Boston Certificate Practice Statement (Baltimore Technologies LTD.)

Secure Hosting Facility - Boston

TITLE PAGE

The information contained in this document is intended for Baltimore Technologies personnel, those persons named as recipients or those persons nominated in the circulation list.

It may contain privileged and confidential information and if you are not the intended recipient you must not copy, distribute or take any action in reliance on it.

If you have received this document in error, please notify the author immediately by reverse charge telephone call and return the original to the sender by mail. You will be reimbursed for postage.

Contact:

Secure Hosting Services

77 A Street

Needham Heights, MA 02494

Tel: 781 455 3300

Fax: 781 455 4082

Signature Director Business Development

Version history

Doc. Version	PVCS Version	Status	Date of Issue	Issued By	Comments
0.1		DRAFT	16NOV2000	TAS	Document Created
0.2		DRAFT	26JAN2001	LMD	Document updated
0.3		Released for Comment	28FEB2001	LMD	Document Updated
0.4		DRAFT	07MAR2001	JPT	Document Updated
0.5		DRAFT	03AUG2001	EXD	Document Updated
0.6		DRAFT	31 Jan 2002	GTR	Document Updated
1.0		Released	13 Mar 2003	KTV	Document Updated
1.1		Released	27 May 2003	GRC	Document Updated

Table of Contents

1 INTRODUCTION

1.1 Overview

This Certificate Practice Statement (CPS) is written expressly for use within the Baltimore Secure Hosting Facility - Boston (Baltimore Technologies LTD.) Public Key Infrastructure (PKI).

The Boston PKI supports the creation and use of asymmetric key pairs and their associated Public Key Certificates. Key pairs and Public Key Certificates are used in the provision of Boston's PKI Certificate services, including but not limited to:

1. authentication services (authentication, integrity, and non-repudiation); and
2. confidentiality services.

This CPS provides information that describes the:

1. practices employed within the Boston PKI to support Certificate services;
2. attendant use of technologies and processes to support the underlying operational infrastructure.

The practices described in this CPS together with the technologies and processes referred to in other specific operational documentation serve to support the trustworthiness and integrity of Boston's Certificate operations from Certificate generation and signing to expiration.

A number of CPS may be operated under the Boston PKI, depending on the commercial arrangements in place between Boston and a Customer and the nature and number of the separate legal entities involved. Each CPS will always have associated specified CP(s).

1.2 Boston PKI Certificate services

Boston's Certificate services provide a range of security and assurance levels to support various commercial electronic transactions.

1.2.1 Standards

This CPS is referred to as the "Certificate Practice Statement Boston".

The structure of this CPS is based on the RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX RFC2527, by S. Chokhani and W. Ford, March 1999. For more information, see the Section - *Standards* in the applicable CP.

This CPS differs from the RFC 2527 standard only to the degree necessary to adequately describe the operational practices used within the Boston PKI.

1.2.2 Certificate types issued

This CPS supports the operation of:

1. nominated Customer CA and RA Certificates issued by the Boston CA;
2. nominated Certificates issued by Boston Customer CAs; and
3. such other Certificates and supporting CP as may be approved by the Boston PAA.

1.2.2.1 X.509 Certificate extensions

Boston complies with the X.509 Version 3 standard. Certificate extensions consist of three fields:

1.	type	this field indicates the type of data in the value field;
2.	criticality	this indicates the importance of the information contained in the value field;
3.	value	this field contains the additional Certificate information.

The Boston PKI supports Certificate extensions to provide additional information about a Certificate, as prescribed within an applicable CP.

Boston will maintain a list of certificate extension Object Identifiers used within its infrastructure.

1.2.2.2 Policy qualifier extension

Boston PKI Certificates use Policy Qualifier extensions. Policy Qualifiers operate to convey important information for the attention of the Certificate Owner or a relying party, including information such as:

1. liability; or,
2. information about the signing authority.

Boston will publish in the applicable CP Policy Qualifiers that have been approved for use within the Boston PKI.

1.2.2.3 Other Certificate extensions

Certificates may be issued containing private or service-oriented extensions. Communities of interest may define these extensions to carry information unique to those communities; for example to include additional attributes in an Attribute Certificate.

1.2.2.4 Criticality of Certificate extensions

Certificate extensions are assigned a criticality value of "true" or "false" during Certificate issuance.

Where the extension criticality extension is:

"true", relying parties must understand the purpose of the extension and adhere to any applicable specific processing requirements, prior to placing any reliance on the Certificate;

"false", the relying party may make their own determination of the importance of the information and of the need to adhere to any specific processing requirements.

Key Usage fields in all Certificates issued within the Boston PKI have a criticality value of "true".

1.2.3 Definitions

This CPS assumes that the reader is familiar with basic PKI concepts, including:

1. the use of digital signatures for authentication, integrity and non-repudiation;
2. the use of encryption for confidentiality;
3. the principles of asymmetric encryption, Public Key Certificates and key pairs;
4. the role of Certification Authorities and Registration Authorities.

Definitions used within this document are based on the ISO Glossary of IT Security Technology[1]. The definitions differ from this glossary only in so far as it is necessary for clarity within the framework of the Boston PKI.

The term "Customer" is used in this CPS to define the entity that is requesting Hosting and Certificate services from Boston and has executed a Hosting Services Agreement with Boston.

[1] Glossary of IT security terminology prepared by JTC1 SC 27 at http://www.iso.ch:8080/jtc1/sc27/27sd698a.htm

The term "Certificate Owner" is used in this CPS to define an entity which requests, obtains, and uses Certificates under the Boston PKI, and who has entered into a Subscriber Agreement with the Boston Customer. This may include any agents, employees, independent contractors, officers, directors, or other such natural persons who have authorization from the Certificate Owner to use Certificates issues by components of the Boston PKI.

1.2.4 X.500 Object Identifier hierarchy

Object Identifiers (OID) have been assigned by Boston and documented in a Configuration baseline document for X.500 OID Schema.

OIDs are assigned to:

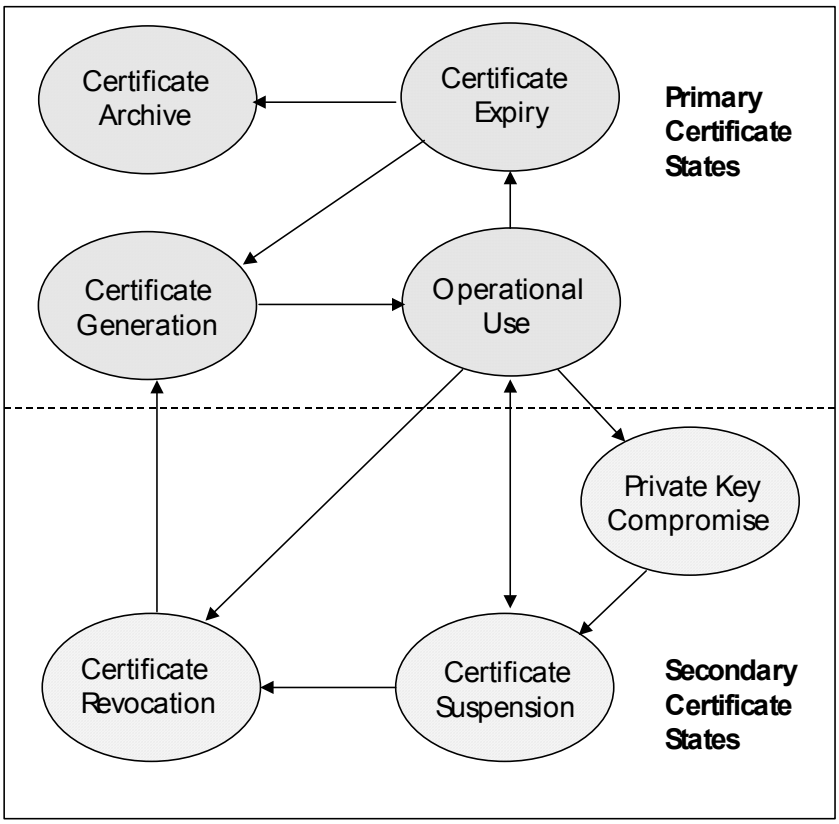
1. each CA and CP within the Boston PKI; and
2. where required, certificate extensions.

OIDs are not assigned to RAs, or to this CPS.

1.2.5 Certificate Management Life Cycle

A Certificate Management Life Cycle (CMLC) is illustrated in Figure 1.1 below. The CMLC applies to all Certificates issued within a PKI.

Figure 1.1 Certificate Management Life Cycle



The CMLC represents the high-level Certificate management process within a PKI. It consists of primary and secondary Certificate states. The primary states are:

1. generation;
2. operational use;
3. expiration; and
4. archive (used only with the UniCERT product when applicable)

All Certificate types issued pass through the first three primary states as part of their life cycle. Some may pass through all four primary states as part of their life cycle.

The secondary states are:

1. compromise;
2. suspension; and,
3. revocation.

Because these secondary states represent exception situations, it is expected that:

1. most Certificates will pass through only the primary states during their life cycle;
2. a small number of Certificates may pass through one or more of the secondary states.

It should be noted that some Certificate states may be supported on a procedural basis only.

The CMLC does not support a provisional Certificate state. Certificates are issued after a Certificate application has been submitted and approved, and are deemed to be in operational use in accordance with the CP.

