Unisys Internal PKI Certificate Policy

Unisys Corporation

April 27, 2021

Content:	**This document contains the text for the Certificate Policy, which will govern the issuance and management of Certificates for the Unisys Internal PKI.**
Name:	**Unisys Internal PKI Certificate Policy**
Version / Last Revision:	**See header**
Classification:	**Public document**

Approval:

Responsible	**Name**	**Date**	**Signature**
Unisys InfoSec / PMA	Christopher Hawley		
Unisys UIT	Mat Newfield		

Compliance Status:

Compliance needed with Document	**Status**	**Remarks**
Not applicable		CP is the governing document that will establish high level criteria for all other project requirements documents.

Contents

Part 1 Document Information

History

History Version	Changes
Version 1.0	First published version 5-15-2004
Version 1.1	Typographical corrections; Section 6.2.9 Method of Destroying Subscribers Private Key, destruction of only private signing keys specified at time of certificate revocation. 5-12-2005
Version 1.2	Incorporation of stand-alone Registration Authority in the UIPKI. 4-12-2007
Version 1.3	Incorporation of wild card SSL certificates; correction of security level of smart cards / tokens; indemnification exception for Employees; correction of typos; staff and organizational name changes. 1-14-2008
Version 1.4, September 2008	Sec 4.5.1 Clarify Auditable events
Version 1.5 March 2009	For mobile users without a computer capable of generating certificates, we allow certificate generation to be requested by the user's manager. Section 4.1 Staff name changes
Version 1.6 June 1, 2009	3.4 Authentication for Certificate Revocation: allow automated certificate revocation process 4.2.1 Allow generation of Subscriber's private key on the Registration Authority
Version 1.7, April 7, 2010	6.2.1 Clarification that cryptographic modules holding End User keys must correspond to FIPS 140-1 level 2 or better. 9.1 Correction of definition of FIPS 140-1. Update of current staff names
Version 1.8, April 15, 2011	p10 Contacts table update 1.4 Update Contact address and details 2.4.2 Update Unisys address for General Counsel 3.2.1 Authentication for Routine Rekey or Renewal -- . The UICA private key(s) will be destroyed at the end of the CA certificate life cycle. 4.4.1 Circumstance of Revocation – destruction of CA private keys 6.1.5 Key Sizes – show change to 2048 bits effective 4Q2011
Version 1.9, 06 February 2012	Part 1 Alignment with CA Browser Forum
Version 1.10, 11 June 2013	Misc typos;
Version 1.11, 09 April 2014	-Formatting changes and misc typos -4.8.3 Fixed lettering for items in the "After addressing" section

	-p12 Included requirement to update CP annually based on CABF updates -1.2 SSL certificates follow CABF Baseline Requirements -Acronyms – addition of CABF
Version 1.12, 28 March 2015	-Add Basic Assurance Level 4.1 Add a statement that Certification Authority Authorization (CAA) DNS Resource Records are not in use.
Version 1.12a, 08 August 2015	Change legal review to Michelle Beistle
Version 1.14, 28 April 2017	Changes in Unisys staff roles: a-Contacts, b-responsible Reviewers, c-1.4 Contact details. Add CA Browser Forum to the Definitions. Updates per CA Browser Forum. a-7.1.9 Certificate Serial Numbers – establishing compatibility with CA Browser Forum. b-4.4.1 Circumstances for revocation – adding suspected misuse of Private Key as a reason for required revocation. c-3.1.9 Authentication of Devices and Applications – state validation of request via FQDN method and collateral acceptance. d-3.1.9 State conformance with CA Authorization Record checking requirements. e-6.3.2 State maximum allowed lifetime of external SSL certificates f-3.1.9 State validity period of any checking on authority of requestor to obtain external SSL certificates Remove Legal Review
Version 1-15, 09 April 2018	2.7.6 Audit results will be made public per CABF Baseline Requirements. 1.3.2; Glossary Removal of Certificate Manufacturing Authority provision. Statement that any delegation from a CA to an entity such as an RA can only involve an RA within the UIPKI, i.e., no delegated third parties are permitted. 4.1 Added statement of the mechanism for verifying Unisys ownership of domains to which SSL certificates are issued. 4.4 Revocation updates 5.3.3 Training requirements updated 2.2.2 Warranties updated to CABF 2.4.2 Severability updated to CABF 4.4 Certificate Suspension and Revocation updated to CABF

Version 1-16, 30 March 2020	4.7 Changed reference to issuing certificates after a CA has been rekeyed to restrict it only to end-entity certificates. This will allow for OCSP Responder certificates to be issued. 6.1.5 Added ECC algorithm 6.1.5 Updated from SHA-1 to SHA-2
Version 1-17, 27 April 2021	Remove references to external SSL certificates. Removed references to web enrolment page Updated author name

Management Summary

Certificate Policy

- A single Certificate Policy will be published to support the issuance of all types of Certificates at various Assurance Levels by Unisys Internal CAs.
- This Certificate Policy has been developed in accordance with the policy mapping guidelines for U.S. Federal Bridge compliance**.**
- The body of this document will be published on the Unisys Internal PKI web site and will be incorporated by reference in all agreements related to the provision of Unisys Internal PKI services.

Contacts

Responsible	Name	E-Mail Address
Authors	Grae Crofoot	grae.crofoot@unisys.com
Business Review	Mat Newfield	mathew.newfield@unisys.com
InfoSec Review	Christopher Hawley	christopher.hawley@unisys.com

Part 1 – Background

Preamble

Unisys Corporation (Unisys) has established the Unisys Internal Public Key Infrastructure (UIPKI) to provide Certificate based security services for the benefit of the Corporation, its Business Associates and Employees in doing business with and for Unisys.

The Unisys Internal PKI is a closed PKI. The community of persons and Entities authorized to rely on UIPKI Certificates is limited to Employees of the Corporation, Business Associates of the Corporation and the Corporation itself. A *third party* who is not an Employee or Business Associate engaged in Unisys business cannot be a Qualified Relying Party and may not rely on Certificates issued in accordance with this Certificate Policy (CP).

Introduction

This CP establishes the minimum requirements to issue, maintain, use, and rely upon Certificates that reference this CP. The terms and conditions of this CP including all limitations on liability are binding on all Users.

The policy specification (Part 2) follows and complies with the Internet Engineering Task Force Public Key Infrastructure Working Group (IETF PKIX) RFC2527 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework,* March, 1999(RFC2527).

The technical requirements stipulated in this CP, which relate to the structure and content of Certificates, follow and comply with IETF PKIX RFC3280 *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,* April, 2002 (=X.509v3”).

This document uses many terms and acronyms associated with public key technology. For those not familiar with this technology, definitions and acronyms are provided in the Glossary section. In addition, some common terms are given specific definition in the Glossary. Throughout this document, defined terms are capitalized. Because of the importance of a Certificate Policy in establishing trust in a public key Certificate, it is fundamental that the CP be consulted, understood and followed not only by Subscribers but also by all Qualified Relying Parties.

Certificate Policy Concepts

When a Certification Authority (CA) issues a Certificate, it provides a statement to the Certificate User that a particular Public Key is bound to a particular Entity. Different Certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes. The X.509 standard defines a Certificate Policy as "a named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements."

A CP states what Assurance Level can be placed in a Certificate. In this context, the term ‘Assurance Level’ is used to represent the degree of confidence that a Qualified Relying Party can have regarding the legitimacy of the identity binding between the Public Key and the subject name cited in the Certificate.

The Assurance Level also reflects the degree of confidence the Qualified Relying Party can have regarding the Subscriber's maintenance and control of the Private Key that corresponds to the Public Key in the Certificate, and how securely the system, which was used to produce the Certificate, performs its task.

UIPKI Certificates contain a policy Object Identifier (OID), which may be used to determine whether a Certificate may be trusted for a particular purpose. These OIDs correspond to the Certificate's Assurance Level as well as any restrictions on the appropriate use of the Certificate as defined in this CP. Each UIPKI CP OID is defined in Section 1.2 (Identification).

Certificate policies constitute a basis for accreditation of CAs. Each UIPKI CA must be accredited to issue Certificates containing one or more of the UIPKI CP OIDs.

Certificate policies are also used to establish a trust relationship between CAs (Cross-Certification). When CAs issue Cross-Certificates, one CA assesses and recognizes one or more Certificate policies of the other CA. When a trust relationship is established directly between two CAs or indirectly through Intermediate CAs, the X.509 Certification Path processing logic is employed to identify a common Certificate policy OID.

Relationship Between a Certificate Policy and a Certification Practice Statement

The term Certification Practice Statement (CPS) is defined in RFC2527 as: "A statement of the practices, which a Certification Authority employs in issuing Certificates." It is a comprehensive description of such details as the precise implementation of service offerings and procedures for Certificate life-cycle management and will be significantly more detailed in operational detail than the CPs supported by the CA. Due to the extensive and sensitive details in a CPS, it is often not prudent to publish a CPS; thus it is maintained as a confidential document. Additionally, because of the extensive policy detail, the CP, rather than the CPS, provides a more suitable basis for establishing trust agreements among CAs operated by different organizations for purposes of Cross-Certification.

Alignment of UIPKI with CA Browser Forum

The UIPKI conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

The UIPKI shall review updates to the Baseline Requirements at least annually and implement changes to the CP and CPS as required to maintain compliance with these updates.

The Entrust 2048 Root certificate cross-certifies the Intermediate B Certification Authority of UIPKI.

Part 2 – Policy Specification

1 INTRODUCTION

1.1. Overview

Unisys Internal Public Key Infrastructure (UIPKI) Certificate Policy has been established and will be maintained by the UIPKI Policy Management Authority (PMA).

The UIPKI has been established to provide public key certificate based security services for the benefit of the Corporation, its Business Associates and Employees. The UIPKI is a **closed PKI**, in that the Certificates issued are applicable for use in electronic transactions solely between the Corporation, its Business Associates and Employees for purposes approved by Unisys. The UIPKI is not and never will be a public PKI. Therefore, the issuance and use of UIPKI Certificates is governed by the contractual relationships established between participants in the UIPKI and by this CP, rather than any public signature law. This CP establishes the terms and requirements to issue, maintain, use, rely upon, and Revoke a digital Certificate (Certificate). Only a Unisys Internal Certification Authority (UICA) accredited by the PMA may issue and manage Certificates that reference this CP. UICAs, Registration Authorities (RAs), Subscribers, Qualified Relying Parties, Registration Authorities, other Service Providers, and all trusted personnel who support the issuance of Certificates that reference this CP and all other Users are obligated to comply with this CP.

Unisys may outsource the hosting and operation of any component of the UIPKI to one or more Service Providers. Service Providers may include but are not limited to:

a. Certificate Manufacturing Authority (CMA),
b. CA Service Provider (CASP), and
c. Repository Service Provider (RSP).

Subscribers and Qualified Relying Parties may use and rely upon Certificates in accordance with Section 1.3.8 (Applicability).

Specifically, this CP provides the rules for issuing different types of Certificates to individuals, organizational roles, devices or applications, which may be used for

a. authentication,
b. confidentiality, or
c. the validation of a Digital Signature.

Subscribers and Qualified Relying Parties must read this CP to determine the suitability of a Certificate for a specific use.

This CP is subject to change in accordance with Section 8 (Certificate Policy Administration).

1.2. Identification

This CP is called the *Unisys Internal PKI Certificate Policy* . There are four Assurance Levels supported by this CP. The specific criteria for the issuance of a Certificate at a given Assurance Level is defined in subsequent sections. Each Assurance Level has one or more associated policy Object Identifiers (OIDs).

To facilitate policy mapping for purposes of Cross-Certification with other established PKIs, a precise policy OID structure has been established for the UIPKI that corresponds to the Assurance Level under which the Certificate has been issued, the applicable use of the Certificate, and the type of Subject as defined in Section 3.1.2 (Need for Names to be Meaningful).

A UICA issuing Certificates that reference this CP must use the following criteria to determine which of the specific policy OIDs will be contained in the Certificate.

If the Assurance Level of the Certificate is …	and the applicable use is ….	and the Subject Type is ….	then the policy OID is the following ..
Test	No stipulation	No stipulation	2.16.840.1.114352.1.1.1
Basic	Authentication / Digital Signature	Individual or Device	2.16.840.1.114352.1.1.14
Medium	Authentication / Digital Signature	Individual	2.16.840.1.114352.1.1.2
Medium	Data or Key Encryption	Individual	2.16.840.1.114352.1.1.3
Medium	Authentication / Digital Signature	Organizational Role	2.16.840.1.114352.1.1.4
Medium	Data or Key Encryption	Organizational Role	2.16.840.1.114352.1.1.5
Medium	Authentication / Digital Signature	Application or Device	2.16.840.1.114352.1.1.61
Medium	Data or Key Encryption	Application or Device	2.16.840.1.114352.1.1.7
High	Authentication / Digital Signature	Individual	2.16.840.1.114352.1.1.8
High	Data or Key Encryption	Individual	2.16.840.1.114352.1.1.9
High	Authentication / Digital Signature	Organizational Role	2.16.840.1.114352.1.1.10
High	Data or Key Encryption	Organizational Role	2.16.840.1.114352.1.1.11
High	Authentication / Digital Signature	Application or Device	2.16.840.1.114352.1.1.12
High	Data or Key Encryption	Application or Device	2.16.840.1.114352.1.1.13

1.3. Community and Applicability

1.3.1. Policy Management Authority

Unisys Policy Management Authority (PMA) is a body established by Unisys to:

a. oversee the creation and update of this UIPKI CP in accordance with Section 8 (Certificate Policy Administration);
b. review and approve the CPS of UICAs/RAs applying to issue Certificates that reference this CP;
c. review the results of UICA/RA compliance audits in accordance with Section 2.7 (Compliance Audit);
d. authorize the issuance of Cross-Certificates to another organization's CA; and
e. authorize requests for name space modifications.

1.3.2. Certification Authorities

The UIPKI architecture includes multiple Certification Authorities (CAs), specifically

a. A single Root CA[1];

b. Multiple first level Internal CAs, subordinated to the Root CA, which may issue Certificates to Subordinate second level CAs. One or more of these first level CAs may be cross-certified with outside PKIs in order to provide a trust reference for Qualified Relying Parties outside the Corporation; and

c. Multiple second level Internal CAs, subordinate to the first level Internal CAs, which may issue Certificates to End-Entities.

A UICA issuing Certificates referencing this CP is responsible for:

a. the identification and authentication of Subscribers;
b. the creation, signing, and distribution of Certificates binding Certificate Subjects with their Public Keys;
c. promulgating Certificate status through Certificate Revocation Lists (CRLs); and
d. ensuring adherence to this CP.

UICAs may be authorized to issue Certificates referencing this CP at the sole discretion of the PMA, following verification of the UICA's CPS for compliance to this CP using procedures to be established by the PMA.

A first-level UICA may issue Cross-Certificates to other CAs, including Cross-Certification from commercial or "open" CAs upon written authorization by the PMA. The PMA establishes the criteria for the issuance of Cross-Certificates subject to the following conditions:

a. Policy mapping between this CP and the CP published by the Cross-Certificate Applicant; and
b. Successful completion of technical interoperability testing between the UICA and the Cross-Certificate Applicant.

A UICA may delegate functions for which it is responsible to internal Registration Authorities which are part of the UIPKI, provided that the UICA remains responsible for performance of services in accordance with this CP. No delegated third parties are permitted.

[1] Which is the central anchor of trust for the UIPKI

1.3.3. Registration Authorities

A UICA may delegate functions to an Entity acting as a Registration Authority (RA) which is part of the UIPKI. An RA is an Entity that enters into an agreement with a CA to collect and/or verify Subscribers' identity and information which is to be entered into public key Certificates. An RA must perform its functions in accordance with this CP and the UICA's CPS.

RA functions are initially performed by employees or agents of Unisys, who collect Applicant or Subscriber information and authenticate and/or verify the identity of Applicants for UICA issued Certificates.

In those operating systems which support it, the UIPKI may employ auto-issuance techniques for Test, Basic, and Medium assurance Certificates. This issuance will be based on existing security credentials of Subscribers and machines, where management sponsorship of security account information exists, and due diligence has been exercised in screening the individuals who have internal Unisys accounts. By providing user and machine Certificates during the Kerberos-mediated credentials verification in this manner, the Unisys global Active Directory (AD) administration is supporting Registration Authority functions.

