MANCHESTER
1824
The University of Manchester

University of Manchester Certification Practice Statement

Faculty, School, Directorate Name	IT PSS
Sponsor	Tony Brown, Head of Information Governance
ITS Team	Rachid Chalabi, Directory Services
Date and Version	March 2018, v 1.0

Contents

1 Introduction

This Certification Practice Statement (CPS) of the University of Manchester Certification Authority (from now on, UoM CA) applies to the services of the University of Manchester associated with the issuance of and management of digital certificates.

It addresses the technical, procedural personnel policies and practices of the CA in all services and during the complete life cycle of certificates as issued by UoM.

The initial release of this certificate policy is written to support the issuance of digital certificates to subscribing entities within the University of Manchester, which include client computers for trusted device authentication. At the time of writing, no other subscribing entities are included under the provision of this policy.

A PKI that uses this CP may provide some, or all, of the following security management services:

- Key generation/storage
- Certificate generation, modification, re-key, and distribution
- Key escrow and recovery of private keys associated with encryption (e.g. key management, key establishment) certificates
- Certificate revocation list (CRL) generation and distribution
- Directory management of certificate related items
- Certificate token initialization/programming/management
- System management functions (e.g., security audit, configuration management, archive.)

This policy does not presume any particular PKI architecture. CAs that issue certificates under this policy may operate simultaneously under other policies. CAs must not assert this policy in certificates unless they are issued in accordance with all the requirements of this policy.

1.1 Overview

A CA is a collection of hardware, software, personnel, and operating procedures that issue and manage public key certificates. The digital certificate binds a public key to a named subject, allowing relying parties to trust signatures or assertions made by the subject using the private key that corresponds to the public key contained in the certificate.

A fundamental element of modern secure communications is establishing trust in public keys, beginning with a Relying Party obtaining a Subscriber's public key certificate issued by a trusted entity certifying that the public key belongs to that Subscriber.

Subscriber certificates that are not trusted directly may become trusted through successive validation of a chain of CA certificates from the Subscriber's certificate to a trust anchor, such as the University's Root-CA public key.

Relying Parties explicitly trust trust anchors. Relying parties are responsible for securely obtaining trust anchors and for securely managing their trust anchor store. Relying parties, including the Trust Anchor Managers, should configure trust anchors with caution and should give full consideration to the requirements of this CP and associated compliance annual audit requirements.

1.2 Name and Identification

The top-level arc OID assigned to the University of Manchester by IANA, as a private enterprise number, is as follows (see https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers):

1.3.6.1.4.1.13661

Below the top level OID, further OIDs are defined as follows:

Company CA OID root	1.3.6.1.4.1.13661.100
Company Root CA ID	1.3.6.1.4.1.13661.100.1
Company Issuing CA 01 ID	1.3.6.1.4.1.13661.100.10
Company Issuing CA 01 CPS	1.3.6.1.4.1.13661.100.10.1
Company Issuing CA 01 - Computer certs	1.3.6.1.4.1.13661.100.10.1.1
Company Issuing CA 01 - Computer certs - low assurance client	1.3.6.1.4.1.13661.100.10.1.1.1
Company Issuing CA 01 - Computer certs - medium assurance client	1.3.6.1.4.1.13661.100.10.1.1.2
Company Issuing CA 01 - Computer certs - high assurance client *	1.3.6.1.4.1.13661.100.10.1.1.3
Company Issuing CA 01 - Computer certs - low assurance server	1.3.6.1.4.1.13661.100.10.1.1.101
Company Issuing CA 01 - Computer certs - medium assurance server	1.3.6.1.4.1.13661.100.10.1.1.102
Company Issuing CA 01 - Computer certs - high assurance server	1.3.6.1.4.1.13661.100.10.1.1.103
Company Issuing CA 01 - User certs	1.3.6.1.4.1.13661.100.10.1.2
Company Issuing CA 01 - User certs - low assurance	1.3.6.1.4.1.13661.100.10.1.2.1
Company Issuing CA 01 - User certs - medium assurance	1.3.6.1.4.1.13661.100.10.1.2.2
Company Issuing CA 01 - User certs - high assurance	1.3.6.1.4.1.13661.100.10.1.2.3

* At the time of writing, this CPS defines services used for the issuance of High assurance client computer certificates only.

1.3 PKI participants

1.3.1 PKI Authorities

Policy Authority - This is the entity that decides that a set of requirements for certificate issuance and use are sufficient for a given application. The Policy Authority approves the establishment of trust relationships with external PKIs that offer appropriately comparable assurance. For the University this may be Strategy, Security and Architecture, or it may be the Head of Information Governance, or a combination of both.

Trust Anchor Managers - the authorities who manage a repository of trusted root CA Certificates and subordinate CA certificates signed by these. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. A TAM sets requirements for inclusion of a CA's root public key in their store, based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of compliance audit results, on initial acceptance of a root, and on an ongoing basis. As specified in Section 5.7, the TAM will require the CA to provide notification of a compromise, and in response, the TAM will take appropriate action.

The University of Manchester IT Services – Directories Team, will be accountable for the deployment of trusted root CA certificates and associated subordinate certificates to Active Directory infrastructure.

The University of Manchester IT Services – Security Operations Team, will be accountable for the deployment of trusted root CA certificates and associated subordinate certificates to Palo Alto GlobalProtect infrastructure.

1.3.1.1 Certification Authority

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. The CA is responsible for issuing and managing certificates including:

- Approving the issuance of all certificates, including those issued to subordinate CAs and RAs.
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys
- Establishing and maintaining the CA system
- Establishing and maintaining this Certificate Policy (CP) & Certification Practice Statement (CPS)
- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under the CP are performed in accordance with the requirements, representations, and warranties of the CP

CA Operations Staff - CA components are operated and managed by individuals holding trusted, sensitive roles. Specific responsibilities for these roles, as well as any requirements for separation of duties, are described in Section 5.2.

1.3.1.2 Certificate Status Servers

The University PKI will include a service that provides status information about certificates on behalf of a CA through on-line transactions. In particular, the PKI will include Online Certificate Status Protocol (OCSP) responders to provide on-line status information. Such a service is termed a Certificate Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information or issued a delegated Responder certificate, the operations of that authority are considered within the scope of this CP. A CSS shall assert all the policy OIDs for which it is authoritative. Examples include OCSP servers that are identified in the Authority Information Access (AIA) extension.

1.3.2 Registration Authorities

The registration authorities (RAs) collect and verify each subscriber’s identity and information that is to be entered into the subscriber’s public key certificate. The RA performs its function in accordance with a CPS approved by the Policy Authority. The RA is responsible for:

- The registration process
- The identification and authentication process.

- Recording subject details for entities that request certification

1.3.3 Trusted Agents

The trusted agent is a person who satisfies all the appointment requirements for an RA and who performs identity proofing as a proxy for the RA, such as the HR department or NIC database manager. The trusted agent records information from and verifies presented credentials for an applicant's identity on behalf of the RA. The CPS will identify the parties responsible for providing such services, and the mechanisms for determining their trustworthiness.

1.3.4 Subscribers

A subscriber is the entity whose name appears as the subject in a certificate. The subscriber asserts the use of the key and certificate in accordance with the certificate policy asserted in the certificate, and does not issue certificates. The term "subscriber" as used in this document refers only to those who request certificates, such as users or computers, for uses other than signing and issuing certificates or certificate status information.

1.3.5 Relying Parties

A Relying Party is an entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party uses a Subscriber's certificate to verify or establish the identity and status of a system or device. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate to determine the suitability of the certificate for a particular use.

1.3.6 Other Participants

The CAs and RAs operating under the CP may require the services of other security, community, and application authorities. The CPS will identify the parties responsible for providing such services, and the mechanisms used to support these services.

One such participant is the Compliance Auditor. Compliance auditors are typically required to engage organisationally independent parties to perform compliance audits on a regular basis. To be effective, it is expected that compliance auditors will have a working knowledge in information security, cryptography, and PKI, risk mitigation strategies, and industry best practices.

1.4 Certificate usage

1.4.1 Appropriate Certificate Uses

Computer authentication – certificates will be issued to known devices through appropriate trusted delivery mechanisms for the purposes of device authentication.

1.4.2 Prohibited Certificate Uses

The use of certificates issued by Certificate Authorities governed by this Certificate Policy are prohibited for any use cases not explicitly described in section 1.4.1.

Device authentication through possession of a valid device certificate will not authorise further access to information or other systems alone. It will be used only to establish the identity of a device or verify it as a trusted platform for certain activities.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The Policy Authority is responsible for all aspects of this CP.