1.2.5.1 Key Pairs

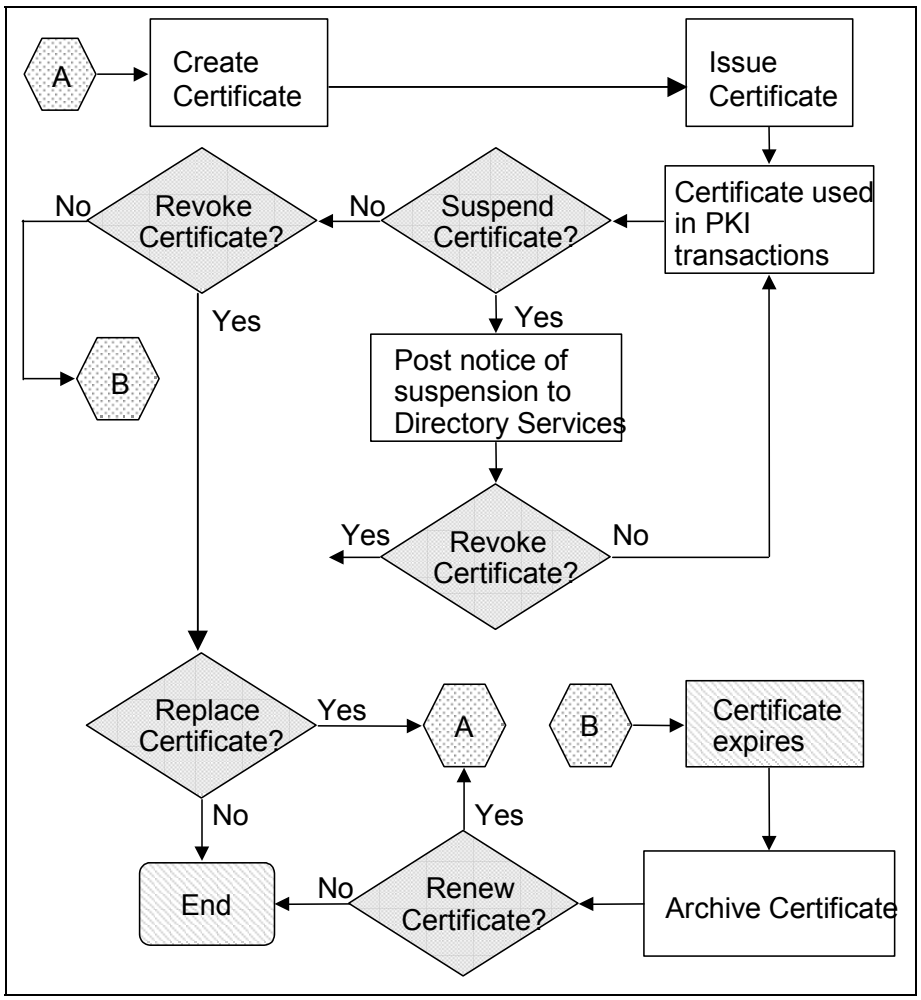
Key pairs are bound to Certificates and are programmed to expire at the same time that the Certificate expires. Key pairs can be registered under more than one Certificate.

Expired key pairs are not re-issued.

1.2.5.2 High level process

The CMLC high-level process is outlined in the decision tree illustrated below.

Figure 1.2 CMLC High Level Process



1.2.5.3 Generation

The Boston PKI generates Certificates upon receipt of an authorized and validated request for:

1. new Certificates; and
2. Certificate renewal (i.e. the generation of new Certificates for Certificate Owners whose Certificates have expired).

Generation involves:

1. receipt of an approved and verified Certificate request;
2. creating a new Certificate;
3. binding the Key Pair associated with the Certificate to a Certificate Owner; and
4. issuing the Certificate and the associated Public Key for operational use under:

– a Distinguished Name associated with a Certificate Owner; and,

– a Baltimore recognized and approved CP.

Generation is performed in a physically secure facility, on the receipt of a properly authorized digital Certificate request. Only an approved Registration Authority (RA) initiates certificate processing.

Certificate requests shall:

1. confirm that the user's name does not appear in its list of compromised users;
2. comply with a nominated registration procedure in a CP including verification of identification and/or employment;
3. comply with all privacy requirements;
4. have approval for the Certificate request; and
5. have an acknowledgement that the Certificate Details can be published on a directory service.

Certificate Owner names are unique and comply with the X.500 standard for Distinguished Names.

1.2.5.4 Operational use

A Certificate comes into operational use upon acceptance of the Certificate by the Certificate Owner in accordance with Section 4.3 of this CPS; and remains in operational use until it:

1. expires; or
2. is suspended or revoked.

A Certificate that is suspended returns to operational use if the suspension is withdrawn, or if a notice of revocation is not received by the end of the suspension period (i.e. "grace period").

1.2.5.5 Certificate lifetimes

Certificates have a fixed operational lifetime that is determined by the PAA. Subordinate CAs and RAs in a PKI are only enabled to support specific Certificate profiles that include validity dates and periods.

The validity period of a Certificate depends on its intended usage and the policy domain within which it is issued. All Certificates are issued with a designated expiration date.

1.2.5.6 Expiration

Certificates expire automatically upon reaching the designated expiration date, at which time the Certificate is archived if this is supported by the Customer's PKI model.

Note that:

1. the life of a Certificate can not be, and is not, extended;
2. expired Certificates cannot be and are not re-issued.

1.2.5.7 Archive

Expired Certificates issued under the CyberTrust model are not archived. Certificates may be archived for a UniCERT customer if that is part of the customer's architecture.

1.2.5.8 Compromise

Certificates in operational use that become compromised are revoked in accordance with a Customer defined procedure, which is consistent with this CPS. Consistent with a nominated CP, Certificates remain in the compromised state for only such time as it takes to arrange for revocation.

1.2.5.9 Suspension

Certificate suspension temporarily invalidates any trusted use of a Certificate.

Certificates are suspended, in accordance with Section 4.4 of this CPS, typically when:

1. there is a suspected compromise of the Certificate Owner's Private Key; or
2. there is a suspected misrepresentation or errors in the Certificate;

Suspended Certificates are added to the PKI X.500 Directory Certificate Revocation List (CRL). A suspension notice warns PKI users that a particular Certificate is under investigation for until the suspension is withdrawn, or the suspension period ends.

Suspension may be used as interim step before revocation is effected. The suspension notice does not set out the reasons for suspension or the results of any investigation. Only the fact of the suspension is provided.

1.2.5.10 Revocation

Certificate revocation permanently invalidates any trusted use of a Certificate.

Certificates are revoked, in accordance with Section 4.4 of this CPS, typically when:

3. there is a compromise of the Certificate Owner's Private Key;
4. there is a misrepresentation or errors in the Certificate;
5. the Certificate is no longer required, including Employee Certificates that are no longer required because the employee has left the employment of the

user organization, etc.

Revoked Certificates are added to the PKI X.500 Directory Certificate Revocation List (CRL).

1.2.5.11 Operational compliance

All Boston Certificate operations comply with:

1. the policy requirements of:
   - a Boston recognized and approved Certificate Policy (CP);
   - a Boston recognized and approved Customer CPS;
   - this CPS;
   - a Boston recognized and approved Certificate Profile; and
   - Boston recognized and approved external and internal security policies and practices.

2. the technology requirements of:
   - applicable guidelines for the physical protection of technology assets;
   - X.500 Directory services;
   - X.509 Certificate format;
   - X.509 Certificate Revocation List (CRL) format;
   - X.500 Distinguished name standards;
   - PKCS#7 format for Digital Encryption and Digital Signatures; and
   - PKCS#10 Certificate Request formats.
   - PKCS#12 Certificate format (public/private) for archiving/retrieval

3. legal requirements of domestic and, where applicable, international privacy legislation;
4. appropriate international and domestic standards applicable to PKI operations; and
5. Boston audit requirements for PKI and/or Certificate operations.

1.2.6 PKI Operational Infrastructure

1.2.6.1 The PKI operational infrastructure:

1. uses Boston approved products to automate key and Certificate management functions;
2. employs a common architectural model under which Certification and Registration functions are separated.

The PKI operational infrastructure comprise three distinct domains:

1. Production Domain, (including the Root CA and subsidiary CA environment);
2. RA Services Domain; and
3. User Services Domain.

1.2.6.2 Production domain

The hierarchy in the Production Domain consists of the Root CA (RCA) and all subsidiary CAs (CAs) that are operated by Boston. The RCA establishes and maintains the PKI while the CAs are responsible for issuing Certificates.

Note that those CAs (including RCAs) which are not the Boston Root CA, are legally Customer entities.

1.2.6.3 RA service domain

The RA Services Domain consists of all RAs that are operated under the Boston PKI. RAs supply Certificate Owner registration and key generation services to Certificate Owners from data collected and verified by the Customer in accordance with an approved Customer CPS.

Note that RAs are legally Customer entities or agents.

1.2.6.4 User service domain

The User Service Domain includes Certificate Owners and relying third parties, which use or rely on Certificates for authentication, integrity non-repudiation, and confidentiality.

1.2.6.5 Validation of digital signatures

The Customer application selected for use within, and supported by, the Boston PKI provides the following functions:

1. verification that the digital signature has been created by the Private Key bound to the Certificate listed for the signing party in the Boston X.500 Directory;
2. a mechanism by which the message, transaction or other file ("signed file") may be checked to determine that it has not been altered since the digital signature was appended.

The Customer application must accomplish these functions by:

1. establishing a Certificate chain[2] for validation of the signature, commencing with the signing party's Certificate and ending with the RCA's Certificate. Note that it is possible to establish more than one Certificate chain for a signature, through cross-certification.
2. where more than one Certificate chain can be established, the Customer application can be utilized to:
   - allow the Certificate Owner various options to manually establish the chain; or,
   - establish a chain through a series of user-defined preferences; or,
   - establish the shortest possible chain; or,
   - validate all possible chains.
3. validating all Certificates in the established chain(s);
4. application of a hash function to the signed file;
5. comparing the resulting hash to the hash that is appended to the signed file, produced using the signing party's Private Key.

A Relying Party is able to verify:

1. the validity of the transaction, by inspecting the applicable CP to ensure the Certificate Owner has acted:
   - in a valid and authorized manner in terms of the Certificate usage allowed by the CP;
   - in compliance with any special requirements of the CP.
2. whether any Certificate in the Certificate's "chain of trust" has been revoked or suspended by checking the applicable CRL in the appropriate X.500 Directory.

