

Certicom Certificate Practice Statement

Certicom Corp.

Version 1.0

www.Certicom.com

TABLE OF CONTENTS

| | | |
|--------|---|----|
| 1. | INTRODUCTION | 10 |
| 1.1. | Overview | 10 |
| 1.2. | Document Name and Identification | 10 |
| 1.3. | PKI Participants..... | 10 |
| 1.3.1. | Certification Authorities | 10 |
| 1.3.2. | Registration Authorities..... | 11 |
| 1.3.3. | Subscribers | 11 |
| 1.3.4. | Relying Parties..... | 12 |
| 1.3.5. | Other Participants | 12 |
| 1.4. | Certificate Usage..... | 12 |
| 1.4.1. | Appropriate Certificate Use..... | 12 |
| 1.4.2. | Prohibited Certificate Use | 13 |
| 1.5. | Policy Administration..... | 13 |
| 1.5.1. | Organization Administering the Document | 13 |
| 1.5.2. | Contact Person | 13 |
| 1.5.3. | Person Determining CPS Suitability for the Policy | 13 |
| 1.5.4. | CPS Approval Procedures..... | 13 |
| 1.6. | Definitions and Acronyms | 14 |
| 2. | PUBLICATION AND REPOSITORY RESPONSIBILITIES | 15 |
| 2.1. | Repositories | 15 |
| 2.2. | Publication of Certificate Information | 15 |
| 2.3. | Time or Frequency of Publication | 15 |
| 2.4. | Access Controls on Repositories | 16 |
| 3. | IDENTIFICATION AND AUTHENTICATION..... | 16 |
| 3.1. | Naming..... | 16 |
| 3.1.1. | Types of Names..... | 16 |
| 3.1.2. | Need for Names to be Meaningful | 17 |
| 3.1.3. | Anonymity or Pseudonymity of Subscribers | 17 |
| 3.1.4. | Rules for Interpreting Various name Forms..... | 17 |
| 3.1.5. | Uniqueness of Names..... | 17 |
| 3.1.6. | Recognition, Authentication, and Role of Trademarks | 17 |
| 3.2. | Initial Identity Validation | 18 |
| 3.2.1. | Method to Prove Possession of Private Key | 18 |
| 3.2.2. | Authentication of Organization Identity | 18 |
| 3.2.3. | Authentication of Individual Identity | 19 |

| | | |
|----------|--|----|
| 3.2.4. | Non-Verified Subscriber Information..... | 20 |
| 3.2.5. | Validation of Authority | 20 |
| 3.2.6. | Criteria for Interoperation | 20 |
| 3.3. | Identification and Authentication for Re-key Requests | 20 |
| 3.3.1. | Identification and Authentication for Routines Re-key..... | 20 |
| 3.3.2. | Identification and Authentication for Re-key After Revocation | 20 |
| 3.4. | Identification and Authentication for Revocation Requests | 21 |
| 4. | CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS | 21 |
| 4.1. | Certificate Application | 21 |
| 4.1.1. | Who Can Submit a Certificate Application..... | 21 |
| 4.1.2. | Enrollment Process and Responsibilities..... | 21 |
| 4.2. | Certificate Application Processing..... | 22 |
| 4.2.1. | Performing Identification and Authentication Functions | 22 |
| 4.2.1.1. | Low Assurance Certificates..... | 22 |
| 4.2.1.2. | High Assurance Certificates..... | 22 |
| 4.2.1.3. | EV Certificates..... | 23 |
| 4.2.1.4. | Code Signing..... | 23 |
| 4.2.1.5. | Secure Email/ Client Certificates..... | 23 |
| 4.2.2. | Approval or Rejection of Certificate Applications..... | 23 |
| 4.2.3. | Time to Process Certificate Applications | 24 |
| 4.3. | Certificate Issuance..... | 24 |
| 4.3.1. | CA Actions During Certificate Issuance..... | 24 |
| 4.3.2. | Notification to Subscriber by the CA of Issuance of Certificate | 24 |
| 4.4. | Certificate Acceptance | 24 |
| 4.4.1. | Conduct Constituting Certificate Acceptance | 24 |
| 4.4.2. | Publication of the Certificate by the CA | 24 |
| 4.4.3. | Notification of Certificate Issuance by the CA to Other Entities | 24 |
| 4.5. | Key Pair and Certificate Usage | 24 |
| 4.5.1. | Subscriber Private Key and Certificate Usage | 24 |
| 4.5.2. | Relying Party Public Key and Certificate Usage..... | 24 |
| 4.6. | Certificate Renewal | 25 |
| 4.6.1. | Circumstances for Certificate Renewal..... | 25 |
| 4.6.2. | Who May Request Renewal | 25 |
| 4.6.3. | Processing Certificate Renewal Requests..... | 25 |
| 4.6.4. | Notification of New Certificate Issuance to Subscriber..... | 25 |
| 4.6.5. | Conduct Constituting Acceptance of a Renewal Certificate | 25 |
| 4.6.6. | Publication of the Renewal Certificate by the CA | 25 |