1.3.4. Repositories

The UIPKI Repository stores and supports access to, at a minimum,

a. this CP,
b. UICA Certificates and Public Keys, and
c. CRLs.

A Repository may also store and support access to End-Entity Certificates and other information pertinent to the UIPKI. The Repository information published outside the Corporation will not include the Certificate or CRL of the internal Root CA.

A UICA must perform all associated functions necessary to coordinate publication of information to Repositories.

At its discretion, Unisys may contract the operation and management of the UIPKI Repository to a Repository Service Provider (RSP) under the terms and conditions of an operational agreement, memorandum of understanding, or similar contract executed with Unisys. This CP is incorporated by reference in such operational agreement, memorandum of understanding, or contract.

1.3.5. Subscribers

A Subscriber is a person who:

a. is the Subject named or identified in a Certificate issued to such person, or
b. applies for a Certificate on behalf of the Subject named or identified in a Certificate, and
c. holds a Private Key that corresponds to a Public Key listed in that Certificate, and
d. to whom digitally signed messages verified by reference to such Certificate are to be attributed.

Authorized Subscribers in the UIPKI are limited to:

a. Employees and Business Associates with a need to access Unisys internal networks and systems, who are identified as the Subject named in a Certificate;

b. Employees and Business Associates responsible for the administration, management or operation of a certificate-enabled device or application hosted by the Corporation including workstations, firewalls, routers, in-line network encryption devices, or any other trusted network component that is the Subject named in a UIPKI Certificate request;

c. Organizations within the Corporation who service customer equipment employing a Certificate on that equipment in order to securely complete maintenance / service operations with Unisys;

d. Organizations within the Corporation which employ software signing to ensure validity of software distributed within the Corporation; and

e. Organizations within the Corporation which employ Certificates in order to securely transmit data across untrusted network connections and/or digitally sign communications.

1.3.6. Qualified Relying Parties

A ”relying party” is generally defined as any entity that relies upon the binding of the Subject’s identity and Public Key contained in a Certificate.

The Unisys Internal PKI is a closed PKI in which all relying parties must be Qualified Relying Parties. Qualified Relying Parties in the UIPKI are limited to:

a. Employees of the Corporation,

b. Business Associates of the Corporation, and

c. The Corporation itself.

A *third party* therefore can never successfully claim that she or he was a Qualified Relying Party.

A Qualified Relying Party must:

a. Check the validity of the Certificate in accordance with Section 4.4 (Certificate Suspension and Revocation); and
b. Use information in the Certificate (e.g., Certificate policy OID) to determine the suitability of the Certificate for a particular use in accordance with Section 1.3.8 (Applicability).

Qualified Relying Parties may or may not also be Subscribers.

1.3.7. Service Providers

Unisys in its sole discretion may outsource the hosting and operation of a UICA to a Service Provider or contract with a Service Provider to perform specific services on behalf of the UICA related to the issuance, management, or distribution of Certificates to Subscribers. Any such Service Provider must meet all requirements imposed on a UICA for any services provided under the terms and conditions of an operational agreement, memorandum of understanding, or similar contract executed with Unisys. This CP is incorporated by reference in such operational agreement, memorandum of understanding, or contract.

1.3.8. Applicability

Since the Unisys Internal PKI is a closed PKI, Certificates can only be used for purposes approved by the Corporation. The suitability of a Certificate, and its corresponding Key Pair for a given application (e.g., privacy, authentication, integrity, non-repudiation) will be based on the assertions made in the X.509 keyUsage and extendedKeyUsage extensions in the Certificate.

Qualified Relying Parties who rely on Certificates issued in accordance with this CP do so at their own risk; all terms and conditions including limitations of liability and indemnification provisions of this CP shall apply to all such transactions.

Guidelines for Determining Usage

Subscribers and Qualified Relying Parties may determine the suitability of a Certificate for a particular purpose using the Certificate policy OID contained in the Certificate as defined in Section 1.2 (Identification).

The Assurance Level attributed to a particular Certificate policy OID is based on several criteria including the methods required for the validation of the Subscriber's identity and security requirements for the protection of the Certificate Subject's Private Key. The specifications for the issuance and management of Certificates are set forth in this CP. Primary distinctions in the specifications for the issuance of Certificates at different Assurance Levels are described in the following table.

Assurance Level	**In person identity validation required**	**Private Key Protection: Hardware or Software**	**Private Key Protection: Cryptographic Module Standard**
Test	Not required	Hardware or Software	FIPS 140-1 Level 1
Basic	Not required	Hardware or Software	FIPS 140-1 Level 1
Medium	Either corporate security credentials or In Person validation	Hardware or Software	FIPS 140-1 Level 1
High	Yes	Hardware	FIPS 140-1 Level 2

The sensitivity of the information processed or protected using Certificates issued by a UICA will vary significantly. Qualified Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each Qualified Relying Party and is not controlled by this CP.

To provide sufficient specificity, this CP describes security requirements for three increasing, qualitative Levels of Assurance: Basic, Medium and High. It also defines an Assurance Level used for testing purposes.

The following table provides guidance to help Qualified Relying Parties determine at which Assurance Level to permit or disallow reliance. The Qualified Relying Party is solely responsible for making this determination and for any resulting liability or loss.

Assurance Level	**Applicability Guideline**

Test	This Assurance Level is suitable for testing functionality and interoperability of applications with a UICA. It is used solely for this purpose and conveys no assurance information.
Basic	This Assurance Level may be suitable for an environment where risks and consequences of data compromise are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high.
Medium	This Assurance Level may be suitable for an environment where risks and consequences of data compromise are moderate to substantial. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
High	This Assurance Level may be suitable for an environment where risks and consequences of data compromise are high. This may include very high value transactions or high levels of fraud risk.

1.4. Contact details

The PMA administers this CP. Inquiries regarding this CP or related policies should be directed to:

Unisys Corporation
801 Lakeview Drive
Suite 100
Blue Bell, PA 19422
Attn: Unisys Internal PKI Policy Management Authority, Mat Newfield

1.4.1. Person Determining CPS Suitability for the Policy

The PMA determines the suitability of a UICA’s CPS for issuing Certificates in accordance with this CP.

2. GENERAL PROVISIONS

2.1. Obligations

This sub-section contains, for each Entity type, any applicable provisions regarding the Entity's obligations to other Entities.

2.1.1. UICA Obligations

A UICA issuing Certificates that reference this CP must:

a. provide to the PMA its CPS, as well as any subsequent changes, for conformance assessment;
b. operate in accordance with its CPS, this CP, and any applicable laws of the governing jurisdiction named in this CP and its CPS;
c. have in place mechanisms and procedures to ensure that its personnel are aware of and agree to abide with the stipulations in this CP that apply to them;
d. incorporate this CP into any operational agreement, memorandum of understanding, or similar contract executed between the UICA and a Service Provider;
e. take commercially reasonable measures to ensure that Subscribers and Qualified Relying Parties are aware of their respective rights and obligations with respect to the operation and management of any keys, Certificates, or End-Entity hardware and software used in connection with the PKI; and
f. provide notice of limitations of liability and restrictions related to the use of Certificates as defined in this CP and its CPS. Such notice must, at a minimum, be provided through the publication of this CP, and be publicly accessible by Qualified Relying Parties via an Internet accessible web browser. Such measures shall include the publication of Relying Party Agreements defining Qualified Relying Parties’ rights and obligations with respect to the use of UICA issued Certificates. Such agreements must incorporate this CP by reference and include, at a minimum, Section 2.1.5, and Sections 2.2 through 2.4 of this CP.

Notice of limited liability and any restriction on usage shall also be referenced in the Certificate in accordance with Section 7.1.8 (Policy Qualifiers Syntax and Semantics).

The UICA must ensure that its Certificate signing Private Key is used only to sign Certificates and CRLs.

The UICA must ensure that Private Keys held by individuals serving in Trusted Roles, to access and operate UICA applications, are used only for such purposes.

UICA personnel associated with Trusted Roles as defined in Section 5.2.1 (Trusted Roles) must be individually accountable for actions they perform. “Individually accountable” means that there must be evidence that attributes an action to the person performing the action.

2.1.2. RA Obligations

An RA, as defined in Section 1.3.3 (Registration Authorities), that performs registration functions on behalf of a UICA issuing Certificates that reference this CP, is required to conform to the stipulations of this CP and comply with the applicable UICA’s CPS.

The RA must have in place mechanisms and procedures to ensure that its personnel are aware of and agree to abide with the stipulations in this CP that apply to them.

The RA must ensure that any Private Keys issued to its personnel to access and operate RA applications are used only for such purposes.

RA personnel must be individually accountable for actions performed. “Individually accountable” means that there must be evidence that attributes an action to the person performing the action.

2.1.3. Repository Obligations

A Repository operated by Unisys or an RSP in accordance with Section 1.3.4 (Repositories) should be available for a high proportion of every 24-hour period.

CRLs must be made available to Qualified Relying Parties in accordance with Section 4.4.3 (CRL Issuance Frequency).

2.1.4. Subscriber Obligations

A Subscriber must accept the terms and conditions set forth by the UICA with respect to Certificate use, including permitted applications and purposes defined in this CP and the Subscriber notice as per Section 2.1.1 (UICA Obligations).

A Subscriber must:

a. generate a Key Pair using a Trustworthy System and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the Private Key;
b. implement procedures to preclude key reuse among different roles or across multiple Certificates, unless the original Certificate is Renewed;
c. not use his or her Private Key for signing purposes until after the Public Key Certificate is formally accepted, unless the Applicant uses his or her Private Key to sign the Certificate request;
d. provide accurate information to the RA, or its agent as part of the Certificate application;
e. acknowledge that accepting the Certificate or enabling a device to automatically accept a Certificate means the Subscriber is certifying that all information and representations in the Certificate are accurate. In cases where a Certificate is auto-issued or issued from a web enrollment point, Unisys IT policies will state the terms under which these Certificates may be used by the individuals, and an email to the Subscriber will provide a link to the policy and a synopsis of the content ;
f. use the Certificate only in accordance with Section 1.3.8 (Applicability);
g. not attempt to reverse engineer any Certificate issued by a UICA or to compromise the security of the UIPKI;
h. send a Certificate revocation request to the issuing UICA promptly upon any actual or suspected loss, disclosure, or other compromise of a Subscriber’s Private Key;
i. ensure compliance with applicable import and export laws;
j. abide by all the terms, conditions, and restrictions levied upon his or her Private Keys and Certificates; and
k. notify the UICA immediately of any change to the information appearing in the Subscriber's Certificate that occurs during the Operational Period of a Certificate.

If the Subscriber fails to meet any of these obligations, the Issuing UICA may Revoke the Certificate.

2.1.5. Qualified Relying Party Obligations

A Qualified Relying Party may rely on a Certificate that references this CP, only if the Certificate is used and relied upon for lawful purposes and under circumstances where the Qualified Relying Party:

a. assents to the terms of a Qualified Relying Party Agreement, which incorporates by reference this CP, as a condition of using or otherwise relying on Certificates;
b. uses the Certificate in accordance with Section 1.3.8 (Applicability)
c. considers all facts listed or incorporated by reference in the Certificate and facts that the Qualified Relying Party knows and facts for which the Qualified Relying Party has received notice before relying on the Certificate;
d. verifies the signature on the Certificate;
e. checks the status of the Certificate before reliance in accordance with Section 4.4.4 (CRL Checking Requirements); and
f. checks the status of all Certificates in the Certificate trust chain, and all Certificates in the trust chain were neither Revoked, Expired, nor Suspended at the time the transaction was consummated.

A Qualified Relying Party must:

a. assume the risk that a Certificate is invalid, if reliance on the Certificate is not reasonable or the Qualified Relying Party failed to meet these obligations;
b. not reverse engineer any Certificate issued by the UICA; and
c. not compromise the security of the UIPKI.

2.2. Liability

2.2.1. UICA Liability

NOTHING IN THIS CP SHALL CREATE, ALTER, OR ELIMINATE ANY OTHER OBLIGATION, RESPONSIBILITY OR LIABILITY THAT MAY BE IMPOSED ON ANY ENTITY BY VIRTUE OF ANY OTHER CONTRACT OR OBLIGATION APPLICABLE UNDER LAW.

2.2.2. Warranties and Limitations on Warranties

UNISYS AND ITS SERVICE PROVIDERS MAKE NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, CONCERNING THE PRODUCTION, USE, AND MAINTENANCE OF CERTIFICATES UNDER THIS CP except as noted.

CA Representations and Warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

- Right to Use Domain Name or IP Address: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- Authorization for Certificate: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- Accuracy of Information: That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- No Misleading Information: That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- Identity of Applicant: That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement;
- Subscriber Agreement: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
- Status: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
- Revocation: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates.

Subscriber Representations and Warranties

The CA SHALL require, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries. Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either:

- The Applicant's agreement to the Subscriber Agreement with the CA, or
- The Applicant's acknowledgement of the Terms of Use.

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA;
- Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
- Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Reporting and Revocation: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate.
- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

2.2.3. Disclaimers

UNISYS AND ITS SERVICE PROVIDERS ARE NOT LIABLE FOR ANY LOSSES:

a. **DUE TO UNAVAILABILITY OF UICA, RA, OR REPOSITORY SERVICES DUE TO WAR, NATURAL DISASTERS OR OTHER UNCONTROLLABLE FORCES.**

b. **INCURRED BETWEEN THE TIME A CERTIFICATE REVOCATION REQUEST IS RECEIVED, THE CERTIFICATE IS REVOKED, AND THE NEXT SCHEDULED ISSUANCE OF A CERTIFICATE REVOCATION LIST.**

c. **DUE TO UNAUTHORIZED USE OF CERTIFICATES ISSUED BY A UICA OR USE OF CERTIFICATES NOT CONSISTENT WITH THE PRESCRIBED USE DEFINED IN THIS CP, OR OTHERWISE NOT IN ACCORDANCE WITH THE REQUIREMENTS OF THIS CP.**

d. **CAUSED BY FRAUDULENT OR NEGLIGENT USE OF A CERTIFICATE OR CERTIFICATE REVOCATION LIST ISSUED BY A UICA.**

e. **DUE TO DISCLOSURE OF INFORMATION CONTAINED WITHIN A CERTIFICATE OR CERTIFICATE REVOCATION LIST.**

TO THE EXTENT PERMITTED BY LAW, UNISYS AND ITS SERVICE PROVIDERS DISCLAIM ALL WARRANTIES AND OBLIGATIONS OF ANY TYPE, INCLUDING ANY WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY OF THE ACCURACY OF INFORMATION PROVIDED.

2.2.4. Loss Limitations

IF UNISYS OR ITS SERVICE PROVIDERS FAIL TO CONFORM TO THIS CP, THE TOTAL CUMULATIVE LIABILITY OF UNISYS AND ITS SERVICE PROVIDERS TO ANY ENTITY ARISING OUT OF OR RELATING TO ANY CERTIFICATE OR SERVICES PROVIDED BY OR ON BEHALF OF UNISYS IN CONNECTION WITH CERTIFICATES, INCLUDING ANY USE OR RELIANCE ON ANY CERTIFICATE, SHALL NOT EXCEED ONE HUNDRED U.S. DOLLARS ($100.00 U.S.). THIS LIMITATION SHALL APPLY ON A PER CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS, DIGITAL SIGNATURES, OR CAUSES OF ACTION ARISING OUT OF OR RELATED TO SUCH CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT OF SUCH CERTIFICATE. UNISYS TOTAL LIABILITY TO ANY SUCH ENTITY SHALL NOT EXCEED ONE THOUSAND U.S. DOLLARS ($1000.00 U.S.). THE FOREGOING LIMITATIONS SHALL APPLY TO ANY LIABILITY WHETHER BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR ANY OTHER FORM OF LIABILITY.