1.2.7 Scope

The practices described in this CPS are:

1. based upon but not limited to, the roles, responsibilities, duties and obligations contained within the Boston System Security Plan;
2. binding upon all parties within the Boston PKI, through the inter-linking contractual responsibilities, obligations and duties between:
   - RCAs and their subordinate CAs; and
   - CAs and their subordinate RAs.

[2] A list of Certificates, typically commencing with a Certificate Owner Certificate, then progressing to the Certificates of the Certificate Owner's RA, the issuing CA, and the RCA.

3. binding on those parties who rely on Certificates issued under the Boston PKI through this CPS and the use of COE Baltimore validation services.

This CPS incorporates information from other documents regarding practices involved in the issue, use and validation of Certificates, and in the operational maintenance of the PKI infrastructure. It includes, but is not limited to the:

1. Certificate categories that may be created;
2. functions and obligations of Boston;
3. functions and obligations of Customers;
4. process of approving new Certificate categories and Certificate policy.

1.2.8 Staffing Arrangements

Boston has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of its staff.

The personnel standards, which are typically applied, may require:

1. personnel to undergo a background check;
2. Boston operations staff entering into non-disclosure agreements to protect against the unauthorized disclosure of confidential information; and
3. Boston operations staff being trained in:
   - basic PKI concepts;
   - the use and operation of CA or RA software;
   - documented CA and RA procedures; and
   - computer security awareness and procedures.

1.2.9 Right of Inquiry

Boston reserves the right to make reasonable inquiry in accordance with arrangements agreed with the Customer to determine the validity of a suspension or revocation request.

1.3 Identification

This CPS is referred to as the "Baltimore Secure Hosting Facility - Boston CPS".

Object Identifiers (OIDs) are not applicable to CPS documents.

1.4 Community and Applicability

This CPS supports:

1. all CA and RA services that operate under Boston, i.e., that are within the

Boston "chain of trust";
2. all types of Certificates issued under the Boston PKI.

The practices described in this document allow for a wide range and variety of:

1. Certificate types that have differing levels of information sensitivity and financial value; and
2. Customers.

The practices in this CPS:

1. accommodate the diversity of the community and the scope of applicability within the Boston chain of trust;
2. adhere to the primary purpose of the CPS, of ensuring the uniformity and efficiency of practices throughout the PKI.

In keeping with their primary purpose, the practices in this CPS are the minimum requirements necessary so that Customers are provided an appropriate level of assurance, and that critical functions are provided at appropriate levels of trust. Boston Customers should use this CPS as a minimum baseline for the development of their own documentation.

1.4.1 Policy Authorities

1.4.1.1 Baltimore Secure Hosting - Boston Policy Approval Authority (Boston PAA)

The Boston PAA has been established to maintain the integrity of the policy infrastructure in the Boston PKI.

The Boston PAA performs the following functions:

1. CP approval within the Boston PKI;
2. ensure the integrity of PKI policy structures; and
3. administer subordinate policy infrastructure to maintain the total integrity of the PKI.

The contact details for the Boston PAA are published in each CP within the Boston PKI.

1.4.1.2 Policy Creation Authorities (PCA)

A PCA is responsible for formulating policy relating to a specific part of the Boston PKI, for example for Certificates issued by a specific CA.

Within the Boston PKI, the PCA function for the Boston RCA, and the Boston CA is carried out directly by the Boston PAA. A register of PCAs will be maintained by Boston and published on its web site.

The PCA performs the following functions:

1. formulate new policy and policy changes within the Boston PKI;
2. submit new or changed policies to the Boston PAA for approval.

The contact details for the Boston PAA are published in each CP within the Boston PKI.

1.4.2 Certification authorities

1.4.2.1 Root Certification Authority

The RCA is the highest point of trust within the Boston PKI. The primary purpose of the RCA is to certify subordinate CAs, by digitally signing their Certificates. The Boston RCA self-signs its own Certificate. Customer RCAs self-sign their own Certificates.

The RCA is accessed by dual person control to be used solely for the purpose of creating subordinate CA Certificates.

The key length of the RCA's Signing Key, used to sign Certificates, is as determined by an applicable Certificate profile. Generation of the RCA's keys is performed on a platform in a physically secure facility.

The contact details for the RCA are described and published in each CP within the Boston PKI.

1.4.2.2 Certification Authorities

The primary purpose of the various CAs operating under the Boston PKI is to provide Certificate management services (generation, operational use, compromise, suspension, revocation and expiration) for Certificate Owners within their respective policy domain(s). These CAs consist of:

1. the Boston CA, that provides Certificate management services for customers who do not wish to operate their own CA; or
2. branded client CAs, that operate under a customer's name but are maintained and supported by Boston.

CA key lengths are as determined by an applicable Certificate Profile. Generation of a CA's keys is performed on a platform in a physically secure facility.

The contact details for CAs that operate under the Boston PKI are published in each CP that they issue Certificates under, or the CP may advise a web site address or other location where the contact details may be found.

1.4.3 Registration Authorities

The primary purpose of an RA is to register Certificate Owners. RAs have the responsibility of accepting Certificate applications, authenticating the identity or other credentials of the applicant, then approving or rejecting the application. These obligations are enforced in contract and are set out in a Boston Customer's CPS, CP, and a set of RA Operating Procedures.

Each RA within the Boston PKI is subordinate to a nominated CA; this is a function of the operating hierarchy.

The contact details for RAs that operate under the Boston PKI are published in each applicable CP that they issue Certificates under, or the CP may publish a web site address or other location where the contact details may be found.

In the case of its SureServer certificate offering, Baltimore Technologies outsources the verification and authentication of the applicant's identity and credentials to a trusted third party. Final approval of all SureServer certificate requests is performed by Baltimore.

1.4.4 Certificate Owners

Certificate Owners may be Government agencies, statutory authorities or corporate or natural persons.

A Certificate Holder acts as a Subscriber when they use their keys to encrypt and/or digitally sign a message, transaction or other electronic file.

A Certificate Holder acts as a relying party when they rely on another user's Public Keys to decrypt and/or authenticate a message, transaction or other electronic file.

Certificate Holder key pairs are generated in accordance with the Customer's CPS.

1.4.5 Applicability

Certificates issued by the Boston PKI are used to support secure electronic commerce and the secure exchange of information by electronic means.

The Boston PKI community may regard the practices described in this CPS as:

1. ensuring standard operating procedures and uniform quality of service delivery across the PKI;
2. fostering and promoting appropriate levels of trust and integrity across the PKI.

1.4.5.1 Applicable Certificate usage

The Boston PKI supports a variety of functional classes which are defined by the Customer's CPS and applicable CP.

1.4.5.2 Restricted Certificate usage

Specific restrictions on the use of a Certificate are contained in the CP under which the Certificate is issued. These restrictions may, for example, limit or prescribe the:

1. community of interest;
2. conditions which must be satisfied before a Certificate is used;
3. actual usage of the Certificate; or
4. processing steps or other actions that are to be performed after a Certificate has been used.

Parties within the Boston PKI are to use Certificates only in the manner, and for the purposes, prescribed in an applicable CP. Any use of a Certificate in a manner or for a purpose not in accordance with an applicable CP is not recognized nor supported by this CPS.

1.5 Contact Details

1.5.1 Specification administration organization

Baltimore Secure Hosting Facility Boston administers this CPS.

Enquiries or other communications about this document should be addressed to:

Secure Hosting Manager
Secure Hosting Facility - Boston
77 A Street
Needham Heights, MA 02494

E-mail may be sent to:

Kathleen.Vieira@baltimore.com

2 GENERAL PROVISIONS

2.1 Obligations

2.1.1 Boston Obligations

Changes to this CPS can only be made at the direction of the Boston Manager. Factors that will normally result in change requests include, but are not limited to:

1. a change in the technology supporting the PKI (e.g., ITSEC E3 EPL Approval);or,
2. a change required to ensure compliance with published international standards.

2.1.1.1 Boston PAA Obligations

The Boston PAA has no Certificate practice obligations under this CPS. The Boston PAA's general obligations in regard to approving CP and maintaining the Boston PKI policy infrastructure are detailed in applicable contractual agreements.

2.1.1.2 RCA Obligations

RCAs operating under the Boston PKI discharge their obligations under this CPS by:

1. making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the RCA to operating in compliance with:
   - the applicable Concept of Operations (CONOPS);
   - an applicable contract;
   - this CPS;
   - an approved (if applicable) Customer CPS;
   - an applicable System Security Plan; and
   - applicable internal operational procedures.
2. approving the establishment of all new CAs at any subordinate level in the Boston PKI; and on approval, if applicable, executing an RCA-CA operating agreement;
3. where applicable, maintaining a CPS not in conflict with this CPS, and enforcing the practices described within both;
4. publishing its RCA Hash on the Baltimore Global Hosting Boston web site

and other nominated web sites;

5. issuing Certificates to authorized CAs, that comply with X.509 standards and are suitable for the purpose required;
6. issuing Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
7. publishing issued Certificates without alteration in the X.500 Directory;
8. making reasonable inquiry to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level it deems warranted in its chain of trust;
9. revoking Certificates on receipt of properly authenticated revocation requests, or when its inquiries into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
10. suspending Certificates on receipt of properly authenticated suspension requests;
11. promptly notifying Certificate Owners in the event it initiates revocation or suspension of their Certificates;
12. conducting compliance audits of immediately subordinate CAs when Certificate renewal is due.

2.1.2 CA Obligations

CAs operating under the Boston PKI discharge their obligations under this CPS by:

1. making reasonable efforts to ensure they conduct an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the CA to operating in compliance with:

– the applicable Concept of Operations (CONOPS);
– an appropriate (if applicable) contract;
– all CP under which Certificates are issued;
– this CPS;
– an approved (if applicable) Customer CPS; and
– an applicable System Security Plan.