| | | |
|---------|--|----|
| 4.6.7. | Notification of Certificate Issuance by the CA to other Entities | 25 |
| 4.7. | Certificate Re-key..... | 26 |
| 4.7.1. | Circumstances for Certificate Re-Key..... | 26 |
| 4.7.2. | Who May Request Certificate of a New Public Key..... | 26 |
| 4.7.3. | Processing Certificate Re-keying Requests | 26 |
| 4.7.4. | Notification of New Certificate Issuance to Subscriber..... | 26 |
| 4.7.5. | Conduct Constituting Acceptance of a Re-keyed Certificate..... | 26 |
| 4.7.6. | Publication of the Re-keyed Certificate by the CA..... | 26 |
| 4.7.7. | Notification of Certificate Issuance by the CA to Other Entities | 26 |
| 4.8. | Certificate Modification..... | 26 |
| 4.8.1. | Circumstance for Certificate Modification | 26 |
| 4.8.2. | Who May Request Certificate Modification..... | 26 |
| 4.8.3. | Processing Certificate Modification Requests | 26 |
| 4.8.4. | Notification of New Certificate Issuance to Subscriber..... | 26 |
| 4.8.5. | Conduct Constituting Acceptance of Modified Certificate..... | 27 |
| 4.8.6. | Publication of the Modified Certificate by the CA | 27 |
| 4.8.7. | Notification of Certificate Issuance by the CA to Other Entities | 27 |
| 4.9. | Certificate Revocation and Suspension..... | 27 |
| 4.9.1. | Circumstances for Revocation..... | 27 |
| 4.9.2. | Who can Request Revocation | 28 |
| 4.9.3. | Procedure for Revocation Request..... | 28 |
| 4.9.4. | Revocation Request Grace Period | 28 |
| 4.9.5. | Revocation Checking Requirement for Relying Parties..... | 28 |
| 4.9.6. | Time Within Which CA Must Process the Revocation Request | 28 |
| 4.9.7. | CRL Issuance Frequency | 28 |
| 4.9.8. | Maximum Latency for CRLs | 28 |
| 4.9.9. | On-line Revocation/Status Checking Availability..... | 28 |
| 4.9.10. | On-line Revocation Checking Requirements | 29 |
| 4.9.11. | Other Forms for Revocation Advertisements available..... | 29 |
| 4.9.12. | Special Requirements Re-key Compromise | 29 |
| 4.9.13. | Circumstances for Suspension..... | 29 |
| 4.9.14. | Who can Request Suspension | 29 |
| 4.9.15. | Procedure for Suspension Request | 29 |
| 4.9.16. | Limits on Suspension Period..... | 29 |
| 4.10. | Certificate Status Services | 29 |
| 4.10.1. | Operational Characteristics | 29 |
| 4.10.2. | Service Availability..... | 29 |