1.5.2 Contact Person

Head of Data Protection, Governance and Records Management - Mr Alex Daybank
alex.daybank@manchester.ac.uk
Head of Information Governance, the University of Manchester - Tony Brown

1.5.3 Person Determining CPS Suitability for the Policy

The Policy Authority shall approve the CPS for each CA that issues certificates under the policy.

1.5.4 CPS Approval Procedures

The Policy Authority shall make the determination that a CPS complies with University policy, including digital certificate policy. The CA and RA must meet all requirements of an approved CPS before commencing operations. The Policy Authority will make this determination based on the nature of the system function, the type of communications, or the operating environment.

2 Publication and Repository Responsibilities

2.1 Repositories

All CAs that issue certificates under this policy are obligated to post all CA certificates issued by or to the CA and CRLs issued by the CA in a repository that is accessible to all interested parties through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. Not all URI references will be publicly accessible.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

The repository system shall be designed and implemented so as to provide high availability overall and limit scheduled down-time in line with The University of Manchester IT service level agreements.

2.2.2 Publication of CA Information

The CPS shall be made available to authorised interested parties as/when required. The CP shall not be publicly accessible while CAs under this policy are not issuing certificates trusted outside the University. The CPS of the CA will not be published externally unless certificates issued by that CA are used externally to infer trust.

2.3 Time or frequency of publication

An updated version of the CPS will be made available within 30 days of the incorporation of changes.

2.4 Access Controls on Repositories

The CA shall protect information not intended for public dissemination or modification. CA certificates and CRLs in the repository shall be made publicly available through the Internet as and when required. Direct and/or remote access to other information in the CA repositories shall be determined by Policy Authority. The CPS shall detail what information in the repository shall be exempt from automatic availability and to whom, and under which conditions the restricted information may be made available.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

The CA shall assign an X.501 Distinguished Name (DN) to each subscriber. Subscriber certificates may contain any name type appropriate to the application.

3.1.2 Need for Names to Be Meaningful

Names used in certificates must represent an unambiguous identifier for the subject. Names should be meaningful enough for a human to identify the named entity, irrespective of whether the entity is a person, machine, or process. Interpreting the name semantic may require a reference database (e.g., human resources directory or inventory catalogue) external to the PKI.

Examples are:

Computer Name
User account name
Website common name/URL

While the issuer name in CA certificates is not generally interpreted by relying parties, this CP still requires use of meaningful names by CAs issuing under this policy. CA certificates that assert this policy shall not include a personal name, but rather shall identify the subject as a CA and include the name-space for which the CA is authoritative. For example:

CN = The University of Manchester Offline Root CA
DC = man
DC = ac
DC = uk

The subject name in CA certificates must match the issuer name in certificates issued by the subject, as required by [RFC5280].

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA shall not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting distinguished name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

3.1.5 Uniqueness of names

Each CA must ensure that each of its subscribers is identifiable by a unique name. Each X.500 name assigned to a subscriber by a CA (i.e., in that CA's namespace) must identify that subscriber uniquely. When other name forms are used, they too must be allocated such that each name identifies only one subscriber of that CA. Name uniqueness is not violated when multiple certificates are issued to the same entity. For certificates that assert names that do not identify individual people, the name shall be uniquely associated with a specific AOR.

The CPS shall identify the method for the assignment of unique subject names.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organization Identity

Requests for CA certificates shall include the CA name, University department, purpose, and documentation of the existence and purpose of the CA. Before issuing CA certificates, an authority for the University Root CA shall verify the information, in addition to the CA purpose, authenticity of the requesting representative and the representative's authorization to act in the name of the University department and CA.

3.2.3 Authentication of Individual Identity

Requests for identity certificates via one of the Universities electronic systems, such as Active Directory, will require authentication by the University IAM system, or other recognised identity systems. Successful authentication through those systems will be presumed as valid authentication for associated certificate requests.

3.2.3.1 Authentication of Human Subscribers

No stipulation at present.

3.2.3.2 Authentication of Devices

Some computing devices (PCs, mobiles, etc.) will be named as certificate subjects. In cases where devices are not capable of auto enrolment through a system authorised by the Policy Authority, an Authorised Organizational Representative (AOR), or in certain cases the device itself must provide identifying information for the device. The AOR/device is responsible for providing registration information which may include:

- Equipment identification (e.g., serial number)
- Equipment certificate signing request CSR
- Equipment authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable the CA or RA to communicate with the AOR when required.

The registration information provided by the AOR/device shall be verified. The identity of the AOR/device shall be authenticated.

3.2.3.3 Authentication of Applications or Services

Not stipulated.

3.2.3.4 Authentication for Role Certificates

Not stipulated.

3.2.3.5 Authentication for Code Signing Certificates

Not stipulated.

3.2.4 Non-verified Subscriber Information

Information that is not verified shall not be included in certificates.

3.2.5 Validation of Authority

Before issuing CA certificates or signature certificates that assert organisational authority, the CA shall validate the subscriber’s authority to act in the name of the organization. For role certificates that identify subjects by their organizational roles, the CA shall validate that the individual either holds that role or has been delegated the authority to sign on behalf of the role.

An example of signature certificates that assert organizational authority is code signing certificates.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key requests

3.3.1 Identification and Authentication for Routine Re-key

For re-key of any CA certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures as the initial registration at least once every 10 years from the time of original registration.

For re-key of any subscriber certificate issued under this certificate policy, identity may be established through use of current signature key, except that identity shall be established following the same procedures as the initial registration at least once every 10 years from the time of original registration.

3.3.2 Identification and Authentication for Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process per Section 3.2 above.

3.4 Identification and Authentication for Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The Certificate application process must provide sufficient information to:

- Establish the applicant’s authorisation (by the employing or sponsoring organization) to obtain a certificate. (per Section 3.2.3)
- Establish and record identity of the applicant. (per Section 3.2.3)
- Obtain the applicant’s public key and verify the applicant’s possession of the private key for each certificate required. (per Section 3.2.1)
- Verify any role or authorisation information requested for inclusion in the certificate.

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application?

A certificate application may be submitted to the CA by the Subscriber or an RA on behalf of the Subscriber.

4.1.2 Enrolment Process and Responsibilities

All communications among PKI Authorities supporting the certificate application and issuance process shall be authenticated and protected from modification; any electronic transmission of shared secrets and personally identifiable information shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications.

4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate before certificates are issued. Procedures to verify information in certificate applications shall be specified in the CPS.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the subscriber must meet the requirements specified for subscriber authentication as specified in Sections 3.2 and 3.3.

4.2.2 Approval or Rejection of Certificate Applications

Any certificate application that is received by a CA under this policy, for which the identity and authorisation of the applicant has been validated, will be duly processed. However, the CA must reject any application for which such validation cannot be completed, or when the CA has cause to lack confidence in the application or certification process.

4.2.3 Time to Process Certificate Applications

Certificate applications must be processed and a certificate issued in line with University Service level agreements.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, the CAs/RAs will:

- Verify the identity of the requester as specified in Section 3.2.
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in Section 4.1.
- Build and sign a certificate if all certificate requirements have been met (in the case of an RA, have the CA sign the certificate).
- Make the certificate available to the subscriber

The certificate request may already contain a certificate built by either the RA or the subscriber. This certificate will not be signed until all verifications and modifications, if any, have been completed to the CA's satisfaction.

All authorisation and other attribute information received from a prospective subscriber shall be verified before inclusion in a certificate.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

CAs operating under this policy shall inform the subscriber (or other certificate subject) of the creation of a certificate and make the certificate available to the subscriber. For device certificates, the CA shall issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorised organizational representative of the issuance (this may be in batch).

4.4 Certificate Acceptance

No stipulation.

4.4.1 Conduct Constituting Certificate Acceptance

No stipulation.

4.4.2 Publication of the Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.
This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The Policy Authority must be notified whenever a CA operating under this policy issues a CA certificate.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The intended scope of usage for a private key is specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public key and Certificate Usage

Certificates may specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs specifying the current status of all unexpired certificates except for OCSP responder certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key, as specified in Section 5.6. The identity proofing requirements listed in Section 3.3.1 shall also be met.

CA Certificates and OCSP responder certificates may be renewed so long as the aggregated lifetime of the public key does not exceed the certificate lifetime specified in Section 6.3.2. The CA may renew certificates during recovery from key compromise without subject request or approval as long as the CA is confident of the accuracy of information to be included in the certificates.

4.6.2 Who May Request Renewal

For all CAs and OCSP responders operating under this policy, the corresponding operating authority may request renewal of its own certificate.

4.6.3 Processing Certificate Renewal Requests

Digital signatures on subscriber renewal requests shall be validated before electronic renewal requests are processed. Alternatively, subscriber renewal requests may be processed using the same process used for initial certificate issuance.