2.2.5. Other Exclusions

IN NO EVENT WILL UNISYS OR ITS SERVICE PROVIDERS BE LIABLE FOR (A) ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, (INCLUDING, BUT NOT LIMITED TO, LOSS OF USE, REVENUES, PROFITS OR SAVINGS), EVEN IF UNISYS OR ITS SERVICE PROVIDERS KNEW OR SHOULD HAVE KNOWN OF

THE POSSIBILITY OF SUCH DAMAGES, (B) CLAIMS, DEMANDS, OR ACTIONS, AGAINST A SUBSCRIBER OR RELYING PARTY BY ANY PERSON, OR (C) LOSS OF OR DAMAGE TO DATA FROM ANY CAUSE.

2.2.6. RA Liability

SEE SECTIONS 2.2.2 – 2.2.5 OF THIS CP.

2.3. Financial Responsibility

2.3.1. Indemnification by Relying Parties

A relying party, including, but not limited to, a Qualified Relying Party, at its own expense, shall defend and indemnify Unisys and its Service Providers as applicable, against all claims with respect to any liabilities, losses, costs, expenses, damages, and settlement amounts arising out of or relating to the use by the relying party of the UIPKI including but not limited to (a) failure of the relying party to comply with the terms and conditions set forth in this CP and/or any contractual arrangement with Unisys or its Service Providers, (b) lack of proper validation of a Certificate by relying party, (c) reliance by the relying party on an expired or Revoked Certificate, (d) use of a Certificate other than as permitted under this CP, and/or any contractual terms and conditions set forth between the relying party and Unisys or its Service Providers or any applicable law, (e) failure by the relying party to exercise reasonable judgment in the circumstances in relying on a Certificate, (f) any claim or allegation that the reliance by a relying party on a Certificate or the contents of the Certificate infringes, misappropriates, or unfairly competes with a patent, copyright, trade secret protected or other Intellectual Property right.

Unisys or its Service Providers shall be entitled to compensation from a relying party if it can be shown that negligent or wrongful acts of a relying party have caused Unisys or its Service Providers loss, either financially or in reputation.

2.3.2. Indemnification by Subscribers

Subscriber, at its own expense, shall defend and indemnify Unisys and its Service Providers as applicable, against all claims with respect to any liabilities, losses, costs, expenses, damages, and settlement amounts arising out of or relating to the use by the Subscriber of the UIPKI including but not limited to (a) failure of the Subscriber to comply with the terms and conditions set forth in this CP and/or any contractual arrangement with Unisys or its Service Providers, (b) misrepresentations or incomplete information made by Subscriber in using or applying for a Certificate, (c) use of a Certificate other than as set forth in this CP and/or any contractual terms and conditions set forth between the Subscriber and Unisys or its Service Providers, or any applicable law, (d) modification by Subscriber of a Certificate, (e) failure of the Subscriber to take the necessary precautions to prevent loss, disclosure, compromise, or unauthorized use of the Private Key corresponding to the Public Key in the Subscriber’s Certificate, (f) any claim or allegation that the use by Subscriber of a Certificate or the contents of the Certificate infringes, misappropriates, or unfairly competes with a patent, copyright, trade secret, or other Intellectual Property right. Unisys or its Service Providers may seek compensation from a Subscriber if it can be shown that negligent or wrongful acts of a Subscriber have caused Unisys or its Service Providers loss, either financially or in reputation. Notwithstanding the foregoing, this paragraph shall not apply to a Subscriber who is an Employee.

2.3.3. Fiduciary Relationships

Issuance of Certificates in accordance with this CP does not make a UICA or its Service Providers an agent, fiduciary, trustee, or other representative of Subscribers or Qualified Relying Parties.

Assisting in the issuance of Certificates in accordance with this CP does not make an RA an agent, fiduciary, trustee, or other representative of Subscribers or Qualified Relying Parties.

2.4. Interpretation and Enforcement

2.4.1. Governing Law

THIS POLICY AND ANY TRANSACTIONS GOVERNED BY THIS POLICY STATEMENT WILL BE GOVERNED BY THE LOCAL LAWS OF THE COMMONWEALTH OF PENNSYLVANIA.

2.4.2. Severability, Survival, Merger, Notice

Each paragraph and provision of this CP is severable, and if a court of competent jurisdiction finds any paragraph or provision of this CP, or portion thereof, to be unenforceable, that provision of the CP shall be enforced to the maximum extent permissible so as to effect its intent and the remaining provisions of this CP will remain in full force and effect.

All notices related to indemnities and dispute resolution and all requests for information will be deemed given on the day they are received either by messenger, nationally recognized delivery service, or in the U.S. Mail , postage prepaid, certified or registered, return receipt requested, and addressed as follows:

Office of the General Counsel
Unisys Corporation
801 Lakeview Drive
Suite 100
Blue Bell, PA 19422
United States

In addition, in the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA’s CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

2.4.3. Conflict of provisions

In the event of a conflict between the provisions of this CP, and any express written agreement between Unisys and a Subscriber or Qualified Relying Party, with respect to a Unisys Certificate or any services provided by Unisys, such other express written agreement shall take precedence.

Waiver

Any failure or delay by either party in exercising any right or remedy will not constitute a waiver.

Assignment

Unisys may assign this CP or its interest in the UIPKI, or assign the right to receive payments, without the User's consent. Any such assignment, however, will not change the obligations of the UICA to the User. User will not assign or transfer its rights or obligations under this CP without prior written consent of the UICA. Any assignment or transfer prohibited by this provision will be void. Unisys may subcontract any services described in this CP to third parties selected by Unisys.

2.4.4. Dispute resolution procedures

The Unisys PMA shall resolve any disputes associated with Certificates issued by a UICA.

2.5. Fees

A UICA shall not impose any fees for the reading of this CP. A UICA may charge fees for the issuance, renewal, suspension, or revocation of Certificates, access fees to Certificates, Certificate status information, or CRLs, and other related services.

2.5.1. Certificate Issuance or Renewal Fees

Fees charged for Certificate Issuance or Renewal, if any, are subject to agreement between the UICA and the Subscriber and/or other Entities and will be in accordance with the terms and conditions defined in such agreements.

2.5.2. Certificate Suspension or Revocation Fees

Fees charged for Certificate Suspension or Revocation, if any, are subject to agreement between the UICA and the Subscriber and/or other Entities and will be in accordance with the terms and conditions defined in such agreements.

2.5.3. Certificate Access Fees

Fees charged for access to Certificates, if any, are subject to agreement between the UICA and the Subscriber, Qualified Relying Party, and/or other Entities and will be in accordance with the terms and conditions defined in such agreements.

2.5.4. Certificate Status Information or CRL Access Fees

Fees charged for access to Certificate status information or CRLs, if any, are subject to agreement between the UICA and the Subscriber or Qualified Relying Party and other Entities and will be in accordance with the terms and conditions defined in such agreements.

2.5.5. Fees for Other Services such as Private Key Archive or Trusted Time Stamp Services

Fees charged for other services such as Private Key Archive or Trusted Time Stamp services, if any, are subject to agreement between the UICA and the Subscriber, Qualified Relying Party and other Entities and will be in accordance with the terms and conditions defined in such agreements.

2.5.6. Refund Policy

Refunds of fees charged, if any, are subject to agreement between the UICA and the Subscriber, Qualified Relying Party, and/or other Entities and will be in accordance with the terms and conditions defined in such agreements.

2.6. Publication and Repositories

2.6.1. Publication of Certification Authority Information

A UICA must:

a. ensure the publication of this CP on a web site maintained by, or on behalf of, the UICA, the location of which must be indicated in compliance with Section 8.2 (Publication and Notification Procedures);
b. ensure that operating system and Repository access controls will be configured so that only authorized personnel can write or modify the on-line version of the CP;
c. provide a full text version of this CP when necessary for the purposes of any audit, inspection, accreditation, or Cross-Certification;
d. ensure the publication of the Root UICA Certificate or a Cross-Certificate and all other UICA Certificates in a trust path anchored by the Root UICA or public trust path established through Cross-Certification to a Repository or web site, maintained by, or on behalf of, the UICA, the location of which must be indicated in accordance with Section 7 (Certificate and CRL Profiles), noting that the Root CA Certificate is not permitted to be published outside the Corporation; and
e. ensure the publication of CRLs issued by the Root UICA and all other UICAs in a trust path anchored by the Root UICA or public trust path established through Cross-Certification to a Repository or web site, maintained by, or on behalf of, the UICA, the location of which must be indicated in accordance with Section 7 (Certificate and CRL Profiles) noting that the Root CA CRL is not permitted to be published outside the Corporation.

A UICA may:

a. publish End-Entity Certificates to a Repository or a web site, maintained by, or on behalf of, the UICA, or both;
b. provide access to Certificate status; and
c. publish other information pertinent to the UIPKI for the benefit of Subscribers, Qualified Relying Parties and other Entities.

2.6.2. Frequency of Publication

UICA Certificates, and End-Entity Certificates when applicable, must be published by the Root UICA or Issuing UICA promptly upon issuance.

A UICA must publish CRLs in accordance with Section 4.4.3 (CRL Issuance Frequency).

2.6.3. Access Controls

Access controls may be instituted at the discretion of the UICA with respect to published End-Entity Certificates or on-line Certificate status checks (if provided as a service by the UICA).

A UICA must ensure unrestricted access to this CP, CA Certificates, and CRLs published in accordance with Section 2.6.1 (Publication of Certification Authority Information).

2.7. Compliance Audit (Inspection)

A compliance inspection determines whether a UICA/RA’s performance meets the standards established in its CPS and satisfies the requirements of the Certificate Policies it supports. UICAs that reference this CP must have a compliance audit mechanism in place that satisfies the requirements stipulated within this section.

2.7.1. Frequency of Compliance Audit

UICAs and RAs shall be subject to a periodic compliance audit that is no less frequent than once per year for High and Medium Assurance. There is no audit requirement for UICAs and RAs operating at the Test Level of Assurance.

The PMA has the right to require periodic and aperiodic compliance audits or inspections of UICAs and RAs issuing Certificates referencing this CP to validate that the Entities are operating in accordance with the security practices and procedures described in their respective CPSs.

2.7.2. Identity/Qualifications of Auditor

The auditor must demonstrate competence in the field of compliance audits and possess significant experience with PKI and cryptographic technologies. The auditor must perform such compliance audits as a primary responsibility.

2.7.3. Auditor’s Relationship to Audited Party

The auditor either shall be a private firm, which is independent from the Entity being audited, or it shall be sufficiently organizationally separated from that Entity to provide an unbiased, independent evaluation.

2.7.4. Topics Covered by Audit

The compliance audit shall conform to generally accepted industry practices for PKI compliance audits using guidelines such as those described in the *AICPA/CICA WebTrust Program for Certification Authorities*, American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants, August 2000.

At a minimum, the audit will assess whether:

a. the terms of any Cross-Certification agreement(s) with outside CAs are being observed;
b. the CPS outlines, in sufficient detail, the technical, procedural and personnel policies and practices of the UICA/RA which meet the requirements of this CP for all Assurance Levels supported by the UIPKI; and
c. the UIPKI implements and complies with those technical, procedural and personnel practices and policies.

2.7.5. Actions Taken as a Result of Deficiency

When the auditor finds a discrepancy between how a UICA or RA is designed or is being operated or maintained and the applicable CPS, the following actions shall be performed:

a. The auditor shall note the discrepancy;
b. The auditor shall notify the UICA/RA of the discrepancy. If the discrepancy is judged by the UICA/RA to be severe in nature (that is, it is determined to be a “material discrepancy” relative to the applicable requirements), the UICA/RA shall promptly notify the PMA and all CAs with which it has cross-certified; and
c. The party responsible for correcting the discrepancy shall determine what further notifications or actions are necessary pursuant to the requirements of this CP and related agreements, and then proceed to make such notifications and take such actions without delay.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may:

a. allow the UICA/RA to continue to operate at the same or a lower Assurance Level,
b. temporarily or permanently halt operation of a UICA/RA,
c. Revoke a subordinate or Cross-Certificate issued by a UICA/RA, or
d. take other actions it deems appropriate.

Any decision regarding which of these actions will take place will be based on the severity of the discrepancy and will be at the sole discretion of the PMA.

2.7.6. Communication of Results

The UICA must provide to the PMA a copy of the results of compliance audits or inspections of its own or a subordinate Entity’s operations. Results will be made public per Baseline Requirements..

The method and detail of notification of compliance audit or inspection results to CAs cross-certified with a UICA shall be defined within the applicable agreement between the parties.

2.8. Confidentiality

UICAs and RAs must not disclose Confidential Information unless the disclosure is required by law or the Subscriber provides written consent that authorizes the release of Confidential Information.

This Section 2.8 (Confidentiality) and all subordinate sections shall survive termination or cancellation of this CP.

2.8.1. Types of Information to Be Kept Confidential

Subscriber Personal Data. For the purpose of proper administration of Certificates, a UICA or RA may request Subscriber personal data on Certificate application forms. A UICA or RA may also receive personal information in other forms of correspondence with a Subscriber. In the event that this type of information is received, it is handled as Confidential Information and access is restricted to those with an official need to access that information in performance of his or her official duties.

Subscriber Private Keys. The Subscriber must keep his/her Private Keys confidential. Disclosure by the Subscriber is at the Subscriber's own risk. A UICA must have no access to and may not store a Subscriber's private signature key. A Subscriber's private decryption key may be backed-up and/or escrowed by the Issuing UICA or another party on behalf of the UICA, in which case these keys must be protected in accordance with Section 6.2 (Private Key Protection).

Inspection Information. Inspection information is considered sensitive and must not be disclosed to anyone for any purpose except as stipulated in Section 2.7 (Compliance Audit). Information pertaining to a UICA's or RA's management of a Subscriber's Certificate may only be disclosed to the Subscriber, or where required by law.

Unisys Confidential Information. Users of Unisys Confidential Information must protect such information from disclosure to third parties and restrict its use as set forth in this CP and in related agreements.

Unisys Confidential Information may not be copied, or modified, in whole or in part, except when essential for authorized use in accordance with this CP.

2.8.2. Types of Information Not Considered Confidential

The following information is not considered confidential:

a. all data appearing in issued Certificates;
b. all data appearing in a CRL;
c. any information that can be obtained from public sources;
d. this CP;
e. all Certificates issued referencing this CP; and
f. a Subscriber's Public Key.

2.8.3. Disclosure of Certificate Revocation or Suspension Information

The Issuing UICA is the authorized source for Subscriber Certificate revocation and suspension information. This information is made available to Subscribers and Qualified Relying Parties in accordance with Section 4.4 (Certificate Suspension and Revocation). A UICA shall provide revocation reason codes through an approved revocation reporting mechanism (e.g., the reason code in an X.509 Version 2 CRL).

2.8.4. Release of Confidential Information to Law Enforcement Officials

A UICA or RA may disclose Confidential Information to law enforcement officials where required by law, government rule or regulation, or by order of a court of competent jurisdiction.

The UICA or RA must authenticate and process a request to release information in accordance with procedures documented in the UICA's CPS.

2.8.5. Release as Part of Civil Discovery

A UICA or RA may disclose Confidential Information to authorized parties as part of civil discovery where required by law, government rule or regulation; or by order of a court of competent jurisdiction.

The UICA or RA must authenticate and process a request to release information in accordance with procedures documented in the UICA's CPS.

2.8.6. Disclosure upon Owner's Request

A UICA or RA may disclose Confidential Information to a third party, if the Subscriber provides prior written consent or a digitally signed and authenticated request.

The UICA or RA must authenticate and process a request from the Subscriber to release information in accordance with procedures documented in the UICA's CPS. The procedure must also be described in the Subscriber Agreement.

2.8.7. Other Information Release Circumstances

A UICA or RA may disclose Confidential Information under other circumstances where required by law, government rule or regulation; or by order of a court of competent jurisdiction.

The UICA or RA must authenticate and process a request to release information in accordance with procedures documented in the UICA's CPS.

2.9. Intellectual Property Rights

This CP does not transfer to any party title to any Intellectual Property contained in any software, documentation or Unisys Confidential Information.

Any ideas, concepts, know-how, data-processing techniques, software, documentation, diagrams, schematics or blueprints, whether confidential or not, furnished or developed by Unisys personnel (alone or jointly with User) in connection with the UIPKI (the "Proprietary Information") are the exclusive property of Unisys. Unless otherwise set forth in an agreement with Unisys, Unisys grants to User a non-exclusive, royalty-free license to use the Proprietary Information furnished in accordance with this CP solely for User's internal requirements related to the UIPKI and use of Certificates issues hereunder. No license is granted to User to sub-license to others any Proprietary Information , and such Proprietary Information will not be copied or modified, in whole or in part, except as reasonably required for User's authorized use.

