.

The Managing Director of Digitary may appoint additional, authenticated and approved RAs to operate RA functions on behalf of the Digitary CA at his/her discretion.

5.2.2. Number of persons required per task

Digitary CA requires the Security Officer to activate its private signing key.

5.2.3. Identification and authentication for each role

System Administrators are authenticated by procedures outlined in section 5.1.2.

The Security Officer is authenticated to the CA system by means of a FIPS 140-2 certified hardware security device over a HTTPS connection from a specific, physically and logically secured machine.

5.3. Personnel Controls

5.3.1. Background, qualifications, experience, and clearance requirements

Background checks for Geotrust personnel operating the Digitary CA systems are subject to the policies of GeoTrust Inc.

The background, qualifications, experience, and clearance requirements of Digitary Trusted Roles have been satisfactorily checked by Digitary senior management.

5.3.2. Background check procedures

No stipulation.

5.3.3. Training requirements

The Digitary CA personnel are trained in:

1. Basic PKI concepts
2. The use and operation of the PKI software
3. This CPS
4. Computer, network and application security

5.3.4. Retraining frequency and requirements

Training is provided to Digitary personnel as required from time to time.

Training in the use and operation of the PKI software is provided whenever the software is updated.

Any changes to the CPS are communicated to Digitary CA personnel immediately so that certificate issuance stays consistent with the most up-to-date CPS.

5.3.5. Job rotation frequency and sequence

No stipulation

5.3.6. Sanctions for unauthorized actions

Unauthorized actions will be escalated to the Managing Director of Digitary, and where applicable, to officers of GeoTrust Inc.

5.3.7. Contracting personnel requirements

Not applicable

5.3.8. Documentation supplied to personnel

Digitary CA personnel are supplied with documentation including this CPS, and documentation pertaining to the correct usage of the CA software

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

Key pairs for the Digitary CA are generated exclusively by authorised Geotrust personnel acting on behalf of the Digitary CA.

End entity key pairs can be generated either by the end entity themselves, or by a Digitary CA System Operator. In the case where the Digitary CA generates key pairs on behalf of the end entity, the Digitary CA does **not** retain a copy of the key pair.

6.1.2. Private key delivery to entity

Where generated by the Digitary CA and held on a SSCD, private keys are physically delivered to the subject. They are either:

- a) Physically handed to the subject (or their authorised delegate) by the Enrolment Officer
- b) Sent by secure courier/registered post to the subject at their organisation's address.

Subjects are required to sign a written declaration that they have received the private key and return this to the Digitary CA.

Where key pairs are generated by the Digitary CA and **not** held on a SSCD, private keys are either physically delivered to the subject, or may be securely delivered to the subject over an encrypted SSL connection.

6.1.3. Public key delivery to certificate issuer

The Digitary CA accepts certificate requests in PKCS#10 request format. (See RFC 2314). Where keys are generated by the subject, the certificate requests are transported to the Digitary CA by the RA via a secure means of transport (i.e. encrypted S/MIME email).

6.1.4. CA public key delivery to users

CA public keys are published on the Digitary CA certificate repository. See Section 2.6.

6.1.5. Key sizes

The Digitary CA uses the RSA public key algorithm.

The Digitary CA private key **MUST** be of 2048 bit key size.

All other private keys **MUST** be of at least 1024 bit key size.

6.1.6. Public key parameters generation

Public key parameters are generated by the relevant applications.

6.1.7. Parameter quality checking

The Digitary CA does not require checking of the quality of the public keys parameters. Quality checking is performed by the user's key generation applications. The Digitary CA recommends to

users that they use up-to-date key generation procedures. Where the Digitary CA generates key pairs, it uses up-to-date key generation procedures.

6.1.8. Hardware/software key generation

The Digitary CA keys are generated in hardware security module certified to be compliant with FIPS 140-2 level 3.

Under the Digitary CA SSCD Qualified Certificate Profile, subject keys are generated on FIPS 140-2 level 2 hardware devices.

Under all other certificate profiles, subject keys may be generated on FIPS 140-2 level 2 hardware devices, or may be generated in software using approved software.

6.1.9. Key usage purposes (as per X.509 v3 key usage field)

The X.509 v3 keyUsage extension field is set to: Digital Signature, Non-Repudiation, Key Encipherment (e0)

6.2. Private Key Protection

6.2.1. Standards for cryptographic module

The Digitary CA hardware security module used to generate its signing keys and signatures is compliant with FIPS 140-1 level 3.

6.2.2. Private key (n out of m) multi-person control

The Digitary CA does not use multi-person control of keys.