4.6.4 Notification of New Certificate Issuance to Subscriber

The CA shall inform the subscriber of the renewal of his or her certificate and the contents of the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Failure to object to the renewal of the certificate or its contents constitutes acceptance of the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 2.1, all CA certificates shall be published in repositories.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-Key

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key. Re-key of a certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Subscribers shall identify themselves for the purpose of re-keying as required in section 3.3.

4.7.1 Circumstance for Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtain new keys. (Section 6.3.2 establishes usage periods for private keys for both CAs and subscribers.) Examples of circumstances requiring certificate re-key include: expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

4.7.2 Who May Request Certification of a New Public Key

Requests for certification of a new public key shall be considered as follows:

- Subscribers with a currently valid certificate may request certification of a new public key.
- CAs and RAs may request certification of a new public key on behalf of a subscriber.
- For device certificates, an authorised representative of the organization that owns or controls the device may request re-key.

4.7.3 Processing Certificate Re-keying Requests

Digital signatures on subscriber re-key requests shall be validated before electronic re-key requests are processed. Alternatively, subscriber re-key requests may be processed using the same process used for initial certificate issuance.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

All CA certificates must be published as specified in Section 2.

This policy makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate modification

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

Because of the requirement to validate a name change, and the sometimes complex combination of permissive and restrictive interpretation of certificate contents, no certificate modification will be provided, rather a subject will be expected to re-certify.

4.9 Certificate Revocation and Suspension

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued under this policy except for OCSP responder. Relying party client software may support on-line status checking and some support only CRLs. CAs should strongly consider offering online status checking in addition to CRLs.

CAs operating under this policy shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to subscribers during certificate request or issuance, and shall be readily available to any potential relying party.

Revocation requests must be authenticated. See Section 3.4 for more details.

Certificate suspension for CA certificates is not allowed by this policy. However, the use of certificate suspension for end entity certificates is allowed.

4.9.1 Circumstances for revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid.
- Privilege attributes asserted in the subscriber's certificate are reduced, such as re-purposing a personal computer from one user/department to another
- The subscriber can be shown to have violated the stipulations of its subscriber agreement.
- There is reason to believe the private key has been compromised.
- The subscriber or other authorised party (as defined in the CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

Within the PKI, a CA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the subscriber when practical. The RA can request the revocation of a subscriber's certificate on behalf of any authorised party as specified in the CPS. A subscriber may request that its own certificate be revoked. The AOR of the organization that owns or controls a device can request the revocation of the device's certificate. Other authorised individuals of the organisation may request revocation as described in the CPS.

4.9.3 Procedure for Revocation Request

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The steps involved in the process of requesting a certification revocation are detailed in the CPS.

4.9.4 Revocation Request Grace Period

There is no revocation grace period under this policy.

4.9.5 Time within which CA must Process the Revocation Request

CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

CRLs shall be issued periodically per the CPS, even if there are no changes to be made, to ensure timeliness of information. Certificate status information may be issued more frequently than the issuance frequency described below.

Certificate status information shall be published no later than the next scheduled update. This will facilitate the local caching of certificate status information for off-line or remote (laptop) operation.

Circumstances related to emergency CRL issuance are specified in section 4.9.12.

4.9.8 Maximum latency for CRLs

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9 On-line Revocation/Status Checking Availability

Where on-line status checking is supported, status information must be updated and available to relying parties within 4 hours of CRL publication.

4.9.10 On-line Revocation Checking Requirements

Relying party client software may optionally support on-line status checking. Client software using online status checking need not obtain or process CRLs.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related To Key Compromise

Certificate revocation for reason of key compromise must appear in a published CRL (or OCSP response) within 6 hours of the decision to revoke.

4.9.13 Circumstances for Suspension

Certificate suspension is not currently permitted under this policy.

4.10 Certificate Status Services

Certificate status will be made available through publication of CRLs to designated CRL distribution points, as defined within certificates issued by the University of Manchester, and through Online Certificate Status servers.

4.11 End of subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private keys will not be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

All CA and RA equipment, including cryptographic modules, shall be protected from theft, loss, and unauthorised access at all times. Unauthorised use of CA and RA equipment is prohibited. CA equipment shall be dedicated to performing CA functions. RA equipment shall be operated to ensure that the equipment meets all physical controls at all times.

5.1.1 Site location and construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, shall be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, shall provide robust protection against unauthorised access to the CA equipment and records.

5.1.2 Physical access

5.1.2.1 Physical access for CA equipment

Physical access to CA equipment shall be limited to CA Operations Staff and Security Auditors. The security mechanisms shall be commensurate with the level of threat in the equipment environment. (presuming that offline CAs will be stored securely with named access, but need to determine if ok to locate issuing CA in data centre without additional physical controls.)

At a minimum, physical access controls for CA equipment shall meet the following requirements:

- Ensure that no unauthorised access to the hardware is permitted
- Be manually or electronically monitored for unauthorised intrusion at all times
- Ensure an access log is maintained and inspected periodically.
- Mandate at least two-person access requirements. At least one individual shall be a member of the CA Operations Staff. Technical or mechanical mechanisms (e.g., dual locks) shall be used to enforce the two-person physical access control.
- Access to keys protecting physical access to CA equipment shall be provided to two nominated individuals
- Access to CA equipment, through full disk encryption and PKI administrator authentication shall be provided to two nominated individuals
- No person shall be nominated as both a key holder and PKI administrator simultaneously to ensure separation of duties

When not in use, removable CA cryptographic modules, removable media, and any activation information used to access or enable CA cryptographic modules or CA equipment, or paper containing sensitive plaintext information shall be placed in locked containers sufficient for housing equipment and information commensurate with the sensitivity, or value of the information being protected by the certificates issued by the CA. Access to the contents of the locked containers shall be restricted to individuals holding CA trusted roles as defined in Section 5.2.1, utilizing two-person access controls, and two-person integrity while the container is unlocked.

Any activation information used to access or enable the cryptographic modules or CA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

A security check of the room/rack housing CA equipment shall occur prior to leaving the room/rack unattended by the CA Operations Staff. The check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed")
- Any security containers are properly secured
- Physical security systems (e.g., door locks, vent covers) are functioning properly
- The area is secured against unauthorised access

If unattended, the facility housing CA equipment shall be protected by an intrusion detection system (IDS).

If a facility is not continuously attended and does not include an IDS, a check shall be made at least once every <24> hours to ensure that no attempts to defeat the physical security mechanisms have been made. A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons are responsible, a log identifying the person performing a check at each instance shall be maintained. The last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

RA equipment shall be protected from unauthorised, and shall implement physical access controls to reduce the risk of equipment tampering. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

Any activation information used to access or enable the RA equipment shall be stored separately from the associated modules and equipment. Such information shall either be memorized or recorded and stored in a manner commensurate with the security afforded the associated cryptographic module or equipment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment (if implemented), shall meet the CA physical access requirements specified in Section 5.1.2.1

5.1.3 Power and Air Conditioning

The CA shall have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown. The repositories (containing CA certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water.

5.1.5 Fire Prevention and Protection

CA equipment shall be installed such that it is not in danger of exposure to fire.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic) and unauthorised physical access. Media not required for daily operation or not required by policy to remain with the CA or RA that contains security audit, archive, or backup information shall be stored securely in a location separate from the CA or RA equipment.

Media containing private key material shall be handled, packaged, and stored in a manner compliant with the requirements for the sensitivity level of the information it protects or provides access. Storage protection of CA and RA private key material shall be consistent with stipulations in Section 5.1.2.

5.1.7 Waste Disposal

No stipulation.

5.1.8 Off-site Backup

A system backup shall be made when a CA system is activated, and at regular intervals in line with operational policy. Backup media or content shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

The data backup media shall be stored in a facility approved for storage of information of the same value of the information that will be protected by the certificates and associated private keys issued or managed using the equipment with a minimum requirement of transferring, handling, packaging, and storage of the information in a manner compliant with requirements for sensitive material identified in Section 6.2.4.1.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. It is essential that the people selected to fill these roles shall be held accountable to perform designated actions correctly or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust in the CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to minimize the number of trusted roles and ensure that the people filling those roles are trustworthy and properly trained. The second is to enforce the concept of least privilege and distribute the functions of the roles among several people, so that any malicious activity requires collusion. Trusted role operations include:

- The validation, authentication, and handling of information in Certificate Applications
- The acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrolment information
- The issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository
- Access to safe combinations and/or keys to security containers that contain materials supporting production services
- Access to hardware security modules (HSMs), their associated keying material, and the secret share splits of the PINS that protect access to the HSMs
- Providing enterprise customer support
- Access to any source code for the digital certificate applications or systems.
- Access to restricted portions of the certificate repository

- The ability to grant physical and/or logical access to the CA equipment
- The ability to administer the background investigation policy processes

The only mandatory trusted roles defined by this policy are the Administrators, CA Operations Staff, Offline Root CA key holders, and Security Auditors. Multiple people may hold the same trusted role, with collective privileges sufficient to fill the role. Other trusted roles may be defined in other documents, which describe or impose requirements on the CA operation.