Certificate Applicants (and, upon acceptance of a Certificate, Subscribers) represent and warrant that the information they provide during the Certificate application process does not infringe upon or violate in any way the trademarks, service marks, trade names, company names, or any other Intellectual Property rights of any third party. Applicants (and, upon acceptance of a Certificate, Subscribers) will defend, indemnify, and absolve Unisys and its Service Providers from all financial responsibility and any claims of loss or damage resulting from such an infringement or violation. An Applicant (and, upon acceptance of a Certificate, Subscriber), who brings about a claim of loss or damage by violating or infringing upon the Intellectual Property right of any third party shall pay all legal fees and any losses or damages incurred by Unisys or its Service Providers as a result of such claim.

Copyrights and all other intellectual property rights in this CP, Certificates and UIPKI policy OIDs are the property of Unisys and may only be used in accordance with this CP. Without the express written permission from Unisys, Unisys prohibits the use of Certificates and Unisys-registered OIDs in a manner that is inconsistent with this CP.

This Section 2.9 (Intellectual Property Rights) shall survive termination or cancellation of this CP.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1. Types of Names

Each Certificate must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the Subjectname field in accordance with X.509v3.

The DN must be in the form of a `printableString` or `utf8String` and must not be blank.

A Certificate may contain one or more alternative names in the `subjectAlternateName` field, which must also be in accordance with X.509v3.

Specific attribute types and the value to be associated with these attributes, which must or may be included in the Subject DN of End-Entity Certificates will depend on the type of Subject for which the Certificate is issued. A description of these attributes for each type of Subject is defined in Section 3.1.2 (Need for Names to be Meaningful).

A UICA may include other attributes in the DN so long as these attributes are in accordance with X.509v3.

Where technically necessary, the DN may contain the emailAddress attribute. However, the preferred location for this attribute is as an `rfc822Name` type in the `subjectAlternateName` field.

A UICA may issue Certificates containing one or more alternative name types in the `subjectAlternateName` field, which must also be in accordance with X.509v3.

3.1.2. Need for Names to be Meaningful

Certificates are meaningful only if the names that appear in the Certificates can be understood and used by Qualified Relying Parties. Names used in the Certificates issued pursuant to this CP must identify the organization, person or object to which they are assigned in a meaningful way.

The Subject DN in End-Entity Certificates shall be formed in accordance with the following naming conventions:

a. If the Subject is a Person, the Subject DN shall contain the commonName attribute, derived from the Unisys AD user name assigned to the Subscriber and an e-mail attribute equal to the e-mail address linked to the AD User; and
b. If the Subscriber is not a Person, the Subject DN identifies the organization, for which the Certificate is issued and a commonName containing the organizational role, the fully qualified domain name, or a unique machine or device name, as appropriate to uniquely identity the Subject. Issuance of "wild card" SSL certificates, in which the unique machine or device name is omitted and replaced by a wild card designator, is permitted, providing the domain name is owned by and registered to Unisys.

3.1.3. Rules for Interpreting Various Name Forms

Name forms shall be interpreted in accordance with Section 7 (Certificate and CRL Profiles).

3.1.4. Uniqueness of Names

A UICA must issue Certificates to each Entity using a Subject DN that is unique from the Subject DN used in Certificates issued to other Entities by the UICA.

For Certificates issued to Persons, the Subject DN is derived from the AD User name, which is unique to all individuals within the Corporation.

For Certificates issued to roles, devices, or applications a UICA may include a distinguished name qualifier or serial number attribute in the Subject DN where necessary to guarantee uniqueness. Use of these attributes must be in accordance with X.509v3.

Certificates issued to the same Entity may have identical Subject DNs.

3.1.5. Name Claim Dispute Resolution Procedure

The Issuing UICA shall make all decisions regarding Entity names in all issued Certificates. A party requesting a Certificate must demonstrate its right to use a particular name.

The Issuing UICA resolves any name collisions brought to its attention. A name collision occurs when more than one Applicant submits identical DN attributes. The UICA may append an attribute to the DN attributes submitted by an Applicant in accordance with Section 3.1.4 (Uniqueness of Names).

When the Issuing UICA resolves a name dispute, all affected parties waive all claims of loss arising from the Issuing UICA's decision to assign or to reassign a specific DN to a Subscriber.

3.1.6. Recognition, authentication and roles of trademarks

Each Applicant (and, upon acceptance, each Subscriber) represents that:

a. the submission and use of a subject name and all other information connected or related to the Certificate application does not infringe on the Intellectual Property rights or any other right of any third parties; and
b. he or she is not intending to, and will not, use the subject name for any unlawful purpose.

Each Applicant and Subscriber indemnifies Unisys and its Service Providers in respect of all claims, demands, actions, costs, expenses, losses and damages with regard to any breach of this warranty.

The Issuing UICA is not obligated to seek evidence of trademarks, court orders, or any other right to use the subject name before issuance.

The Issuing UICA is not obligated to issue or to reissue a Certificate with a particular subject name, even if the Certificate application contains a registered trademark owned by the Applicant or for which the Applicant has submitted a trademark registration application.

3.1.7. Proof of possession of private key

The Issuing UICA or RA must establish that the Applicant is in possession of the Private Key corresponding to the Public Key submitted by an Applicant in a Certificate request. Such proof of possession must be in accordance with IETF PKIX RFC2510 *Internet X.509 Public Key Infrastructure Certificate Management Protocols* March, 1999 or through another equally secure and verifiable method.

Where Private Keys are generated and stored on tokens under the control of a UICA, Service Provider, or an RA, secure distribution procedures must be employed that:

a. require the use of a shared secret (e.g., a password or PIN) for activation of the token that is distributed under separate cover from the token distributed to the Applicant; or
b. require the personal presence of the Applicant before the UICA, Service Provider, or RA for acceptance of the token containing the Private Key(s).

The UICA, Service Provider, or RA must maintain a record of validation for receipt of the token by the Applicant.

When any mechanism that includes a shared secret is used, the mechanism must ensure that the Applicant and the UICA, Service Provider, or RA are the only recipients of this shared secret.

3.1.8. Authentication of Individual Identity

An Individual's identity is authenticated by the verification of identity information provided by the Applicant. Such information may include but is not limited to the Applicant's:

a. name;
b. corporate employee identification number;
c. e-mail address; and
d. corporate security credentials.

Acceptable authentication methods for an Individual's identity are dependent on the Assurance Level under which the Certificate is to be issued.

Assurance Level	Identity Authentication Requirements
Test	In cases where automatic enrollment is not enabled: Identity must be established by existence in the Unisys AD security database or by In-Person Proofing before an agent of a UIPKI RA. Information provided shall be verified to ensure legitimacy. Automatic enrollment is not supported for test assurance level certificates.
Basic	No identity authentication is required.
Medium	In cases where automatic enrollment is not enabled: Identity must be established by existence in the Unisys AD security database or by In-Person Proofing before an agent of a UIPKI RA. Information provided shall be verified to ensure legitimacy. Where automatic enrollment is enabled, identity may be verified using Kerberos authentication with an appropriate corporate security credential and established based on existence in the AD security database.
High	Identity information provided by an Applicant must be verified to ensure legitimacy by a comparison of identity information supplied by the Applicant with

Assurance Level	Identity Authentication Requirements
	information in one or more trusted data bases containing Unisys, government or user supplied information, obtained and/or checked electronically or through other trusted means; and Identity must be established by In-Person Proofing before an agent of a UIPKI RA.

Where In-Person Proofing is employed

a. the Applicant must sign a statement attesting to the authenticity of the information and credentials provided in the presence of the person performing the In-Person Proofing, and
b. the person performing the In-Person Proofing must sign a statement, which includes such person's unique employee identifier, attesting to the date and time on which the In-Person Proofing was performed.

A Subscriber that holds a valid Identity Certificate may apply for an additional Certificate at the same or lower Assurance Level by digitally signing an application for the additional Certificate or through an automated issuance process that supports the issuance of multiple Certificates to individuals after identity is established using corporate security credentials as described above. Additional Certificates that may be applied for in this manner include but are not limited to Certificates in which the keyUsage extension specifies that the Private Key may be used for data or key encipherment.

The RA must keep a record of the method and information provided for identity authentication including but not limited to:

a. the identification information and/or credentials provided and verified;
b. any statements attested to and/or signed by the Applicant or Subscriber; and
c. where applicable, any statements attested to and signed by the person performing the In-Person Proofing.

These records must be archived in accordance with Section 4.6 (Records Archival).

3.1.9. Authentication of Devices and Applications

The individual responsible for the management or administration of a given device or application may request a Certificate on its behalf. The Applicant must be authenticated in accordance with Section 3.1.8 (Authentication of Individuals) and must demonstrate his or her authority to act as such a manager or administrator.

Where automatic enrollment is enabled for devices or applications, Unisys AD administration may support the RA function to provide selected devices with Certificates through automatic issuance mechanisms, when those devices are known in the security database and authenticated with Kerberos credentials or equivalent.

The RA must keep a record of the method and information provided for identity authentication including but not limited to:

a. the identification information and/or credentials provided and verified;
b. any statements attested to and/or signed by the Applicant; and

c. any statements attested to and/or signed by a responsible individual.

These records must be archived in accordance with Section 4.6 (Records Archival).

3.1.10. Authentication of Organization Role

The manager of multiple individuals responsible for the performance of duties assigned to a given organizational role may apply for a Certificate for that organizational role.

The Applicant must be authenticated either in accordance with Section 3.1.8 (Authentication of Individuals) or by digitally signing the application using his or her valid Identity Certificate issued at the same or higher Level of Assurance as the Certificate being requested. The Applicant must also demonstrate his or her authority to act as such a manager.

The manager must keep a record of all persons identified and authorized by the manager to use the Certificate and its corresponding Private Key.

The RA must keep a record of the method used for identity authentication and where applicable, the digitally signed application form or statement prepared by the manager.

These records must be archived in accordance with Section 4.6 (Records Archival).

3.2. Routine Certificate Re-Key, Renewal, or Update

3.2.1. Authentication for Routine Re-Key or Renewal

Re-keying a Certificate means that a new Certificate is created that has the same characteristics as the old one, except that the new Certificate has a new, different Public Key (corresponding to a new, different Private Key) and a different serial number and Operational Period.

Renewing a Certificate means that a new Certificate is created that has the same characteristics and Public Key (corresponding to the same Private Key) as the old one, except that the new Certificate has a different serial number and Operational Period.

A UICA may Re-key or Renew any Entity's Certificate using the Entity's valid Identity Certificate Key Pair for authentication provided that the Certificate to be Re-keyed or Renewed has not expired and has not been Revoked or Suspended. The UICA private key(s) will be destroyed at the end of the CA certificate life cycle.

For Identity Certificates issued at Basic, Medium or High Assurance Levels, a Subscriber's identity must be periodically re-established, and his or her Identity Certificate must be Re-keyed, in accordance with the methods stipulated in Section 3.1 (Initial Registration) and the following schedule.

Assurance Level	Re-authentication and Re-key Required
Test	No stipulation
Basic	At least once every 9 years from the time of initial registration
Medium	At least once every 9 years from the time of initial registration

High	At least once every 3 years from the time of initial registration

3.2.2. Authentication for Certificate Update

Updating a Certificate means creating a new Certificate that has the same or a different key and a different serial number, and that also differs in one or more other fields, from the old Certificate. For example, a UICA may choose to Update a Certificate of a Subscriber whose characteristics have changed (e.g., has a new e-mail address).

The old Certificate may or may not be Revoked by the UICA, but it must not be further Re-keyed, Renewed, or Updated.

Further, if attributes within the Subject DN change (e.g., due to corporate reorganization or marriage), then proof of the name change must be provided to the UICA in order for an Updated Certificate having the new name to be issued.

When a UICA's signing Certificate is Updated, the UICA must generate a new Key Pair and the UICA must notify all CAs, RAs, and Subscribers that rely on the UICA's Certificate that it has been changed.

If the Root UICA signing Certificate is Updated it must be distributed to other UIPKI Entities in a secure fashion to preclude malicious substitution attacks.

3.3. Authentication for Certificate Re-Key, Renewal, or Update after Revocation

Revoked, Suspended or expired Certificates shall not be Re-keyed, Renewed, or Updated. A new Certificate may be issued to the Subscriber in the same manner as that described in Section 3.1 (Initial Registration). Subscribers without a valid Identity Certificate must be re-authenticated in accordance with Section 3.1 (Initial Registration).

3.4. Authentication for Certificate Revocation

A revocation request may be submitted electronically or verbally in accordance with Section 4.4 (Certificate Revocation and Suspension), and as detailed in the CPS.

The Certificate Manager must authenticate and authorize a request made by an individual to Revoke a Certificate by verifying the requestor's Digital Signature on the signed request or via another method that identifies the Certificate to be Revoked and affords reasonable assurance that the requestor is authorized to make the Certificate revocation request.

An Issuing UICA or RA must furnish detailed Certificate revocation procedures to Subscribers. Such procedures may be provided through publication in a web page.

4. OPERATIONAL REQUIREMENTS

4.1. Application for a Certificate

The procedure for application for a Certificate must be detailed in the Issuing UICA's CPS. The application process may be initiated by the Applicant, which may include Unisys IT, as well as individuals themselves. The application procedure must contain at a minimum:

a. an indication of the policy under which the Certificate is to be issued;
b. the intended purpose(s) for which the Certificate is to be issued (e.g., confidentiality, authentication, non-repudiation);
c. proof of the Applicant's identity, verified for accuracy and correctness, in accordance with Section 3.1(Initial Registration), 3.1.8 (Authentication of Individual Identity), 3.1.9 (Authentication of Devices and Applications), or 3.1.10 (Authentication of Organization Role);
d. proof of the Applicant's authority to request the Certificate, where applicable, in accordance with Section 3.1(Initial Registration), 3.1.9 (Authentication of Devices and Applications), or 3.1.10 (Authentication of Organization Role);
e. submission of the Public Key generated by the Applicant or an indication that the UICA or RA is to generate the corresponding Key Pair; and
f. proof of Private Key possession in accordance with Section 3.1.7 (Proof of Possession of Private Key).

The information provided through the RA enrollment pages or through auto-enrollment by a User presenting Unisys AD credentials will satisfy these requirements. If databases are used to verify identity information provided by an Applicant, these databases must be protected from unauthorized modification to a level commensurate with the Level of Assurance of the Certificate being sought.

Applicants must protect the Private Key and the proper use of the Certificate.

If the Certificate is issued automatically to an individual, notice of the Policy under which the Certificate is issued will be given to the individual.

The act of completing the application process shall be construed as the Applicant's consent for the UICA to issue the Certificate.

Requesting a Certificate does not oblige a UICA to issue a Certificate.

Certification Authority Authorization (CAA) DNS Resource Records are not in use.

4.1.1. Delivery of Public Key for Certificate issuance

Key Pairs must be generated in accordance with Section 6.1 (Key Pair Generation and Installation).

Public keys must be delivered for Certificate issuance in a way that binds the Applicant's verified identity to the Public Key. For all levels of assurance, this binding may be accomplished using cryptography in accordance with Section 6.1.3 (Public key delivery to Certificate issuer). If cryptography is used, it must be at least as strong as that employed in Certificate issuance.

The methods employed for Public Key delivery must be detailed in an Issuing UICA's CPS.

For Test Assurance and Basic Assurance, no trusted delivery mechanism is required.

For Medium Assurance, the binding of the Certificate Subject's verified identity to the Public Key may be accomplished using cryptography or an equivalently secure physical and procedural mechanism (e.g., via floppy disk sent via registered mail or courier).

In those cases where Key Pairs are generated by the Issuing UICA, RA, or a Service Provider on behalf of the Subscriber, the UICA, RA, or Service Provider must implement secure mechanisms to ensure that the Key Pair is securely distributed to the proper Subscriber. The Issuing UICA, RA, or Service Provider must also implement procedures to ensure that the certificate is not used by an unauthorized Entity.