2. applicable internal operational procedures approving the establishment of subordinate RAs and on approval, (where appropriate) an operating agreement or procedure;
3. enforcing within the sphere of their operations the practices described within this CPS, and an approved CPS applicable to the CA operating environment;
4. publishing applicable CP and CPS on the web site(s) nominated in the CP;
5. upon receipt of a valid Certificate request, issuing Certificates which comply with X.509 standards and meet the requirements of the request;
6. issuing Certificates that are factually correct from the information known to

them at the time of issue, and that are free from data entry errors;

7. publishing issued Certificates without alteration in a nominated X.500 Directory;
8. making reasonable inquiry in accordance with arrangements agreed with the customer to determine the validity of compromises and suspected compromises of Private Keys at any subordinate level they deem warranted in their chain of trust;
9. revoking Certificates on receipt of authenticated digitally signed revocation requests, or when their inquiries into the compromise or suspected compromise of a Private Key have established the validity of a revocation request;
10. suspending Certificates on receipt of properly authenticated suspension requests;
11. promptly notifying Certificate Owners in the event the CA initiates revocation or suspension of a Certificate;
12. maintain a list of suspended or revoked Keys and Certificates, and periodically provide these to an X.500 directory to ensure their publication in a CRL.
13. conducting compliance audits of immediately subordinate CAs and RAs when Certificate renewal is due; and
14. assisting in audits conducted by the RCA to validate the renewal of their own Certificates.

2.1.3 RA Obligations

RAs operating under the Boston hierarchy discharge their obligations under this CPS by:

1. making reasonable efforts to ensure they conduct an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the RA to operating in compliance with:

- the applicable Concept of Operations (CONOPS);
- an appropriate (if applicable) contract;
- all CP under which Certificates are issued;
- this CPS;
- an approved (if applicable) Customer CPS; and
- an applicable System Security Plan.

2. enforcing within the sphere of their operations the practices described within this CPS;
3. accepting End Entity Certificate applications, including authenticating material (including, where relevant, evidence of identity), Certificate information, obtaining a Subscriber Agreement and, where required, a relying party agreement, and accepting or rejecting the application;
4. where required, archiving private confidentiality keys they have generated;
5. verifying the integrity and possession of, and establishing the End Entity's right to use, user generated keys presented for certification;
6. advising End Entities of their obligations under the relevant CP, this CPS and the appropriate Subscriber Agreement and relying party agreement, and providing End Entities with copies of the relevant CP and this CPS or advising them how these documents may be accessed;
7. submitting Certificate requests that comply with X.509 standards and meet the requirements of approved Certificate applications;
8. submitting Certificate requests that are factually correct from the information known to it at the time of issue, and that are free from data entry errors;
9. issuing keys and Certificates to End Entities;
10. inquiring (in accordance with arrangements agreed with the customer) into any suspected compromise which may threaten the integrity of the PKI at any subordinate level within its chain of trust;
11. revoking Certificates in terms of section 4.4.1 - *Circumstances for revocation*;
12. promptly notifying Certificate owners in the event it initiates revocation of their Certificates;
13. maintaining a list of compromised keys and compromised users. The compromised list is to include relevant information regarding the identity of the individual(s) concerned, reasons and causes for inclusion on the list and such other information as might be required to minimise damage or liability to all Boston End Entities. This information is to be protected;
14. keeping such registration records as may be required;
15. assisting in audits conducted by the Boston OCA to validate the renewal of its own Certificates.

2.1.4 Certificate Owner Obligations

Certificate owner obligations are set out in the Customer CPS and any applicable contractual documents executed between the Boston Customer and the Certificate Owner.

2.1.5 Relying party obligations

Relying Parties have no certificate obligations under this CPS.

2.1.6 Repository Obligations

The Boston Repository functions are performed by:

- the Sureserver Site Index for the Server Certificate CA;
- CRL distribution points for Private branded CAs;
- a X.500 Directory for Managed services.

The Boston provides and maintains the operational infrastructure for these repositories. CAs operating under the Boston PKI post Certificates and CRLs to them as appropriate.

2.2 Liability

2.2.1 Boston Liability

Boston has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to inhibit misuse of those resources by authorized personnel or prohibit access to those resources by unauthorized individuals.

These measures include but are not limited to:

1. identifying contingency events and appropriate recovery actions in a Contingency & Disaster Recovery Plan;
2. performing regular system data backups;
3. performing a backup of the current operating software and certain software configuration files;
4. storing all backups in secure local and offsite storage;
5. maintaining secure offsite storage of other material needed for disaster recovery;
6. periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure;
7. periodically reviewing its Contingency & Disaster Recovery Plan, including the identification, analysis, evaluation and prioritization of risks;
8. periodically testing uninterrupted power supplies.

All Boston liability is apportioned in accordance with the applicable contractual agreements.

2.2.2 CA Liability

CA liability arising under this, or any other applicable CPS, is apportioned in accordance with the applicable contractual agreements by and among the CA and other entities within the Boston PKI.

2.2.3 RA Liability

RA liability arising under this, or any other applicable CPS, is apportioned in accordance with the applicable contractual agreements by and among the RA and other entities within the Boston PKI.

2.2.4 Customer Liability

Customer liability arising under this, or any other applicable CPS, is apportioned in accordance with the applicable contractual agreements by and among the Customer and other entities within the Boston PKI.

2.2.5 Fiduciary relationships

Issuing Certificates, or assisting in the issue of Certificates in accordance with this CPS does not make Boston or the Boston Root an agent, fiduciary, trustee, or other representative of Certificate Owners or Relying Parties.

2.3 Interpretation and Enforcement

2.3.1 Governing Law

The law of the Commonwealth of Massachusetts will govern this CPS.

2.3.1.1 Applicable contract structure

The contractual structure that underpins the policies and practices described in this document include, but are not limited to, the:

Service Level Agreement: Describes contractual arrangements under which Boston will offer CA Services to Customers and includes the roles and responsibilities of each party.

Product Licensing Agreement: Describes the license terms and conditions of products sold to Boston Customers and which are operated in conjunction with Boston CA services.

Customer Subscriber Agreement: Establishes a contractual relationship between Boston Customer and Certificate Owners for the provision of services by the Customer; and between a Customer and other entities, such as relying parties, who rely upon the proffered Certificate.

2.3.2 Severability, Transferability, notice

2.3.2.1 Severability

If any one or more of the provisions of this CPS shall for any reason be held to be invalid, illegal, or unenforceable by the law, the unenforceability of that provision shall not affect any other provision of this CPS. This CPS shall then be construed as if the unenforceable provision or provisions had never been contained within it, and as far as possible, construed to maintain the original intent of the CPS.

2.3.2.2 Transferability

This CPS shall be binding upon all entities within the Boston PKI. The rights and obligations detailed in this CPS are not transferable; provided however that Boston may delegate duties under this CPS to outside Boston PKI components engaged by Boston for the operation, maintenance, or deployment of the Boston PKI.

2.3.2.3 Notice

A notice, consent, or request required under this CPS, or an applicable Customer CPS, shall be in a form provided by the relevant contractual agreement.

Specific acknowledgement is not required except as otherwise provided for within the applicable CPS and by the relevant contractual agreement.

2.3.3 Dispute resolution procedures

2.3.3.1 Hierarchy of Certificate policy

If there is a conflict between this CPS and other policies, plans, agreements, contracts or procedures, where the subject of the dispute is between this CPS and:

1. A Customer CPS, this CPS shall prevail
2. A CP, this CPS shall prevail;
3. A Customer Agreement, the Customer Agreement shall prevail; or
4. Any policy, plan, procedures or any other operational or practices documentation whatsoever, this CPS shall prevail, except where documents executed or authorized by Boston expressly change or exclude practices contained within this CPS.

2.4 Publication and repository

2.4.1 Publication of Boston information

This CPS is published under the International Standard Book Number (ISBN) system.

2.4.1.1 Electronic Publication

This CPS is published electronically in PDF format on the Baltimore Boston web site. The PDF file is downloadable from the web site.

2.4.1.2 Hard Copy Publication

Paper copies of this document are available from Boston, for a fee. Requests should be directed to:

Secure Hosting Manager
Secure Hosting Facility - Boston
77 A Street
Needham Heights, MA 02494

2.4.1.3 Publication by CAs

All applicable CAs within the Boston PKI must:

1. publish this CPS and their own CPS (where applicable) on the web site(s) where they publish their CP; or,
2. provide a link on their CP web site(s) to the Boston web site, with an appropriate explanation that the link may be used to access a copy of all applicable CPS.

2.4.2 Frequency of publication

Newly approved versions of CP, Customer CPS, and this CPS shall be published promptly. Certificates are published promptly following their generation and issue. CRL Publication is in accordance with the Customer CPS, which must be consistent with this CPS.

2.4.3 Access controls

There are no access controls on the reading of this CPS or of applicable CP on the web sites nominated for publication.

Access to Certificate information (including CRLs) within the X.500 Directory is limited to a single name search enquiry.

Appropriate access controls are used to restrict to authorized personnel the ability to write to or modify these items.

2.4.4 Repositories

The Repository for the Boston PKI is provided through the Sureserver Site Index, private CRL Distribution points, and a Boston X.500 Directory or another endorsed Directory or repository.

The Repositories do not contain any information of a confidential nature.

The Boston repositories provide the following services to authorized enquirers:

1. advice of Certificate status, including:

– access to CRLs for revoked Certificates;
– access to notices of suspension for suspended Certificates.

2. download facility for all Boston PKI component and Customer Certificates;
3. the directory services provided to an inquirer will span only nominated policy domains.