The CA shall maintain lists, including names, organisations, contact information, and organisational affiliation for those who act in Administrator, CA Operations Staff, RAs, and Security Auditor trusted roles, and shall make them available during compliance audits. The RA shall maintain lists, including names, organizations, and contact information of those who act in RA Operations Staff, RA Administrators, and RA Security Auditor roles for that RA.

5.2.1.1 Administrator

The administrator role shall be responsible for:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Configuring certificate profiles or templates
- Configuring CA, RA audit parameters
- Generating and backing up CA keys
- System backups and recovery

Administrators do not typically issue certificates to subscribers.

5.2.1.2 CA Operation Staff

The CA Operation Staff role shall be responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates
- Verifying the identity of subscribers and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving and executing the revocation of certificates
- Approving infrastructure certificates issued to support the operations of the CA
- Approving revocation of certificates issued to CAs or to support the operations of the CA
- Approving certificates issued to RAs
- Authorizing RAs
- Approving revocation of certificates issued to RAs
- Providing Certificate revocation and suspension status information
- Posting Certificates and CRLs

5.2.1.3 Auditor

Security Auditors are responsible for auditing CAs and RAs. This is a sensitive role and must not be combined with any other sensitive role, e.g. the Security Auditor cannot also be part of the CA Operations Staff. Security Auditors are responsible for reviewing, maintaining, and archiving audit logs, and for performing or overseeing internal audits (independent of formal compliance audits) to ensure that CAs and RAs are operating in accordance with the associated CPSs.

5.2.1.4 RA Staff

RA Staff are the individuals holding trusted roles that operate and manage RA components. RA Staff is responsible for the following:

- Operation of the RA and its component systems
- Establishing and maintaining RA operating system and application accounts
- Routine operation of the RA equipment such as system backup and recovery or changing recording media
- Registering new Subscriber and requesting the issuance of certificates
- Verifying the identity of Subscribers
- Verifying the accuracy of information included in certificates
- Approving and executing the issuance of certificates
- Requesting, approving, and executing the suspension, restoration, and revocation of certificates

5.2.2 Number of Persons Required per Task

Where multi-party control is required, all participants shall hold a trusted role. Multi-party control shall not be achieved using personnel that serve in a Security Auditor role with the exception of audit functions. The following tasks may require two or more persons:

- Generation, activation, and backup of CA keys
- Performance of CA administration or maintenance tasks
- Archiving or deleting CA audit logs. At least one of the participants shall serve in a Security Auditor role.
- Physical access to CA equipment
- Access to any copy of the CA cryptographic module
- Processing of third party key recovery requests

5.2.3 Identification and Authentication for Each Role

Individuals holding trusted roles shall identify themselves and be authenticated by the CA and RA before being permitted to perform any actions set forth above for that role or identity. CA Operations Staff and RA Staff shall authenticate using a credential that is distinct from any credential they use to perform other non-trusted role functions. This credential shall be generated and stored in a system that is protected to the same level as the CA system.

CA and RA equipment shall require, at a minimum, strong authenticated access control for remote access using multi-factor authentication. Examples of multi factor authentication include use of a password or PIN along with a time-based token, digital certificate on a hardware token or other device that enforce a policy of what a user has and what a user knows.

CA and RA equipment shall require, at a minimum, authenticated access control (e.g., strong passwords) for local multi-party access.

Individuals holding trusted roles shall be appointed to the trusted role by an appropriate approving authority. The approval shall be recorded in a secure and auditable fashion. Individuals holding trusted roles shall accept the responsibilities of the trusted role, and this acceptance shall be recorded in a secure and auditable fashion.

Identity proofing of the RA shall be performed by a member of the CA Operations Staff. Users shall authenticate themselves to all aspects of the network (servers, operating systems, applications, databases, processes, and so on) before they can access that resource.

5.2.3.1 Authentication: Passwords and Accounts

Where passwords are required, strong passwords shall be employed, as defined in the University password technical security standard. Account lock-out shall be applied as per local policy for privileged user accounts.

The CA shall have the minimum number of accounts that are necessary for its operation.

5.2.4 Roles Requiring Separation of Duties

Individuals serving as Security Auditors shall not perform or hold any other CA trusted role.

Individuals serving as key holders shall not perform any CA administration or CA operations trusted role.

Only an individual serving in a Security Auditor role may perform internal auditing functions, with the exception of those security audit functions (e.g., configuring, archiving, deleting) that require multi-person control.

An individual that performs any trusted role shall only have one identity when accessing CA equipment.

5.3 Personnel controls

Personnel Security plays a critical role in the CA facility’s overall security system. Personnel Security shall be designed to prevent both unauthorised access to the CA facility and CA systems and compromise of sensitive CA operations by CA personnel.

Inadequate personnel security procedures or negligent enforcement of personnel security policies can pose potentially threats to security and undermine confidence in the status of a CAs trust.

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel seeking to become Trusted Persons shall possess the requisite background, qualifications and experience needed to perform their prospective job responsibilities competently and satisfactorily.

Individuals appointed to any trusted role shall meet the following:

- Be employees of or contractor/vendor of the CA and bound by terms of employment or contract
- Be appointed in writing
- Have demonstrated the ability to perform their duties
- Have no other duties that would interfere or conflict with their responsibilities as defined in Section 5.2.1
- Have not been previously relieved of trusted role duties for reasons of negligence or non-performance of duties

5.3.2 Background Check Procedures

University staff being considered for CA trusted roles must be checked in accordance with University HR procedures for IT operations.

5.3.3 Training Requirements

Appropriate training will be made available to all personnel performing duties with respect to the operation of the CA, or RA. Training shall be conducted in the following areas:

- CA/RA security principles and mechanisms
- All PKI software versions in use on the CA/ RA system
- All PKI duties they are expected to perform
- Disaster recovery and business continuity procedures
- Stipulations of this policy

5.3.4 Retraining Frequency and Requirements

All individuals responsible for PKI Trusted Roles shall be made aware of changes in the CA, RA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

No stipulation.

5.3.7 Independent Contractor Requirements

Contractor personnel filling trusted roles shall be subject to all requirements stipulated in this document. Independent contractors and consultants who have not completed or passed the background check procedures specified above shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by a person holding trusted role at all times.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the CAs and RAs. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.1 Types of events recorded

All security auditing capabilities of CA and RA operating system and applications shall be enabled during installation. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

- The type of event;
- The date and time the event occurred;
- Success or failure where appropriate, and
- The identity of the entity and/or operator that caused the event.

5.4.2 Frequency of processing log

Audit logs shall be reviewed regularly and checked for tampering, with live exports to a dedicated Security Incident Event Monitoring (SIEM) system. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention period for audit log

Audit logs shall be retained separately within a dedicated Security Incident Event Monitoring system in line with agreed retention policy for a period not less than 12 months.

5.4.4 Protection of audit log

The security audit data shall not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing.

Electronic logs shall be protected to prevent alteration and detect tampering.

Security audit data shall be moved to a safe, secure storage location separate from the location where the data was generated.

CA/ RA system configuration and procedures must be implemented together to ensure that only authorised people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access).

5.4.5 Audit Collection System (Internal vs. External)

The audit log collection system will be external to the CA/ RA system. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems shall be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files).

5.4.6 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.7 Vulnerability Assessments

The CA shall perform routine self-assessments of security controls.

5.5 Records Archival

5.5.1 Types of Events Archived

CA/RA archive records shall be sufficiently detailed to determine the proper operation of the CA/RA and the validity of any certificate (including those revoked or expired) issued by the CA. At a minimum, the following data shall be recorded for archive:

- Certificate policy
- Certification practice statement
- Contractual obligations
- Other agreements concerning operations of the CA/CSS/RA
- System and equipment configuration
- Subscriber identity authentication data as per section 3.2.3
- Documentation of receipt and acceptance of certificates (if applicable)
- Subscriber agreements
- All Audit logs
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- All access to certificate subject private keys retained within the CA for key recovery purposes
- All changes to the trusted public keys, including additions and deletions
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

Many other relevant CA operations events are recorded in the audit logs, and archived with those logs.

5.5.2 Retention Period for Archive

Archive records must be kept for a minimum of 1 year.

5.5.3 Protection of archive

No unauthorised user shall be permitted to write to, modify, or delete the archive. For the CA and RA authorised individuals are Security Auditors.