4.2. Certificate issuance

Only the PMA can authorize a UICA to issue a Certificate for a Subordinate CA in accordance with Section 1.3.1.

After successful completion of the application procedure or autoenrollment process for an End-Entity Certificate in accordance with Section 4.1 (Application for a Certificate), the Issuing UICA, its RA, or a Service Provider acting on the UICA's behalf, must:

a. provide Activation Data and instructions for the collection and/or acceptance of a Certificate from the UICA;
b. create a Certificate using the contents of the Certificate request in the format specified in Section 7 (Certificate and CRL profiles); and
c. distribute the new Certificate(s), and any associated Private Keys if appropriate, directly to the Subscriber in accordance with Section 4.2.1 (Delivery of Subscriber's Private Key to Subscriber).

4.2.1. Delivery of Subscriber's Private Key to Subscriber

In most cases, a Subscriber's private signing key is generated and remains within the cryptographic boundary of an operating system or hardware module under the control of the Subscriber. If the Subscriber generates the Key Pair, there is no need to deliver the Private Key. If the key is generated on the Registration Authority it must be delivered securely to the Subscriber and not retained on the Registration Authority.

If the key is generated elsewhere on a hardware cryptographic module, then the module must be delivered to the Subscriber. Accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. The Subscriber must acknowledge receipt of the module. Under no circumstances shall anyone other than the Subscriber have substantive knowledge of or control over private signing keys after generation of the key. Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the Private Key to the Subscriber, other than by the Key Escrow mechanism provided for in Section 6.2.4.

Hardware tokens containing UICA private signature keys may be backed-up in accordance with security audit requirements defined Section 4.5.1 (Types of Events Recorded) and Section 6.2.4 (Private Key back-up).

Normally, a Certificate is issued to a single Subscriber. For cases where there are several persons acting in one capacity, and where non-repudiation for transactions is not desired, a Certificate may be issued that corresponds to a Private Key that is shared by multiple persons (e.g., a Certificate whose Subject is an organizational role). In these cases:

A Responsible Individual acts as the Subscriber to ensure control of the Private Key, including maintaining a list of persons who have been given a copy of the Private Key or authorized to access and use the Private Key, and accounting for which person or persons had control of the key at what time.

The list of those holding the shared Private Key must be retained by the Responsible Individual and provided to the Issuing UICA or its designated representative upon request. The procedures for issuing tokens for use by multiple persons must comply with all other stipulations of this CP (e.g., key generation, Private Key protection, and Subscriber obligations).

4.2.2. Delivery of the UICA's Public Keys

An Issuing UICA must ensure that its Subscribers and Qualified Relying Parties may obtain a copy of its Public Key as well as the Public Key of all superior CA keys up to the self-signed Root UICA's Public Key and Certificate in a trustworthy fashion.

The Public Key and Certificate of the Issuing UICA may be included with the delivery of the Subscriber's Certificate. The Public Key and Certificate must also be posted in the Repository in accordance with Section 1.3.4 (Repositories). Acceptable methods for delivery of any Intermediate UICA and the Root UICA's Public Key and Certificate include but are not limited to:

a. loading the Certificate onto tokens delivered to Subscribers or Qualified Relying Parties via secure mechanisms;
b. distribution of the Certificate through secure out-of-band mechanisms; and
c. providing for the download of the Certificate from a web site secured with a currently Valid Certificate of equal or greater Assurance Level than any Certificate which may be issued to a Subscriber by the Issuing UICA.

4.3. Certificate acceptance

Where a Subscriber has initiated a request for a Certificate he or she must explicitly indicate acceptance of a Certificate to the Issuing UICA or RA. During this process the Subscriber must certify that at the time of Certificate acceptance that to his or her knowledge:

a. all information in the Certificate is true and complete; and
b. the Private Key associated with the Certificate will be used in accordance with the usage restrictions contained in the Certificate and in this CP.

In the case of automatically-issued Certificates, Unisys IT Administration will act on behalf of the Subscriber and enable the transparent issuance of some types of Certificates to an individual User or User-controlled device based on the existence of the User or device in the Unisys AD security database. In web-enrollment, Users may acquire Certificates through direct request at the UICA. In these cases no explicit acceptance of the Certificate is required. The policy restriction in items a) and b) will be communicated to the User through an email notification upon initial enrollment, and through web-based corporate policies relevant to appropriate use of email and certificates. The Unisys Ethics Training program requires employees annually to acknowledge their understanding and their acceptance of Unisys corporate policies.

The Operational Period for a Certificate begins on the date of issue not on the date of acceptance.

4.4. Certificate suspension and revocation

4.4.1. Circumstances for revocation

A Certificate must be Revoked if:

a. The AD account on which the Certificate is based is terminated;

b. the Private Key corresponding to the Public Key identified in the Certificate is known or suspected to be misused or compromised (e.g., unauthorized access to the Private Key is known or suspected, the Private Key is lost, the Cryptographic Module in which the Private Key is stored is damaged or destroyed, etc.);
c. it is determined that the name or other identifying information contained in the Certificate is no longer valid, or that there has been any other material change in the information contained in the Certificate;
d. the CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
e. any person who has been provided authorization to use the private key of an organizational role certificate leaves the group controlling that certificate or is otherwise not authorized continued use of the key, unless the key is maintained on a cryptographic device from which user export is not possible;
f. it is determined that the Certificate was not properly issued in accordance with the CP or this CPS;
g. it is determined that the Subscriber has failed to meet its material obligations under the CP, or any other agreement, regulation, or law applicable to the Certificate that may be in force;
h. the UICA/RA determines that the Subscriber has not accepted the Certificate in a timely manner;
i. a higher level or Issuing CA's Private Key is compromised;
j. the Subscriber requests in writing that the CA revoke the Certificate;
k. the Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
l. the CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
m. the CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
n. the CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
o. revocation is required by the CA's Certificate Policy and/or Certification Practice Statement;
p. the technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties; or
q. a certificate will be Revoked if The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate.

A Certificate must be Revoked for any reason upon receipt by the UICA of a properly authenticated request initiated by a Subscriber.

In the event that a UICA ceases operations, all active Certificates issued by the UICA must be Revoked before the date that the UICA ceases operations; the UICA key pair(s) will be destroyed.

A Subordinate CA Certificate will be revoked within seven (7) days if:

a. the Subordinate CA requests revocation in writing;
b. the Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

c. the Issuing CA obtains evidence that the Subordinate CA’s Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
d. the Issuing CA obtains evidence that the Certificate was misused;
e. the Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice statement;
f. the Issuing CA determines that any of the information appearing in the Certificate is inaccurate or
g. misleading;
h. the Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
i. the Issuing CA’s or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
j. revocation is required by the Issuing CA’s Certificate Policy and/or Certification Practice Statement; or
k. the technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

Who can request revocation

A revocation request may be initiated by:

a. the Subscriber;
b. an agent of the issuing UICA, or RA; or
c. other responsible individuals so authorized by the Corporation (e.g., Unisys AD Administrators, Human Resources personnel, the supervisor of a given employee or contractor)

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

Procedures for Revocation Request

Revocation requests may be initiated in person, via telephone or by digitally signed email requests submitted to the UIPKI CM at ~PKI Certificate Manager (pki.cm@unisys.com) when requested in accordance with Authentication for Certificate Revocation (Section 3.4). Revocation requests may also be made by notice from AD Administration.

Each revocation request must indicate the reason for the revocation (e.g., key compromise, change in affiliation, Subscriber request) and identify the Certificate to be Revoked.

The authentication of the requester’s identity and authority to initiate the revocation request must be performed in accordance with Section 3.4 (Authentication for Certificate Revocation).

A properly authenticated and complete request will be processed by the UIPKI CM after call-back to the number listed for Subscriber in the Corporate directory in order to confirm the request.

The next published CRL must contain the Revoked Certificate.

When a Certificate is Revoked, the Issuing UICA or RA must notify the Subscriber in accordance with the procedure specified in the UICA's CPS.

If an individual Subscriber terminates his/her relationship with Unisys, hardware tokens containing certificates issued with that Subscriber's name must be surrendered. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction. If the token cannot be obtained, then all Subscriber's certificates associated with the unretrieved tokens shall be immediately revoked.

Time within which CA Must Process the Revocation Request

The CA SHALL begin investigation of a Certificate Problem Report within twenty four hours of receipt, and decide whether revocation or other appropriate action is warranted based on at least the following criteria:
1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight
than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
4. Relevant legislation.

Certificate Revocation List

A Certificate Revocation List (CRL) is generated in accordance with the schedule in Section 4.4.3 (CRL Issuance Frequency). A Revoked Certificate is removed from the CRL after it expires.

Revocation Request Grace Period

No stipulation.

4.4.2. Circumstances for Suspension

A Certificate may be Suspended, at the discretion of an agent of the UIPKI RA, if a revocation request is received but the revocation request cannot be immediately authenticated in accordance with Section 3.4 (Authentication for Certificate Revocation).

Who Can Request Suspension

Only an agent of a UICA can request a suspension of Certificates issued by that UICA.

Procedure for Suspension Request

A suspension request must indicate the reason for the revocation (e.g., key compromise, change in affiliation, Subscriber request) and identify the Certificate to be Suspended.

The UIPKI RA must investigate the circumstances of the suspension and attempt to authenticate the original revocation request. The Suspended Certificate must be either Revoked or reinstated prior to the end of the suspension period defined below under Limits on Suspension Period.

When a Certificate is Suspended, the UICA or RA must notify the Subscriber in accordance with the procedures defined in its CPS.

Limits on Suspension Period

The suspension period may not exceed two (2) weeks.

4.4.3. CRL Issuance Frequency

The Root and Intermediate UICAs must issue a CRL at least annually, or more frequently as required by Cross-Certification agreements with other enterprises and organizations, and within 6 hours of confirmation that a Subordinate UICA has been compromised. An Issuing UICA must issue CRLs within the time limits specified in the following table. CRLs may be issued more frequently than captured therein, however, they may not be published later than the next scheduled update. Issuance of periodic base CRLs with "delta" updates is acceptable.

Assurance Level	**CRL Issuance Frequency**
Test	At least once each day
Basic	At least once each day
Medium	At least once each 24 hours
High	At least once each 6 hours

4.4.4. CRL Checking Requirements

Prior to reliance, a Qualified Relying Party must check the status of Certificates using a CRL checking mechanism that includes:

a. verifying the authenticity of the CRL by checking its Digital Signature and the Digital Signatures associated with all Certificates in the Certification Path using a method equivalent to that defined in X.509v3; and
b. checking the Operational Period of the CRL to ensure that the CRL is the most current CRL and has not expired.

Certificates may be stored locally on a Qualified Relying Party's system. However, the Certificate must be validated before each use through a check on the current CRL.

If no valid CRL can be obtained due to system failure or service interruption, the Qualified Relying Party should not rely on the Certificate. Reliance on a Certificate under these circumstances is at the Qualified Relying Party's risk.

The previous CRL may be re-signed to extend the CRL Issuing Frequency interval, in the case of unavailability of the UICA.

It is the Qualified Relying Party's responsibility to determine how often new revocation data should be obtained, taking into consideration the risk, responsibility, and consequences for using a Certificate whose revocation status cannot be guaranteed. This determination is under the sole control and discretion of the Qualified Relying Party.

Where other protocols are supported for Certificate status checking, a Qualified Relying Party may use these protocols in lieu of CRL checking.

4.4.5. Online Certificate Status Checking Availability

A UICA may enable Qualified Relying Parties to check Certificate status on-line using industry standard protocols such as that defined in the IETF PKIX RFC2560 *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, June 1999.

Online Certificate status checking protocols supported must be identified in the UICA's CPS.

Online Revocation Checking Requirements

See Section 4.4.4 (CRL Checking Requirements).

4.4.6. Other Forms of Revocation Advertisements Available

No stipulation.

4.4.7. Checking Requirements for Other Forms of Revocation Advertisements

No stipulation.

4.4.8. Special Requirements Regarding Key Compromise

See Section 4.8.3 (Key Compromise Plan).

4.5. Security Audit Procedures

There are no security audit procedure requirements for UICAs operating at a Test Assurance Level.

For all other Assurance Levels, audit log files must be automatically or manually generated for all events relating to the physical and electronic security of the UICA. If possible, the UICA system's security audit logs should be automatically collected. Where this is not possible, the UICA must use a logbook, paper form, or other physical mechanism. The UICA must retain all security audit logs, both electronic and non-electronic. Reviewers may access security logs during compliance audits or inspections. The UICA must archive and retain all security audit logs related to each audit event defined in this section in accordance with Section 4.6.2 (Retention Period for Archive).

4.5.1. Types of Events Recorded

Auditing capabilities of the UICA operating system and supporting PKI components must be enabled to support the automatic recording and time-stamping of audit records. The system time referenced to create the time stamp must be synchronized to a root time reference source.

If there is no technical support for automatic logging, the UICA or RA as appropriate must employ a manual method to record and timestamp the audited event.

At a minimum, each audit record includes the following:

a. event type;
b. date and time of occurrence.
c. success or failure indicator, where appropriate; and
d. identity of the Entity that caused the event.

A message from any source requesting an action by the UICA or RA is an audited event and must include date and time, source, destination, and contents.

The PKI function and associated events that must be audited are described in the table below.

CA or RA Function	Auditable Event
Security Audit	❑ Changes to the audit parameters. ❑ Any attempt to delete or modify the audit logs.
Identification and Authentication	❑ Successful and unsuccessful attempts to assume a role. ❑ Change in the value of maximum authentication attempts. ❑ Maximum number of unsuccessful authentication attempts during User login. ❑ An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts. ❑ An administrator changes the type of required authenticator (i.e., from password to biometrics).
Key Generation	❑ Whenever the CA or RA generates a key (not mandatory for single session or one-time use symmetric keys).
Private Key Load and Storage	❑ The loading of Entity private keys ❑ All access to an End-Entities private keys backed-up for purposes of Key Recovery
Trusted Public Key Entry, Deletion, and Storage	❑ All changes to the trusted public keys, including additions and deletions.
CA Private Key Export	❑ The export of private keys (keys used for a single User session or message are excluded).
Certificate Registration	❑ All Certificate requests.

	□ All Certificate generations. □
Certificate Revocation or Suspension	□ CRL Issuance. □ All Certificate revocation requests. □ All Certificate suspension requests. □ All Certificate reinstatement requests.
Certificate Status Change Approval	□ The approval or rejection of a Certificate status change request.
CA/RA Configuration	□ Any security-relevant changes to the CA or RA’s configuration.
Account Administration	□ Roles and Users are added or deleted. □ The access control privileges of a User account or a role are modified.
Certificate Profile Management	□ All changes to Certificate profiles.
Revocation Profile Management	□ All changes to revocation request profiles.
Certificate Revocation List Profile Management	□ All changes to the Certificate Revocation List profile.
Miscellaneous	□ Installation of the operating system. □ Installation of the CA or RA software. □ Installation of hardware Cryptographic Modules. □ Removal of hardware Cryptographic Modules. □ Destruction of hardware Cryptographic Modules. □ System start-up. □ Logon attempts to the CA or RA application. □ Receipt of hardware or software. □ Attempts to set or modify passwords. □ Backing up of CA or RA internal database. □ Restoring of the CA or RA internal database.

	❑ File manipulation (creation, modification, renaming, moving). ❑ Posting of any material to a Repository. ❑ Access to the CA or RA internal database. ❑ All Certificate compromise notification requests. ❑ Loading tokens with Certificates. ❑ Shipment of tokens. ❑ Zeroizing tokens. ❑ Re-key, Renewal, or Update of a CA Certificate. ❑ Configuration changes to the CA or RA server including: ○ Hardware ○ Software ○ Operating System ○ Patches ❑ Security Profile
Physical Access/Site Security	❑ Personnel access to room housing the CA. ❑ Access to the CA or RA server. ❑ Known or suspected violations to physical security.
Anomalies	❑ Software error conditions. ❑ Software integrity-check failures. ❑ Receipt of improper messages. ❑ Misrouted messages. ❑ Network attacks (suspected or confirmed). ❑ Equipment failure. ❑ Electrical power outages. ❑ Uninterruptible power supply (UPS) failure. ❑ Obvious and significant network service or access failures. ❑ Violations of Certificate Policy

	□ Violations of the Certification Practice Statement □ Resetting operating system clock.