2.4.4.1 Repository Availability

Guaranteed availability for the repository services is during standard business hours, i.e., 9:00 a.m. – 5:00 p.m. Monday to Friday. If covered under a specific customer agreement, 7 days x 24-hour service is available.

2.4.4.2 Restrictions on Repository access and services

Access to information in a repository is limited to authorized individuals or services. Search inquiries allow an inquirer to determine, within the span of the services provided:

1. if agreed to by the Subscriber, the number of Certificates held by the nominated person;
2. the type of each Certificate; and
3. the status of each Certificate, i.e., valid, revoked or expired.

The repository does not:

1. provide access to End Entities in any manner other than that stated in this CPS;
2. provide any information or services to End Entities other than that information and those services listed in this CPS; or
3. alter any Certificate details or notices that it receives.

Where OCSP responder functions are available with a Directory service, public access to the Directory may be denied, and access only to the OCSP Responder provided for certificate status checking purposes.

2.4.4.3 Repository publication

The Boston Repository promptly publishes new Certificates and changes in Certificate status, including revocation, notices of suspension and expiration.

The X.500 Directory is published on the Boston and other nominated web sites.

Copies of the Directory may be published at such other locations as are required for the efficient operation of the Boston PKI and as may be prescribed in various CP. These copies may contain the whole of the Directory structure or parts thereof.

2.5 Fees

All fees associated with the provision of Certificate services by Boston for Customers are furnished in the applicable contractual agreements.

2.6 Compliance Audit

2.6.1 Frequency of component compliance audit

Any RCA must conduct a comprehensive compliance audit of the practices documented in this CPS:

1. within one year of the commencement of operations of a customer operated CA or RA service, at the sole expense of the customer provided such expense is reasonable in all the circumstances; and
2. at any other time that it deems warranted and at its own expense, provided a minimum of one month's notice is given.

2.6.1.1 CA and RA Certificate Renewal Compliance Audit

All private-branded RCAs may conduct general compliance audits of their CA hierarchy whenever required by their business, at the sole expense of the private-branded CA.

Boston may endorse an audit conducted by a subordinate CA.

A substantial level of non-compliance with any of the following may result in corrective action up to, and including, the RCA rejecting the CA's request for Certificate renewal:

1. Service Level Agreement;
2. various CP under which Certificates are issued;
3. this CPS; or
4. any applicable Customer CPS.

2.6.2 Auditor's relationship to audited party

Aside from the audit function, the audit Boston PKI component shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest.

2.6.3 Topics covered by audit

The topics covered by a compliance audit consist of:

1. physical security;
2. documentation and process;
3. selection of operations personnel;
4. technology;
5. privacy; and
6. financial viability and industry development.

2.6.4 Actions taken as a result of deficiency

Copies of the Audit report are submitted to:

- Manager – Boston; and
- the audited body.

When irregularities are found, the COE Manager shall promptly oversee or implement an appropriate corrective action.

2.6.5 Communication of results

Audit results are considered to be sensitive commercial information. Unless otherwise specified in contract, they are protected in accordance with section 2.8.

2.7 Confidentiality and privacy

2.7.1 Types of information to be kept confidential

Access to confidential information by operational staff is on a need-to-know basis.

Paper-based records and other documentation containing confidential information are kept in secure and locked containers or filing systems, separate from all other records.

2.7.1.1 Registration information

All information collected or held by Boston shall only be used in support of the operations of the Boston PKI, or in support of a compliant transaction.

Personal Information collected in support of this CPS is the responsibility of the Boston Customer. Treatment of such Personal Information is addressed in the Boston Customer CPS and may not be inconsistent with this CPS.

At the time a registration record is created by the RA, information collected includes Personal Information. Some of this information will, pursuant to the *ITU – T Recommendation X.500 (1993) ISO/IEC 9594 – 1: 1993, Information technology – Open Systems Interconnection – The Directory: Overview of Concepts, Models and Services*, and in accordance with the Boston approved Distinguished Name conventions, be included in the Certificate.

Information embodied in a Certificate held as part of the Registration Record, and included in the Certificate and in accordance with the previous paragraph, is not considered to be confidential.

All other information concerning the registration record is considered confidential. This provision does not operate to prevent Publication of the Certificate information.

2.7.1.2 Boston documentation

The following Boston documents are considered to be confidential:

1. CONOPS;
2. Service Level Agreement;
3. Protective Security Risk Review;
4. System Security Plan;
5. Contingency & Disaster Recovery Plan;
6. Configuration Baseline; and
7. Operating Procedures.

2.7.2 Types of information that may be disclosed

2.7.2.1 Certificate information

The information included on the Certificate that identifies the Certificate Owner is not treated as confidential and is deemed to be Public knowledge where:

1. the Certificate is used in its intended fashion;
2. the information appears in a Public directory.

2.7.2.2 Boston documentation

The following Boston documents are public documents and are not considered to be confidential information:

1. CP;
2. this CPS;
3. Security Policy (Public);
4. Privacy Policy (Public).

2.7.3 Disclosure of Certificate revocation/suspension information

2.7.3.1 Disclosure of Certificate suspension information

Information on Certificate suspension is not disclosed. The Directory provides information indicating the fact of suspension, but not the reason for the suspension status.

2.7.3.2 Disclosure of Certificate revocation information

Certificate revocation information contained in the Certificate Revocation List (CRL) shall be publicly available via a Boston X.500 Directory.

Note that information leading to a decision to revoke remains confidential - only the fact of revocation shall become Public through the Boston X.500 Directory.

Access to the Directory shall be via a web page on a single search basis.

2.7.4 Release to law enforcement officials

As a general principle, no document or record belonging to or held by the Boston PKI shall be released to law enforcement agencies or officials except where:

1. a properly constituted warrant is produced or the information is otherwise legally required to be disclosed; and,
2. the law enforcement official is properly identified and has the authority to present the warrant or other similar instrument.

Records are only releasable to law enforcement agencies and officials of those agencies where:

1. a properly constituted warrant is produced or the information is otherwise

legally required to be disclosed; and,

2. the law enforcement official is properly identified and has the authority to present the warrant or other similar instrument.

2.7.5 Release as part of civil discovery

As a general principle, no document or record belonging to or held by the Boston PKI shall be released to any person except where:

1. a properly constituted instrument that has emanated from a court or other authority having legal jurisdiction requiring production of the information; and,
2. the person requiring production is a person authorized to do so.

2.7.6 Disclosure upon owner's request

Certificate Owners are empowered to authorize release of their records to another person. No release of information is permitted without a formal authorization. Formal authorization is addressed in the Customer's CPS or the applicable CP.

2.7.7 Other information release circumstances

No other release of information is permitted unless authorized by a person the information is about, or unless required by law.

2.8 Intellectual Property rights

2.8.1 General Provision

All intellectual property rights including all copyright in all Certificates and all documents (electronic or otherwise) belong to and will remain the property of Boston.

2.8.1.1 Public and Private Keys

Certificate Holders shall have all intellectual property rights in their private keys but not their public keys; provided, however, that Certificate Holders shall not obtain any rights whatsoever in relation to the format or structure of the Certificate that encompasses the Certificate Holder's public key or private key. Boston retains such rights to all public and private keys that are necessary for the deployment, administration and maintenance of the Boston PKI.

2.8.1.2 Distinguished Names

Intellectual property rights in distinguished names vest in Boston unless otherwise specified in a CP, contract or other agreement, e.g., a Customer Agreement.

2.8.2 Copyright

The intellectual property in this CPS is the exclusive property of Boston.

2.8.3 Recognition, authentication, and role of trademarks

Recognition, authentication and the role of trademarks are a commercial issue. Nothing in this CPS shall prevent the use of a trademark in a Distinguished Name.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial registration

3.1.1 Types of names

All Certificate Holders require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The Boston RCA approves naming conventions for the creation of distinguished names for Certificate applicants. Different naming conventions may be used in different policy domains.

3.1.2 Need for names to be meaningful

Distinguished names must be meaningful. Pseudonymous names may be used in the common name component of a distinguished name where requested by a Certificate Owner, provided the Certificate Owner can satisfactorily establish their right to use the pseudonym.

The Boston PKI supports the use of Certificates as a form of identification within a particular community of interest. The Boston PKI does not support anonymous Certificates.

3.1.3 Rules for interpreting various name forms

The normal operation of some types of Certificate generation requires the insertion of an organization name and department as part of the distinguished name.

Where a CP does not require an organization identifier or department identifier in a Certificate, the following changes are to be made to the distinguished name:

Organization name	Not Applicable
Department name	Not Applicable

3.1.4 Uniqueness of names

Distinguished names are to be unambiguous and unique.

3.1.5 Name claim dispute resolution procedure

Any dispute regarding a Distinguished Name is resolved in the applicable Customer CPS.

3.1.6 Method to prove possession of Private Key

The procedure used to prove possession of a self-generated private key is contained in the applicable CP.

3.1.7 Authentication of identity

No exclusively on-line techniques are approved for organisational or individual identification.

3.2 Routine Rekey

Rekey is not permitted after Certificate revocation. Certificate Holders requiring a replacement Certificate after revocation must complete the procedure required for a new Certificate contained in the applicable CP or the Customer CPS.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

It is the responsibility of potential Certificate Owners requiring keys and Certificates to make that request to an approved RA. This procedure is governed by the applicable CP or the Customer's CPS

Certificate applicants must choose the type of Certificate they require. RAs may advise applicants on the functionality, authority levels, security services and other attributes or characteristics of differing Certificate types and may recommend the Certificate type that best suits the applicant's needs. However, the decision to apply for a Certificate is to be made solely by the applicant, and the applicant is to independently assess and determine the appropriateness of any type of Certificate for a specific purpose.

There may be many RAs issuing Certificates for a particular policy domain. These RAs may be differentiated by their geographical proximity to the Certificate applicant, the type of Certificates they are authorized to issue or by their organizational relationship to the Certificate applicant's department.