For the CA /RA, archived records may be moved to another medium. The contents of the archive shall not be released except in accordance with sections 9.3 and 9.4. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognised agents.

Archive media shall be stored in a safe, secure storage facility separate from the CA/RA with physical and procedural security controls equivalent to or better than those of the CA/RA. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.

5.5.4 Archive backup procedures

The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed.

5.5.5 Requirements for time stamping of records

CA/RA archive records shall be automatically time-stamped by the SIEM system as they are created.

5.6 Key changeover

CA private keys will not be routinely renewed without an identified reason, such as new concern over the protection afforded through the chosen key length due to advances in crypto techniques.

5.7 Compromise and disaster recovery

5.7.1 Incident and Compromise Handling Procedures

The University shall have an Incident Response Plan and a Disaster Recovery Plan.

If compromise of a CA is suspected, an investigation shall be performed in order to determine the nature and the degree of damage. Certificates issuance from that CA shall be stopped immediately upon detection of a compromise. If a CA private signing key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA private key needs to be declared compromised.

The trust anchor managers shall be notified as soon as possible should any of the following occur:

- Suspected or detected compromise of any CA system or subsystem
- Physical or electronic penetration of any CA system or subsystem
- Successful denial of service attacks on any CA system or subsystem
- Any incident preventing a CA from issuing and publishing a CRL or OCSP prior to the time indicated in the nextUpdate field in the currently published CRL or OCSP

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy shall respond as follows:

- Notify trust anchor managers or the superior CA as soon as possible.
- Ensure that the system’s integrity has been restored prior to returning to operation and determine the extent of loss of data since the last point of backup.
- If the CA signing keys are not destroyed, the integrity of the system has been restored, and the risk is deemed negligible, re-establish CA operations, giving priority to the ability to generate certificate status information within the CRL issuance schedule.
- If the CA signing keys are destroyed, the integrity of the system cannot be restored, or the risk is deemed substantial, re-establish CA operations as quickly as possible, giving priority to the generation of a new CA signing key pair.

5.7.3 CA Private Key Compromise Procedures

5.7.3.1 Root CA Compromise Procedures

In the case of the Root CA compromise, the CA operations team shall notify the trust anchor managers and relying parties as soon as possible, and any cross-certified PKIs, of the Root

CA compromise so that they can revoke any cross certificates issued to the Root CA or any Subordinate CAs and notify all Subscribers and Relying Parties to remove the trusted self-signed certificate from their trust stores.

Notification shall be made in an authenticated and trusted manner. Initiation of notification to the trust anchor managers and any cross-certified PKIs shall be made at the earliest feasible time and shall not exceed 24 hours beyond determination of compromise or loss unless otherwise required by law enforcement. Initiation of notification to relying parties and subscribers may be made after mediations are in place to ensure continued operation of applications and services. If the cause of the compromise can be adequately addressed, and it is determined that the PKI can be securely re-established, the University shall then generate a new Root CA certificate, solicit requests and issue new Subordinate CA certificates, securely distribute the new Root CA certificate, and re-establish any cross certificates.

5.7.3.2 Intermediate or Subordinate CA Compromise Procedures

In the event of an Intermediate CA key compromise, the CA operations team shall notify the trust anchor managers. The intermediate CA’s certificate shall be revoked, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner but within 24 hours after the notification. The Compromised CA operator shall also investigate and report to the trust anchor mangers and Superior CA what caused the compromise or loss, and what measures have been taken to preclude recurrence. If the cause of the compromise can be adequately addressed and it is determined that the CA can be securely re-established, then, the CA shall be re-established. Upon re-establishment of the CA, new Subscriber certificates shall be requested and issued.

For Subordinate CAs, when a Subscriber certificate is revoked because of compromise, suspected compromise, or loss of the private key, a CRL shall be published at the earliest feasible time by the supporting CA, but in no case more than 6 hours after notification.

5.7.3.3 CSS Compromise Procedures

In case of a CSS key compromise, the CA that issued the CSS a certificate shall revoke that certificate, and the revocation information shall be published immediately in the most expedient, authenticated, and trusted manner. The CSS shall subsequently be re-keyed. If the CSS is self-signed and the CSS certificate expiration is more than <7> days away, the vendor shall immediately notify the trust anchor managers, relying parties, and any cross-certified PKIs of the CSS compromise so that they can notify all Subscribers and Relying Parties to remove trust in the CSS certificate from each Relying Party application, and install the re-keyed certificate.

5.7.3.4 RA Compromise Procedures

In case of an RA compromise, the CA shall disable the RA. In the case that an RA’s key is compromised, the CA that issued the RA certificate shall revoke it, and the revocation information shall be published within 24 hours in the most expedient, authenticated, and trusted manner. The compromise shall be investigated by the CA in order to determine the actual or potential date and scope of the RA compromise. All certificates approved by that RA since the date of actual or potential RA compromise shall be revoked. In the event that the scope is indeterminate, then the CA compromise procedures in Section 5.7.3.2 shall be followed.

5.7.4 Business Continuity Capabilities after a Disaster

The University shall maintain a Disaster Recovery Plan.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be re-established as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CA cannot re-establish revocation capabilities prior to date and time specified in the nextUpdate field in the currently published CRL issued by the CA, then the inoperative status of the CA shall be reported to the trust anchor managers. The trust anchor managers shall decide whether to declare the CA private signing key as compromised and re-establish the CA keys and certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA shall request that its certificates be revoked. The CA installation shall then be completely rebuilt by re-establishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates will be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk, and the risk of others to whom the data is forwarded, as no revocation information will be available (if the CRL signing key was destroyed).

5.8 CA or RA Termination

When a CA operating under this policy terminates operations before all certificates have expired, Entities will be given as much advance notice as circumstances permit.

Prior to CA termination, notice shall be provided to all cross-certified CAs requesting revocation of all certificates issued to it. In addition:

- The CA shall issue a CRL revoking all unexpired certificates prior to termination. This CRL shall be available until all certificates issued by the CA expire.
- The CA and RA shall archive all audit logs and other records prior to termination
- The CA and RA shall destroy all associated private keys upon termination
- The CA and RA archive records shall be transferred to an appropriate authority specified in the CPS

If a Root CA is terminated, the University shall use secure means to notify the subscribers to delete all trust anchors representing the terminated CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated using University approved mechanisms, such as self-generation on approved CAs.

CA key pair generation must create a verifiable audit trail demonstrating that the security requirements for procedures were followed. The documentation of the procedure must be detailed enough to show that appropriate role separation was used. A third party independent from IT and CA Operations management shall validate the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 RA Key Pair Generation

Not stipulated.

6.1.1.3 Subscriber Key Pair Generation

Subscriber key pair generation will be performed by the subscriber.

University approved mechanisms shall be used to generate all subscriber key pairs, as well as pseudo-random numbers and parameters used in key pair generation.

6.1.2 Private Key Delivery to Subscriber

Not stipulated as subscribers are expected to generate their own key pairs.

6.1.3 Public Key Delivery to Certificate Issuer

Where key pairs are generated by the subscriber or RA, the public key and the subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA Public Key Delivery to Relying Parties

The public key of a root CA shall be provided to the subscribers acting as relying parties in a secure manner so that it is not vulnerable to modification or substitution. Examples of acceptable methods for delivery of the public key include:

- Secure distribution of self-signed certificates through secure out-of-band mechanisms
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism);

When a CA updates its signature key pair, the key rollover certificates may be signed with the CA's current private key; in this case secure distribution is not required.

6.1.5 Key Sizes

This CP requires use of RSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys.

Root CA certificates shall contain subject public keys of at least 4096 bits for RSA and be signed with the corresponding private key.

CAs that generate certificates and CRLs under this policy should use the SHA-256, or SHA-384 hash algorithm when generating digital signatures. CAs that issue certificates signed with SHA-256 or SHA-384 must not issue certificates signed with SHA-1.

RSA signatures on CRLs that only provide status information for certificates that were generated using SHA-1 may continue to be generated using SHA-1.

6.1.6 Key Usage Purposes (as per X.509 v3 Key Usage Field)

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Public keys that are bound into user certificates shall be used only for signing or encrypting, but not both. User certificates that contain signature keys shall assert the digitalSignature bit. User certificates that contain RSA public keys that are to be used for key transport shall assert the keyEncipherment bit. User certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the keyAgreement bit.

Public keys that are bound into CA certificates shall be used only for signing certificates and status information (e.g., CRLs). CA certificates whose subject public key is to be used to verify other certificates shall assert the keyCertSign bit. CA certificates whose subject public key is to be used to verify CRLs shall assert the cRLSign bit. CA certificates whose subject public key is to be used to verify Online Certificate Status Protocol (OCSP) responses shall assert the digitalSignature bit.

