AUTHENTA DEVICE PUBLIC KEY INFRASTRUCTURE ROOT CERTIFICATE POLICY

Version 1.2

Approved for Publication: 20230207

Table of Contents

Section 1 Introduction 1

1.1 Overview 1
1.1.1 Terminology 1
1.2 Document Name and Identification 2
1.3 PKI Participants 2
1.3.1 Policy Authority 2
1.3.2 Certification Authority 3
1.3.3 Registration Authority 43
1.3.4 Subscribers 4
1.3.5 Relying Parties 4
1.3.6 OCSP Responders 4
1.3.7 Other Participants 4
1.4 Certificate Usage 4
1.5 Policy Administration 54

Section 2 Publication and Repository Response 65

2.1 Repositories 65
2.2 Publication of Certificate Information 65
2.2.1 Publication of Certificate and Certificate Status 65
2.2.2 Publication of CA Information 65
2.3 Time or Frequency of Publication 65
2.4 Access Controls on Repositories 65

Section 3 Identification and Authentication 76

3.1 Naming 76
3.1.1 Types of Names 76
3.1.2 Meaningfulness 76
3.1.3 Anonymity of Pseudonymity of Subjects 76
3.1.4 Rules for Interpreting Various Name Forms 76
3.1.5 Uniqueness of Names 76
3.1.6 Recognition, Authentication, and Role of Trademarks 87
3.2 Initial Identity Validation 87
3.2.1 Method to Prove Possession of Private Key 87
3.2.2 Authentication of Organization Identity 87
3.2.3 Authentication of Subject Identity 87
3.2.4 Non-verified Subject Information 87
3.2.5 Validation of Authority 87
3.2.6 Criteria for Interoperation 87
3.3 Identification and Authentication for Re-key and Renewal Requests 8
3.3.1 Identification and Authentication of Re-Key and Renewal Requests 98
3.3.2 Identification and Authentication of Re-Key and Renewal Requests After Revocation 98
3.4 Identification and Authentication for Revocation Requests 98

Section 4 Certificate Life-Cycle Operational Requirements 109

4.1 Certificate Application 109
4.1.1 Who Can Submit a Certificate Application 109
4.1.2 Enrollment Process and Responsibilities 109
4.2 Certificate Application Processing 109
4.2.1 Performing Identification and Authentication Functions 109
4.2.2 Approval or Rejection of Certificate Applications 109
4.2.3 Time to Process Certificate Applications 109
4.3 Certificate Issuance 109

4.3.1 CA Actions During Certificate Issuance 109
4.3.2 Notification to Applicant of Certificate Issuance 109
4.4 Certificate Acceptance 1110
4.4.1 Conduct Constituting Certificate Acceptance 1110
4.4.2 Publication of the Certificate by the CA 1110
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 1110
4.5 Key Pair and Certificate Usage 1110
4.5.1 Private Key Usage 1110
4.5.2 Relying Party Public Key and Certificate Usage 1110
4.6 Certificate Renewal 1110
4.6.1 Circumstance for Certificate Renewal 1110
4.6.2 Who May Request Renewal 11
4.6.3 Processing Certificate Renewal Requests 1211
4.6.4 Notification of New Certificate Issuance to Applicant 1211
4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 1211
4.6.6 Publication of the Renewal Certificate by the CA 1211
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 1211
4.7 Certificate Re-key 1211
4.7.1 Circumstance for Certificate Re-key 1211
4.7.2 Who May Request Certification of a New Public Key 1211
4.7.3 Processing Certificate Re-key Requests 1211
4.7.4 Notification of New Certificate Issuance to Applicant 1211
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 12
4.7.6 Publication of the Re-keyed Certificate by the CA 1312
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 1312
4.8 Certificate Modification 1312
4.8.1 Circumstance for Modification 1312
4.8.2 Who May Request Certificate Modification 1312
4.8.3 Processing Certificate Modification Requests 1312
4.8.4 Notification of New Certificate Issuance to Applicant 1312
4.8.5 Conduct Constituting Acceptance of a Modified Certificate 1312
4.8.6 Publication of the Modified Certificate by the CA 1312
4.8.7 Notification of Certificate Issuance by the CA to Other Entities 1312
4.9 Certificate Revocation and Suspension 1312
4.9.1 Circumstances for Revocation 13
4.9.2 Who Can Request Revocation 1413
4.9.3 Procedure for Revocation Request 1413
4.9.4 Revocation Request Grace Period 1413
4.9.5 Time within which CA Must Process the Revocation Request 1413
4.9.6 Revocation Checking Requirements for Relying Parties 1413
4.9.7 CRL Issuance Frequency 1413
4.9.8 Maximum Latency for CRLs 1413
4.9.9 On-line Revocation/Status Checking Availability 1413
4.9.10 On-line Revocation Checking Requirements 1514
4.9.11 Other Forms of Revocation Advertisements Available 1514
4.9.12 Special Requirements Related to Key Compromise 1514
4.9.13 Circumstances for Suspension 1514
4.9.14 Who can Request Suspension 1514
4.9.15 Procedure for Suspension Request 1514
4.9.16 Limits on Suspension Period 1514
4.10 Certificate Status Services 1514
4.10.1 Operational Characteristics 1514
4.10.2 Service Availability 1514
4.10.3 Optional Features 1514
4.11 End of Subscription 15
4.12 Key Escrow and Recovery 1615

4.12.1 Key Escrow and Recovery Policy and Practices 1615
4.12.2 Session Key Encapsulation and Recovery Policy and Practices 1615

Section 5 Facility, Management, and Operational Controls 1716

5.1 Physical Security Controls 1716
5.1.1 Site Location and Construction 1716
5.1.2 Physical Access 1716
5.1.3 Power and Air Conditioning 1817
5.1.4 Water Exposures 1817
5.1.5 Fire Prevention and Protection 1817
5.1.6 Media Storage 1817
5.1.7 Waste Disposal 1817
5.1.8 Off-Site backup 1817
5.2 Procedural Controls 1918
5.2.1 Trusted Roles 1918
5.2.2 Number of Persons Required Per Task 1918
5.2.3 Identification and Authentication for Each Role 1918
5.2.4 Roles Requiring Separation of Duties 1918
5.3 Personnel Controls 2019
5.3.1 Qualifications, Experience, and Clearance Requirements 2019
5.3.2 Background Check Procedures 2019
5.3.3 Training Requirements 2019
5.3.4 Retraining Frequency and Requirements 2019
5.3.5 Job Rotation Frequency and Sequence 2019
5.3.6 Sanctions for Unauthorized Actions 2019
5.3.7 Independent Contractor Requirements 2019
5.3.8 Documentation Supplied to Personnel 2019
5.4 Audit Logging Procedures 2120
5.4.1 Types of Events Recorded 2120
5.4.2 Frequency of Processing Log 2120
5.4.3 Retention Period for Audit Log 2120
5.4.4 Protection of Audit Log 2120
5.4.5 Audit Log Backup Procedures 2221
5.4.6 Audit Collection System (Internal vs. External) 2221
5.4.7 Notification to Event-Causing Subject 2221
5.4.8 Vulnerability Assessments 2221
5.5 Records Archival 2221
5.5.1 Types of Events Archived 2221
5.5.2 Retention Period for Archive 2221
5.5.3 Protection of Archive 2221
5.5.4 Archive Backup Procedures 2322
5.5.5 Requirements for Time-Stamping of Records 2322
5.5.6 Archive Collection System (Internal or External) 2322
5.5.7 Procedures to Obtain and Verify Archive Information 2322
5.6 Key Changeover 2322
5.7 Compromise and Disaster Recovery 2322
5.7.1 Incident and Compromise Handling Procedures 2322
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 2322
5.7.3 CA Private Key Compromise Procedures 2322
5.7.4 Business Continuity Capabilities After a Disaster 2422
5.8 CA Termination 2423

Section 6 Technical Security Controls 2524

6.1 Key Pair Generation and Installation 2524
6.1.1 Key Pair Generation 2524
6.1.2 Private Key Delivery to Subject 2524

6.1.3 Public Key Delivery to Certificate Issuer 2524
6.1.4 CA Public Key Delivery to Relying Parties 2524
6.1.5 Key Sizes 2524
6.1.6 Public Key Parameters Generation and Quality Checking 2524
6.1.7 Key Usage Purposes (as per X.509v3 key usage field) 2524
6.2 Private Key Protection and Cryptographic Module Engineering Controls 2625
6.2.1 Cryptographic Module Standards and Controls 2625
6.2.2 Private Key Multi-Person Control 2625
6.2.3 Private Key Escrow 2625
6.2.4 Private Key Backup 2625
6.2.5 Private Key Archival 2625
6.2.6 Private Key Transfer into or from a Cryptographic Module 2625
6.2.7 Private Key Storage on Cryptographic Module 2625
6.2.8 Method of Activating Private Keys 2625
6.2.9 Methods of Deactivating Private Keys 2625
6.2.10 Method of Destroying Private Key 2625
6.2.11 Cryptographic Module Rating 2726
6.3 Other Aspects of Key Pair Management 2726
6.3.1 Public Key Archival 2726
6.3.2 Certificate Operational Periods/Key Usage Periods 2726
6.4 Activation Data 2726
6.4.1 Activation Data Generation and Installation 2726
6.4.2 Activation Data Protection 2726
6.4.3 Other Aspects of Activation Data 2726
6.5 Computer Security Controls 2826
6.5.1 Specific Computer Security Technical Requirements 2826
6.5.2 Computer Security Rating 2827
6.6 Life Cycle Security Controls 2827
6.6.1 System Development Controls 2827
6.6.2 Security Management Controls 2927
6.6.3 Life Cycle Security Ratings 2927
6.7 Network Security Controls 2927
6.8 Timestamping 2928

Section 7 Certificate, CRL, and OCSP Profiles. 3029

7.1 Certificate Profiles 3029
7.2 CRL Profile 3029
7.3 PKCS#10 Profile 3029
7.4 PKCS#7s Profile ..... **Error! Bookmark not defined.**29
7.5 OCSP Profile 3029

Section 8 Compliance Audit and Other Assessments 3130

8.1 Frequency of Audit or Assessments 3130
8.2 Identity and Qualifications of Assessor 3130
8.3 Assessor's Relationship to Assessed Entity 3130
8.4 Topics Covered By Assessment 3130
8.5 Actions Taken As A Result of Deficiency 3130
8.6 Communication of Results 3130

Section 9 Other Business and Legal Matters 3231

9.1 Fees 3231
9.1.1 Certificate Issuance/Renewal Fees 3231
9.1.2 Certificate Access Fees 3231
9.1.3 Revocation or Status Information Access Fee 3231
9.1.4 Fees for other Services 3231
9.1.5 Refund Policy 3231