| | | |
|---------|--|----|
| 4.10.3. | Optional Features | 29 |
| 4.11. | End of Subscription | 29 |
| 4.12. | Key Escrow and Recovery | 29 |
| 5. | FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS..... | 29 |
| 5.1. | Physical Security Controls | 29 |
| 5.1.1. | Site Location and Construction..... | 30 |
| 5.1.2. | Physical Access | 30 |
| 5.1.3. | Power and Air Conditioning | 30 |
| 5.1.4. | Water Exposures | 30 |
| 5.1.5. | Fire Prevention and Protection | 30 |
| 5.1.6. | Media Storage..... | 30 |
| 5.1.7. | Waste Disposal..... | 30 |
| 5.1.8. | Off-site Backup | 30 |
| 5.2. | Procedural Controls | 30 |
| 5.2.1. | Trusted Roles..... | 30 |
| 5.2.2. | Number of Persons Required Per Task..... | 30 |
| 5.2.3. | Identification and Authentication for Each Role..... | 31 |
| 5.2.4. | Roles Requiring Separation of Duties..... | 31 |
| 5.3. | Personnel Security Controls..... | 31 |
| 5.3.1. | Qualifications, Experience, and Clearance Requirements | 31 |
| 5.3.2. | Background Check Procedures | 31 |
| 5.3.3. | Training Requirements..... | 31 |
| 5.3.4. | Retraining Frequency and Requirements..... | 31 |
| 5.3.5. | Job Rotation Frequency and Sequence | 31 |
| 5.3.6. | Sanctions for Unauthorized Actions..... | 31 |
| 5.3.7. | Independent Contractor Requirements..... | 32 |
| 5.3.8. | Documentation Supplied to Personnel | 32 |
| 5.4. | Audit Logging Procedures..... | 32 |
| 5.4.1. | Types of Events Recoded..... | 32 |
| 5.4.2. | Frequency of Processing Log | 32 |
| 5.4.3. | Retention Period of Audit Log..... | 33 |
| 5.4.4. | Protection of Audit Log..... | 33 |
| 5.4.5. | Audit Log Backup Procedures | 33 |
| 5.4.6. | Audit Collection System..... | 33 |
| 5.4.7. | Notification to Event-Causing Subject | 33 |
| 5.4.8. | Vulnerability Assessments..... | 33 |
| 5.5. | Records archival..... | 33 |

| | | |
|----------|--|----|
| 5.5.1. | Types of records archived | 33 |
| 5.5.2. | Retention period for archive..... | 33 |
| 5.5.3. | Protection of archive | 34 |
| 5.5.4. | Archive backup procedures | 34 |
| 5.5.5. | Requirements for time-stamping of records | 34 |
| 5.5.6. | Archive collection system | 34 |
| 5.5.7. | Procedures to obtain and verify archive information | 34 |
| 5.6. | Key changeover | 34 |
| 5.7. | Compromise and disaster recovery | 34 |
| 5.7.1. | Incident and compromise handling procedures..... | 34 |
| 5.7.2. | Computing resources, software, and/or data are corrupted | 34 |
| 5.7.3. | Business continuity capabilities after a disaster | 34 |
| 5.8. | CA or RA termination | 35 |
| 6. | TECHNICAL SECURITY CONTROLS | 35 |
| 6.1. | Key pair generation and installation..... | 35 |
| 6.1.1. | Key pair generation..... | 35 |
| 6.1.2. | Private key delivery to subscriber | 36 |
| 6.1.2.1. | Secure Server Certificate | 36 |
| 6.1.2.2. | Code Signing Certificates..... | 36 |
| 6.1.2.3. | Delivery of other Certificates | 36 |
| 6.1.2.4. | Secure Email Certificate..... | 36 |
| 6.1.3. | Public key delivery to certificate issuer | 36 |
| 6.1.4. | CA public key delivery to relying parties | 37 |
| 6.1.5. | Key sizes..... | 37 |
| 6.1.6. | Public key parameters generation and quality checking | 37 |
| 6.1.7. | Key usage purposes (as per X.509 v3 key usage field) | 37 |
| 6.2. | Private Key Protection and Cryptographic Module Engineering Controls | 37 |
| 6.2.1. | Cryptographic module standards and controls | 37 |
| 6.2.2. | Private key (n out of m) multi-person control | 38 |
| 6.2.3. | Private key escrow | 38 |
| 6.2.4. | Private key backup..... | 38 |
| 6.2.5. | Private key archival..... | 38 |
| 6.2.6. | Private key transfer into or from a cryptographic module | 38 |
| 6.2.7. | Private key storage on cryptographic module | 38 |
| 6.2.8. | Method of activating private key | 38 |
| 6.2.9. | Method of deactivating private key | 38 |
| 6.2.10. | Method of destroying private key | 38 |