Public keys that are bound into device, applications, and service certificates may be used for digital signature (including authentication), key management, or both. Device certificates to be used for digital signatures shall assert the digitalSignature bit. Device certificates that contain RSA public keys that are to be used for key transport shall assert the keyEncipherment bit. Device certificates that contain elliptic curve public keys that are to be used for key agreement shall assert the keyAgreement bit. Device certificates to be used for both digital signatures and key management shall assert the digitalSignature bit and either the keyEncipherment (for RSA) or keyAgreement (for elliptic curve) bit. Device certificates shall not assert the nonRepudiation bit.

The dataEncipherment, encipherOnly, and decipherOnly bits shall not be asserted in certificates issued under this policy. In addition, anyExtendedKeyUsage shall not be asserted in extended key usage extensions.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

CAs shall not require a hardware cryptographic module for signing operations.

6.2.2 Private Key (N of M) Multi-Person Control

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA signing key. CA signing keys may be backed up only under two-person control. Access to CA signing keys backed up for disaster recovery shall be under at least two-person control. The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Subscriber key management keys may be escrowed to provide key recovery as described in section 4.12.1. If a device has a separate key management key certificate, the key management private key may be escrowed. The private key associated with a certificate that asserts a digitalSignatrue key usage shall not be escrowed.

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

The CA private signature keys shall be backed up under the same multiparty control as the original signature key. All copies of the CA private signature key shall be accounted for and protected in the same manner as the original. Backup procedures shall be included in the CA's CPS.

6.2.4.2 Backup of human subscriber keys

Not stipulated.

6.2.5 Private Key Archival

CA private signature keys and subscriber private signature keys shall not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of Deactivating Private Key

Private keys shall not be available to unauthorised access. After use, the private key shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the applicable CPS.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles shall destroy CA, RA, and CSS (e.g., OCSP server) private signature keys when they are no longer needed. Physical destruction of hardware is not required.

To ensure future access to encrypted data, subscriber private key management keys may be secured in long-term backups or archived.

6.2.11 Cryptographic Module Rating

Not stipulated.

6.3 Other aspects of key pair management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Usage Periods

The suitability of the Root CA key pair shall be reviewed every 20 years, in line with the lifespan of the Root CA certificate. Unless exceptional circumstances dictate otherwise, the strength of keys and architectural suitability of the PKI will be reviewed, conclusions of which will influence this certificate policy.

For all other CAs operating under this policy, the usage period for a CA key pair that meets the same key length and signing algorithm as used for the Root CA key pair shall be the same as used for the Root CA key pair. For CA key pairs that are shorter length than used by the Root CA key pair the maximum usage period will be specified in the CPS for each CA. The CA private key may be used to sign certificates ,CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair’s usage period.

For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years. Subscriber signature private keys have the same usage period as their corresponding public key. The usage period for subscriber key management private keys is not restricted.

6.4 Computer Security Controls

6.4.1 Specific Computer Security Technical Requirements

6.4.1.1 Access control

Access to information such as passwords, and ultimately, CA related private keys will be carefully guarded, along with the machines housing such information.

6.4.1.1.1 Access Control Policy and Procedures

The CA shall create and document roles and responsibilities for each employee job function in the CPS. The CA shall create and maintain a mapping of these roles and their associated responsibilities to specific employees and their accounts on CA systems.

6.4.1.1.2 Account management

Information system account management features shall ensure that users access only that functionality permitted by their role or function. All privileged access accounts shall be documented along with the conditions and procedures to follow in creating new accounts. Groups and roles shall have a documented relationship to the business or mission roles involved in operating the CA.

Section 5.2.1 of this document defines roles and job functions for personnel that the CA will use when defining access control mechanisms. The CA shall employ the principle of least privilege when creating users and assigning them to groups and roles; membership to a group or role is granted shall be justified based upon business need. The CA shall take appropriate action when a user no longer requires an account, their business role changes, or the user is terminated or transferred. Periodically, the CA shall review all active accounts to match active authorised users with accounts, and disable any accounts no longer associated with an active authorised user.

All account administration activities shall be logged and made available for inspection by appropriate security personnel. Account administration activities that shall be audited include account creation, modification, enabling, disabling, group or role changes, and removal actions.

The use of shared/group and guest/anonymous accounts for logon to information systems shall be prohibited.

6.4.1.1.3 Least privilege

In granting rights to accounts and groups, the CA shall employ the principle of least privilege, allowing only authorised access for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organisational missions and business functions. The CA shall explicitly authorise access to accounts and groups for controlling security functions and security relevant information. The CA shall authorise access to privileged commands and features of information systems only for specific, organisation-defined compelling operational needs and documents the rationale for such access. The CA shall require that users of information systems with access to administrative privileges to utilise non-privileged accounts or roles when accessing non-privileged functions (such as reading email).

6.4.1.1.4 Permitted Actions without Identification or Authentication

The organization shall document a specific list of actions that can be performed on specifically enumerated information systems without identification or authentication, such as retrieving or verifying a published CRL from an Internet-accessible server or accessing a publicly available website. Furthermore, the organization shall document and provide supporting rationale in its security policy and procedures an enumerated list of user actions and systems not requiring identification or authentication (i.e., anonymous access).

6.4.1.2 System Integrity

6.4.1.2.1 System isolation and partitioning

CA systems shall be configured, operated, and maintained so as to ensure the continuous logical separation of processes and their assigned resources. This separation shall be enforced by

- physical and/or logical isolation mechanisms, such as dedicated systems or virtualization
- protecting an active process and any assigned resources from access by or interference from another process
- ensuring that any exception condition raised by one process will have no lasting detrimental effect on the operation or assigned resources of another process

Servers hosting CA roles must not be used to host other roles that are not specifically related to operation of the CA.

If there are system resources shared amongst trusted and/or untrusted processes, the underlying system(s) shall prevent any unauthorised and unintended information transfer between processes via those shared system resources.

The CA shall develop and document controlled procedures for transferring software updates, configuration files, certificate requests, and other data files between trusted components.

6.4.1.2.2 Malicious Code Protection

The CA system shall employ malicious code protection mechanisms to mitigate the risk of malicious code on CA system components. Malicious code on trusted CA components could allow an attacker to issue fraudulent certificates, create a rogue intermediate or signing CA server, or compromise the availability of the system.

CA system components running standard operating systems that are not air-gapped from the Internet shall employ host-based anti-malware tools to detect and prevent the execution of known malicious code. These tools shall be configured to automatically scan removable media when it is inserted, as well as files received over the network. Introduction of removable media shall not cause automatic execution of any software residing on the media.

Anti-malware tools employed by a CA shall be properly maintained and updated by the CA. Antimalware tools on networked systems shall be updated automatically as updates become available, or CA system administrators shall push updates to system components on a regular basis in line with operational policy. Anti-malware tools will not be employed on air-gapped systems such as offline CAs.

Anti-malware tools shall alert system administrators of any malware detected by the tools. On system components that do not implement host-based anti-malware tools, the CA shall identify and employ other malicious code protection mechanisms to prevent the execution of malicious code, detect infected files or executables, and remediate infected systems. These mechanisms could include, but are not limited to, compensating physical protection on hosts, network-based malware detection tools at boundary points, application whitelisting, and manually scanning removable media by trusted CA personnel. The CA shall document all malware protection mechanisms in the CPS.

6.4.1.2.3 Software and Firmware Integrity

The CA shall employ technical and procedural controls to prevent and detect unauthorised changes to firmware and software on CA systems. Access control mechanisms and configuration management processes (see Section 6.5.1.1 and 6.6.2) shall ensure that only authorised system administrators are capable of installing or modifying firmware and software on CA systems.

All changes to CA software and firmware shall be documented formally under the University change control procedures with date, time, person responsible for making the change, old version number, new version number, reason for change.

6.4.1.2.4 Information Protection

The CA shall protect the confidentiality and integrity of sensitive information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect customer data that could allow an attacker to impersonate a customer. The CA shall employ technical mechanisms to prevent unauthorised changes or accesses to this information, such as access control mechanisms that limit which users are authorised to view or modify files. Sensitive information stored on devices that are not physically protected from potential attackers shall be stored in an encrypted format, using a University approved encryption algorithm and mode of operation.

6.4.2 Computer Security Rating

No stipulation.

6.5 Lifecycle Technical Controls

6.5.1 System Development Controls

The system development controls address various aspects related to the development and change of the CA system through aspects of its life-cycle.

The CA system shall be implemented and tested in a non-production environment prior to implementation in a production environment. No change shall be made to the production environment unless the change has gone through the change control process as defined for the system baseline.