9.2 Financial Responsibility 3231
9.2.1 Insurance Coverage 3231
9.2.2 Other Assets 3231
9.2.3 Insurance/Warranty Coverage for Subscribers 3231
9.3 Confidentiality 3231
9.3.1 Scope of Confidential Information and Responsibility to Protect Confidential Information 32
9.3.2 Information Not Within the Scope of Confidential Information 3332
9.4 Privacy of Personal Information 3332
9.4.1 Privacy Plan 3332
9.4.2 Information Treated as Personal Information 3332
9.4.3 Information Not Deemed Personal Information 3332
9.4.4 Responsibility to Protect Personal Information 3332
9.4.5 Notice and Consent to use Persoanl Information 33
9.4.6 Disclosure Pursuant to Judicial/Administrative Process 33
9.4.7 Other Information Disclosure Circumstances 3433
9.5 Intellectual Property Rights 3433
9.6 Representations and Warranties 3433
9.6.1 PA / Authenta 3433
9.6.2 CA Representations and Warranties 34
9.6.3 RA Representations and Warranties 3534
9.6.4 Subscriber Representations and Warranties 3534
9.6.5 Relying Party Representations and Warranties 3534
9.6.6 Representations and Warranties of Other Participants 3534
9.7 Disclaimers of Warranties 3534
9.8 Limitations of Liability 3635
9.9 Indemnities 36
9.10 Term and Termination 3736
9.10.1 Term 3736
9.10.2 Termination 3736
9.10.3 Effect of Termination and Survival 3736
9.11 Individual Notices and Communications With Participants 3736
9.12 Amendments 37
9.12.1 Procedure for Amendment 37
9.12.2 Notification Mechanism and Period 37
9.12.3 Circumstances Under Which OID Must Be Changed 3837
9.13 Dispute Resolution Provisions 3837
9.14 Governing Law; Jurisdiction and Venue 3837
9.15 Compliance with Applicable Law 38
9.16 Miscellaneous Provisions 38
9.16.1 Document Incorporated into CP 38
9.16.2 Entire agreement 38
9.16.3 Assignment 38
9.16.4 Severability 3938
9.16.5 Enforcement (attorney's fees and waiver of rights) 3938
9.16.6 Force Majeure 3938
9.17 Other Provisions 39

Section 10 Bibliography 4140

Section 11 Acronyms & Abbreviations 4241

Section 12 Glossary 4342

Section 1 Introduction

1.1 Overview

This Certificate Policy (“CP”) governs the operations of the Authenta Device Public Key Infrastructure (the “Authenta Device PKI”) for the Authenta Device Public Key Infrastructure Root Certification Authority (“ADP Root CA”). Authenta Services LLC (“Authenta”) has established the Authenta Device PKI in order to issue Certificates for use by Device Customers.

Other documents may also apply to Authenta's certification services and the Authenta Device PKI. These documents include both public and private documents, such as applicable Certification Practice Statements (“CPSes”), agreements with Subscribers, if any, Relying Party agreements, if any, and agreements with customers of Authenta or its Affiliates for the sale or other provision of products or services that incorporate Certificates.

This CP is consistent with the IETF (Internet Engineering Task Force) PKIX (Public Key Infrastructure using X.509) Certificate Policy and Certification Practices Framework as defined in RFC 3647. Additionally, all Certificates and Certificate Revocation Lists (“CRLs”) issued under this CP will conform to RFC 5280.

1.1.1 Terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “NOT RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described below, taken from IETF RFC 2119 and updated by RFC 8174.

Note that the force of these words is modified by the requirement level of the document in which they are used.

- MUST: This word, or the terms “REQUIRED” or “SHALL”, means that the definition is an absolute requirement of the specification.
- MUST NOT: This phrase, or the phrase “SHALL NOT”, means that the definition is an absolute prohibition of the specification.
- SHOULD: This word, or the adjective “RECOMMENDED”, means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
- SHOULD NOT: This phrase, or the phrase “NOT RECOMMENDED” means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
- MAY: This word, or the adjective “OPTIONAL”, means that an item is truly optional. An implementation that does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, though perhaps with reduced functionality. Similarly, an implementation that does include a particular option MUST be prepared to interoperate with another implementation that does not include the option (except for the feature the option provides.)

1.2 Document Name and Identification

This document is the Certificate Policy for the ADP Root CA and has been approved for publication by the Authenta PA as of the date indicated on the cover page. The following table lists the revisions that have been made to the original document.

Date	Changes	Version
03 February 2023	Renew and Re-key definitions in Sections 4.6 and 4.7 removed for Section 12. Checking status information is optional for RPs in Section 4.9.10. ADP Root CA OCSP Responder changed to ADP OCSP Responder in Section 4.10.1. Removed PKCS#7 profile from Section 7. Updated definition of Device Certificate, Personal Information, Privacy, Re-Key, Renew, Self-signed, and Subscriber in glossary.	1.2
14 November 2022	Country name naming attribute made optional in Section 3.1.1.	1.1
01 November 2022	Initial version.	1.0

The ADP Root CA Self-Signed Certificate MUST NOT contain a Certificate Policy Object Identifier (“OID”).

The ADP Root CA MUST include the CP Object Identifier (“OID”) { iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) authenta(58902) id-cp(1) id-cp-device(2) } in the certificate policies extension for ADP Intermediate CA’s and the ADP OCSP Responder’s Certificates.

The ADP Root CA MUST include only the CP OID { iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) authenta(58902) id-cp(1) id-cp-TEST(120) } in the certificate policies extension for ADP Qualification Intermediate CA’s and the ADP Qualification OCSP Responder’s Certificates.

Within the Authenta Device PKI, the ADP Root CA issues Certificates to ADP Intermediate CAs. The ADP Intermediate CAs MUST use the same OID in the Certificates issued by the ADP Intermediate CAs that is present in the Certificates issued to the ADP Intermediate CAs by the ADP Root CA.

The Authenta PA MAY in the future define additional CP OIDs for use in the Authenta Device PKI by publishing an update to this CP.

1.3 PKI Participants

The following are roles relevant to the administration and operation of the Authenta Device PKI.

1.3.1 Policy Authority

1.3.1.1 Authenta Policy Authority

The Authenta PA is comprised of individuals appointed by Authenta. The Authenta Policy Authority (“Authenta PA”) is the governance body responsible for managing the ADP Root CA and ADP Intermediate CAs; see Section 1.3.2 below. The Authenta PA is responsible for this CP, the approval of related CPSes, and overseeing the conformance of CA practices with this CP, as well as approval of all other agreements and documents in the Authenta Device PKI, including CPSes, Relying Party agreements, if any, and Subscriber agreements, if any. Authenta MAY establish or recognize other CAs (e.g., subordinate CAs) in accordance with this CP.

The Authenta PA SHALL make the latest approved version of this CP available to Subscribers and Relying Parties on an as needed basis. All CPSes MAY be kept private or made available publicly in the sole discretion of the Authenta PA.

The Authenta PA MAY, in its sole discretion, delegate any or all of the above functions to a committee or specific individual.

The Authenta PA MAY publish additional Certificate Policies or Certification Practice Statements, as necessary, to describe other products or service offerings in its sole discretion.

1.3.2 Certification Authority

A Certification Authority ("CA") is the collection of technologies and procedures to issue Certificates under this CP. A "CA Operator" is the legal entity responsible for all aspects of the issuance and management of a Certificate including:

- Registration,
- Identification and authentication,
- Issuance,
- Revocation, and
- Ensuring that all aspects of the CA services and CA operations and infrastructure related to Certificates issued under this CP are performed in accordance with the requirements, representations, and warranties of their respective CPS.

The following are the different categories of CAs in the Authenta Device PKI:

- The ADP Root CA creates, signs, and issues Certificates to ADP Intermediate CAs as well as provides Certificate status information for RPs. There is one ADP Root CA.
- The two types of ADP Intermediate CAs are as follows:
  - An ADP Production Intermediate CA creates, signs, and issues Certificates to CAs that are subordinate to it and to Subscribers. ADP Production Intermediate CAs also provide Certificate status information to Relying Parties.
  - The ADP Qualification Intermediate CA creates, signs, and issues Certificates to CAs that are subordinate to it and to Subscribers for qualification purposes only. The ADP Qualification Intermediate CA also provides Certificate status information for qualification.

As used in the remainder of this document, the term "CA" only applies to CAs and not to Registration Authorities or Online Certificate Status Protocol ("OCSP") Responders. The ADP Root CA Operator MUST perform any activity the Registration Authority would have performed under this CP had a Registration Authority been established, and each reference to a Registration Authority in this CP is replaced with a reference to the ADP Root CA Operator.

Further, unless otherwise noted, the term "CA" will refer to the ADP Root CA. A specific distinction between ADP Root CAs and ADP Intermediate CAs will only be made when the stated requirements are different for each category of CA. Additionally, a specific distinction between ADP Intermediate CAs generally, on the one hand, and ADP Production Intermediate CAs and ADP Qualification Intermediate CAs, on the other hand, will only be made when the stated requirements are different for each category of CA.

This CP only addresses requirements for the ADP Root CA. The intent is that the ADP Root CA Operator will only need to consult this CP. This necessarily means that some information related to ADP Root CA and ADP Intermediate CAs will be duplicated in other CPs.

1.3.3 Registration Authority

A Registration Authority (“RA”) is authorized by the CA to collect, verify, and submit information provided by potential Subscribers, which is to be entered into Certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. This CP makes no stipulation about Registration Authorities. However, CPs for ADP Intermediate CAs that do utilize an RA MUST include RA-related stipulations.

1.3.4 Subscribers

A “Subscriber” is any entity whose name appears in the subject of a Certificate and who asserts that the Certificate and the keying material will be used in accordance with this CP. As used throughout this CP, none of the various types of CAs, RAs, or OCSP Responders are referred to as Subscribers.

Because the ADP Root CA only issues Certificates to ADP Intermediate CAs, this CP makes no stipulations about Subscribers. However, CPs for ADP Intermediate CAs that do issue Subscriber Certificates MUST include Subscriber-related stipulations, where appropriate.

1.3.5 Relying Parties

Relying Parties (“RPs”) are recipients of a Certificate who rely on the Certificate and/or the digital signatures verified by the Certificate in the Authenta Device PKI. As used in the remainder of this CP, the term RP only applies to such entities, and not to CAs, RAs, or OCSP Responders.

1.3.6 OCSP Responders

The ADP Root CA supports an “OCSP Responder” that is compliant with RFC 6960. One or more OCSP Responders act on behalf of the Authenta Device PKI for the sole purpose of signing OCSP responses. Therefore, as used in the remainder of this document, ADP OCSP Responders are not addressed as separate entities from the corresponding CAs unless specific requirements differ.

1.3.7 Other Participants

The ADP Root CA and ADP Intermediate CAs MAY require the services of other security, community, and application authorities. If so required, the applicable ADP Root CPS and ADP Intermediate CPSes SHALL identify the parties, define the services, and designate the mechanisms used to support such services.

1.4 Certificate Usage

The ADP Root CA SHALL be used to validate Certificates issued to ADP Intermediate CAs and to validate revocation information.

All other uses of the ADP Root CA Certificate are expressly prohibited. In addition, the ADP Root CA Certificate MUST NOT be used if and to the extent prohibited by law.

The Authenta Device PKI and any Certificate MUST NOT be used or accessed in or with products or components if failure or compromise of any aspect of the Authenta Device PKI or Certificates or any information or content in or provided through them, or that otherwise may be exposed as a result of such failure or compromise, could result, directly or indirectly in death, personal injury, or severe property or environmental damage.