| | | |
|----------|--|----|
| 6.2.11. | Cryptographic Module Rating | 38 |
| 6.3. | Other aspects of key pair management | 38 |
| 6.3.1. | Public key archival | 39 |
| 6.3.2. | Certificate operational periods and key pair usage periods..... | 39 |
| 6.4. | Activation data..... | 39 |
| 6.4.1. | Activation data generation and installation | 39 |
| 6.4.2. | Activation data protection | 39 |
| 6.4.3. | Other aspects of activation data | 39 |
| 6.5. | Computer security controls | 39 |
| 6.5.1. | Specific computer security technical requirements | 39 |
| 6.5.2. | Computer security rating..... | 39 |
| 6.6. | Life cycle technical controls | 39 |
| 6.6.1. | System development controls..... | 39 |
| 6.6.2. | Security management controls | 40 |
| 6.6.3. | Life cycle security controls..... | 40 |
| 6.7. | Network security controls | 40 |
| 6.8. | Time-stamping..... | 40 |
| 7. | CERTIFICATE, CRL, AND OCSP PROFILES | 40 |
| 7.1. | Certificate profile | 40 |
| 7.1.1. | Version number(s) | 40 |
| 7.1.2. | Certificate extensions..... | 40 |
| 7.1.2.1. | Key Usage Extension field | 40 |
| 7.1.2.2. | Extension Criticality Field | 41 |
| 7.1.2.3. | Basic Constraints Extension | 41 |
| 7.1.3. | Algorithm object identifiers..... | 41 |
| 7.1.4. | Name forms | 41 |
| 7.1.5. | Name constraints | 41 |
| 7.1.6. | Certificate policy object identifier | 41 |
| 7.1.7. | Usage of Policy Constraints extension | 42 |
| 7.1.8. | Policy qualifiers syntax and semantics | 42 |
| 7.1.9. | Processing semantics for the critical Certificate Policies extension | 42 |
| 7.2. | CRL profile | 42 |
| 7.2.1. | Version number(s) | 42 |
| 7.2.2. | CRL and CRL entry extensions | 42 |
| 7.3. | OCSP profile | 42 |
| 7.3.1. | Version Number(s)..... | 43 |
| 7.3.2. | OCSP Extensions | 43 |