6.2.3. Private key escrow

The Digitary CA private keys are not given in escrow. The Digitary CA is also not available for accepting escrow copies of keys of other parties.

6.2.4. Private key backup

The Digitary CA private keys are backup protected.

6.2.5. Private key archival

The Digitary CA private keys are archived on encrypted media.

6.2.6. Private key entry into cryptographic module

All private keys managed by the Digitary CA are generated by the hardware security module and cannot be exported.

6.2.7. Method of activating private key

The Digitary CA's private signing keys are activated by one representative of the Security Officer role authenticated by a cryptographic hardware token and a pass phrase.

6.2.8. Method of deactivating private key

Cryptographic modules which have been activated are never left unattended. They are deactivated after use by logging out.

6.2.9. Method of destroying private key

The Digitary CA private keys are archived. After the retention period (see Section 4.6.2) the archive media will be destroyed.

6.3. Other Aspects of Key Pair Management

6.3.1. Public key archival

Public keys are archived as part of the certificate archival.

6.3.2. Usage periods for the public and private keys

The validity period for issued certificates is set to three years for all certificates.

6.4. Activation Data

6.4.1. Activation data generation and installation

The pass phrases used by the Digitary CA are at least 15 characters long.

6.4.2. Activation data protection

The Digitary CA private key activation data, which is stored in a physical activation device, is protected with a password of minimum 15 characters. The pass phrases are known to authorized Digitary CA personnel only. The pass phrases are used only in secure physical environment.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific computer security technical requirements

The Digitary CA computer system, operated by Geotrust Inc., satisfies the following requirements:

1. The Digitary CA is run on dedicated computer system.
2. Only the software needed to perform the Digitary CA tasks is installed on the system
3. Access to the operating system is only permitted to authorized Geotrust System Administrators
4. Access to the Digitary CA software is allowed only to the authorized Digitary CA personnel, and to authorised Geotrust System Administrators
5. Physical access to the system is allowed only to the authorized Geotrust System Administrators.
6. All security related events are audited

The Digitary CA remote computer system, used to access the Digitary CA system, is operated by Digitary and satisfies the following requirements:

1. The Digitary CA remote computer system is run on dedicated computer system.
2. Only the software needed to perform the Digitary CA tasks is installed on the system
3. Access to the operating system is only permitted to authorized Digitary CA System Administrators
4. Access to the Digitary CA software is allowed only to the authorized Digitary CA trusted roles
5. Physical access to the system is allowed only to the authorized Digitary CA System Administrators.
6. All security related events are audited

6.5.2. Computer security rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System development controls

No stipulation

6.6.2. Security management controls

The logs, the configuration files and the entire file system of the Digitary CA computer systems are regularly checked.

6.6.3. Life cycle security ratings

No stipulation

6.7. Network Security Controls

The Digitary CA computer system is operated in a controlled network environment protected by packet filtering firewalls.

6.8. Cryptographic Module Engineering Controls

No stipulation

7. CERTIFICATE AND CRL PROFILES

7.1. Certificate Profile

7.1.1. Version number(s)

Certificates issued under this CPS are X.509 version 3 certificates. The version field in certificates MUST be set to 0x2 to indicate this.

7.1.2. Certificate extensions

This CPS allows using the extensions defined in PKI RFCs and some major vendor extensions. The typical certificate SHOULD populate following extensions:

7.1.2.1. Basic Constraints

CRITICAL

Set to FALSE in all cases, as the Digitary CA does not issue CA certificates.

7.1.2.2. Key Usage

CRITICAL

The X.509 v3 `keyUsage` extension field is set to: `Digital Signature, Non-Repudiation, Key Encipherment (e0)`

7.1.2.3. Subject Key Identifier

Unique identifier of the subject key according to RFC 3280.

The `subjectKeyIdentifier` extension is non-critical.

7.1.2.4. Authority Key Identifier

Unique identifier of the issuer key according to RFC 3280.

The `authorityKeyIdentifier` extension is non-critical.

7.1.2.5. Subject Alternative Name

No stipulation.

7.1.2.6. CRL Distribution Points

URIs of the current CRL. <http://crl.geotrust.com/crls/digitary.crl>

The `cRLDistributionPoint` extension is non-critical.

7.1.2.7. Certificate Policies

No stipulation.

7.1.3. Algorithm object identifiers

The Digitary CA issues certificates using following algorithms:

7.1.3.1. Signature algorithms

`sha-1WithRSAEncryption`

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }

7.1.3.2. Subject public key algorithms

`rsaEncryption`

{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }

7.1.4. Name forms

See Section 3.1.1.