Certificates will not be used for authenticating monetary transactions or as proof of identity of any natural person or as support of non-repudiation of identity or authority of any natural person.

1.5 Policy Administration

All ADP Intermediate CAs SHALL submit their CPSes and the results of their Authenta compliance audit to the Authenta PA for approval.

All communications regarding this CP should be directed to acpa@micron.com.

Section 2 Publication and Repository Response

2.1 Repositories

The Authenta PA will make the Authenta Repository available on the Internet.

2.2 Publication of Certificate Information

2.2.1 Publication of Certificate and Certificate Status

The ADP Root CA Certificate and CRLs MUST be published in the Authenta Repository.

The Authenta Repository SHALL be designed to make the ADP Root CA Certificate and CRLs available for retrieval with minimal scheduled interruptions under normal operating conditions. Certificate status information ~~MAY~~SHALL be made available from an OCSP Responder.

2.2.2 Publication of CA Information

The Authenta PA will make the approved CP and the ADP Root CA Certificate available to RPs, as needed.

2.3 Time or Frequency of Publication

The CRLs MUST be published at least yearly.

2.4 Access Controls on Repositories

The Authenta Repository SHALL implement controls to mitigate the risk of unauthorized adding, modifying or deleting of Authenta Repository entries.

Section 3 Identification and Authentication

This section specifies the requirements for Identification and Authentication ("I&A") of Certificates issued by the ADP Root CA Operator.

3.1 Naming

3.1.1 Types of Names

Within the Authenta Device PKI, the following X.501 Distinguished Name ("DN") SHALL be carried in the ADP Root CA Certificate and CRLs issued by the ADP Root CA:

- O=Authenta Services LLC, CN=Authenta Device Root CA

Within the Authenta Device PKI, the following X.501 DN naming attributes SHALL be carried in the ADP Intermediate CA Certificates and CRLs issued by ADP Intermediate CAs: organization and common name. The country name X.501 DN naming attribute MAY be carried in the ADP Intermediate CA Certificates and CRLs issued by ADP Intermediate CAs. The value included in each of these naming attributes SHALL be approved by the Authenta PA.

Within the Authenta Device PKI, the ADP Production OCSP Responder Certificate SHALL contain the following X.501 DN:

- O=Authenta Services LLC, CN=Authenta Device OCSP Responder #

Within the Authenta Device PKI, the ADP Qualification OCSP Responder Certificate SHALL contain the following X.501 DN:

- O=Authenta Services LLC, CN=Authenta Device Qualification OCSP Responder 1

The order of the naming attributes, if present, MUST be as follows (X.500 compliant order): Country (C=), Organization (O=), and Common Name (CN).

To allow for rollover of Certificates issued by the ADP Root CA Operator that are about to expire, a monotonically increasing integer is added to the end of the common name naming attribute to distinguish between ADP Intermediate CA Certificates issued to the same CA.

When the naming element is a DirectoryString, PrintableString SHALL be used for Certificates and CRLs issued by the ADP Root CA.

3.1.2 Meaningfulness

Names SHALL be meaningful and unambiguously identify all entities with Certificates.

3.1.3 Anonymity of Pseudonymity of Subjects

Names SHALL NOT be anonymous or be pseudonyms.

3.1.4 Rules for Interpreting Various Name Forms

See Section 3.1.1.

3.1.5 Uniqueness of Names

Name uniqueness MUST be enforced by the ADP Root CA system.

The Authenta PA is responsible for ensuring name uniqueness in Certificates issued by the ADP Root CA Operator.

3.1.6 Recognition, Authentication, and Role of Trademarks

The ADP Root CA Certificate, ADP Root CA issued Certificates, and ADP Root CA issued CRLs include the string “Authenta” in their names. Other than the display of the Authenta name within these strings and names, no other rights are granted hereunder for use of the Authenta brands and marks.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

CAs SHALL generate their own keys. To obtain a Certificate, possession of the Private Key that corresponds to the Public Key MUST be demonstrated to the ADP Root CA Operator by digitally signing the Certificate Signing Request (“CSR”).

3.2.2 Authentication of Organization Identity

The Authenta PA SHALL authorize the issuance of each ADP Intermediate CA Certificate. Organizations SHALL be authenticated for issuance of Intermediate CA Certificates if the organization is an entity within the Authenta Group or if the Authenta PA confirms that the organization is an entity that has a valid and existing agreement with an entity within the Authenta Group that authorizes issuance of an Intermediate CA Certificate to such organization entity.

3.2.3 Authentication of Subject Identity

The ADP Root CA Operator SHALL NOT issue any new Certificate for ADP Intermediate CAs without approval from the Authenta PA. Subject identities SHALL be affiliated with authenticated organizations pursuant to Section 3.2.2.

3.2.4 Non-verified Subject Information

The ADP Root CA Operator SHALL NOT include non-verified subject information in Certificates issued to ADP Intermediate CAs.

3.2.5 Validation of Authority

The ADP Root CA Operator SHALL issue Certificates to ADP Intermediate CA Operators only at the request of the Authenta PA.

3.2.6 Criteria for Interoperation

See Section 1.4.

3.3 Identification and Authentication for Re-key and Renewal Requests

This Section 3.3 describes the identification and authentication process for the following:

- Renewal refers to the creation of a new Certificate, using some or all of the information submitted for an existing Certificate and using the previously certified Public Key. Subordinate CAs of the ADP Root CA MAY request Renewal of a Certificate prior to the Certificate's expiration. The Renewal process is described more fully in Section 4.6.

- Re-keying (also referred to as reissuing) refers to the creation of a new Certificate, using some or all of the information submitted for an existing Certificate and using a newly generated Private Key. Subordinate CAs of the ADP Root CAs MAY request Re-keying of a Certificate registered by them prior to the Certificate's expiration. The Re-keying process is described more fully in Section 4.7.

Prior to the expiration of an existing Certificate, it is necessary to Re-key or Renew the Certificate to maintain continuity of Certificate usage. An overlap period of validity of at least 30 days is RECOMMENDED to ensure continuity. This continuity is supported with both Re-keys (see Section 4.7) and Renewals (see Section 4.6).

3.3.1 Identification and Authentication of Re-Key and Renewal Requests

If an ADP Intermediate CA Re-key or Renewal is required, a new Certificate will be issued by the ADP Root CA Operator after approval by the Authenta PA. Before issuance, the ADP Intermediate CA Operator SHALL identify itself through use of the ADP Intermediate CA’s current signature Private Key.

3.3.2 Identification and Authentication of Re-Key and Renewal Requests After Revocation

Re-key and Renewal after revocation is not permitted if the revocation occurred for any of the following reasons, as determined by the Authenta PA in its sole discretion:

- The Certificate was issued to an entity other than the one named as the subject of the Certificate, or an entity authorized by the certified entity.
- The Certificate was issued without the authorization of the entity named as the subject of the Certificate.
- The entity approving the CSR has reason to believe that a material fact in the CSR is false.
- The Authenta PA deemed the Certificate harmful to Authenta.

Provided none of the above reasons apply, Re-key or Renewal following Certificate revocation is permitted using the procedures to obtain the original Certificate; see Section 3.2.

3.4 Identification and Authentication for Revocation Requests

The Authenta PA MUST authorize any revocation of a Certificate issued to an ADP Intermediate CA. Once so authorized, the ADP Root CA Operator will revoke the Certificate; see Section 4.9.

Section 4 Certificate Life-Cycle Operational Requirements

This section specifies the requirements for life-cycle management of Certificates issued by the ADP Root CA Operator by all entities in the Authenta Device PKI.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

ADP Intermediate CA Operators can submit CSRs.

4.1.2 Enrollment Process and Responsibilities

ADP Intermediate CA Operators SHALL provide their credentials to the ADP Root CA to demonstrate their identity, to demonstrate their authority, and to provide contact information.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The ADP Root CA SHALL verify and authenticate the identity of each Applicant, as described in Section 3.2 for initial requests and in Section 3.3 for Re-key and Renewal requests.

4.2.2 Approval or Rejection of Certificate Applications

The Authenta PA SHALL approve any CSR if the Applicant's identity has been authenticated as described in Section 3.2 for initial requests and Section 3.3 for Re-key and Renewal requests, and payment, if required, has been received. The Authenta PA MAY reject any CSR in the event of inability to successfully authenticate the Applicant, not receiving required information from the Applicant, or not receiving required payment for the Certificate.

The Authenta PA SHALL authorize the issuance of each new, Re-keyed, and Renewed ADP Intermediate CA Certificate.

4.2.3 Time to Process Certificate Applications

CSRs SHALL be processed in a timely manner.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

The ADP Root CA Operator SHALL verify and authenticate the source of each CSR, ensure that the Public Key is bound to the correct Applicant, obtain a proof of possession of the Private Key, generate a properly formed Certificate, post the Certificate in the Authenta Repository, and provide the Certificate to the Applicant.

4.3.2 Notification to Applicant of Certificate Issuance

After obtaining authorization from the Authenta PA for new, Re-keyed, and Renewed ADP Intermediate CA Operator requests, the ADP Root CA Operator SHALL notify the Applicant of Certificate issuance by returning the Certificate to the Applicant.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Certificate SHALL be deemed accepted once the Certificate is delivered to the Authenta PA by the Root CA Operator and no notice of rejection is received from the Authenta PA within 5 business days of delivery.

4.4.2 Publication of the Certificate by the CA

Certificates issued by the ADP Root CA Operator will be posted in the Authenta Repository; see Section 2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The ADP Root CA Operator MUST provide post-issuance notification to the Authenta PA of all issued Certificates.

4.5 Key Pair and Certificate Usage

4.5.1 Private Key Usage

The ADP Root CA Operator and all ADP Intermediate CA Operators SHALL protect, in accordance with Section 6, their Private Keys to mitigate against the risk of access by unauthorized parties.

The ADP Root CA Operator SHALL use Private Keys only for purposes identified in Section 1.4.

4.5.2 Relying Party Public Key and Certificate Usage

RPs SHALL ensure that the Public Key in a Certificate is used only for appropriate purposes as identified in critical Certificate extensions; see Section 7.

4.6 Certificate Renewal

4.6.1 Circumstance for Certificate Renewal

Only upon approval from the Authenta PA, the ADP Root CA Operator MAY Renew an ADP Intermediate CA Certificate prior to its expiration to maintain continuity of operations if:

- The original Certificate's Private Key has not been compromised;
- The life of the key has not exceeded validity period as stated in Section 6.3.2;
- All information within the Certificate remains valid, other than the *notAfter* field; the ADP Root CA will change the Certificate's *serialNumber*, validity, and subjectPublicKeyInfo fields as well as apply a new digital signature as part of the issuance process;
- The validation checks on the information provided in the request passes; and
- Beyond repeating the initial validation steps, no more or further steps are required.

Certificates MAY also be Renewed after expiration.

4.6.2 Who May Request Renewal

ADP Intermediate CA Operators can submit Certificate Renewal requests.