| | | |
|--------|---|----|
| 8. | COMPLIANCE AUDIT AND OTHER ASSESSMENTS..... | 43 |
| 8.1. | Frequency or Circumstances of Assessment | 43 |
| 8.2. | Identity/Qualifications of Assessor | 43 |
| 8.3. | Assessor's Relationship to Assessed Entity | 44 |
| 8.4. | Topics Covered by Assessment..... | 44 |
| 8.5. | Actions Taken as a Result of Deficiency..... | 44 |
| 8.6. | Communication of Results | 44 |
| 9. | OTHER BUSINESS AND LEGAL MATTERS | 44 |
| 9.1. | Fees | 44 |
| 9.1.1. | Certificate Issuance or Renewal Fees | 44 |
| 9.1.2. | Certificate Access Fees | 44 |
| 9.1.3. | Revocation or Status Information Access Fees..... | 44 |
| 9.1.4. | Fees for Other Services..... | 45 |
| 9.1.5. | Refund Policy | 45 |
| 9.2. | Financial Responsibility..... | 45 |
| 9.2.1. | Insurance Coverage..... | 45 |
| 9.2.2. | Other Assets | 45 |
| 9.2.3. | Insurance or Warranty Coverage for End-Entities..... | 45 |
| 9.3. | Confidentiality of Business Information..... | 45 |
| 9.3.1. | Scope of Confidential Information..... | 45 |
| 9.3.2. | Information Not Within the Scope of Confidential Information..... | 46 |
| 9.3.3. | Responsibility to Protect Confidential Information | 46 |
| 9.4. | Privacy of Personal Information | 46 |
| 9.4.1. | Privacy Plan | 46 |
| 9.4.2. | Information Treated as Private | 46 |
| 9.4.3. | Information Not Deemed Private | 46 |
| 9.4.4. | Responsibility to Protect Private Information | 46 |
| 9.4.5. | Notice and Consent to Use Private Information | 46 |
| 9.4.6. | Disclosure Pursuant to Judicial or Administrative Process..... | 46 |
| 9.4.7. | Other Information Disclosure Circumstances | 47 |
| 9.5. | Intellectual Property Rights | 47 |
| 9.5.1. | Certificates | 47 |
| 9.5.2. | Copyright..... | 47 |
| 9.5.3. | Trademarks..... | 47 |
| 9.5.4. | Infringement | 47 |
| 9.6. | Representations and Warranties..... | 47 |
| 9.6.1. | CA Representations and Warranties | 48 |

| | | |
|---------|---|----|
| 9.6.2. | RA Representations and Warranties | 48 |
| 9.6.3. | Subscriber Representations and Warranties | 49 |
| 9.6.4. | Relying Party Representations and Warranties..... | 50 |
| 9.6.5. | Representations and Warranties of Other Participants | 50 |
| 9.7. | Disclaimers of Warranties | 50 |
| 9.8. | Limitations of Liability | 51 |
| 9.9. | Indemnities | 52 |
| 9.9.1. | Subscriber Indemnity to Certicom..... | 52 |
| 9.9.2. | Subscriber Indemnity to Relying Parties..... | 52 |
| 9.10. | Term and Termination | 52 |
| 9.10.1. | Term | 52 |
| 9.10.2. | Termination..... | 53 |
| 9.10.3. | Effect of Termination and Survival | 53 |
| 9.11. | Individual notices and Communications with Participants | 53 |
| 9.12. | Amendments | 53 |
| 9.12.1. | Procedure for Amendment | 53 |
| 9.12.2. | Notification Mechanism and Period..... | 53 |
| 9.12.3. | Circumstances Under Which OID Must be Changed..... | 54 |
| 9.13. | Dispute Resolution Procedures..... | 54 |
| 9.14. | Governing Law | 54 |
| 9.15. | Compliance with Applicable Law..... | 54 |
| 9.16. | Miscellaneous Provisions | 54 |
| 9.16.1. | Entire Agreement..... | 54 |
| 9.16.2. | Assignment..... | 54 |
| 9.16.3. | Severability | 55 |
| 9.16.4. | Enforcement | 55 |
| 9.16.5. | Force Majeure | 55 |
| 9.17. | Other Provisions..... | 55 |
| | APPENDIX A..... | 56 |
| | APPENDIX B | 57 |

1. INTRODUCTION

Certicom Secure Certificate Authority (“Certicom”) is a Certification Authority (CA) that issues both ECC and RSA based digital certificates to various subscribing entities, including private and public companies and individuals. Certicom performs functions associated with public key operations which include receiving application requests for, issuing, revoking and renewing digital certificates and the maintenance, issuance, and publication of Certificate Revocation Lists (“CRLs”) and an Online Certificate Status Protocol (“OCSP”).

Certicom extends, through various affiliate programs, membership into its PKI to approved third parties (known as Registration Authorities or RAs). The international network of Certicom RAs uses Certicom’s developed policies, practices, and CA infrastructure to sell, provide, and issue Certicom digital certificates and, if appropriate, private labeled digital certificates.