4.5.2. Frequency of Audit Log Processing

The Root and Intermediate UICA systems are normally in a powered down state. Inspection of audit logs after each session is required.

The Issuing UICA systems are normally powered up and online; trusted personnel, who serve in the UICA Auditor role per Section 5.2.1.3 (UICA Auditor), will review audit logs at least weekly. The trusted personnel who review the audit logs must explain all significant events in an audit log summary. The review must include but is not limited to:

a. verifying that logs have not been tampered with;
b. inspecting all log entries and focusing special attention on investigating any alerts or irregularities among the log entries;
c. examining a statistically significant set of security audit data generated in the time interval between reviews and conducting a reasonable search for malicious activity; and
d. recording any action that UICA personnel take as a result of the review.

4.5.3. Period for which Audit Logs are Kept

Audit logs must be kept onsite for at least 2 months and archived in accordance with Section 4.6 (Records Archival).

4.5.4. Protection of Audit Logs

Audit logs to the extent possible, must be closed to modification by any human or computer process. The audit log must be controlled in such a manner that:

a. Only authorized personnel have access to read audit logs; and
b. Only authorized personnel are allowed to archive audit logs.

The individual who removes audit logs from the UICA system must be a trusted individual different from the individuals who control the UICA signing keys.

Only those authorized personnel responsible for the destruction of archived audit logs at the end of the retention period, as defined in Section 4.6.2 (Retention Period for Archive), may be granted modification access to the archived audit log.

4.5.5. Audit Log Back Up Procedures

Audit logs and audit log summaries must be backed up daily. At periodic intervals, not to exceed 1 month, a copy of the audit log back up must be delivered offsite for storage in a separate location from the UICA. See Section 4.6 (Records Archival) for additional storage requirements.

4.5.6. Audit Collection System

The audit log collection system may be internal or external. Audit log processes must be invoked at system startup, and cease only at system shutdown.

Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, then the UICA operations manager must determine whether to suspend UICA operations until the problem is remedied.

4.5.7. Notification of Audit Subjects

There is no requirement to provide notice that an event was audited to the individual, organization, device, or application that caused the event.

4.5.8. Vulnerability Assessments

The UICA must perform routine self assessments of security controls. Such assessments must be performed in accordance with the UICA's CPS.

4.6. Records Archival

4.6.1. Types of Events Archived

A UICA's archive must contain sufficient detail to prove that the UICA was operating properly and in accordance with its CPS at a point in time or the validity of any Certificate issued by the UICA.

A UICA operating at a test Assurance Level does not have any archive requirements. For all other Assurance Levels, the UICA at a minimum, must record and archive:

a. the UICA's accreditation by the PMA;
b. its CPS;
c. contractual agreements related to the operation of the UICA or RA;
d. PKI software, operating system, and equipment configuration.
e. modifications and updates to the configuration;
f. requests to issue, Renew, Re-key, Update, or Revoke a Certificate.
g. identity information used to authenticate a Subscriber's identity in accordance with Section 3 (Identification and Authentication);
h. documentation of receipt and acceptance of Certificates;
i. Certificate application forms;
j. Subscriber agreement forms;
k. documentation related to the receipt of tokens;
l. all Certificates issued or published;
m. record of the Re-key of UICA Certificate or CRL signing Certificate;
n. all CRLs issued, published, or both;
o. all security audit logs;
p. other data or applications used to verify the content in the archive; and
q. operational documentation required by compliance auditors.

4.6.2. Retention Period for Archive

The minimum retention periods required for archive data are identified in the following table.

If the medium on which the data is stored cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media. The UICA must maintain the applications required to access the archived data during its retention period.

Assurance Level	Retention Period
Test	No minimum.
Basic	7 years
Medium	10 years and 6 months.
High	20 years and 6 months.

4.6.3. Protection of Archive

The UICA must ensure that no unauthorized person or process can write to, modify, or delete the archive.

Trusted personnel must transfer archived records to new media when authorized by the UICA under controlled, supervised, and documented procedures.

Archive media must be stored in a safe, secure storage facility separate from the UICA facility.

4.6.4. Archive Backup Procedures

No stipulation

4.6.5. Requirements for Time-Stamping of Records

No stipulation.

4.6.6. Archive Collection System (Internal or External)

No stipulation.

4.6.7. Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store the UICA archive information must be contained in the UICA’s CPS.

4.7. Key Changeover

Trusted personnel must Re-key a UICA Certificate following the procedures defined in the UICA’s CPS.

A UICA’s signing Certificate must be periodically Re-keyed. When a UICA signing Certificate is Re-keyed the old Certificate and signing key may no longer be used to issue new end-entity Certificates. The old

Certificate and Public Key, however, must be kept available to provide for the validation of Certificates issued by the UICA until the last Certificate issued using the old UICA signing key has expired. If the old Private Key is also used to sign CRLs that contain Certificates signed with that key, then the old key must be retained and protected. The Key Changeover period is the interval of time when the UICA phases out its usage of the old Private Key.

The required Key Changeover schedule determined by the UICA based on the Operational Period of its signing Certificate and the Operational Periods of the Certificates that it issues.

The following UICA Key Changeover schedule must be employed:

a. The Root UICA Certificate Operational Period must be equal to 20 years, with Re-key 10 years prior to the Operational Period end;
b. An Intermediate UICA's Certificate Operational Period must be equal to 10 years, with Re-key 4 years prior to the Operational Period end; and
c. An Issuing UICA's Certificate Operational Period must be equal to 6 years, with Re-key at no less than 2 years prior to the Operational Period end.

An Issuing UICA that issues Certificates with Operational Periods in excess of 2 years must adjust the Key Changeover schedule as required to provide for the use of the old UICA signing key and Certificate until the last Certificate issued by the UICA has expired.

4.8. Compromise and Disaster Recovery

4.8.1. Computing Resources, Software, and/or Data Are Corrupted

If a UICA's equipment is damaged or rendered inoperative, but the UICA signature keys are not destroyed, trusted UICA personnel must reestablish the UICA's operational servers as quickly as possible giving priority to the generation and publication of CRLs.

4.8.2. UICA Certificate is Revoked

In the event of the need for revocation of a UICA's Signing Certificate, the UICA must immediately notify:

a. the PMA;
b. all CAs to whom it has issued Cross-Certificates;
c. all of its RAs; and
d. all Subscribers;

The UICA must also publish the Certificate serial number on an appropriate CRL.

After addressing the factors that led to revocation, the UICA may:

a. generate a new CA signing Key Pair; and
b. re-issue Certificates to all Entities and ensure all CRLs are signed using the new key.

Revoking a Subordinate UICA key requires the secure and witnessed generation of a replacement Private Key and the trustworthy distribution of its corresponding Public Key. The Root UICA or must act as quickly as possible, but in accordance with documented procedures, to re-establish a valid Subordinate UICA Public Key.

If it is determined that the CRL and Certificate issuing processes will not be functioning properly in time to meet the requirements for CRL issuance in accordance with Section 4.4.3 (CRL Issuance Frequency), the UICA must take commercially reasonable steps to notify Qualified Relying Parties.

If an End-Entity Certificate is Revoked it may not be Re-keyed, Renewed, or Updated. The Subscriber may reapply for a new Certificate in accordance with Section 4.1 (Certificate Application)

4.8.3. Private Key is Compromised (Key Compromise Plan)

In the event of the compromise of a UICA's private signing key, prior to re-certification a UICA must:

a. request revocation of Cross-Certificates issued to the UICA;
b. revoke all Certificates issued using the compromised Private Key; and
c. provide appropriate notice in accordance with Section 4.8.2(UICA Certificate is Revoked).

After addressing the factors that led to key compromise, the UICA may:

a. generate a new UICA signing Key Pair; and
b. re-issue Certificates to all Entities and ensure all CRLs are signed using the new key.

In the event of the compromise, or suspected compromise, of any other Entity's Private Key, the Entity must immediately notify the Issuing UICA and request the revocation of the Certificate in accordance with Procedures for Revocation Request in Section 4.4.1 (Circumstances for Revocation).

A UICA must ensure that its CPS and appropriate agreements contain provisions outlining the means it will use to provide notice of compromise or suspected compromise.

4.8.4. Secure Facility after a Natural or Other Disaster (Disaster Recovery Plan)

A UICA must have in place an appropriate disaster recovery and business resumption plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. The plan must include giving priority to the generation and publication of CRLs of Issuing CAs.

4.9. UICA Termination

In the event of the termination of a UICA, the UICA must:

a. notify all Subscribers and any Entities with whom it has cross-certified prior to the cessation of operations;
b. Revoke all active Certificates issued by the UICA; and
c. publish revocation information.

The UICA must make appropriate provisions for the retention of the archive in accordance with Section 4.6 (Records Archival).

The UICA must also take commercially reasonable steps to notify Qualified Relying Parties of the termination of CA services, to provide for the removal of the UICA from the Qualified Relying Parties list of Trusted Authorities.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Security Controls

The Physical Security controls described in this section apply to the facility housing the UICA and any related component systems.

Where RA equipment is not co-located with the UICA, RA equipment must be protected from unauthorized access while the Cryptographic Module is installed and activated. The RA must implement physical access controls to reduce the risk of equipment tampering even when the Cryptographic Module is not installed and activated. These security mechanisms must be commensurate with the level of threat in the RA equipment environment.

5.1.1. Site Location and Construction

The location and construction of the facility that houses UICA equipment must be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, must provide robust protection against unauthorized access to UICA equipment and records.

5.1.2. Physical Access

UICA equipment must be protected from unauthorized access. At a minimum, physical security controls must protect UICA equipment, records, and Cryptographic Modules such that:

a. unauthorized or inappropriate access to hardware is not permitted;
b. all removable media and paper containing sensitive plain-text information is stored in secure containers and securely disposed;
c. manual or electronic monitoring for physical intrusion is in place at all times;
d. an access log is maintained and periodically inspected;
e. removable Cryptographic Modules are inactivated prior to storage.
f. Activation Data is securely stored in a container separate from the cryptographic hardware security module or memorized;
g. a security checklist of the UICA enclave is executed whenever the facility is to be left unattended and the time and date of the check and the name of its executor(s) is logged;
h. trusted UICA personnel supervise all visitors allowed into the secure UICA room and ensure that the date and time of their entry and departure is recorded;
i. dual (two-person) authentication is required for entry into or exit from the secure UICA room; and
j. any remote administration solution must be approved by the PMA and must be initiated from a secure facility.

The perimeter of the building that houses the secure UICA room must be physically sound such that no gaps in the perimeter exist where a break-in could easily occur (e.g., roof access points, perimeter and emergency doors, and main egress doors are monitored or alarmed at all times).

All personnel display visible identification that is checked prior to facility entry. Either a physical inspections of badges or electronic verification of the identification badge using card readers with supplemental code-punching device, biometrics, or equivalent is required.

Visitors to the facility that houses the secure UICA room must be supervised and their date and time of entry and departure are recorded.

5.1.3. Power and Air Conditioning

The UICA facility must have sufficient power and air conditioning to sustain a reliable operating environment and to support a smooth shutdown of operations in the absence of commercial power.

The UICA must have sufficient backup capability to automatically lockout input, finish any pending actions, and record the state of the equipment before the lack of power or air conditioning causes a shutdown.

The UIPKI Repository must have the same level of uninterrupted power supply (UPS) to preclude shutdown or to support a smooth shutdown of UICA operations. Power and telecommunications cabling carrying data or supporting UICA services is protected from interception or damage.

5.1.4. Water Exposures

UICA equipment must be elevated or protected to minimize the exposure to water. Moisture detectors must be installed in areas susceptible to flooding.

5.1.5. Fire Prevention and Protection

UICA facility must have an automatic fire (smoke) detection system and fire extinguishing equipment. Any fire doors on the security perimeter around the UICA facility must be alarmed and automatically shut. Either the UICA security plan or the disaster recovery plan must address egress during and after a fire emergency.

5.1.6. Media Storage

UICA media must be stored in a manner to protect it from theft, unauthorized alteration, and accidental damage (i.e., water, fire, and electromagnetic emanations). Media that contains audit, archive or backup data must be duplicated and stored in a location separate from the UICA.

5.1.7. Waste Disposal

Media used to collect or transmit sensitive data must be destroyed such that the information is unrecoverable prior to disposal.

5.1.8. Off-site Backup

The UICA systems must be backed-up, sufficient to recover from system failure, on a daily schedule during the workweek. The UICA must store one full system backup copy onsite and a second full backup copy at an offsite location at least weekly. Both back-up copies must be protected with physical and procedural controls commensurate with those employed for the protection of the UICA.

5.2. Procedural Controls

5.2.1. Trusted Roles

A “Trusted Role” refers to one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

All employees, representatives, contractors, and consultants of the UICA (collectively, "personnel") that have access to or control over cryptographic operations that may materially affect the UICA's issuance, use, suspension, or revocation of Certificates, including access to restricted operations of the UICA's Repository, serve in a Trusted Role. Such personnel must be properly trained to perform the duties assigned to the Trusted Role and the UICA must provide for the separation of duties or the assignment of tasks to more than one person such that malicious activity would require collusion.

The CPS will define the roles used during key generation, based on the hardware and software employed. A UICA must provide for separation of duties between the following Trusted Roles in its ongoing operations:

a. UICA administrator,
b. certificate manager,
c. system auditor, and
d. system operator.

UICA Administrator

A UICA Administrator may be authorized to:

a. Install, configure, and maintain the UICA,
b. Establish and maintain UICA system accounts,
c. Configure Certificate profiles or templates and audit parameters, and
d. Generate and backup UICA keys.

A UICA Administrator may not issue Certificates to Subscribers.

Certificate Manager

A Certificate Manager may be authorized to:

a. Register new Subscribers and request the issuance of Certificates,
b. Verify the identity of Subscribers and accuracy of information included in Certificates,
c. Approve and execute the issuance of Certificates, and
d. Request, approve, and execute the revocation of Certificates.

System Auditor

A System Auditor may be authorized to:

a. Review, maintain, and archive audit logs, and
b. Perform or oversee internal compliance reviews to ensure that the UICA is operating in accordance with its CPS.

System Operator

A System operator may be authorized to:

a. perform the routine day to day operations such as system backups and recovery or changing recording media, and
b. monitor system and network performance.

5.2.2. Separation of Roles

To ensure that one person cannot act alone to circumvent safeguards, the UICA must identify separate individuals for each Trusted Role to the extent that such separation is operationally feasible.

For UICAs issuing medium or high assurance Certificates, controls must exist to preclude the same individual assuming both:

a. a UICA Administrator and a Certificate Manager role;
b. a UICA Administrator and a System Auditor role;
c. a System Auditor and a System Operator role; and
d. a System Auditor and a Certificate manager role.

5.2.3. Number of Persons Required Per Task

Key-pair generation and the initialization of the Root and Intermediate authorities require the participation of UICA trusted individuals, the KeyGen trustees, named to represent the corporation. At least three (3) UICA trustees are required to activate the Root and Intermediate UICA signing keys.

5.2.4. Identification and Authentication for Each Role

Identification and authentication mechanisms must be employed to control account access for each role.

5.3. PERSONNEL CONTROLS

5.3.1. Background and Qualifications

A UICA must identify the individual or group accountable for the operation of the UICA in its CPS.

All individuals assigned to a Trusted Role must have the background, qualifications, and training to perform assigned duties in a trustworthy and competent manner.

5.3.2. Background Investigation

All individuals assigned to Trusted Roles must undergo background checks to verify their trustworthiness and qualifications. The criteria and procedures for such background checks must be defined in the UICA’s CPS.

5.3.3. Training Requirements

Individuals assigned to a Trusted Roles must be trained to competently and securely perform the duties associated with their respective roles. This training, at a minimum, must cover:

a. UICA/RA security principles and mechanisms;
b. UIPKI Certificate Policy and Certificate Practice Statements;
c. PKI software and versions used for UICA or RA systems;
d. PKI duties they are expected to perform; and
e. disaster recovery and business continuity procedures.

Documentation must be maintained identifying all personnel who received training and the type of training completed.

5.3.4. Retraining Frequency and Requirements

Individuals assigned to Trusted Roles must be made aware of changes in operations and receive appropriate training whenever a change in the PKI configuration, policies, or procedures occurs.