4.6.3 Processing Certificate Renewal Requests

See Section 4.2.

4.6.4 Notification of New Certificate Issuance to Applicant

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 Certificate Re-key

4.7.1 Circumstance for Certificate Re-key

Only upon approval of the Authenta PA, the ADP Root CA Operator MAY Re-key an ADP Intermediate CA Certificate prior to its expiration to main continuity of operations if:

- The original Certificate's Private Key has not been compromised;
- All information within the Certificate remains accurate, other than the subject, validity, and subjectPublicKeyInfo; the ADP Root CA will change the Certificate's *serialNumber*, *validity*, *subject* (see Section 3.1), and *subjectPublicKeyInfo* fields as well as apply a new digital signature as part of the issuance process;
- The validation checks on the information provided in the request passes; and
- Beyond repeating the initial validation steps, no more or further steps are required.

Certificates MAY also be Re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key

ADP Intermediate CA Operators can submit Re-key requests.

4.7.3 Processing Certificate Re-key Requests

See Section 4.2.

4.7.4 Notification of New Certificate Issuance to Applicant

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

4.8.1 Circumstance for Modification

Certificate modification is not supported.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Applicant

No stipulation.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking the Certificate, the ADP Root CA Operator SHALL verify that the request was made by the Authenta PA, the ADP Intermediate CA Operator, or any other entity listed in Section 4.9.2.

Suspension of a Certificate is prohibited.

4.9.1 Circumstances for Revocation

A Certificate SHALL be revoked when the binding between the subject and the subject's Public Key within the Certificate is no longer considered valid (e.g., loss or compromise of the Private Key). A Certificate MAY also be revoked in the event the Authenta PA, in its sole discretion, deems further use of the Certificate to be detrimental.

ADP Intermediate CA Certificates MAY be revoked when (1) the Authenta PA, in its sole discretion, requests that such Certificate be revoked; (2) an ADP Intermediate CA Operator submits an authenticated revocation request; or (3) when the ADP Root CA Operator or the Authenta PA determines a situation has occurred that MAY affect the integrity of the Certificate.

4.9.2 Who Can Request Revocation

The Authenta PA, in its sole discretion, may require revocation of any ADP Intermediate CA Certificate by the ADP Root CA Operator. Additionally, any ADP Intermediate CA Operator MAY request approval from Authenta PA for revocation of its Certificate

4.9.3 Procedure for Revocation Request

Certificates SHALL be revoked upon receipt by the Authenta PA of sufficient evidence of compromise or loss of the corresponding Private Key. A request to revoke a Certificate SHALL identify the Certificate to be revoked, include a reason code for the revocation, and be authenticated (e.g., manually signed).

The Authenta PA MUST authorize all revocations of ADP Root CA issued Certificates.

4.9.4 Revocation Request Grace Period

There is no grace period under this CP.

4.9.5 Time Within which CA Must Process the Revocation Request

The ADP Root CA Operator MUST process revocation requests in a timely manner following receipt of the revocation request.

4.9.6 Revocation Checking Requirements for Relying Parties

RPs MAY check the status of Certificates on which they wish to rely at the appropriate ADP OCSP Responder or by checking the appropriate CRL, as applicable.

4.9.7 CRL Issuance Frequency

The ADP Root CA Operator SHALL generate an updated CRL at least yearly. However, if a revocation event occurs, an updated CRL MUST be generated.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-line Revocation/Status Checking Availability

ADP Intermediate CA Operators or an entity in the Authenta Group as determined by Authenta MAY support online status checking via OCSP (see Section 7) for Certificates issued under this CP. The ADP OCSP Responder MUST be available with minimal scheduled interruptions under normal operating conditions.

Certificate status information SHALL be updated for the ADP Intermediate CA Certificates within 1 week of Certificate revocation.

The ADP Intermediate CA Operators (or an entity in the Authenta Group as determined by Authenta) SHALL operate and maintain an OCSP Responder capability with resources sufficient to provide a response time of no more than 5 seconds under normal operating conditions.

4.9.10 On-line Revocation Checking Requirements

RPs MAY check the status information of Certificates on which they wish to rely using methods as specified in this section.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Suspension of a Certificate is prohibited.

4.9.14 Who can Request Suspension

Suspension of a Certificate is prohibited.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The ADP Root CA Certificate's status SHALL be available through a CRL via the Authenta Repository. ADP Intermediate CA Certificate status MAY be available via CRL through the Authenta Repository or through the ADP OCSP Responder.

4.10.2 Service Availability

The Authenta Repository and ADP OCSP Responders MUST be available with minimal scheduled interruptions under normal operating conditions.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscriptions SHALL end when a Certificate is revoked, or the Certificate expiry time passes without Renewal.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Private Keys MUST NOT be escrowed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

Section 5 Facility, Management, and Operational Controls

This section specifies the requirements for facility, management, and operational controls related to the ADP Root CA equipment and operations. This section does not cover facility management and operational controls for ADP Intermediate CAs or ADP OCSP Responders.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

The location and construction of the facility that will house the ADP Root CA equipment and operations SHALL be in accordance with that afforded the most sensitive business and financial information. ADP Root CA operations SHALL be conducted within a physically-protected environment designed to deter, mitigate against the risk of, and detect unauthorized access to such operations.

5.1.2 Physical Access

The physical security requirements pertaining to the facility that will house the ADP Root CA equipment and operations are designed to:

- Ensure no unauthorized access to the hardware is permitted;
- Ensure manual or electronic monitoring for unauthorized intrusion at all times;
- Ensure an access log is maintained and inspected periodically; and
- Require two-person physical access control to both the cryptographic module and computer system.

When not in use:

- Paper containing sensitive plain-text information SHALL be stored in secure containers; and
- Media storing ADP Root CA Private Key material SHALL be deactivated. The media and the activation information (see Section 6.4) for the ADP Root CA Private Keys SHALL be stored in a secure container. Activation Data SHALL either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and SHALL NOT be stored with the cryptographic module.
- If the facility is not continuously attended, the last people to depart SHALL initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated. A security check of the facility housing the ADP Root CA equipment SHALL occur if the facility is to be left unattended. At a minimum, the check SHALL verify the following:
  - The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for the ADP Root CA, that all equipment other than the Authenta Repository is shut down);
  - Any security containers are properly secured;
  - Physical security systems (e.g., door locks, vent covers) are functioning properly; and
  - The area is secured against unauthorized access.

If at any time the Hardware Security Module (“HSM”) containing the ADP Root CA Private Key is physically moved permanently from one location to another (i.e., not during normal activation), then:

- The HSM MUST be protected to mitigate against destruction, unauthorized disclosure, and unauthorized modification;
- The Authenta PA MUST approve the movement, the movement MUST be videotaped, and the Authenta PA or authorized representatives MUST be present; and
- The Authenta PA or an authorized representative MUST record when the HSM leaves the old location and when the HSM arrives at the new location.

5.1.3 Power and Air Conditioning

Facilities that house the ADP Root CA equipment SHALL be supplied with power and air conditioning sufficient to create a reliable operating environment.

5.1.4 Water Exposures

Facilities that house the ADP Root CA SHALL be installed such that they are not in danger of exposure to water (e.g., on tables or elevated floors). Moisture detectors SHALL be installed in nearby areas susceptible to flooding. ADP Root CA Operators who have sprinklers for fire control SHALL have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

Facilities that house the ADP Root CA SHALL be constructed and equipped, and procedures SHALL be implemented to mitigate and extinguish fires or other damaging exposure to flame or smoke. These measures SHALL meet all local applicable safety regulations. A description of the ADP Root CA Operator’s approach for recovery from a fire disaster SHALL be included in the Disaster Recovery Plan as specified in Section 5.7.4.

5.1.6 Media Storage

When not in operation, the cryptographic modules storing the ADP Root CA Private Key SHALL be stored in a secure container and in a secure room in encrypted form. Media that contains security audit and backup information SHALL be stored in a separate location from any ADP Root CA equipment.

5.1.7 Waste Disposal

The ADP Root CA Operator SHALL implement procedures for the disposal of waste (paper, media, or any other waste) to mitigate against the risk of unauthorized use of, access to, or disclosure of waste containing sensitive information.

5.1.8 Off-Site backup

The ADP Root CA Operator SHALL perform system backups, sufficient to recover from system failure, on a periodic schedule. Only the latest full backup need be retained. Such backup SHALL be stored at an offsite location (separate from the ADP Root CA equipment) with physical and procedural controls commensurate to that of the operational ADP Root CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

A Trusted Role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles MUST be responsible and free from conflicts of interests that might prejudice the impartiality of the ADP Root CA operations. The functions performed in these roles form the basis of trust for all uses of the ADP Root CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The following are the Trusted Roles within the Authenta Device PKI:

- Administrator: installs, configures, and maintains the ADP Root CA; configures Certificate profiles and parameters; generates and performs backup of ADP Root CA keys;
- Officer: approves/rejects CSRs and Certificate revocations;
- Auditor: maintains and reviews audit logs; and
- Backup Operator: performs routine system backup and recovery.

Additional Trusted Roles MAY be included in CPSes that support the ADP Root CP.

Applicable multi-person control requirements are specified in Section 5.2.2 and Section 6.2.2.

5.2.2 Number of Persons Required Per Task

The following ADP Root CA Private Key actions require at least two-party control:

- Generation of ADP Root CA keys;
- Access to ADP Root CA keys;
- Transport of HSM containing ADP Root CA keys;
- Destruction of ADP Root CA keys;
- Backup of ADP Root CA keys; and
- Access to backup copies of ADP Root CA keys.

Where multi-person control is required, at least one of the participants SHALL be an Administrator. All participants MUST serve in a Trusted Role as defined in Section 5.2.1. Notwithstanding the foregoing, multi-person control SHALL NOT be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for Each Role

A person occupying a Trusted Role SHALL have their identity and authorization verified by the ADP Root CA, before being permitted to perform any action for that role.

5.2.4 Roles Requiring Separation of Duties

Individuals MUST NOT hold more than one of the Officer, Administrator, and Auditor roles, but any individual (including an individual holding one of the aforementioned roles) MAY assume the Backup Operator role. The ADP Root CA software and hardware SHALL identify and authenticate its users and SHALL ensure that no user identity can assume both an Administrator and an Officer role, assume both the Administrator and Auditor roles, and assume both the Auditor and Officer roles.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel engaged in the Authenta Device PKI SHALL have suitable qualifications and experience, as may be determined by the Authenta PA in its sole discretion.

5.3.2 Background Check Procedures

The vetting process approved by the Authenta PA SHALL be used for personnel in Trusted Roles who are engaged in the Authenta Device PKI; see Section 5.2.1.

5.3.3 Training Requirements

Prior to operation of the ADP Root CA, personnel of the ADP Root CA Operator SHALL be appropriately trained. Topics of such training SHALL include the operation of the ADP Root CA software and hardware, operational and security procedures, and the stipulations of this CP and any applicable local guidance.