4.2 Certificate Issuance

RAs and CAs are to take reasonable care in accepting and processing Certificate applications. They are to comply with the practices described in this CPS and with any requirements imposed by the CP under which the Certificate is being issued.

In particular, care should be taken to ensure Certificate information does not contain any factual misrepresentations and that no data entry errors are made when accepting an application or generating a Certificate.

RAs and CAs are responsible for monitoring, inquiring into investigating, and confirming the accuracy of Certificate information after a Certificate has been issued. Where advice is received that Certificate information is inaccurate or no longer applicable, the matter is to be referred to the Agency concerned before any action is taken in relation to the Certificate.

In the case of the SureServer certificate offering, an outsourced authentication service provider:

1. Verifies the existence of the applying company/organization;
2. Verifies the applicant's domain name;
3. Confirms that the certificate requestor is authorized to act on behalf of the organization.

Based on this information, Baltimore Technologies makes the final RA approval decision on all SureServer certificate requests.

4.2.1 Certificate issue process

The Customer CPS or the CP under which the Certificate is issued governs the Certificate issue process. Typically, Certificate issue involves:

1. the Certificate Owner following a registration process required by the Boston Customer's operational model, and described in the applicable CP or CPS. Such processes usually:
   - obtain Certificate Owner's registration details and Certificate information;
   - authenticate critical Certificate information;
   - explain the appropriate CP and CPS, and the responsibilities attached to possession and use of their Public Keys and Certificates to the Certificate Owner; and
   - obtain the Certificate Owner's signature on a Subscriber Agreement.
2. the RA processing the Certificate Owner's Certificate application and submitting a Certificate request to the issuing CA for each Public Key, together with the Public Keys;
3. the issuing CA receiving the Certificate requests and Public Key. On receipt of the request, the CA verifies each request, generates and signs the requested Certificate(s), then:
   - posts the Certificate(s) to the Boston X.500 Directory;
   - issues the Certificate(s) to the RA or end-entity, as appropriate.
4. the RA sending the Certificate Owner notice that their keys and Certificates are available; and
5. the Certificate Owner:
   - installs an approved Customer application on their PC;
   - accesses their keys and Certificates in a secure format.

4.2.1.1 Relying parties

Relying parties need to access nominated Certificates for the authentication of digital signatures and/or decryption of secured files. They may obtain the Certificates they require directly from Certificate Owners, or by requesting Certificates from the Boston X.500 Directory services, if available.

4.2.1.2 Certificate Owner's consent required

Certificates should not be issued:

1. without a Certificate Owner's consent;
2. through an RA other than where the Certificate application was made.

For the purposes of this CPS, a signed Subscriber Agreement is deemed to be the Certificate Owner's specific consent to, and request for the issue of Certificates through the registering RA.

4.2.1.3 CA's right to reject Certificate requests

Certificates are issued at the discretion of the CA receiving a Certificate request. All CAs have the right to reject a Certificate request. If a Certificate request is rejected, the RA is to promptly inform the applicant. CAs are under no obligation to disclose the reason for the rejection of any Certificate request, except where required by the CP under which the Certificate was to have been issued, or by law or government regulation.

4.2.1.4 Operational periods

All Certificates begin their operational period on the date of issue. The operational period of a Certificate is governed by:

1. the Service Level Agreement;
2. the Certificate Profile;
3. the CP;
4. this CPS.

The expiration date of issued Certificates must not result in an operational period greater than that permitted by the above instruments. In the event that a Certificate is issued with a greater than permitted operational period, the Certificate is to be revoked.

4.3 Certificate Acceptance

A Certificate Owner's receipt of a Certificate, and their subsequent use of their keys and Certificates, constitutes Certificate acceptance.

By accepting a Certificate, the Certificate Owner:

1. agrees to be bound by the continuing responsibilities, obligations and duties imposed on them by their Subscriber Agreement, the associated CP, the applicable Customer CPS, and this CPS;
2. warrants that to their knowledge no unauthorized person has had access to the Private Key associated with the Certificate;
3. asserts that the Certificate information they have supplied during their registration is truthful and has been accurately and fully published within the Certificate.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

Revocation can be described as no longer being able to use a Certificate. A Certificate must be revoked when:

1. the Certificate Owner or their keys or Certificates are compromised;
2. a Certificate Owner leaves the Boston community of interest;
3. there is an improper or faulty issue of a Certificate due to:
   - a material prerequisite to the issue of the Certificate not being satisfied;
   - a material fact in the Certificate is known or reasonably believed to be false;
   - data entry or other processing errors;
4. a Certificate Owner generates the keys associated with a Certificate and those keys are found to be weak;
5. material Certificate information becomes inaccurate;
6. a properly formatted request is received from a Certificate Owner;
7. the Certificate of a superior RA or CA is revoked; or
8. any other reasons specifically required in the applicable CP or Customer CPS.

4.4.2 Procedure for revocation request

The procedure for a revocation request, and the entities allowed to initiate a revocation request are detailed in the applicable CP, or the Customer CPS.

4.4.3 Certificate Owner duties

The owner of a revoked Certificate is to:

1. continue to safeguard the Private Key associated with the revoked Certificate, until the date of Certificate expiration; or,
2. securely destroy the Authentication Private Key associated with the revoked Certificate.

4.4.4 Revocation request grace period

Revocation requests are to be:

1. verified on receipt;
2. viewed as appropriate within the processing times stipulated within the applicable CP.

4.4.5 Circumstances for suspension

The Boston CA shall suspend a Certificate where:

1. there are reasonable grounds for believing that the keys or Certificate have been compromised;
2. there are reasonable grounds for believing that the media holding the Private Key is compromised;
3. upon a properly formatted request from the Certificate Owner ; or
4. any other reasons specifically required in the applicable CP or Customer CPS.

4.4.6 Procedure for suspension request

The procedure for a suspension request, and the entities allowed to initiate a suspension request are detailed in the applicable CP, or the Customer CPS.

4.4.7 Limits on suspension period

Suspension shall be no longer than one business day. The suspension notice for the Certificate shall be removed where the CA is reasonably satisfied that:

1. the keys or Certificate have not been compromised;
2. the media holding the Private Key is not compromised.

[Notwithstanding the above, Certificate suspension shall be lifted, or the Certificate revoked, on receipt of a formal notice from the Certificate Owner.]

4.4.8 CRL issuance frequency

The CRL is updated at the CRL issuance frequency stated in the applicable CP.

4.4.9 CRL checking requirements

Relying parties must check the validity and currency of a Certificate prior to reliance on such Certificate.

4.4.10 On-Line revocation/status checking availability

Boston provides various repositories for verifying the status of Certificates issued within the Boston PKI. Boston does not provide signed error message in response to certificate status requests. See section 2.1.6

4.4.11 On-Line revocation checking requirements

Refer to the section *CRL checking requirements.*

4.4.12 Other forms of revocation advertisements available

Some CP may support other forms of revocation advertisement, such as a locally distributed CRL.

Boston operated CAs use only the X.500 Directory for CRLs.

4.4.13 Checking requirements for other forms of revocation advertisements

Where other forms of revocation advertisement are supported, checking requirements are specified in the applicable CP.

4.5 Security Audit procedures

The Boston RCA and all approved Boston CAs and RAs are obliged under contract to maintain, adequate records and archives of information pertaining to the operation of the Public Key infrastructure.

RCA, CA, and RA software automatically preserves an audit trail for the three primary states in the Certificate Management Life Cycle (CMLC) of generation, operational use, and expiration.

4.5.1 Types of event recorded

The minimum audit records to be kept include all:

1. types of registration records, including records relating to rejected applications;
2. key generation requests, whether or not key generation was successful;
3. Certificate generation requests, whether or not Certificate generation was successful;
4. Certificate issuance records, including CRLs;
5. audit records, including security related events; and
6. revocation records.

4.5.2 Frequency of processing log

Audit logs are processed on a daily, weekly, monthly and annual basis.

4.5.3 Retention period for audit log

Audit logs are retained for a minimum of seven years. They are maintained 'on site' for a minimum period of three months and a maximum period of twelve months.

The audit log shall be retained in archives for a minimum period of seven years or such other time (not exceeding ten years) as required. If at the completion of that term, Boston is required by a person to keep the audit log on-line Boston may charge that person a fee for the provision of that service.

4.5.4 Protection of audit log

Audit logs may be encrypted using a key and Certificate specifically generated for the purpose.

4.5.5 Audit log backup procedures

Each Boston PKI component in the Boston PKI is to establish and maintain a backup procedure for audit logs.

4.5.6 Audit collection system

The Boston PKI audit collection system is a combination of automated and manual processes performed by the CA or RA operating system, the CA or RA application, and by operational personnel.

Type of event	**Collection System**	**Recorded by**	**Service type**
Successful and failed attempts to change operating system security parameters.	Automatic	Operating system	UniCERT
Application startup and shutdown.	Automatic	Operating system	UniCERT CMS
Successful and failed login and log-off attempts.	Automatic	Operating system	UniCERT CMS
Successful and failed attempts to create, modify, or delete system accounts.	Automatic	Operating system	UniCERT
Successful and failed attempts to create, modify or delete authorised system users.	Automatic	Operating system	UniCERT
Successful and failed attempts to request, generate, sign, issue or revoke keys and Certificates.	Automatic	CA or RA software	
Successful and failed attempts to create, modify or delete Certificate holder information.	Automatic	CA and RA software	

Type of event	Collection System	Recorded by	Service type
Backup, archiving and restoration.	Automatic and manual	Operating system and operations personnel	
System configuration changes.	Manual	Operations personnel	
Software and hardware updates.	Manual	Operations personnel	
System maintenance.	Manual	Operations personnel	
Personnel changes	Manual	Operations personnel	

4.5.7 Notification to event-causing subject

Operations personnel notify their Security Officer when a process or action causes a critical security event or discrepancy.