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy Object Identifier

The Certificate Policy for a given certificate is explicitly stated in certificates issued after 5 May 2008 by the inclusion of the X.509 CertificatePolicies extension. Prior to 5 May 2008, certificates issued by the Digitary CA did not contain an explicit CertificatePolicies extension. In these cases, certificates issued to named natural persons were issued as Qualified Certificates. Certificates issued to non-natural persons were not issued as Qualified Certificates.

Object identifiers for the Digitary CA Certificate Policies, as contained in the X.509 CertificatePolicies extension for certificates issued after 5 May 2008, are as follows:

Policy Name	Object Identifier
Digitary CA SSCD Qualified Certificate Policy	1.3.6.1.4.1.27691.1.2.1.1
Digitary CA Qualified Certificate Policy	1.3.6.1.4.1.27691.1.2.2.1
Digitary CA General Certificate Policy	1.3.6.1.4.1.27691.1.2.3.1

7.1.7. Usage of Policy Constraints extension

No stipulation.

7.1.8. Policy qualifiers syntax and semantics

The certificates issued under this CPS SHOULD NOT use the policy qualifiers.

7.1.9. Processing semantics for the critical certificate policy extension

No stipulation.

7.2. CRL Profile

7.2.1. Version number(s)

CRLs issued by the Digitary CA are version X.509 version2 CRLs. This is indicated by setting the `version` field in the CRL to value of 1.

7.2.2. CRL and CRL entry extensions

Following CRL and CRL entry extensions are used:

7.2.2.1. Authority Key Identifier

No stipulation.

7.2.2.2. CRL Number

No stipulation.

7.2.2.3. CRL Reason Code

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1. Specification change procedures

Suggested changes to this CPS MUST be communicated to the contact person (see Section 1.4). The significance of the change is evaluated by the Digitary CA. If the change is determined to influence the trust procedures of relying parties and/or cooperating CAs, the Digitary CA MUST assign a new OID to the modified CPS.

Minor editorial or typographical changes to this CPS may be made without approval. All changes will be communicated to the interested parties. See Section 8.2.

8.2. Publication and notification policies

The CPS is published on <https://trust.digitary.eu/>

8.3. CP and CPS approval procedures

The Digitary CA Certificate Policies and Certification Practices Statement are subject to internal review and approval by Digitary CA personnel. Any changes to this document will be subject to internal review and approval procedures.

Glossary

Certificate subject The entity (person, organization, or server) whose public key is certified in the certificate.

Certification Authority (CA) An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA-certificate A certificate for one CA's public key issued by another CA.

Certificate policy A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement

A statement of the practices which a certification authority employs in issuing certificates.

Certificate revocation list A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

Issuing certification authority In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Public Key Certificate A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.

Registration authority An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Relevant CP The CP under which the certificate is being issued.

Relying party A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority In the context of a particular CA-certificate, the subject CA is the CA whose public key is certified in the certificate

Subscriber In the case of certificates issued to resources (such as web servers), the person responsible for the certificate for that resource. For certificates issued to individuals, same as certificate subject.

References

- [EuroPKI] *EuroPKI Certificate Policy : VERSION 1.1 (DRAFT 4)*. October 2000.
<http://www.europki.org/ca/root/>.
- [RFC 791] *Internet Protocol*. J. Postel. RFC 791. September 1981.
- [RFC 822] *Standard for the format of ARPA Internet text messages*. D. Crocker. RFC 822. August 1992.
- [RFC 1034] *Domain Names - Concepts and Facilities*. P. Mockapetris. RFC 1034. November 1987.
- [RFC 1883] *Internet Protocol, Version 6 (IPv6) Specification*. S. Deering and R. Hinden. RFC 1883. December 1995.
- [RFC 2119] *Key words for use in RFCs to Indicate Requirement Levels*. S. Bradner. RFC 2119. March 1997.
- [RFC 2314] *PKCS #10 : Certification Request Syntax Version 1.5*. B. Kaliski. RFC 2314. February 1993.
- [RFC 3280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. R. Housley, W. Polk, W. Ford, and D. Solo. RFC 3280. April 2002.
- [RFC 2527] *Internet X.509 Public Key Infrastructure : Certificate Policy and Certification Practices Framework*. S. Chokhani and W. Ford. RFC 2527. March 1999.
- [X.501] *ITU-T Recommendation X.501 - Information technology - Open Systems Interconnection - The Directory: Models*.