5.3.4 Retraining Frequency and Requirements

Refresher training SHALL be provided to the extent and frequency required to ensure maintenance of the required level of proficiency to perform job responsibilities competently.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

If an unauthorized action takes place, then an appropriate action SHALL be taken to ensure disciplinary or other appropriate action is taken. In cases where an unauthorized action brings into question the security of the system, then recovery procedures will be followed; see Section 5.7.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the ADP Root CA Operator SHALL meet the personnel requirements set forth in Section 5.3 and are subject to the sanctions stated above in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Any security auditing capabilities of the underlying ADP Root CA equipment operating system SHALL be enabled during installation and operation. At a minimum, the following events SHALL be included in the audit log:

- ADP Root CA equipment access;
- Operating system logon/logoff;
- ADP Root CA application access;
- ADP Root CA Private Key generation;
- ADP Root CA Private Key use;
- Processing of the CSR and Certificate issuance;
- Processing of Certificate revocation request and CRL issuance;
- Software and/or configuration updates to ADP Root CA and account management;
- Clock Adjustments;
- Anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and
- Any known or suspected violations of physical security, suspected or known attempts to attack the ADP Root CA equipment via network attacks, equipment failures, power outages, network failures, or violations of this CP.

At a minimum, for each auditable event the record SHALL include:

- The type of event;
- The date and time the event occurred;
- A success or failure indication for signing; and
- The identity of the equipment Operator who initiated the action.

Audit logs SHALL be generated automatically and periodically backed up.

5.4.2 Frequency of Processing Log

The ADP Root CA audit logs SHALL be reviewed by the ADP Root CA Operator at least annually or any time the ADP Root CA is made operational.

The audit log review SHALL include searches for anomalous patterns. Any action taken as a result of this review SHALL be documented and shared with the Authenta PA.

Audit log reviews SHALL also be conducted when requested by the Authenta PA.

5.4.3 Retention Period for Audit Log

Audit logs generated on the ADP Root CA equipment SHALL be kept on the ADP Root CA equipment until they are moved to an appropriate archive facility. Audit logs SHALL be available on the ADP Root CA equipment for a minimum of three months, then MAY be moved offsite as archival records; see Section 5.5.

5.4.4 Protection of Audit Log

Only personnel assigned to a Trusted Role have read access to the audit logs. Only authorized personnel MAY archive audit logs. Audit logs MUST be protected to mitigate against unauthorized viewing, modification, and deletion. Audit logs SHALL only be deleted from the ADP Root CA equipment after they have been archived.

5.4.5 Audit Log Backup Procedures

Audit logs SHALL be backed up not less than quarterly. At least one backup copy of the audit logs SHALL be stored at an offsite location (separate from the ADP Root CA equipment).

5.4.6 Audit Collection System (Internal vs. External)

Automated audit processes SHALL be invoked at system (or application) startup and cease only at system (or application) shutdown.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Personnel in Trusted Roles SHALL routinely, but at least annually, assess the ADP Root CA system and its components for anomalous events and malicious activity.

Vulnerability assessments SHALL also be conducted when requested by the Authenta PA.

5.5 Records Archival

5.5.1 Types of Events Archived

ADP Root CA system archive records SHALL be detailed enough to establish the validity of a signature and of the operation of the Authenta Device PKI. The following MUST be recorded at a minimum:

- ADP Root CA equipment certification, if any;
- ADP Root CA Operator documentation for vetting people of Trusted Roles;
- Updates to CPSes;
- System equipment configuration;
- Modification and updates to system or configuration;
- Key ceremony video footage;
- Identity authentication data from Section 3.1.9;
- Documentation of receipt and acceptance of Certificates;
- Audit logs from Section 5.4.1;
- All Certificates issued by the ADP Root CA Operator;
- Other data or applications to verify archive contents; and
- Documentation required by compliance Auditors; see Section 8.

5.5.2 Retention Period for Archive

Archive data SHALL be maintained for a minimum of the period of validity of all Certificates issued by the ADP Root CA Operator plus seven (7) years.

5.5.3 Protection of Archive

Archive data SHALL have adequate physical protection to mitigate against theft, unauthorized disclosure, modification, or destruction. Archive media SHALL be stored in a secure container at a secure storage facility separate from the ADP Root CA equipment itself.

5.5.4 Archive Backup Procedures

The archive facility SHALL support backups.

5.5.5 Requirements for Time-Stamping of Records

The archive data SHALL indicate the date on which the archive was created.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

The Authenta PA or its authorized representatives MUST be granted timely access to archive information upon request.

5.6 Key Changeover

Certificates issued by the ADP Root CA Operator MAY be Renewed (Section 4.6) or Re-keyed (Section 4.7).

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

In the event of suspected compromise of the ADP Root CA, including of a Private Key associated with an ADP Root CA Certificate, the ADP Root CA Operator SHALL notify the Authenta PA and SHALL investigate to determine the nature and the degree of damage. Actions taken as a result of this review SHALL be documented and shared with the Authenta PA. The Authenta PA SHALL authorize any action taken, in advance, by the ADP Root CA Operator.

If the Authenta PA so directs, if a Private Key associated with an ADP Intermediate CA is suspected of being compromised or is actually compromised, then the corresponding ADP Intermediate CA SHALL be decommissioned, and the ADP Root CA Operator SHALL revoke such ADP Intermediate CA Certificate. The revoked Certificate SHALL be removed from the Authenta Repository.

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

Backup or archived data MUST be used when computing resources, software, and data are corrupted.

5.7.3 CA Private Key Compromise Procedures

If the Authenta PA or ADP Root CA Operator reasonably suspects that any ADP Root CA Private Keys have been compromised, such keys MUST be revoked. Compromised ADP Root CA Private Keys MUST NOT be used to sign new Certificates. The ADP Root CA Operator with compromised Private Keys MUST generate new Private Keys. The procedures in Section 5.3.6 SHALL be followed if the ADP Root CA Operator is suspected of compromising the ADP Root CA Private Key.

5.7.4 Business Continuity Capabilities After a Disaster

For any delay or failure to perform an obligation due to a Force Majeure Event (see Section 9.16.6), ADP Root CA Operator SHALL endeavor to re-establish ADP Root CA operations as soon as reasonably practicable.

5.8 CA Termination

In the event the ADP Root CA Operator terminates, or ceases operation, the ADP Root CA Operator will deliver its HSM, containing the ADP Root CA Private Key and any backup copies and archival copies to the Authenta PA.

Additionally, any issued Certificates that have not expired SHALL be revoked and a final long-term ADP Root CA issued CRL with a *nextUpdate* time past the validity period of all issued Certificates SHALL be generated. This final ADP Root CA issued CRL SHALL be available for all RPs until the validity period of all Certificates issued by the ADP Root CA Operator has passed. Once the last CRL has been issued, the Private Keys of the ADP Root CA will be destroyed.

Section 6 Technical Security Controls

This section specifies the ADP Root CA requirements for technical security controls to securely perform the functions of key generation, subject authentication, Certificate issuance, and Certificate revocation.

6.1 Key Pair Generation and Installation

The Private Key associated with the ADP Root CA Certificate MUST be generated offline in the HSM.

6.1.1 Key Pair Generation

ADP Root CA keys are generated in a FIPS 140-2, or later, validated cryptographic module. Modules SHALL meet security level 3 or above and keys are generated as part of a multi-person operation. Any unencrypted copies of the keys SHALL be destroyed after the key ceremony, while encrypted backups MAY exist at secure locations.

ADP Root CA keys MUST be generated on a removable HSM device.

6.1.2 Private Key Delivery to Subject

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key and identity SHALL be delivered securely to the ADP Root CA as part of the CSR; see Section 7.

6.1.4 CA Public Key Delivery to Relying Parties

ADP Intermediate CA Certificates are posted in the Authenta Repository; see Section 2.

The ADP Root CA Self-Signed Certificate SHALL be posted in and conveyed through the Authenta Repository in a reasonably secure fashion to mitigate against substitution attacks.

6.1.5 Key Sizes

The ADP Root CA SHALL use ECDSA with the NIST P-384 elliptic curve to sign all Certificates and CRLs. The associated Public Keys MUST be 768 bits.

The ADP OCSP Responders MAY be provided and if it is the ADP OCSP Responder SHALL use ECDSA with the NIST P-384 elliptic curve to sign all OCSP responses. The associated Public Keys MUST be 768 bits.

6.1.6 Public Key Parameters Generation and Quality Checking

See FIPS 186-4 for the key generation requirements for ECDSA with the NIST P-384 elliptic curve.

6.1.7 Key Usage Purposes (as per X.509v3 key usage field)

See Section 7.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS PUB 140-2, or later.

6.2.2 Private Key Multi-Person Control

Use, generation, transport, and backup of the ADP Root CA Private Key requires action by multiple people; see Section 5.2.2.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

ADP Root CA Private Keys SHALL be backed up under multi-person control, as required in Section 5.2.2. No more than a single copy of the ADP Root CA Private Key SHALL be stored at the ADP Root CA location (i.e., only the operational and backup key MAY be stored at the ADP Root CA location). Additional copies MAY exist off-site, provided that accountability for them is maintained.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

ADP Root CA Private Keys never leave the cryptographic module in an unencrypted form.

6.2.7 Private Key Storage on Cryptographic Module

ADP Root CA Private Keys SHALL be encrypted on removable memory storage devices.

6.2.8 Method of Activating Private Keys

Activation of the ADP Root CA Private Key requires multi-person control, as specified in Section 5.2.2. The ADP Root CA Private Key media SHALL NOT be left unattended when active.

6.2.9 Methods of Deactivating Private Keys

The ADP Root CA Private Keys SHALL be deactivated and the media holding the ADP Root CA Private Key SHALL be stored in a secure container; see Section 5.1.6. ADP Root CA Private Keys SHALL be deactivated and stored in encrypted form in a secure room when not in use; see Section 5.1.6. These actions require multi-person control; see Section 5.2.2. The ADP Root CA Private Key media SHALL NOT be left unattended when not in use.

6.2.10 Method of Destroying Private Key

Private Keys SHALL be destroyed by personnel, acting in Authenta Device PKI Trusted Roles, when they are no longer needed. Such personnel SHALL also zeroize the HSM device and associated backup tokens according to instructions of the hardware manufacturer.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public Keys SHALL be archived as part of the Certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

The ADP Root CA Certificate's lifetime SHALL NOT exceed 20 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The ADP Root CA Private Keys' Activation Data generation and installation SHALL use methods that protect the Activation Data to the extent necessary to mitigate against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such Private Keys.

6.4.2 Activation Data Protection

Activation Data to invoke Private Keys SHALL use methods that protect the Activation Data to the extent necessary to mitigate against loss, theft, modification, unauthorized disclosure, or unauthorized use of such Private Keys by a combination of cryptographic and physical access control mechanisms. The protection mechanism SHALL include an entry of a PIN, and an entry of an incorrect PIN terminates the application.