4.5.8 Vulnerability assessments

A Protective Security Risk Review (PSRR) has been completed for the entire Boston PKI. This PSRR covers the overarching risks and threats that may impact the Public Key infrastructure.

Individual threat and risk assessments are required at each subordinate component level e.g., approved CA and RAs.

4.6 Records Archival

Each Boston PKI component maintains an archive of applicable records described in this policy.

4.6.1 Types of event recorded

The following audit information is recorded and archived by Boston PKI components:

1. audit logs;
2. Certificate request information;
3. Certificates, including CRLs generated;
4. Complete back up records;
5. formal correspondence; and

6. Policy and Practice documentation.

4.6.2 Retention period for archive

4.6.2.1 Secure maintenance of keys

Only Public Keys are archived with the Certificate.

4.6.2.2 Secure maintenance of Certificate

The period for archiving Certificates shall be a minimum period of seven years from the date of expiration or such other time (not exceeding ten years) as required by the applicable Customer CPS or CP. At the completion of that term, the Certificates may be transferred to an external storage facility for which a fee shall be charged.

4.6.2.3 Term of archive maintenance

Audit trail information is kept for a minimum period of seven years from the date of generation, unless another period is specifically required.

4.6.3 Protection of archive

Archive media is protected either by physical security, or by a combination of physical security and cryptographic protection.

4.6.4 Archive backup procedures

Each Boston PKI component has established archive back up procedures to ensure and enable complete restoration of current service in the event of a disaster situation.

4.6.5 Requirements for time-stamping of records

A trusted Time Source is available to all CAs operating under the Boston PKI. The Boston time source is acquired from the Global Positioning System.

Trusted third party time stamping is not presently supported.

Nothing in this CPS will operate to prevent an RA or other third party from offering that service outside of this CPS.

4.6.6 Archive collection system

Each Boston PKI component is to establish an archive collection system that meets the requirements of this CPS.

4.6.7 Procedures to obtain and verify archive information

The integrity of a Boston PKI component's archives are verified:

1. at the time the archive is prepared;
2. annually at the time of a programmed Security Audit;
3. at any other time when a full security audit is required.

4.7 Key changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates. With the exception of the RCA which issues a new Certificate and new keys to itself, all parties within the Boston PKI are to obtain new keys by making an application for a new Certificate a minimum of one month prior to Certificate expiration.

4.8 Compromise and Disaster Recovery

Each Boston PKI component:

1. has established and maintains detailed documentation covering its:
   - Contingency & Disaster Recovery Plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood;
   - Configuration Baseline, including operating software, anti virus software and PKI specific application programs;
   - backup, archiving and offsite storage procedures;
2. provides the above documentation on the request of:
   - the RCA when conducting a CPS practices audit;
   - persons conducting a security or compliance audit;
3. provides appropriate training to all applicable staff in contingency and disaster recovery procedures;
4. at least annually tests its Contingency & Disaster Recovery Plan with the minimum test activity being the full restoration of operational services as follows:
   - the current operational platform is shut down and disconnected from communications links;
   - system operating software, application programs and operational data is restored onto a new hardware platform, solely from backup media and in compliance with the Configuration Baseline;
   - the restored service is connected to the communications links and the correct operation of its Certificate services tested;
   - service operations are resumed using the original operational platform. All files on the hard disk of the test platform are securely deleted;

– the Contingency & Disaster Recovery Plan is reviewed in the light of the test results.

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

Each Boston PKI component has established a configuration baseline plan, and back-up, archiving and response plan to provide data for identifying component failure and subsequent service restoration.

4.8.2 Component Certificate is revoked

Each Boston PKI component has established a key compromise plan that addresses the actions to be taken in the event that the RCA or CA Certificate is revoked.

CAs and RAs are to promptly advise the superior RCA of any compromise or suspected compromise of their Private Keys.

4.8.3 Component Private Key is compromised

Each Boston PKI component has established a key and user compromise plan that addresses the actions to be taken in the event that a Private Key is compromised.

4.8.4 Secure facility after a natural or other type of disaster

Each Boston PKI component manages its backup, archive and offsite storage in accordance with its configuration baseline plan, and back-up, archiving and response plan.

4.8.5 Contingency & Disaster Recovery Plan

The purpose of this plan is to restore core business operations as quickly as practicable when fire, strikes, etc have significantly and adversely impacted systems operations.

The plan should acknowledge that any impact on system operations will not cause a direct and immediate operational impact within the PKI of which the Boston PKI component is a part. Recovery actions approved within the plan should be given a priority that is in keeping with the recovery of other organizational records that do not have a direct and immediate impact on the organization's operations.

To implement a Contingency & Disaster Recovery Plan, a Boston PKI component:

1. identifies an internal owner for the plan;
2. identifies individuals authorized to initiate disaster recovery action;
3. identifies major elements at risk, for example;
– operational hardware;
– CA or RA software application;
– logical records.
4. identifies criteria that might prompt disaster recovery initiation;
5. implements recommended precautionary measures such as setting up:
– an Uninterruptible Power Supply; and
– power surge protectors.
6. considers secondary precautionary measures that may be required, such as:
– a second power supply using an alternate power source;
– a backup site; and
– trained backup staff.
7. develops recovery actions and timeframes;
8. prioritizes recovery actions from most significant to least significant;
9. maintains a record of the hardware and software configuration baseline; and
10. maintains records of the necessary equipment and procedures required to recover from an unexpected event such as a hardware failure, including the intended maximum period that the system is to be down.

To support the disaster recovery plans of associated RAs, private-branded CAs will:

1. maintain dedicated hardware specifically for RA disaster recovery support; and
2. configure and deliver a new hardware platform to RAs who experience hardware failure.

4.9 CA Termination

When it is necessary to terminate a CA service, the impact of the termination is to be minimized as much as possible in light of the prevailing circumstances. This includes:

1. providing as much prior notice as is practicable and reasonable to:
– the RCA; and
– all subordinate entities;
2. the progressive transfer of the service, and operational records, to a successor CA; and
3. preserving any records not transferred to a successor CA.

4.9.1 Notice

In the event of an emergency shut down of a CA, e.g., due to the compromise of the CA's private key, the CA will provide subordinate RAs with as much notice as is practical and reasonable under the prevailing circumstances. All keys and Certificates are to be revoked by the CA immediately and prior to the emergency shut down. The same or a successor CA should recommence services as quickly as possible after the shut down has been effected.

4.9.2 Certificate Holder keys and certificates

In the event that it becomes necessary to terminate a CA:

1. all subordinate Certificate Holder keys and certificates may need to be revoked prior to the shutdown; or
2. all subordinate Certificate Holder keys and certificates may need to be transferred to a Successor CA, provided the transferred certificates do not become operational within the chain of trust of the replacement CA service until after the shutdown of the terminating CA service; or
3. all Certificate Holder certificates may need to be revoked prior to the shutdown of the terminating CA service, and the Certificate Holder keys may be transferred to the successor CA service for the issue of new certificates, provided that such new certificates are not generated until after the shutdown of the terminating CA service.

Where practical, key and Certificate revocation should be timed to coincide with the progressive and planned rollout of new keys and Certificates by a successor CA.

Compensation or restitution to Certificate Holders for the revocation of their Certificates prior to their expiration date is a contractual matter that falls outside the scope of this CPS.

4.9.3 Successor CA CP

The CP under which a successor CA issues Certificates is a contractual matter between the stakeholders and is outside the scope of this CPS. In principle, however, to the extent that it is practical and reasonable:

1. the successor CA should assume the same rights, obligations and duties as the terminating CA;
2. the CP under which the successor CA issues Certificates should impose the same requirements and confer the same benefits as the CP under which the terminating CA issued Certificates;
3. the successor CA should issue new keys and Certificates to all subordinate Boston PKI components and Certificate Holders whose keys and Certificates were revoked by the terminating CA due to its termination,

subject to the individual Boston PKI component or Certificate Holder making an application for a new Certificate, and satisfying the CP initial registration and identification requirements, including the execution of a new Boston PKI component or Subscriber Agreement. Note that the section *Rekey after revocation* prevents the successor CA from renewing Certificates, and that the initial applications by Boston PKI components and Certificate Holders to the successor CA must be for new Certificates.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The site location of the Boston is in a secure office environment occupied by Baltimore Technologies.

The CA service operates within a highly secure physical environment within the office area.

5.1.2 Physical access

Boston permits entry to its secure operating area only to authorized personnel, and to visitors under the constant supervision of an authorized person. The number of personnel authorized to enter the area is kept to a minimum and a log is maintained of all accesses.

5.1.3 Power and air conditioning

The RCA secure operating area is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The UPS is also backed up with a diesel generator to prevent any disruptions due to extended power outages.

The area has an air conditioning system to control the heat and humidity that is independent of the building air conditioning system.

5.1.4 Water exposures

The RCA secure operating area is protected against water exposure by being located on a floor above ground, of an office building that is not in a flood zone.

5.1.5 Fire prevention and protection

Fire suppression systems has been installed as well as fire extinguishers being maintained in the secure operating area, to guard against the possibility of fire.

5.1.6 Media storage

All magnetic media containing RCA information, including backup media, are stored in containers, cabinets or safes and are located either within the RCA service operations area or in a secure off-site storage area.

5.1.7 Waste disposal

Paper documents and magnetic media containing the RCA Private Key or commercially sensitive or confidential information are securely disposed of by:

1. in the case of magnetic media:
   - physical damage to, or complete destruction of the asset;
   - the use of an approved utility to wipe or overwrite magnetic media;
2. in the case of printed material, shredding, or destruction by an approved service.

5.1.8 Off-site backup

Endorsed off site storage agents are used for the storage and retention of backup software and data.

The off site storage:

1. is available to authorized personnel 24 hours per day seven days per week for the purpose of retrieving software and data;
2. has appropriate levels of physical security in place.