When any significant change affecting UICA operations occurs, a training or awareness plan must be developed and execution of the plan must be documented.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

A UICA must take appropriate administrative and disciplinary action when Personnel involved in UICA operations commit unauthorized actions. Such actions may include being barred from serving in Trusted Roles and additional legal and/or disciplinary actions.

5.3.7. Contracting Personnel Requirements

All contracting personnel involved in UICA operations must comply with the applicable sections of this CP and the UICA’s CPS including, but not limited to Sections 5.3.1 through 5.3.6.

5.3.8. Documentation Supplied to Personnel

Personnel involved in UICA or RA operations must be provided a copy of this CP, relevant sections of the UICA’s CPS, and sufficient operational documentation to carry out their duties and responsibilities.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation And Installation

6.1.1. Key Pair Generation

Key Pairs must be generated in Cryptographic Modules in accordance with Section 6.1.8 (Hardware/Software Key Generation) and 6.2.1 (Standards for Cryptographic Modules)

The procedure for the generation of UICA keys must be documented in the UICA's CPS and must generate auditable evidence that the documented procedures were followed. Such documentation must be sufficiently detailed to show that appropriate role separation was used.

6.1.2. Private Key Delivery to Entity

See Section 4.2.1 (Delivery of Subscriber Private Key to Subscriber)

Private signing keys used by UICA or RA personnel and devices and applications employed to support the issuance of Certificates by the UICA may be generated under the control of the Entity or delivered in a hardware token or hardware security module by the UICA. A UICA must detail the method employed for Private Key delivery in its CPS.

6.1.3. Subscriber Public Key Delivery to UICA

See Section 4.1.1 (Delivery of Public Key for Certificate Issuance).

6.1.4. UICA Public Key Delivery to Users

See Section 4.2.2 (Delivery of the CAs Public Keys).

6.1.5. Key Sizes

End-Entity keys must be generated as 2048 bit RSA or DSA, with SHA-2 (or better), in accordance with FIPS 186 or as 256 bit ECC, with SHA-2 (or better).

UICA keys must be 2048 bit RSA or DSA keys or higher, with SHA-2 (or better), in accordance with FIPS 186.

Where SSL or another protocol providing similar security is used to accomplish any of the requirements of this CP, encryption strength must be at least triple-DES or equivalent for the symmetric key, and at least 2048 bit RSA or equivalent for the asymmetric keys.

6.1.6. Public key parameters generation

Public key parameters prescribed in the Digital Signature Standard (DSS) must be generated in accordance with FIPS 186.

6.1.7. Parameter quality checking

Parameter quality checking must be performed in accordance with FIPS 186 or a more stringent standard approved by the PMA.

6.1.8. Hardware/Software Key Generation

The requirement for hardware or software based key generation is based on the Assurance Level of the Certificate as defined in the table below.

Assurance Level	Hardware/Software
Test	no stipulation
Basic	software or hardware
Medium	software or hardware
High	hardware only

6.1.9. Key Usage Purposes

Public keys that are bound into Certificates must be certified for use in signature or encrypting, but not both, except as specified below.

The use of a specific key is determined by the key usage extension in the Certificate in accordance with X.509v3.

For example, Certificates to be used for Digital Signatures (including authentication) must assert the digitalSignature and nonrepudiation bits. Certificates to be used for encryption must assert the dataEncypherment and/or keyEncypherment bits.

UICA Certificates may assert either or both the CRLSign and CertSign bits depending on whether the UICA uses the same or different signing Certificates for both Certificate and CRL signing.

These restrictions are not intended to prohibit use of protocols such as SSL that provide authenticated connections using key management Certificates.

Test and Medium Assurance Level Certificates may be issued with a key usage extension that enables use of the Private Key for both Digital Signature and encryption where required to support legacy Secure Multipurpose Internet Mail Extensions (S/MIME) applications. Such "dual-use" Certificates must be generated and managed in accordance with their respective Certificate requirements, except where otherwise noted in this CP. Such "dual-use" Certificates may never assert the non-repudiation key usage bit, and must not be used for authenticating data that will be verified on the basis of the dual-use Certificate at a future time. Private keys associated with such Certificates may not be escrowed or backed-up by the UICA for purposes of Key Recovery. UICAs are encouraged at all levels of assurance to issue Subscribers two Key Pairs, one for data encryption and one for Digital Signature and authentication.

Multiple sets of private keys and Certificates will be issued to individuals serving in Trusted Roles. One set is for their use in the performance of their role, issued by the UICA. The other is for personal use as an Employee and will be issued by an Issuing UICA.

6.2. Private Key Protection

6.2.1. Standards for Cryptographic Modules

The relevant standard for Cryptographic Modules is *Security Requirements for Cryptographic Modules*, FIPS 140-1, published by the National Institute of Standards and Technology (NIST).

Cryptographic modules holding End User keys must be validated to the FIPS 140-1 level 2 or to an equivalent standard approved by the PMA. Minimum requirements for the security of Cryptographic Module used by different Entities at each Assurance Level are defined below.

Assurance Level	**UICA**	**Subscriber**	**RA**
Test	No stipulation	No stipulation	No stipulation
Basic	level 2 (hardware)	level 1 (hardware or software)	level 2 (hardware)
Medium	level 2 (hardware)	level 1 (hardware or software)	level 2 (hardware)
High	level 3 (hardware)	level 2 (hardware)	level 2 (hardware)

6.2.2. Private Key (n out of m) Multi-Person Control

Multi-person control must be established such that at least two UICA Administrators or a UICA Administrator and an individual serving in another Trusted Role are required to activate a Root or Intermediate UICA's private signing key(s). One person control may be used at an Issuing UICA which supports fewer than 100,000 Subscribers; Issuing UICAs which support more than 100,000 Subscribers require two person control.

6.2.3. Private Key Escrow

Under no circumstance may a UICA's private signing key be escrowed with a third party.

No other Entity's private signing keys or a dual-use Private Keys may be escrowed.

A UICA may provide for the escrow of an Entity's private decryption key.

6.2.4. Private Key Backup

Copies of a UICA's private signing keys (e.g. cloned token) must be backed-up and stored in an encrypted format on physical media under the same multi-person control as the original key. A copy of the private key may be stored at the UICA facility.

Copies of an RA's Private Keys (e.g. cloned token) may be backed-up and stored in an encrypted format on physical media.

A UICA must not back-up a Subscriber's private signing key or a dual-use Private Key. The Subscriber at his or her discretion may make a backup copy of his or her private signing key.

A UICA may back-up a Subscriber's private decryption key which has been escrowed for purposes of Key Recovery.

Security controls for the backup of an Entity's private decryption key must be commensurate with the Assurance Level of the Certificate and in accordance with this CP. A UICA that backs up private decryption keys must specify the controls and procedures employed in its CPS.

A UICA that provides Key Recovery services must specify the procedural and technical controls employed to support such services in its CPS.

6.2.5. Private Key Archival

Entities' private signature keys must not be archived.

End-Entities' private decryption keys backed-up for purposes of Key Recovery must be archived in accordance with Section 4.6 (Records Archival).

6.2.6. Private Key Entry into Cryptographic Module

UICA Private Keys must be generated and remain within or controlled by the UICA's Cryptographic Module.

End-Entity keys at any Assurance Level may be generated in an operating system's or Cryptographic Module's Cryptographic Service Provider and securely injected into the End-Entity's Cryptographic Module in accordance with Section 4.2.1 (Delivery of Subscriber's Private Key to Subscriber)

6.2.7. Method of Activating Private Key

A UICA's Private Key must be activated in accordance with Section 6.2.2 (Private Key (n out of m) Multi-Person Control).

End-Entities must be authenticated to the Cryptographic Module before the activation of any Private Key(s). Acceptable means of authentication include but are not limited to passwords, pass-phrases, PINs or biometrics. Entry of Activation Data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8. Method of Deactivating Private Key

If Cryptographic Modules are used to store Subscriber Private Keys, then the Cryptographic Modules that have been activated must not be left unattended or otherwise available to unauthorized access. After a

Private Key is used, the Cryptographic Module must be deactivated via a manual logout procedure, or automatically after a period of inactivity. Hardware Cryptographic Modules shall be removed and stored in a secure container when not in use.

6.2.9. Method of Destroying Subscriber's Private Key

Subscribers shall securely destroy their Private Keys when they are no longer required, or in the case of private signing keys hen the Certificates to which they correspond expire or are Revoked.

The method used will depend on the type of software or hardware Cryptographic Module. For software Cryptographic Modules, this can be overwriting the data. For hardware Cryptographic Modules, this will likely be executing a "Zeroize" command. Physical destruction of hardware is not required.

6.3. Other Aspects Of Key Pair Management

6.3.1. Public Key Archival

Public keys must be archived with the Certificate in accordance with Section 4.6 (Records Archival).

6.3.2. Usage Periods for the Public and Private Keys (Key Replacement)

See Section 4.7 (Key Changeover) for usage periods for UICA keys.

A UICA must document usage periods for the Certificates that it issues at each Assurance Level in its CPS. The usage period of an End-Entity's private signing key must not exceed 3 years.

For SSL Certificates which are externally deployed, Certificates validity periods must conform to current CA Browser Forum requirements.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The Activation Data used to unlock the UICA Private Keys must be randomly generated and portions of the data distributed to trusted personnel in accordance with Section 6.2.2 (Private Key n of m - Multi-Person Control).

Activation Data used to unlock End-Entity Private Keys must an appropriate level of strength for the keys or data to be protected. For software Cryptographic Modules, the End-Entity may select Activation Data. For hardware Cryptographic Modules, Activation Data must satisfy the policy enforced by the Cryptographic Module.

6.4.2. Activation Data Protection

Activation Data used by UICA and RA personnel must be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation Data should either be biometric in nature or memorized, not written down. If written down, it must be secured and must not be stored with the Cryptographic Module. The protection mechanism must include a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the UICA's CPS.

Subscribers must keep Activation Data private. If a Subscriber circumvents or deactivates the password mechanism or discloses the Activation Data, the Subscriber is fully liable for any losses that arise from the unauthorized use of his or her Private Key.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

The following computer security functions may be automatically provided as part of the operating system or through a combination of operating system, software, and physical safeguards. The UICA and its ancillary parts must include the following functionality:

a. Authenticated logins;
b. Logging of activities;
c. Discretionary access control;
d. Security audit capability;
e. Restricted access control to UICA services and PKI roles;
f. Separation of duties for PKI roles;
g. Require identification and authentication of PKI roles and associated identities;
h. Require use of cryptography for session communication and database security;
i. Archive UICA and Subscriber history and audit data;
j. Require self-test security-related UICA services;
k. A trusted path for identification and authentication of PKI roles and associated identities;
l. Require a recovery mechanism for UICA keys and UICA system; and
m. Enforce domain integrity boundaries for security critical processes.

6.5.2. Computer Security Rating

No stipulation.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

A UICA operating at the Medium Assurance Level or above must:

a. use commercial software that has been designed and developed under a formal, documented development methodology;
b. procure hardware and software to operate the UICA in a manner that reduces the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);
c. develop any hardware or software specifically for the UICA, as required, in a controlled environment, where the development process is defined and documented;
d. employ procedures that provide for the shipment or delivery of hardware and software via controlled methods that provide a continuous chain of accountability, from the purchase location to the UICA physical location;
e. ensure that UICA hardware and software are fully dedicated to the UICA;.

f. ensure that there are no other applications; hardware devices, network connections, or component software installed on UICA equipment which are not part of the PKI operation;
g. take proper care to prevent malicious software from being loaded onto the UICA equipment;
h. ensure that applications required to perform the operation of the UICA are obtained from sources authorized by local policy;
i. for online (Issuing) CAs, scan hardware and software for malicious code on first use and periodically thereafter; and
j. ensure that hardware and software updates are purchased or developed in the same manner as the original equipment, and are installed by trusted and trained personnel in a defined manner.

6.6.2. Security Management Controls

Trusted personnel must document and control all modifications and upgrades to the configuration of the UICA's systems and employ a formal configuration management methodology for installing and maintaining the UICA system.

A mechanism must be in place for detecting unauthorized modification to the UICA or RA software configuration. Trusted personnel must verify that the UICA software, when first loaded, is supplied from the vendor with no modifications, and is the version intended for use. The integrity of the software must be verified at least weekly on systems which are running with network connectivity.

6.6.3. Life Cycle Security Ratings

No stipulation.

6.7. Network Security Controls

UICA and RA systems must reside on networks that are protected from unauthorized users through a series of firewalls, policies, and procedures. Additional protection must also be provided via the use of hardened operating systems in which unused ports and services are turned off. Transactions with the UICA or RA that contain Confidential Information must take place over protected links (e.g., via SSL). Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8. Cryptographic Module Engineering Controls

See Section 6.2.1 (Standards for Cryptographic Modules).

7. CERTIFICATE AND CRL PROFILES

7.1. CERTIFICATE PROFILE

7.1.1. Version Numbers

A UICA issuing Certificates pursuant to this CP must issue X.509, version 3 Certificates. Per X.509v3 the version field for a version 3 Certificate is populated with the integer "2."

7.1.2. Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions, including any proprietary extensions, must be defined in the UICA's CPS or otherwise documented in a referenced operational document. Certificate extensions included in Certificates must conform to X.509v3.

At a minimum all End-Entity Certificates must contain a critical keyUsage and a non-critical Certificate Policy extension.

7.1.3. Algorithm Object Identifiers

Certificates issued pursuant to this CP must use the OIDs defined in the following table for signature algorithms:

Signature Algorithm	OID
`id-dsa-with-sha1`	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
`sha-1WithRSAEncryption`	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

Certificates issued pursuant to this CP must use the following OIDs for identifying the algorithm for which the subject key was generated:

Algorithm	OID
`id-dsa`	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
`RsaEncryption`	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
`Dhpublicnumber`	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
`id-keyExchangeAlgorithm`	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Certificates containing keys generated for use with DSA or for use with KEA must be signed with `id-dsa-with-sha1`. Keys generated for use with RSA must be signed using `sha-1WithRSAEncryption`.

7.1.4. Name Forms

The Subject and Issuer fields must be populated in accordance with Section 3.1.1 (Types of Names) and Section 3.1.2 (Need for Names to be meaningful) and in accordance with X.509v3.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

End-Entity Certificates issued under this CP must assert the policy OID, which represents the Certificate's Assurance Level and other practices employed in the issuance of the Certificate as defined in Section 1.2 (Identification).

7.1.7. Usage of Policy Constraints Extension

No stipulation.

7.1.8. Policy Qualifiers Syntax and Semantics

End-Entity Certificates issued pursuant to this CP must populate the `cPSuri` Policy Qualifier with the uniform resource locator (URL) for a published Relying Party Agreement, which incorporates by reference this CP.

Policy Qualifiers must be interpreted in accordance with X.509v3.

7.1.9 Certificate Serial Numbers

Certification Authorities shall generate Certificate serial numbers which meet the requirements of the CA Browser Forum.

7.2. CRL PROFILE

7.2.1. Version Numbers

UICAs must issue X.509, version 2 CRLs.

7.2.2. CRL Entry Extensions

Subscriber and Qualified Relying Party PKI software must correctly process all CRL extensions identified in X.509v3.

8. CERTIFICATE POLICY ADMINISTRATION

8.1. CERTIFICATE POLICY CHANGE PROCEDURES

8.1.1. Items that can change without notification

Editorial and typographical changes to this CP, and changes to the contact details, may be made without notification.

8.1.2. Changes with notification

Any item in this CP may be changed with 60 days notice.

Changes to items, which, in the judgment of the PMA, will not materially impact the UICAs using this CP, may be changed with 30 days notice.

Notification Mechanism

The PMA will notify all UICAs issuing Certificates pursuant to this CP of all proposed changes that may materially impact Users of this CP.

UICAs shall post notice of such proposed changes in their Repositories and shall advise their registered Subscribers, or Service Providers, as applicable in writing or by e-mail, of such proposed changes.

Comment period

The comment period will be 30 days unless otherwise specified. The comment period will be defined in the notification.

Mechanism to handle comments

Any action taken as a result of comments filed in accordance with Section 8.1.2.2 (Comment period) is at the sole discretion of the PMA.