6.4.3 Other Aspects of Activation Data

Before the ADP Root CA Private Key Activation Data MAY be entered, the media storing the ADP Root CA Private Key MUST be retrieved from the locked container.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

For the ADP Root CA system, the computer security functions listed below are required. These functions MAY be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The ADP Root CA system and its ancillary parts SHALL include the following functionality:

- Require authenticated logins;
- Provide Discretionary Access Control;
- Provide a security audit capability;
- Restrict access control to Trusted Roles;
- Enforce separation of Trusted Roles;
- Require identification and authentication;
- Restrict ADP Root CA application to be the only application running on the computer;
- Require use of cryptography for session communications and database security;
- Archive ADP Root CA history and audit logs; and
- Require a recovery mechanism for keys, ADP Root CA system, and ADP Root CA application.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The “System Development Controls” for the ADP Root CA system are as follows:

- For commercial off-the-shelf software, vendors MUST be selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future, without identifying the purpose for which the software will be used.
- Prior to utilizing open-source software, open-source projects MUST be selected based on their reputation in the market and likelihood of the project remaining viable in the future.
- Hardware and software procured to operate the ADP Root CA SHALL be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- The ADP Root CA software SHALL be dedicated to performing one task: operation of the ADP Root CA. There SHALL be no other applications, hardware devices, network connections, or component software installed which are not part of the ADP Root CA operation.
- The ADP Root CA Operator SHALL only use software from the vendor or from verified open-source projects for the ADP Root CA equipment. Software MUST be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates SHALL be purchased or developed in the same manner as original equipment, and be installed by Trusted Roles trained in a manner defined in the CPS.
- Only code reviewed and approved by the Authenta PA SHALL be contributed to the open-source community to ensure that code does not disclose sensitive security relevant information.

6.6.2 Security Management Controls

The configuration of the ADP Root CA system as well as any modifications and upgrades SHALL be documented and controlled. There SHALL be a mechanism for detecting unauthorized modification to the ADP Root CA software or configuration. A formal configuration management methodology SHALL be used for installation and ongoing maintenance of the ADP Root CA system.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The ADP Root CA system SHALL be protected to mitigate against the unauthorized access, tampering, and denial-of-service. Communications of sensitive information SHALL be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

The ADP Root CA system SHALL be offline. ADP OCSP Responders are online; see Section 4.9.9.

6.8 Timestamping

Times asserted in Certificates SHALL be accurate to within three minutes. Electronic or manual procedures MAY be used to maintain system time. Clock adjustments are auditable events; see Section 5.4.1.

Section 7 Certificate, CRL, and OCSP Profiles

This section specifies the requirements for the Certificate and Certificate status formats.

7.1 Certificate Profiles

See Authenta PKI Profiles.

7.2 CRL Profile

See Authenta PKI Profiles.

7.3 CSR Profile

See Authenta PKI Profiles.

7.4 OCSP Profile

See Authenta PKI Profiles.

Section 8 Compliance Audit and Other Assessments

This section specifies the requirements for ADP Root CA Operator's compliance audits. The ADP Root CA Operator SHALL select the Auditor for the ADP Root CA, subject to the Authenta PA's approval. The ADP Root CA Operator SHALL provide access to the Auditor.

8.1 Frequency of Audit or Assessments

An annual audit will be performed by an independent Auditor (meeting the requirements set forth in this Section 8) to verify that the ADP Root CA Operator is in compliance with this CP.

8.2 Identity and Qualifications of Assessor

The Auditor MUST demonstrate competence in the field of compliance audits.

8.3 Assessor's Relationship to Assessed Entity

The compliance Auditor SHALL either be a private firm, that is independent from the entity being audited, or it SHALL be sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The Authenta PA SHALL determine, in its sole discretion, whether a compliance Auditor meets this requirement.

8.4 Topics Covered By Assessment

The compliance Auditor SHALL verify that the ADP Root CA Operator is implementing all provisions of this CP, as approved by the Authenta PA.

8.5 Actions Taken As A Result of Deficiency

If a compliance audit pursuant to this Section 8 identifies any material noncompliance with applicable law, this CP, or in any other contractual obligations related to the Authenta Device PKI, the Auditor will promptly report such noncompliance to the ADP Root CA Operator. The ADP Root CA Operator SHALL develop a plan to cure such noncompliance, subject to the approval of the Authenta PA.

8.6 Communication of Results

Upon completion, the audit compliance report SHALL be returned to the Authenta PA. The report SHALL be treated as confidential by the Authenta PA. The report SHALL identify the versions of the CP and CPS used in the assessment. In the absence of Auditor imposed restrictions, Authenta MAY elect to share the audit report with others as deemed appropriate in its sole discretion.

Section 9 Other Business and Legal Matters

This section specifies requirements on general business and legal matters.

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

The fee schedule, if any, MUST be approved by an entity within the Authenta Group.

9.1.2 Certificate Access Fees

The fee schedule, if any, MUST be approved by an entity within the Authenta Group.

9.1.3 Revocation or Status Information Access Fee

CRLs and OCSP responses SHALL be available to all Relying Parties without a fee.

9.1.4 Fees for other Services

All fees, if any, MUST be approved by an entity within the Authenta Group.

9.1.5 Refund Policy

Any refund policy MUST be approved by an entity within the Authenta Group.

9.2 Financial Responsibility

The ADP CA Operators MUST have assets and resources that ensure an ability to meet all operational requirements as a CA. The levels of such assets and resources MUST be reasonably acceptable to Authenta.

9.2.1 Insurance Coverage

The insurance type and coverage amount for ADP CA Operators are to be approved by Authenta.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/Warranty Coverage for Subscribers

No stipulation.

9.3 Confidentiality

Each CA Operator will establish appropriate terms and policies to maintain the confidentiality of information of a proprietary or confidential nature while allowing for the publication of such information as is necessary for proper operation of the Authenta Device PKI.

9.3.1 Scope of Confidential Information and Responsibility to Protect Confidential Information

No stipulation.

9.3.2 Information Not Within the Scope of Confidential Information

The following information SHALL NOT be considered confidential:

- Information included in Certificates,
- Information contained in this CP document and related CPSes,
- Any Certificate status or Certificate revocation reason code published by an ADP CA (including Subordinate CAs),
- Information that, at the time of disclosure or thereafter, is generally available to or known by the public (other than as a result of disclosure in violation of this CP),
- Information that was or becomes available to the receiving party on a non-confidential basis from a third party who is not known by the receiving party to be otherwise bound by a confidentiality agreement or is not otherwise prohibited from transmitting the information, or
- Information that, at the time of disclosure, was rightfully in the possession of the receiving party.

9.4 Privacy of Personal Information

It is the responsibility of those persons and entities that use the Authenta Device PKI to ensure privacy of Personal Information under their control. Personal Information MUST NOT be included in any Certificate issued by the ADP Root CA Operator. The ADP Root CA Operator retains business contact information about ADP Intermediate CA Operators; see Section 9.4.2. If a party collects, transmits or stores Personal Information, its practices will comply with all applicable laws.

This CP makes no stipulation concerning Subscriber Certificates; see Section 1.3.4.

9.4.1 Privacy Plan

A privacy plan for the Authenta Device PKI SHALL be required and SHALL describe the process to manage Personal Information for the Authenta Device PKI.

9.4.2 Information Treated as Personal Information

A CA Operator’s business contact information, which MAY include without limitation name, organizational affiliation, physical address, email address, and phone number SHALL be treated as Personal Information.

9.4.3 Information Not Deemed Personal Information

This CP, Certificates, and revocation information are not considered Personal Information.

9.4.4 Responsibility to Protect Personal Information

The ADP CA Operators will protect Personal Information when it is within their control.

9.4.5 Notice and Consent to use Personal Information

Notice and consent practices regarding Personal Information MUST comply with any applicable law.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Disclosure in response to a valid judicial or administrative order MUST be permitted.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

All Private Keys, Certificates, CRLs, information provided by an ADP OCSP Responder (if applicable), this CP, related CPSes, ADP Root CA Self-Signed Certificates, and all Certificates and CRLs issued by the ADP Root CA Operator and all other documentation on the Authenta Device PKI are and shall remain the property of Authenta or an entity within the Authenta Group.

No intellectual property rights of any entity within the Authenta Group (or their successors-in-interest), including, without limitation, any trademark, copyright, trade secret or other proprietary right of any such entity, are granted or SHALL be implied unless such entity has granted an express license to use or otherwise exploit such intellectual property right.

Except as Authenta has expressly authorized in writing, no Participant (see Section 1.3) SHALL:

- Reverse engineer, translate, disassemble, decompile comprising all or any portion of the Authenta Device PKI;
- Attempt to access any software source code embedded or used in any portion of the Authenta Device PKI;
- Attempt to access any proprietary or protected information embedded or used in all or any portion of the Authenta Device PKI, including without limitation, any cryptographic access data or keying material of any kind;
- Remove or alter any trademark or any copyright or other proprietary notice on any software, system or any other materials in connection with the Authenta Device PKI;
- Distribute, create derivative works of or modify any materials, software or system comprising the Authenta Device PKI or any part thereof in any way, or use, copy, duplicate or display same on a commercial or development basis; or
- Provide any service using a Certificate except as authorized and provided in the CP and CPS approved by the Authenta PA.

9.6 Representations and Warranties

9.6.1 PA / Authenta

None.

9.6.2 CA Representations and Warranties

Authenta's agreements with ADP Intermediate CA Operators will include the following warranty:

Authenta warrants to the ADP Intermediate CA Operator that:

- There are no material misrepresentations of fact in the ADP Root Certificate that are known to the entities approving the CSR or issuing such Certificate.
- The entities approving the ADP Root CSR or issuing the ADP Root Certificate have exercised reasonable care in managing the CSR process or creating the ADP Root Certificate.
- Revocation services set forth in Section 4.9 and 4.10 substantially conform to this CP for the ADP Root CA, respectively.

The foregoing warranty with respect to each Certificate and the application, creation, issuance and revocation of such Certificate: (i) commences on the date the Certificate is placed in the Authenta Repository, and (ii) expires on termination of this CP in accordance with Section 9.10.2.

No warranty or condition is made that a Certificate or the process of issuing a Certificate will be secure, error-free or will conform to all requirements of any CP or CPS.

9.6.3 RA Representations and Warranties

While this CP makes no stipulation concerning RAs (see Section 1.3.3), CPs for CAs that use RAs MAY stipulate RA representation and warranties.

9.6.4 Subscriber Representations and Warranties

While this CP makes no stipulation concerning Subscriber Certificates (see Section 1.3.4), CPs for CAs that issue Subscriber Certificates MAY stipulate Subscriber representation and warranties.

9.6.5 Relying Party Representations and Warranties

RPs SHALL use the ADP Root CA Certificate in accordance with this CP (see Section 1.4). Relying Party Agreements, if any, MAY stipulate additional requirements for RP representations and warranties.

9.6.6 Representations and Warranties of Other Participants

Agreements with Other Participants (see Section 1.3.7), if any, MAY stipulate representations and warranties.