5.2 Procedural Controls

5.2.1 Trusted roles

In order to ensure that one person acting alone cannot circumvent the entire system, multiple roles and individuals share responsibilities at a CA service workstation. Oversight may be in the form of a person who is not directly involved in issuing Certificates examining system records or audit logs to ensure that other persons have acted within the realms of their responsibilities and within the stated security policy.

This is accomplished by creating separate roles and accounts on the CA service workstation, each of which has a limited amount of capability. This method allows a system of "checks and balances" to occur among the various roles. At a minimum, the following roles are established:

1. System Administrator;
2. Registrar (RAs only);
3. Security Officer.

5.2.2 Number of persons required per task

Separate individuals fill each of the three roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However:

1. a single individual may assume the roles of the System Administrator and Registrar;
2. the Security Officer must always remain separate from the System Administrator in order to provide an independent review of the audit log;
3. any task requiring the creation, backup or importation into a database of a Boston PKI component Private Key must involve two trusted persons, one performing the function and the second fulfilling a security monitoring role.

5.2.3 Identification and authentication for each role

Persons filling trusted roles must undergo a formal background check conducted by Choicepoint, designated "Position of Trust".

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The recruitment and selection practices for Boston services personnel take into account the background, qualifications, experience, and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.2 Background check procedures

Choicepoint conducts background checks on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

5.3.3 Training requirements

All Boston services personnel staff are trained in:

1. basic PKI concepts;
2. the use and operation of the PKI software;
3. documented CA procedures; and
4. computer security awareness and procedures.

5.3.4 Retraining frequency and requirements

Boston staff receive a security briefing update at least once a year.

Training in the use and operation of the CA software is provided when new versions of the software are installed.

Remedial training is completed when recommended by audit comments.

5.3.5 Job rotation frequency and sequence

Boston may implement formal job rotation practices. Where formal job rotation is not implemented, cross-training activities are conducted to ensure operations continuity.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions by Boston staff are submitted to staff members with the appropriate authority including, but not limited to, the Security Officer.

5.3.7 Contracting personnel requirements

Boston personnel may be contractors who are appointed in writing and given written notification of the terms and conditions of their position. Contractors may not be used in trusted roles.

5.3.8 Documentation supplied to personnel

Boston personnel have access to all applicable:

1. hardware and software documentation;
2. policy documents, including this CP; and
3. operational practice and procedural documents, including any applicable CPS.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

The Boston Key Management Plan governs Boston RCA Key Pair generation and installation. Customer Key Pair generation and installation is governed by the applicable Customer documentation. If the Customer is hosted by the Boston, the Customer Key Pair generation follows the Boston Key Management Plan and all comparable storage and hardware controls are in place for the Customer keys.

6.1.2 Private Key delivery to entity

The self-generated RCA Private Keys do not require delivery. CA, RA, and Certificate Owner Private Key delivery is governed by the applicable Customer documentation.

6.1.3 Public Key delivery to Certificate issuer

The self-generated RCA Public Keys do not require delivery. CA, RA, and Certificate Owner Public Key delivery is governed by the applicable Customer documentation.

6.1.4 CA Public Key delivery to users

CA Public Keys do not require delivery.

6.1.5 Key sizes

An applicable Certificate Profile determines the RCA key lengths. All other key lengths are governed by the applicable Customer documentation.

6.1.6 Public Key parameters generation

The parameters used to create Public Keys are generated by the RCA.

6.1.7 Parameter quality checking

The quality of Public Key parameters is automatically checked by CA software.

6.1.8 Hardware key generation

RCA key generation is performed in a FIPS 140-1 compliant hardware device as prescribed by security policy. ICC's are not used for CA key generation. CA, RA, and Certificate Owner key generation is governed by the applicable Customer documentation

6.1.9 Key usage purposes

Keys may be used for the purposes and in the manner described in Section 1.3.4 *Applicability*. Such key use is governed by the applicable Customer documentation, which may not be inconsistent with this CPS.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

Cryptographic modules that may be in use from time to time as part of the operations of the RCA comply with industry standards. Customer use of cryptographic modules is governed by the applicable Customer documentation, which may not be inconsistent with this CPS.

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

Private Keys are not under n out of m multi-person control.

6.2.3 Private Key escrow

Private Key escrow is not supported.

6.2.4 Private Key backup

The RCA Private Key is stored in an encrypted database, which is backed up under further encryption with backup copies maintained on site and in secures off site storage. Customer and Certificate Owner Private Key backup is governed by the applicable Customer documentation.

6.2.5 Private Key entry into cryptographic module

Where a cryptographic module is used, the Private Key must be generated in it and remain there in encrypted form, and be decrypted only at the time at which it is being used.

6.2.6 Method of activating Private Key

The CA software activates RCA Private Keys, following the successful completion of a login process that requests and validates an authorized control mechanism for user access. Certificate Owner Private Keys are activated in accordance with the applicable CP or Customer CPS.

6.2.7 Method of deactivating Private Key

Private Keys are de-activated when the RCA software application is terminated. Certificate Owner Private Keys are deactivated in accordance with the applicable CP or Customer CPS.

6.2.8 Method of destroying Private Key

The RCA software destroys Private Keys in memory by overwriting them with zeros when the software shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key archival

The RCA archives its Public Key.

6.3.2 Usage periods for the public and Private Keys

The usage period for the RCA private and Public Key is ten years.

6.4 Activation Data

No activation data other than access control mechanisms is required to operate cryptographic modules.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The Boston has established a System Security Plan that incorporates computer security technical requirements for the operation of the RCA.

6.5.2 Computer security rating

The Boston has established a System Security Plan that incorporates computer security ratings for the operation of the RCA.

6.6 Life Cycle Technical Controls

6.6.1 System development controls

Boston operational software is developed in a controlled environment employing appropriate quality controls.

6.6.2 Security management controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in the section *Trusted roles*.

6.6.3 Life cycle security ratings

The Boston has established a Protective Security Risk Review that identifies and addresses all high or significant life cycle security threats.

6.7 Network Security Controls

The Boston has established a Protective Security Risk Review that identifies and addresses all high or significant network security threats.

6.8 Cryptographic Module Engineering Controls

The Boston has established a Protective Security Risk Review that identifies and addresses all high or significant cryptographic module engineering security threats.

7 CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

The Boston supports and uses X.509 Version 3 Certificates, which contain v.3 in the version field.

7.1.2 Certificate extensions

The Boston supports and uses X.509 Version 3 Certificate extensions.

7.1.3 Algorithm object identifiers

OIDs are not allocated to algorithms supported and used within the Boston PKI.

The following hashing/digest algorithms are supported:

1. Secure Hash Algorithm-1 (SHA-1)
2. Message Digest 5 (MD5)

The following padding algorithms are supported:

1. ISO 9796
2. PKCS#1

The following encryption algorithms are supported:

1. RSA
2. DES

The use of multiple algorithms within the same hierarchy is supported.

7.1.4 Name forms

Certificates issued by a CA contain the full X.500 distinguished name of the Certificate issuer and Certificate subject in the issuer name and subject name fields.

7.1.5 Name constraints

Anonymous names are not supported.

7.1.6 Certificate policy Object Identifier

OIDs are carried in the standard extension field of X.509 Certificates and are published in the CP.

7.1.7 Usage of Policy Constraints extension

The Boston supports the use of the Policy Constraints extension.

7.1.8 Policy qualifiers syntax and semantics

The Boston supports the use of syntax and semantics policy qualifiers.

7.2 CRL Profile

7.2.1 Version number(s)

The Boston supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The Boston supports and uses X.509 Version 2 CRL entry extensions.

8 SPECIFICATION ADMINISTRATION

Boston operates a Policy Approval Authority, which is responsible for setting Certificate policy direction for the overall Public Key infrastructure. Contact details for the PAA appear in each CP applicable to the Boston PKI.

A Policy Creation Authority is normally vested at the CA or equivalent level in a PKI hierarchy. In the case of the Boston PKI, the PAA and PCA functions are vested in the same authority, the PAA.

Each CP used under the Boston PKI has been allocated an OID which:

1. provides a unique identification for the CP;
2. includes a policy version number.

8.1 Specification change procedures

8.1.1.1 Initial publication

The PAA is the responsible authority for changes to a CP. New CAs apply to the PAA for:

1. formal endorsement of the CP under which they will issue Certificates;
2. the allocation of an OID.

After the CP has been approved and the OID has been granted, the CA:

1. publishes, on a nominated web site, the CP together with this CPS;
2. advises all subordinate parties of the CP and its applicability;
3. forwards a copy of the CP to each subordinate RA, together with an advice regarding the web site of the master CP.

8.1.2 Change

There are two possible types of policy change:

1. the issue of a new CP;
2. a change to or alteration of an existing policy.

If an existing policy requires re-issue, the change process employed is the same as for as for initial publication, as described above. Note that the new OID issued for a policy change differs from the previous OID only in the policy version number.

8.2 Publication and notification policies

New or amended CP is published on the web site nominated in the CP.

The appropriate CA notifies subordinate parties of changes to a CP as and when they are approved. Subordinate CAs and RAs are advised of the changes a minimum of one week prior to publication.

8.3 CPS approval procedures

The Boston PAA must endorse CP intended for use under the Boston RCA. A document setting out the functions of the Boston RCA PAA is made available to all subordinate parties responsible for creating or amending CP, the document is also made available to any approved person conducting a security audit.

8.3.1.1 Revisions

This CPS undergoes a regular review process as prescribed by the Boston Policy Approval Authority (PAA). Revisions of this document are identified through a configuration baseline schema and numbering convention.

9 APPENDIX A – CPs SUPPORTED UNDER THIS CPS

The following CPs are supported under this CPS:

1. Boston RCA CP;
2. Boston CA CP.