6.5.2 Security Management Controls

A list of acceptable products and their versions for each individual CA system component shall be maintained and kept up-to-date within a configuration management system.

Mechanisms and/or procedures shall be in operation designed to prevent the installation and execution of unauthorised software. A signed whitelist of the acceptable software for the system should be one of the ways to control the allowed software. A CA system shall have automated mechanisms to inventory on at least a daily basis software installed on a system and alert operators if invalid software is found.

To reduce the available attack surface of a CA system, only those ports, protocols, and services that are necessary to the CA system architecture are permitted to be installed or operating. The CA system shall maintain a list of ports, protocols, and services that are necessary for the correct function of each component within the CA system. There shall be automated mechanisms to monitor the running processes and open ports against the permitted list.

6.5.3 Life Cycle Security Controls

For flaw remediation, the CA shall scan all online CA systems for vulnerabilities using at least one vulnerability scanner every in real time.

Each vulnerability found shall be assessed, recorded and remediated within an agreed time period based on its nature and severity.

The CA shall monitor relevant notification channels on a regular basis for updates to packages installed on CA systems (including networking hardware). CAs shall have a plan for receiving notification of software and firmware updates, for obtaining and testing those updates, for deciding when to install them, and finally for installing them without undue disruption in accordance with agreed University patching policies. A log shall be kept of the notifications, the decision to apply/not apply including reason, and the application of relevant updates/patches.

From time to time, the CA may discover errors in configuration files, either because of human error, source data error, or changes in the environment which have made an entry erroneous. The CA shall correct such errors at the earliest opportunity, and shall document the reason for the error, and the associated correction.

Under no circumstances should a remediation cause unavailability of revocation information.

6.6 Network Security Controls

The various components of a CA are, for the most part, connected to each other and their customers via various forms of networks. While it is necessary for connections to customers and administrative systems, care shall be taken to ensure those connections do not adversely impact the security of those components.

6.6.1 Availability

Certificate request and issuance services need to be available, but can tolerate some down time.

Revocation services, and any supporting infrastructure on which these services rely, must be highly available.

6.6.1.1 Denial of Service Protection

CA systems shall be configured, operated, and maintained to maximize uptime and availability. Scheduled downtime shall be announced to Subscribers.

CAs shall state acceptable methods to request revocation in their CPS. At least one of those methods shall be out of band (i.e. network connectivity is not required).

CAs shall state in their CPSs their guaranteed availability for revocation information and how they achieve it. CAs shall make revocation information available in at least one form that can be used in a cached, offline manner. The CA revocation information availability required shall be stated in its CPS.

CAs shall take reasonable measures to protect certificate request and issuing services from known DoS attacks. The CA request and issuing availability required by a Subscriber application shall be stated in its CPS

Revocation services need to configured and deployed in such a manner and capacity that overall availability shall be maintained at a minimum of 99.97% equivalent to the University’s Premium Service Tier, with no single outage lasting longer than 1 hour. Additionally, such services shall be homed in a minimum of two geographically independent locations with no single-points of failure which could affect availability.

6.6.1.2 Public Access Protections

"Public Access" in this section shall mean widespread, anonymous access.

Revocation information shall be available to Relying Parties and will be publicly available. The CA shall make CRL information available to the expected relying parties.

The University shall make this CPS summary either available upon request to customers and partners, who have agreed terms and conditions to trust certificates issued by the University under this this CPS.

6.6.2 Communications Security

This section is divided into three sections: Intra-CA communications, CA to RA communications, and RA to Subscriber communications. While communications security is necessary at every stage, the threats, vulnerabilities, and technological capabilities change depending on the environment.

Intra-CA Communications: This stage includes communications between the components that make up the certificate manufacturing and signing function. If the CA is part of a managed network, it may also include a domain controller, directory (e.g., LDAP server), and perhaps other components.

CA to RA Communications: RAs are generally co-located with Subscribers, so communications between the RA and CA will typically be inter-network.

RA to Subscriber Communications: The fewest number of assumptions can be made about the RA to Subscriber environment, because of the variety of models for this relationship, and the relative lack of control over the Subscriber. Where there is no RA, this section shall be construed to provide CA to Subscriber communications security requirements.

6.6.2.1 Cryptographic Key Establishment and Management

Cryptographic key management includes all aspects of cryptographic key life cycle: key generation, distribution, storage, access and destruction for both symmetric and asymmetric keys.

Key generation and management shall be performed using software cryptographic service providers, originating from keys generated by an offline Root CA of length 4096 bytes. Keys that are backed up for business continuity shall have protection comparable to the operational key. All cryptographic key management processes shall be described in the CA's CPS.

The CA service shall employ key protection mechanisms using software cryptographic service providers on servers with controlled access in physically secure locations.

Keys that protect the integrity and confidentiality of an enrolment session shall be generated and managed using SSL.

6.6.2.2 Cryptographic Protection

Intra CA communication protection will be provided through network security controls.

CA/RA communication protection will be provided through network security controls.

6.6.2.3 Session Authenticity

No stipulation.

6.6.3 Network monitoring

No stipulation.

6.6.3.1 Events and Transactions to be monitored

No stipulation. Investigate plans to integrate security event information with the University SIEM system.

6.6.3.2 Monitoring devices

No stipulation.

6.6.3.3 Monitoring of Security Alerts, Advisories, and Directives

No stipulation.

6.6.4 Remote Access/External Information Systems

6.6.4.1 Remote Access

For operational reasons, there may be a need to perform remote management of some CA resources. The requirements in this section are meant to allow remote management while maintaining the desired security posture.

6.6.4.2 Bastion Host

No stipulation. Remote access to CAs may be provided via a dedicated terminal server, or by recognised IT services admin workstations using fixed IP addresses.

6.6.4.3 Documentation

The CA shall document allowed methods of remote access to CA systems, including usage restrictions and implementation guidance for each allowed remote access method.

6.6.4.4 Logging

Logging shall be performed on the CA for each remote connection made, consistent with Section 5.4. In particular, logs should include date and time of the connection, the authenticated identity of the requestor, the IP address of the remote system and the actions carried out. Logs shall be maintained on a University SIEM system.

6.6.4.5 Automated monitoring

Not stipulated.

6.6.4.6 Security of Remote Management System

Machines used for remote access to the CA system must be University managed (including patching).

6.6.4.7 Authentication

Any machine used to access CA systems remotely shall require the user to be authenticated with suitable administrative credentials in line with University IT operations policy.

6.6.4.8 Communications Security for Remote Access

All communications between the remote access host and the CA system shall traverse an approved University VPN connection.

6.6.4.9 Penetration testing

Not stipulated.

6.7 Time stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see section 5.4.1).

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Certificates issued by a CA under this policy shall conform to the certificate types as documented within the PKI detailed design.

7.2 CRL profile

CRLs shall be issued by the University of Manchester CA and made available publicly as defined within the PKI detailed design.

7.3 OCSP Profile

Certificate status servers (CSSs) operated under this policy shall sign responses using algorithms designated for CRL signing.

8 Compliance Audit and Other Assessments

CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CPS are being implemented and enforced.

This specification does not impose a requirement for any particular assessment methodology.

8.1 Frequency or Circumstances of Assessment

CAs and RAs shall be subject to a periodic compliance audit at least annually.

8.2 Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA’s CPS and this CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

8.3 Assessor’s Relationship to Assessed Entity

The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organisationally separated from those entities to provide an unbiased, independent evaluation. The Policy Authority shall determine whether a compliance auditor meets this requirement.

8.4 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of this CP and the CA’s CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

8.5 Actions Taken as a Result of Deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the PKI Authorities, the following actions shall be performed:

- The compliance auditor shall note the discrepancy
- The compliance auditor shall notify the parties identified in section 8.6 of the discrepancy
- The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the Policy Authority

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the Policy Authority may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. The Policy Authority will develop procedures for making and implementing such determinations.

8.6 Communication of Results

An Audit Compliance Report shall be provided to the entity responsible for CA operations. The Audit Compliance Report and identification of corrective measures shall be provided to Policy Authority within 30 days of completion. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

Section 2.2 of this policy requires that CA certificates be publicly available. Access to this information will be provided without charge.

9.1.3 Revocation or Status Information Access Fees

CAs operating under this policy will not charge for access to CRLs and OCSP status information.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

No stipulation.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

The CA shall protect the confidentiality of sensitive business information stored or processed on CA systems that could lead to abuse or fraud. For example, the CA shall protect subject data that could allow an attacker to impersonate a subject.

CA information not requiring protection may be made publicly available.

9.3.1 Scope of Confidential Information

No stipulation.

9.3.2 Information not within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

The CA shall adhere to all relevant privacy policy as required by the University of Manchester. A privacy plan shall document what personally identifiable information is collected if any, how it is stored and processed, and under what conditions the information may be disclosed.