9.7 Disclaimers of Warranties

EXCEPT AS EXPRESSLY SET FORTH IN SECTION 9.6.2, THE AUTHENTA DEVICE PKI AND ANY PART OF IT, INCLUDING CERTIFICATES ISSUED IN CONNECTION WITH THE AUTHENTA DEVICE PKI, ARE PROVIDED “AS IS” AND NO REPRESENTATIONS, WARRANTIES OR CONDITIONS, WHETHER EXPRESS OR IMPLIED AND AT LAW OR IN EQUITY, ARE MADE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, OR QUIET ENJOYMENT, AND ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE. NO REPRESENTATION OR WARRANTY IS MADE THAT USE OF THE AUTHENTA DEVICE PKI OR CERTIFICATES WILL BE UNINTERRUPTED, WILL BE ERROR FREE OR FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT OR DEVICE WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED.

USE OF THE AUTHENTA DEVICE PKI AND EACH PART OF IT IS AT THE SOLE RISK OF THE USER. IT IS POSSIBLE THAT A PRIVATE KEY CORRESPONDING TO A PUBLIC KEY CONTAINED IN A CERTIFICATE CAN BE STOLEN OR OTHERWISE COMPROMISED, AND SUCH THEFT OR COMPROMISE MAY NOT BE IMMEDIATELY DETECTED. ALTHOUGH AUTHENTA MAKES EFFORTS TO PREVENT SUCH THEFT OR COMPROMISE, AUTHENTA IS NOT WARRANTING THAT THE AUTHENTA DEVICE PKI WILL BE FREE FROM THEFT OR COMPROMISE. IT IS EXPRESSLY UNDERSTOOD THAT CERTIFICATES WILL REMAIN VALID AFTER THE CRYPTOGRAPHY, TECHNOLOGY, AND OTHER SECURITY COMPONENTS OF THE AUTHENTA DEVICE PKI BECOME DATED, INEFFECTIVE OR OTHERWISE OBSOLETE, AND THAT AUTHENTA WILL HAVE NO RESPONSIBILITY OR LIABILITY AS A DIRECT OR INDIRECT RESULT OF ANY OF THE FOREGOING ARISING NOTWITHSTANDING ANYTHING TO THE CONTRARY STATED IN THIS CP OR IN THE CPS.

NOTWITHSTANDING THE FOREGOING, NOTHING IN THIS SECTION 9.7 LIMITS ANY RIGHTS OR REMEDIES THAT ANY PERSON OR ENTITY WITHIN THE AUTHENTA GROUP MAY HAVE UNDER SEPARATE AGREEMENTS BETWEEN SUCH PERSON OR ENTITY WITHIN THE

AUTHENTA GROUP AND ANY SERVICE PROVIDER, SUBCONTRACTOR, AGENT, OR LICENSOR OF THE AUTHENTA GROUP.

9.8 Limitations of Liability

“Authenta Protected Parties” means each entity within the Authenta Group; the subcontractors, service providers, and licensors of each entity within the Authenta Group; and the employees, agents, officers, directors, successors and assigns of each entity within the Authenta Group and their subcontractors, service providers and licensors.

THE AUTHENTA PROTECTED PARTIES SHALL NOT BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES OF ANY KIND ARISING OUT OF OR RELATING TO THE AUTHENTA DEVICE PKI OR ANY PART OF IT (INCLUDING CERTIFICATES ISSUED IN CONNECTION WITH THE AUTHENTA DEVICE PKI); THE USE OR OPERATION OF THE AUTHENTA DEVICE PKI AND CERTIFICATES ISSUED IN CONNECTION WITH THE AUTHENTA DEVICE PKI; OR ANY OTHER SUBJECT MATTER RELATING TO THE AUTHENTA DEVICE PKI OR THIS CP. THIS LIMITATION WILL APPLY EVEN IF AN AUTHENTA PROTECTED ENTITY WAS AWARE OF THE POSSIBILITY OF SUCH DAMAGES. FURTHER, NO AUTHENTA PROTECTED ENTITY WILL BE RESPONSIBLE FOR ANY COMPENSATION, REIMBURSEMENT, OR DAMAGES ARISING IN CONNECTION WITH: (A) INABILITY TO USE A CERTIFICATE, INCLUDING AS A RESULT OF (I) ANY TERMINATION OR SUSPENSION OF THIS CP OR THE AUTHENTA DEVICE PKI ROOT CPS OR REVOCATION OF A CERTIFICATE, (II) DISCONTINUATION OF ANY OR ALL SERVICE OFFERINGS IN CONNECTION WITH THIS CP OR THE AUTHENTA DEVICE PKI ROOT CPS, OR, (III) ANY DOWNTIME OF ALL OR A PORTION OF ANY CERTIFICATE SERVICES FOR ANY REASON, INCLUDING AS A RESULT OF POWER OUTAGES, SYSTEM FAILURES OR OTHER INTERRUPTIONS; (B) THE COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; (C) ANY INVESTMENTS, EXPENDITURES, OR COMMITMENTS IN CONNECTION WITH THIS CP OR USE OF OR ACCESS TO CERTIFICATE SERVICES OR CERTIFICATES; OR (D) ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR THE DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY CONTENT OR OTHER DATA.

THE AUTHENTA PROTECTED PARTIES SHALL HAVE NO LIABILITY TO ANY PERSON OR ENTITY OTHER THAN AN ADP INTERMEDIATE CA OPERATOR OR DEVICE CUSTOMER, IN EACH CASE SOLELY PURSUANT TO THE TERMS AND CONDITIONS OF SEPARATE WRITTEN AGREEMENTS BETWEEN SUCH AUTHENTA PROTECTED PARTIES AND SUCH PERSON OR ENTITY. NO WARRANTY OR CONDITION IS MADE THAT A CERTIFICATE OR THE PROCESS OF ISSUING A CERTIFICATE WILL BE SECURE, ERROR-FREE OR WILL CONFORM TO ALL REQUIREMENTS OF THIS CP OR ANY ASSOCIATED CPSES.

THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NOTWITHSTANDING THE FOREGOING, NOTHING IN THIS SECTION 9.8 LIMITS ANY RIGHTS OR REMEDIES THAT ANY PERSON OR ENTITY WITHIN THE AUTHENTA GROUP MAY HAVE UNDER SEPARATE AGREEMENTS BETWEEN SUCH PERSON OR ENTITY WITHIN THE AUTHENTA GROUP AND ANY SERVICE PROVIDER, SUBCONTRACTOR, AGENT OR LICENSOR OF THE AUTHENTA GROUP.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP, and related CPSes will continue in effect until either an updated version is published to the Authenta Repository, or they are terminated in accordance with this CP.

9.10.2 Termination

Termination of the CP is at the discretion of the Authenta PA. The CP remains in force until such time as the Authenta PA terminates it.

9.10.3 Effect of Termination and Survival

9.10.3.1 CP

No stipulation except the provisions found in Section 5.8 of this CP.

9.10.3.2 Survival

No stipulation with respect to survival except that the provisions found in Sections 5.5 (to the extent required pursuant to Sections 5.5.2 and 9.10.3.1), 9.3, 9.4, 9.5, 9.7, 9.8, 9.9, 9.10.3.1, 9.12, 9.13, 9.14 and 9.16 of this CP SHALL survive termination of this CP.

9.11 Individual Notices and Communications With Participants

No stipulation except for the provisions found in Section 5.8 of this CP.

9.12 Amendments

9.12.1 Procedure for Amendment

9.12.1.1 CP

Authenta MAY, in its sole discretion and with the approval of the Authenta PA, issue amendments, clarifications, updates or other new versions of this CP in its sole discretion, or as required by law or pursuant to separate agreements between Authenta and any other person or entity. Any amendments, updates or other new versions of this CP will apply to all activities and Certificates (for clarity, including those issued before the effective time of the change) within the Authenta Device PKI. However, no amendments, updates or other new versions will be applicable to activities within the Authenta Device PKI to the extent performed prior to the effective time of the change or update, or to any causes of action to the extent the event giving rise to the cause of action occurred before the effective time of the amendment, update or new version.

9.12.1.2 CPS

The Authenta PA MUST approve any amendments, clarifications, updates or other new versions of the Authenta Device PKI Root CPS.

9.12.2 Notification Mechanism and Period

Amendments, clarifications, updates or other new versions of this CP SHALL be effective upon making such modifications or updates available by any reasonable means, including posting them to the Authenta Repository.

9.12.3 Circumstances Under Which OID Must Be Changed

The OID representing this CP MAY be changed if significant changes are made to this document. The Authenta PA is solely responsible for determining whether a new version of this CP requires an OID change.

9.13 Dispute Resolution Provisions

In the event of any dispute arising with respect to this CP or any Certificates issued under this CP, the parties to such dispute MUST notify the Authenta PA and first attempt to resolve disputes directly with the Authenta PA before resorting to any other dispute resolution mechanism.

9.14 Governing Law; Jurisdiction and Venue

The laws of the State of Delaware SHALL govern the enforceability, construction, interpretation, and validity of this CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of Delaware. This governing law provision applies only to this CP. Agreements incorporating the CP by reference may have their own governing law provisions, provided that this Section 9.14 will govern the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements.

Any disputes or controversies pertaining to the enforceability, construction, interpretation, and validity of the terms of the CP will be resolved in the State of Delaware.

9.15 Compliance with Applicable Law

This CP is subject to all applicable laws of the State of Delaware and regulations, including United States restrictions on the export of hardware, software and technical information.

9.16 Miscellaneous Provisions

9.16.1 Document Incorporated into CP

The Authenta PKI Profiles are hereby incorporated into this CP by reference.

9.16.2 Entire agreement

No stipulation.

9.16.3 Assignment

Any entities operating under this CP may not assign their rights or obligations without the prior consent of Authenta.

Authenta may assign its rights under this CP and delegate any or all of its obligations in its sole and absolute discretion. Authenta is not required to obtain the consent of or provide notice to any person or entity.

If Authenta assigns this CP to a third party (including an Affiliate of Authenta), all references to Authenta hereunder are hereby automatically replaced by references to such third party assignee and this CP shall be interpreted to refer to such third party assignee in lieu of Authenta.

9.16.4 Severability

If any provision of this CP (including any portion of a provision) or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CP (and the application of the invalid or unenforceable provision (or any portion of a provision) to other persons or circumstances) SHALL remain in full force and effect and SHALL be interpreted in such a manner as to implement the original intention of the parties to the fullest extent possible. Each provision of this CP that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages (or portion of such a provision) is intended to be severable and independent of any other provision (or portion of the provision) and is to be enforced as such.

9.16.5 Enforcement (attorney's fees and waiver of rights)

Participants SHALL reimburse Authenta for all fees, expenses, and costs that Authenta incurs in enforcing the terms of this CP.

9.16.6 Force Majeure

Authenta is not liable for any delay or failure to perform an obligation under this CP if such failure or delay is due to acts of any governmental body, war, insurrection, sabotage, or embargo; fire, flood or other Act of God; strike or other labor disturbance; interruption of or delay in transportation; unavailability of, interruption of or delay in telecommunications (including the Internet) or third party services; epidemic, pandemic or other spread of disease; inability to obtain raw materials, supplies or power used in or equipment needed for performance of its obligations; or any other cause beyond Authenta's reasonable control (individually and collectively, a "Force Majeure Event").