Period for final change notice

If the proposed change is modified as a result of comments pursuant to Section 8.1.2.3 (Mechanism to handle comments), notice of the modified proposed change shall be given, in accordance with Section 8.1.2.1 (Notification Mechanism), at least 30 days prior to the change taking effect.

Items whose change requires a new policy

If a policy change is determined by the PMA to be of such significance that a new policy OID must be registered, the PMA will add a new OID to the list of policy OIDs defined in Section 1.2 (Identification) and remove any policy OID which is no longer supported.

8.2. Publication and Notification Procedures

An electronic copy of this CP, digitally signed by an authorized representative of the PMA, is to be made available on-line via the UICA web site. A copy of this CP will be also be provided upon request in accordance with Section 2.4.2 (Severability, Survival, Merger, Notice).

8.3. CPS Approval Procedures

The procedures for a UICA’s accreditation for the issuance of Certificates pursuant to this CP will be developed by the PMA in accordance with Section 1.3.2 (Certification Authorities).

9. GLOSSARY

9.1. Definition of Terms

The table below explains defined and technical terms used throughout this CP.

Term	Description
Accreditation Authority	A PKI management Entity with the authority to permit a subordinate PKI Entity to operate within a particular domain. Sometimes referred to as Policy Management Authority (PMA)
Activation Data	Data values, other than keys, that are required to operate and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).
Applicant	An Applicant is a person who has applied to a CA for a Certificate, but has not yet been issued a Certificate by the CA.
Assurance Level	*see:* Level of Assurance
Business Associate	An individual or organization which is involved in a business activity with the Corporation. Examples of a Business Associate include a supplier and a business partner which is a subcontractor to the Corporation, or for which the Corporation is a contractor. Stockholders, clients and potential clients are Business Associates for the purposes of this CP.
CAA	CAA: From RFC 6844 (http:tools.ietf.org/html/rfc6844): “The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue.”
Certificate	A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and (f) is digitally signed by the CA issuing it. As used in this CP, the term "Certificate" refers to any Certificate issued pursuant to this CP.
Certification Path	A chain of multiple Certificates comprising a Certificate of the End- Entity signed by one CA, and zero or more additional Certificates of CAs signed by other CAs.
Certificate Revocation List (CRL)	A time-stamped list of Revoked and Suspended Certificates that has been digitally signed by a CA.
Certification Authority (CA)	A Certification Authority is an Entity that is responsible for authorizing and causing the issuance of a Certificate. A Certification Authority can perform the functions of a Registration Authority, or it can delegate or outsource these functions to separate Entities. A Certification Authority performs two essential functions. First, it is responsible for identifying and authenticating the intended Subscriber to be named in a Certificate, and verifying that such Subscriber possesses the Private Key that corresponds to the Public Key that will be listed in the Certificate. Second, the Certification Authority actually creates (or manufactures) and digitally signs the Certificate. The Certificate issued by the Certification Authority then represents that Certification Authority's statement as to the identity of the subject named in the Certificate and the binding of that Subject to a particular public-private Key Pair.

Certificate Authority Browser Forum (CABF)	A voluntary group of certification authorities (CAs), vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing. https://cabforum.org/
Certification Authority Service Provider (CASP)	Certification Authority Service Provider is a Service Provider that provides Certificate lifecycle support to a contracting party.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, Suspending, and Revoking Certificates and providing access to same.
Certificate Policy (CP)	A named set of rules that indicate the applicability of a Certificate to a particular community and/or class of application with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of Certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
Corporation	Unisys Corporation and its subsidiaries.
Cross-Certificate	A certificate issued by a Certification Authority to establish a trust relationship between it and another Certification Authority.
Cross-Certification	The process whereby CAs issue certificates to each other identifying equivalent policy OIDs to establish a trust relationship. Cross-Certification enables Qualified Relying Parties to trust certificates issued by cross-certified CAs.
Confidential Information	Information (in any format or media) that a party has not released publicly and that the party considers to be confidential and/or in which the party has a protectable or proprietary interest.
Cryptographic Module	The set of hardware, software, firmware, or some combination of the three that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has the initial message can determine (a) whether the transformation was created using the key that corresponds to the signer's key; and (b) whether the message has been altered since the transformation was made.
Distinguished Name (DN)	A directory field defined in X.501 comprised of a set of standard X.501 attributes, such as surname, organization, and organizational unit, used to uniquely identify the issuer or Subject of a Certificate
Employee	An individual who is employed by Unisys, or in a contractor or temporary position, and who requires a Unisys Active Directory account in order to perform assigned duties.
End-Entity	An Entity that uses the keys and Certificates created within the PKI for purposes other than the management of the aforementioned keys and Certificates. An End-Entity may be a Subscriber, a Qualified Relying Party, an organization, a device, or an application.
Entity	Any autonomous element within the Public Key Infrastructure. This may be a CA, an RA , Service Provider, or an End-Entity.

FIPS	Federal Information Processing Standards. Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. Federal agencies are expected to apply these standards as specified unless a waiver has been granted by the agency in accordance to agency waiver procedures.
FIPS 140-1	FIPS 140-1 is a published standard detailing the security requirements for Cryptographic Modules to meet graduated levels of assurance from level 1 (lowest assurance) through level 3 (highest assurance). NIST provides a FIPS 140-1 Assurance Level certification service for cryptographic product vendors.
FIPS 180-1	This standard specifies a Secure Hash Algorithm, SHA-1 (defined below), for computing a condensed representation of a message or a data file.
FIPS 186-1	The Digital Signature Standard, which defines the syntax of and methods for the application and verification of Digital Signatures.
IETF	Internet Engineering Task Force. The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
In-Person Proofing	Proofing that requires the physical presence of the person whose identity is being validated and the person responsible for the validation.
Intellectual Property	Useful artistic, technical, or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage, representation or both.
Intermediate CA	In a hierarchical PKI, a CA that is subordinate to the Root CA and issues Certificates to Subordinate CAs.
IPSec	A standards organization that defines network layer security standards for users of the Internet Protocol.
Issuing CA	In a hierarchical PKI, a CA that is subordinate to a Root CA or Intermediate CA and issues Certificates to End-Entities. In the context of a particular Certificate, the Issuing CA is the CA that signed and is identified as the issuer of the Certificate.
Key Changeover	Key Changeover is a procedure a CA uses to replace its active private and public Key Pairs.
Key Escrow	A deposit of the private key and other pertinent information pursuant to an escrow agreement or similar contract, the terms of which require one or more agents to hold the private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Recovery	A procedure that provides for the storage of the Private Key used for data decryption by a trusted third party and provides for the recovery of the Private Key under specific circumstances by appropriately authorized individuals to ensure that encrypted information may be decrypted when the Private Key of the intended recipient is not accessible.
Key Pair	Two mathematically related keys, having the properties that (a) one key can be used to encrypt a message that can only be decrypted using the other key, and

	(b) even knowing one key, it is computationally infeasible to discover the other key.
Level of Assurance or Assurance Level	A ‘Level of Assurance’ represents the practices followed by a CA and RA in validating the identity of the Certificate Applicant and binding this identity to a corresponding private key and other practices that may impact the level of security afforded for issuing and managing Certificates and Private Keys. The Assurance Level may affect the degree of confidence placed in the resultant Certificate.
NIST	The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce’s Technology Administration that works with industry to develop and apply technology, measurements, and standards.
Object Identifier (OID)	An Object Identifier is a unique numeric or alphanumeric identifier that unambiguously names an object and is registered with an internationally recognized standards organization.
Online Certificate Status Protocol (OCSP)	A protocol that enables applications to automatically determine the revocation state of an identified Certificate. This protocol was designed to provide more timely revocation information than is possible with the periodic issuance of a Certificate Revocation List.
Operational Period of a Certificate	The Operational Period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on (a) the date and time it expires as noted in the Certificate or (b) is Revoked or Suspended.
PIN	A Personal Identification Number is used in security systems as a shared secret authentication mechanism (e.g. the PIN used to activate a debit card in an automated teller system).
PKCS	Public Key Cryptography Standards – widely used Certificate management protocols and message syntax published originally by RSA Data Security Inc. These standards form the basis of many other standard protocols (e.g. S/MIME, SET).
PKIX	Public Key Infrastructure X. 509. An IETF Working Group developing technical specifications for PKI components based on X.509v3 Certificates.
Policy Management Authority (PMA)	An Entity in a Public Key Infrastructure responsible for the development of Certificate Policies and /or the accreditation of CAs to issue Certificates under specific Certificate Policies. In the context of this CP, the PMA is Entity responsible for creating and disseminating this CP. The PMA is also responsible for determining the suitability of a CPS to issue Certificates that reference this CP.
Policy Qualifier	Policy-dependent information that accompanies a Certificate Policy identifier in an X.509v3 Certificate.
Private Key	The key of a Key Pair used to create a Digital Signature (a private signing key) or decrypt a message encrypted with the corresponding Public Key (a private decryption key). This key must be kept a secret.
Proofing	The process of validating a set of identity criteria presented by a Certificate Applicant to gain assurance that the identity of the subject named in the Certificate fairly represents the identity of the Certificate Applicant.

Proprietary Information	Software, diagnostics, documentation, including manuals, this CP, any other policies set forth by Unisys, and any other information identified as confidential or proprietary to Unisys and its licensors.
Public Key	The key of a Key Pair that is used to verify a Digital Signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a Certificate issued by a CA and is often obtained by accessing a Repository (as defined below). A Public Key is used to verify the Digital Signature of a message purportedly sent by the holder of the corresponding Private Key. A Public Key is also used to encrypt messages intended to be decrypted by the holder of the corresponding Private Key.
Public Key Infrastructure (PKI)	A Public Key Infrastructure is a set of policies, processes, server platforms, workstations, software and people used for the purpose of administering Certificates and keys.
Qualified Certificate	A draft Certificate profile under review by the IETF PKIX Working Group for non-repudiation Certificates. The latest version of the Internet Draft, *Internet X.509 Public Key Infrastructure Qualified Certificates Profile* was published in February, 2000.
Qualified Relying Party	Qualified Relying Parties are those parties permitted to rely on the UIPKI in order to verify a digitally signed message. Qualified Relying Parties are limited to Employees of the Corporation, Business Associates of the Corporation, and the Corporation itself.
Registered Name	The name of the Subscriber as reported on the Certificate application and verified during the registration process.
Registration Authority (RA)	An Entity that is responsible for identification and authentication of Certificate Subjects, but that does not sign or issue Certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Re-key (a Certificate)	To Re-key (a Certificate) is to change the replace the public key in a Certificate. This may or may not extend the Operational Period of a Certificate and requires the issuance of a new certificate with a new serial number.
Renew (a Certificate)	The act or process of extending the validity of the data binding asserted by a public key Certificate by issuing a new Certificate containing the same public key but with a new Operational Period of a Certificate.
Repository	A Trustworthy System for storing and retrieving Certificates and other information relating to those Certificates.
Repository Services Provider (RSP)	An Entity that maintains a Repository accessible to Qualified Relying Parties for purposes of obtaining copies of Certificates and/or verifying the status of such Certificates.
Revoke (a Certificate)	Prematurely end the Operational Period of a Certificate from a specified time forward as set forth in Section 4.4.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
RSA	A Digital Signature algorithm developed by RSA Data Security Inc.

Service Provider	Entities performing services for a CA on an outsourcing basis. Such entities include but are not limited to a Certificate Manufacturing Authority (CMA) and Repository Service Provider (RSP).
SHA-1	A message digest algorithm developed by the US government used for computing a condensed representation of a message or a data file.
Signature Certificate	A public key Certificate that contains a public key intended for verifying Digital Signatures rather than encrypting data or performing any other cryptographic functions. Also called a signing Certificate or Digital Signature Certificate.
Subject	A person, device, or application whose Public Key is certified in a Certificate. A person who is the Subject of a Certificate is also referred to as a "Subscriber."
Subordinate CA	In a hierarchical PKI, a CA whose Certificate signature key is certified by another CA and whose activities are constrained by that other CA.
Subscriber	A Subscriber is a person who (a) is the Subject named or identified in a Certificate issued to such person, or (b) applies for a Certificate on behalf of the Subject named or identified in a Certificate, and (c) holds a Private Key that corresponds to a Public Key listed in that Certificate, and (d) the person to whom digitally signed messages verified by reference to such Certificate are to be attributed. See also "Subject."
Suspend (a Certificate)	Temporarily Suspend the Operational Period of a Certificate for a specified time period or from a specified time forward.
Trust List	Collection of trusted Certificates used by Qualified Relying Parties to authenticate other Certificates.
Trusted Role	One whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Trustworthy System	A system comprised of computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Unisys IT	The Unisys organization which provides network account management internal to the Corporation.
Unisys Confidential Information	Confidential Information (in any format or media), which Unisys owns or is obligated to protect.
Update (a Certificate)	The act or process by which data items bound in an existing public key Certificate, such as the email address, are changed by issuing a new Certificate.
User	Any individual or Entity who comes in contact with the systems deployed to support the PKI or uses the services provided by the PKI, including but not limited to administrators, operators, RAs, Subscribers, Qualified Relying Parties, Service Providers, other CAs, etc.
Valid Certificate	A Certificate that (a) a CA has issued, (b) the Subscriber has accepted, (c) has not expired, and (d) has not been Revoked or Suspended. Thus, a Certificate is

	not "valid" until it is both issued by a CA and has been accepted by the Subscriber.
WTLS	A specification for wireless transport layer security published by the Wireless Application Protocol Forum Ltd.
X.501	The directory attribute naming standard published by the American National Standards Institute (ANSI)
X.509v3	In this document, X.509v3 refers to the Certificate and CRL profile standard as specified in IETF PKIX RFC3280 *Internet X.509 Public Key Infrastructure Certificate and CRL Profile,* April, 2002, which defines a standard for the use and interpretation of the ANSI X.509 version 3 standard for Certificate profiles and the ANSI X.509 version 2 standard for CRL profiles.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.

9.2. Acronyms

The table below defines acronyms used throughout this CP.

Abbreviation	**Term**
ABA	American Bar Association
AD	Active Directory
ANSI	American National Standards Institute
CA	Certification Authority
CABF	CA/Browser Forum
CASP	Certification Authority Service Provider
CMA	Certificate Manufacturing Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
IPP	In-Person Proofing
ISO	International Organization for Standardization
ITU	International Telecommunications Union
KEA	Key Exchange Algorithm
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PMA	Policy Management Authority

Abbreviation	Term
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (public key cryptography algorithm)
RSP	Repository Service Provider
SHA-1	Secure Hash Algorithm, Version 1
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Sockets Layer
UICA	Unisys Internal Certification Authority
UIPKI	Unisys Internal Public Key Infrastructure
UPS	Uninterrupted Power Supply
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

10 REFERENCES

RFC2510 C. Adams, S. Farrell. ***Internet X.509 Public Key Infrastructure Certificate Management Protocols***, Internet Engineering Task Force (IETF) RFC 2510, Security Area, Public-key Infrastructure (X.509) working group, March 1999. Available online at http://www.ietf.org/rfc/rfc2510.txt.

RFC2527 S. Chokhani, W. Ford, ***Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,*** Internet Engineering Task Force (IETF) RFC 2527, Security Area, Public-key Infrastructure (X.509) working group, March 1999. Available online at http://www.ietf.org/rfc/rfc2427.txt.

RFC3280 R. Housley, W. Ford, W. Polk, and D. Solo**, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile***, Internet Engineering Task Force (IETF) RFC 3280, Security Area, Public-key Infrastructure (X.509) working group, April 2002. Available online at http://www.ietf.org/rfc/rfc3280.txt.

RFC2560 M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams， ***X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP Profile***， Internet Engineering Task Force (IETF) RFC 2460, Security Area, Public-key Infrastructure (X.509) working group, June 1999. Available online at http://www.ietf.org/rfc/rfc2460.txt.

X509 ITU-T Recommendation X.509 (1997 E): ***Information Technology – Open Systems Interconnection – The Directory: Authentication Framework***, June 1997.

PAG American Bar Association, Electronic Commerce Division: **PKI Assessment Guidelines**,
PAG v0.30, Public Draft for Comment. June 18, 2001