Data Protection Policy http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914
Data Protection Officer – Mr Alex Daybank alex.daybank@manchester.ac.uk.

9.4.2 Information treated as private

CAs shall protect all subscriber personally identifying information from unauthorised disclosure. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. The contents of the archives maintained by CAs operating under this policy shall not be released except as allowed by the privacy plan.

9.4.3 Information not deemed private

Information included in certificates is not subject to protections outlined in section 9.4.2.

9.4.4 Responsibility to Protect Private Information

Sensitive information must be stored securely, and may be released only in accordance with other stipulations in section 9.4.

9.4.5 Notice and Consent to Use Private Information

The CA is not required to provide any notice or obtain the consent of the subscriber in order to release private information in accordance with other stipulations of section 9.4.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

The CA shall not disclose private information to any third party unless authorised by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4.7 Other Information Disclosure Circumstances

None.

9.5 Representations and Warranties

The Policy Authority shall:

- Approve the CPS for each CA that issues certificates under this policy;
- Review periodic compliance audits to ensure that CAs are operating in compliance with their approved CPSs;
- Review name space control procedures to ensure that distinguished names are uniquely assigned for all certificates issued under this CP;
- Revise this CP to maintain the level of assurance and operational practicality;
- Publicly distribute this CP; and
- Coordinate modifications to this CP to ensure continued compliance by CAs operating under approved CPSs.

9.5.1 CA Representations and Warranties

CAs operating under this policy shall warrant that their procedures are implemented in accordance with this CP, and that any certificates issued that assert the policy OIDs identified in this CP were issued in accordance with the stipulations of this policy.

A CA that issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- Providing a CPS, as well as any subsequent changes, for conformance assessment.
- Maintaining its operations in conformance to the stipulations of the CPS.
- Ensuring that registration information is accepted only from approved RAs operating under an approved CPS.
- Including only valid and appropriate information in certificates, and maintaining evidence that due diligence was exercised in validating the information contained in the certificates.
- Revoking the certificates of subscribers found to have acted in a manner counter to their obligations in accordance with section 9.6.3.
- Operating or providing for the services of an on-line repository, and informing the repository service provider of their obligations if applicable.

9.5.2 RA Representations and Warranties

An RA that performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the Policy Authority for use with this policy. An RA supporting this policy must conform to the stipulations of this document, including:

- Maintaining its operations in conformance to the stipulations of the approved CPS.
- Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
- Ensuring that obligations are imposed on subscribers in accordance with section 9.6.3, and that subscribers are informed of the consequences of not complying with those obligations.

9.5.3 Subscriber Representations and Warranties

A subscriber (or AOR for device certificates) shall be required to agree the requirements the subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. Subscribers shall:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures.
- Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

9.5.4 Relying Parties Representations and Warranties

This CP does not specify the steps a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. The CA merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation, validation, and CP mappings that the relying party may wish to employ in its determination.

9.5.5 Representations and Warranties of Other Participants

None.

9.6 Disclaimers of Warranties

CAs operating under this policy may not disclaim any responsibilities described in this CP

9.7 Limitations of Liability

No stipulation

9.8 Indemnities

No stipulation.

9.9 Term and Termination

9.9.1 Term

The CP shall document the term for which the CP is effective.

9.9.2 Termination

The CP shall document under what conditions the CP may be terminated.

9.9.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.10 Individual Notices and Communications with Participants

The Policy Authority shall establish appropriate procedures for communications with CAs operating under this policy via contracts or memoranda of agreement as applicable. For all other communications, no stipulation.

9.11 Amendments

9.11.1 Procedure for Amendment

The Policy Authority shall review this CP at least once every year. Corrections, updates, or changes to this CP shall be available to interested parties. Suggested changes to this CP shall be communicated to the contact in section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

9.11.2 Notification Mechanism and Period

No stipulation.

9.11.3 Circumstances under which OID must be changed

OIDs should be changed if there is a change in the CP that reduces the level of assurance provided.

9.12 Dispute Resolution Provisions

The Policy Authority shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.13 Governing Law

No stipulation.

9.14 Compliance with Applicable Law

All CAs operating under this policy are required to comply with applicable law.

9.15 Miscellaneous Provisions

9.15.1 Entire Agreement

No stipulation.

9.15.2 Assignment

No stipulation.

9.15.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.15.4 Enforcement

No stipulation.

9.15.5 Force Majeure

No stipulation.

9.16 Other Provisions

No stipulation.

10 Appendix A – Acronyms

Selected acronyms and abbreviations used in the guide are defined below.

AIA - Authority Information Access
AOR - Authorised Organizational Representative
CA - Certification Authority
CP - Certificate Policy
CPS - Certification Practice Statement
CRL - Certificate Revocation List
CSR - Certificate Signing Request
CSS - Certificate Status Server
DN - Distinguished Name
LAN - Local Area Network
LDAP Lightweight Directory Access Protocol
OCSP Online Certificate Status Protocol
OID - Object Identifier
OZ - Operations Zone
PIN - Personal Identification Number
PIV - Personal Identity Verification
PKI - Public Key Infrastructure
RA - Registration Authority
TAM - Trust Anchor Manager
URL - Uniform Resource Locator
UUID - Universal Unique Identifier
VPN - Virtual Private Network
RA – Registration Authority (e.g. NDES/SCEP server)
CPS – Certification Practice Statement (this document)
NDES – Network Device Enrolment Service (Microsoft SCEP implementation)
SCEP – Simple Certificate Enrolment Protocol
‘University’ or ‘The University’ – The University of Manchester

11 Glossary

Access	Ability to make use of any information system (IS) resource.
Access Control	Process of granting access to information system resources only to authorised users, programs, processes, or other systems.
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Anonymous	Having an unknown name.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.
Authorised Organizational Representative (AOR)	A person (potentially among several) within an organization who is authorised to vouch for non-person identities. Any particular AOR is not permanently linked to any particular non-person identity; the CA must only ascertain that the AOR is legitimately associated with the organisation, and that the AOR is identified as having authority for the identity in question.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioural characteristic of a human being.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CP, the term “certificate” refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a certification authority to perform certificate issuance and revocation.

CA Operating Staff	CA components are operated and managed by individuals holding trusted, sensitive roles.
Certificate Policy (CP)	A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of public key certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
CPS Summary	A publically releasable version of the CPS.
Certificate-Related Information	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates.
Certificate Revocation List (CRL)	A list maintained by a certification authority of the certificates that it has issued that are revoked prior to their stated expiration date.
Certificate Status Server (CSS)	A trusted entity that provides on-line verification to a relying party of a subject certificate's revocation status, and may also provide additional attribute information for the subject certificate. (see OCSP)
Cross-Certificate	A certificate used to establish a trust relationship between two certification authorities.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
End Entity Certificate	A certificate in which the subject is not a CA.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement
Key Exchange	The process of exchanging public keys in order to establish secure communications

Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the public key, it is computationally infeasible to discover the private key.
Key Rollover Certificate	The certificate that is created when a CA signs a new public key with an old private key, and vice versa
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDS are used to uniquely identify certificate policies and cryptographic algorithms.
Online Certificate Status Protocol	Protocol which provides on-line status information for certificates.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses postal service mail to communicate with another party where current communication is occurring on-line).
Policy Authority (PA)	Body established to oversee the creation and update of certificate policies, review certification practice statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an

	authorised CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a Certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Security Auditor	An individual (e.g. employee, contractor, consultant, 3rd party) who is responsible for auditing the security of CAs or Registration Authorities (RAs), including reviewing, maintaining, and archiving audit logs; and performing or overseeing internal audits of CAs or RAs. A single individual may audit both CAs and RAs. Security Auditor is an internal role that is designated as trusted.
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Subscriber	A subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual, an application or network device.
Superior CA	In a hierarchical PKI, a CA that has certified the certificate signature key of another CA, and that constrains the activities of that CA. (See subordinate CA).
Trust List	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorised to act as a representative of a CA in confirming subscriber identification during the registration process. Trusted

	agents do not have automated interfaces with certification authorities.
Trust Anchor Manager	Authorities who manage a repository of trusted Root CA Certificates. They act on behalf of relying parties, basing their decisions on which CAs to trust on the results of compliance audits. A TAM sets requirements for inclusion of a CA's root public key in their store. These requirements are based on both security and business needs. The TAM has a duty to enforce compliance with these requirements, for example, requirements around the supply of audit results, on initial acceptance of a root, and on an ongoing basis. TAMs will follow their normal practice of requiring CAs to submit an annual audit report.
Trusted Certificate	A certificate that is trusted by the relying party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".