9.17 Other Provisions

If any provision of this CP, the CPS corresponding to this CP or any other CP or CPS within the Authenta Device PKI conflicts with the provisions of any separate agreement between Authenta or its Affiliate and any other person or entity, the provisions more favorable to Authenta or its Affiliate SHALL control unless otherwise expressly agreed by Authenta or such Affiliate in a separate, signed agreement that expressly references the relevant CP or CPS and the provisions that are amended thereby.

Notwithstanding the foregoing or anything to the contrary stated in this CP, the CPS corresponding to this CP or any other CP or CPS within the Authenta Device PKI, nothing in CPs or CPSes within the Authenta Device PKI limits any rights or remedies that any person or entity within the Authenta Group may have under any separate agreement between such person or entity within the Authenta Group and any service provider, subcontractor, agent or licensor of the Authenta Group.

This CP will be interpreted according to its plain meaning without presuming it should favor either party. For purposes of interpreting this CP, (a) unless the context otherwise requires, the singular includes the plural, and the plural includes the singular; (b) unless otherwise specifically stated, the words "herein," "hereof," and "hereunder" and other words of similar import refer to this CP as a whole and not to any particular section or paragraph; (c) the words "include" and "including" will not be construed as terms of limitation, and will therefore mean "including but not limited to" and "including without limitation"; (d) unless otherwise specifically stated, the words "writing" or "written" mean preserved or presented in retrievable or reproducible form, whether electronic (including email but excluding voice mail) or hard copy; (e) the captions and section and paragraph headings used in this CP are inserted for convenience only and will not affect the meaning or interpretation of this CP; (f) terms defined in this CP will include their correlative terms; and (g) the references herein to the parties will refer to their permitted successors and assigns. If Authenta provides a

translation of the English language version of this CP, the English language version of the CP will control if there is any conflict.

Section 10 Bibliography

FIPS 140-2, “Security Requirements for Cryptographic Modules”, March 2019.

FIPS 186-4, “Digital Signature Standard”, July 2013.

RFC 2119, “Key words for use in RFCs to Indicate Requirement Levels”, March 1997.

RFC 3647, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”, November 2003.

RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, May 2008.

RFC 6960, “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP”, June 2013.

RFC 8174, “Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words”, May 2017.

Section 11 Acronyms & Abbreviations

ADP	Authenta Device PKI
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DoS	Denial of Service
EE	End-Entity
FIPS	Federal Processing Information Standard
HSM	Hardware Security Module
HTTP	Hypertext Transmission Protocol
I&A	Identification and Authentication
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure using X.509
RFC	Request for Comments
RP	Relying Party
RA	Registration Authority
TA	Trust Anchor
URI	Uniform Resource Identifier

Section 12 Glossary

Access	The ability and means to communicate with or otherwise interact with a system to use system resources either to handle information or to gain knowledge of the information the system contains.
Access Control	Protection of system resources against unauthorized access.
Activation Data	Secret data, other than keys, that is required to access a cryptographic module.
Affiliate	A corporation, partnership or other legal entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with such entity. The term “control” (including the terms “controlled by” and “under common control with”) means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through the ownership of voting securities, by contract, or otherwise.
Applicant	The entity that applies to a CA for a Certificate, but before the Certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Archive Facility	The offsite facility used by a CA to store archive data.
Administrator	A Trusted Role that installs, configures, and maintains the CA.
Audit	An independent review and examination of a system’s records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Auditor	A Trusted Role that performs the Audit.
Audit Log	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authenta Group	Authenta and its Affiliates.
Authenta Protected Parties	(i) Each entity within the Authenta Group, (ii) the subcontractors, service providers, and licensors of each entity within the Authenta Group; and (iii) the employees, agents, officers, directors, successors and assigns of each entity within the Authenta Group and their subcontractors, service providers and licensors.
Authenta Repository	A publicly accessible web server containing information and data relating to Certificates as specified in this CP.
Authenticate	Verify (i.e., establish the truth of) an attribute value claimed by or for a system entity or system resource.
Authentication	The process of verifying a claim that a system entity or system resource has a certain attribute value.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Backup Facility	The offsite facility used by a CA to store backup data.

Certificate	A digital representation of information which at least (1) identifies the CA issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the CA issuing it.
Certificate Validation	An act or process by which an RP establishes that the assertions made by a digital Certificate can be trusted.
CA (Certification Authority)	The CA is responsible for all aspects of the issuance and management of a Certificate including: registration, identification and authentication, issuance, and ensuring that all aspects of the CA services and CA operations and infrastructure related to Certificates issued under the CP are performed in accordance with the requirements, representations, and warranties of their CPS.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a CA to perform Certificate issuance and revocation.
CA Operator	The legal entity responsible for all aspects of the issuance and management of a Certificate. In this CP, there are three types: (1) ADP Root CA Operator, (2) ADP Intermediate CA Operator, (3) Backup Operator.
CP (Certificate Policy)	A CP is a specialized form of administrative policy tuned to electronic transactions performed during Certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of Certificates. Indirectly, a CP can also govern the transactions conducted using a communications system protected by a Certificate-based security system. By controlling critical Certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
CPS (Certification Practice Statement)	A statement of the practices that a CA employs in issuing, suspending, revoking, and Renewing Certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
CRL (Certificate Revocation List)	A list maintained by a CA of the Certificates that it has issued that are revoked prior to their stated expiration date.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module; from FIPS140-2, or later.
CSR (Certificate Signing Request)	A digitally signed message associates the subject, the Public Key, and any attributes together and provided to the CA during the certification request process.
Data Integrity	Assurance that the data are unchanged from creation to reception.

Device Certificate	A Certificate that validates that the unique identifier for a device submitted to the Authenta Device PKI for authentication matches the unique identifier that an entity within the Authenta Group received from a trusted third party for such a device in connection with the Authenta Device PKI. There are two kinds of Device Certificates. The first type of Device Certificate is an End-Entity (EE) Certificate on a device. The second type of Device Certificate is one or more Certificates that validate one or more EE Certificates for elements on the same device.
Device Customer	Any person or entity that does any of the following: (i) obtains a Device Certificate for use with a specific device having a unique device ID as part of the purchase of such device from an entity within the Authenta Group, or (ii) after receiving a Certificate (other than a Device Certificate) from an Authenta Group Entity in response to submission of a CSR in applying to use the Authenta Device PKI, procures from an Authenta Group Entity a Device Certificate for a specific device for which such person or entity has provided to the Authenta Group entity such device's unique identifier as part of Authenta Device PKI services provided to such person or entity by such Authenta Group Entity, or (iii) after receiving a Certificate (other than a Device Certificate) from an Authenta Group Entity in response to submission of a CSR in applying to use the Authenta Device PKI, procures from an Authenta Group Entity a Platform Certificate for which such person or entity has provided to the Authenta Group entity a cryptographic hash of the specific software, firmware, data or other content stored on a device that such person or entity desires to authenticate (alone or as combined with the device's unique identifier), all as part of Authenta Device PKI services provided to such person or entity by such Authenta Group Entity. References to "Authenta Group Entity" in the foregoing definition include successors-in-interest to all or substantially all of the business or assets of an Authenta Group Entity as well as authorized resellers and distributors of each Authenta Group entity.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that an RP can determine: (1) whether the transformation was created using the Private Key that corresponds to the Public Key in the signer's digital Certificate; and (2) whether the message has been altered since the transformation was made.
Integrity	Protection against unauthorized modification or destruction of information.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and that may have one or more CAs subordinate to itself and may have issued Subscriber Certificates.
Issuance (of a Certificate or a CRL)	Generate and sign a digital Certificate or a CRL and, usually, distribute it and make it available to potential RPs.
Key Escrow	A deposit of the Private Key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's Private Key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.

Key Pair	Two mathematically related keys having the properties that (1) one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and (2) even knowing the Public Key, it is computationally infeasible to discover the Private Key.
Modification (of a Certificate)	The act or process by which data items bound in an existing Certificate, especially authorizations granted to the subject, are changed by issuing a new Certificate.
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
OCSP (Online Certificate Status Protocol) Responder	A server that processes OCSP requests and returns OCSP responses on behalf of a CA.
OID (Object Identifier)	A specialized formatted number that is registered with an internationally recognized standards organization to reference a specific object.
PA (Policy Authority)	The individual or group that is responsible for the creation and maintenance of CPs and CPSes, and for ensuring that all PKI components (e.g., CAs, RAs) are audited and operated in compliance with the entity PKI CP. The PA evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI CPs. For the ADP Root CA, the PA is the Authenta PA.
Personal Information	Any information reasonably relating to an identified or identifiable natural person; an identifiable natural person is one who can be uniquely identified, directly or indirectly, by reference to an identifier, or reasonable combination of identifiers, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that specific natural person. For this application, a business or entity name or identifier alone, not combined with additional information directly related to a natural person such as their name, contact information or unique identification number, SHALL NOT be considered Personal Information.
Platform Certificate	"Platform Certificate" means a Certificate that validates that a cryptographic hash for the specific software, firmware, data or other content stored on a device that has been submitted to the Authenta Device PKI for authentication matches the cryptographic hash of a copy of such software, firmware, data or other content that an entity within the Authenta Group received from a trusted third party in connection with the Authenta Device PKI.
Privacy	Restricting access to Subscriber or RP information in accordance with applicable laws.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a Certificate.
PKI (Public Key Infrastructure)	A set of policies, processes, server platforms, software, and workstations used for the purpose of administering Certificates and Public/Private Key pairs, including the ability to issue, maintain, and revoke Certificates.

RA (Registration Authority)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., a RA is delegated certain tasks on behalf of an authorized CA).
Re-key (a Certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this entails issuing a new Certificate that utilizes a new Key Pair, validity period, and serial number.
RP (Relying Party)	An entity that relies on the validity of information signed by a digital Certificate.
RP Agreement	An agreement between a CA and Relying Party that typically establishes the rights and obligations between those parties regarding the verification of digital signatures or other uses of Certificates.
Renew (a Certificate)	The act or process of extending the validity of the data binding asserted by a Certificate, without changing the Public Key or any other information other than the validity dates and the serial number, by issuing a new Certificate.
Revoke (a Certificate)	To prematurely end the operational period of a Certificate effective at a specific date and time.
Root CA	An established point of trust from which an RP begins the validation of a certification path.
Self-Signed Certificate	A Certificate for which the Public Key bound by the Certificate and the Private Key used to sign the Certificate are components of the same key pair, which belongs to the Root CA.
Subordinate CA	A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.
Subscriber	A Subscriber is an entity, not a natural person, that (1) is the subject named or identified in a Certificate issued to that entity, (2) holds a Private Key that corresponds to the Public Key listed in the Certificate, and (3) does not itself issue Certificates to another party.
Subscriber Agreement	An agreement between a CA and a Subscriber that establishes the right and obligations of the parties regarding the issuance and management of Certificates.
Trust Anchor	See Root CA.
Trusted Role	Entity who performs CA-related functions that can introduce security problems if not carried out properly, whether accidentally or maliciously, that would adversely affect the basis of trust for all RPs. In this CP, there are four: (1) Administrator, (2) Officer, (3) Auditor, (4) Backup Operator.
Two-Party Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed and each familiar with established security and safety requirements.