1.1. Overview

This document is the Certicom Certification Practice Statement (CPS). The Certicom CPS outlines the legal, commercial and technical principles and practices that Certicom employs in approving, issuing, using, and managing certification services. This includes approving, issuing, using and managing Digital Certificates and maintaining a X.509 Certificate based public key infrastructure (PKIX). Certicom may update and supplement this CPS with amendments in order to provide for additional product offerings and to comply with certain regulatory or industry standards and requirements.

This CPS describes Certicom’s certification processes, business operations, and repository operations. The CPS is only one of many documents that are relevant to Certicom’s certificate issuance practices. Other important documents include the Certicom subscriber agreement, the relying party agreement, and other ancillary agreements that are posted on the Certicom repository. These documents obligate parties using or relying on a Certicom digital certificate to meet a certain minimum criteria prior to their use or reliance on a Certicom Certificate.

Certicom’s CPS is also a means to notify the public and relevant parties of the roles and responsibilities involved in Certificate based practices within the Certicom PKI. The CPS is formatted and maintained in accordance with IETF PKIX RFC 3647 and is divided into separate sections that cover the practices and procures for applying for, identifying, issuing, and revoking certificates along with information about Certicom’s security controls and auditing process. To preserve the format of RFC 3647, some section headings do not apply and will contain the text “Not applicable” or “No stipulation”. The format is preserved to assist the reader in comparing and contrasting the various CPS documents provided by various CAs.

1.2. Document Name and Identification

This document is the Certicom CPS version 1.0, which was approved for publication on 1 Dec. 2008 by the Certicom Certificate Authority. The CPS is a public statement of the practices of Certicom and the conditions of issuance, revocation and renewal of a certificate issued under Certicom’s PKI hierarchy. Revisions to this document have been made as follows:

| Date | Changes | Version |
|-------------|----------------|----------------|
|-------------|----------------|----------------|

Revisions not denoted “significant” are those deemed by the CA’s Policy Authority to have minimal or no impact on subscribers and relying parties using certificates, the CRLs and the OCSP used by Certicom. Insignificant revisions may be made without changing the version number of this CPS.

1.3. PKI Participants

1.3.1. Certification Authorities

The term “Certificate Authority (CA)” is a generic term used to describe entities that are allowed to issue public key certificates. The Certicom CA:

- Conforms its operations to this CPS as may from time to time be modified by amendments published in the Certicom repository (www.Certicom.com/repository),
- Issues and publishes certificates in a timely manner in accordance with the issuance times set forth in this CPS,
- Revokes certificates upon receipt of a valid revocation request from a person authorized to request revocation,
- Maintains and updates its OCSP on a regular basis and in a timely manner, in accordance with the applicable Certificate Policy and as described in this CPS,
- Publishes CRLs on a regular basis, in accordance with the applicable Certificate Policy and as described in this CPS,
- Distributes issued certificates in accordance with the methods detailed in this CPS,
- Updates CRLs in a timely manner as detailed in this CPS, and
- Notifies subscribers via email of expiring Certicom issued certificates (for a period disclosed in this CPS).

1.3.2. Registration Authorities

Although Certicom has established the necessary secure infrastructure to fully manage the lifecycle of digital certificates within its PKI, Certicom also makes its certification authority services available to subscribers through a network of Registration Authorities (RAs). Certicom RAs:

- Accept, evaluate, approve, or reject the registration of certificate applications,
- Verify the accuracy and authenticity of application information provided by a subscriber as specified in the Certicom validation guidelines,
- Use official, notarized, or otherwise acceptable documentation to evaluate a subscriber application, and
- Verify the accuracy and authenticity of the information provided by a subscriber at the time of reissue or renewal as specified herein.

A Certicom RA acts within its own geographical or business partnerships with Certicom’s approval and authorization and may issue certificates that it has validated. RAs are restricted to operating only within the validation guidelines published by Certicom and must agree to do so prior to or when the RA joins the program. Certificates issued through an RA contain an amended Certificate Profile within the issued certificate to represent to a Relying Party the involvement of the RA in the issuance process.

Certificates issued by RAs that are compliant with and operating under Certicom’s practices and procedures have the same warranty as those certificates issued under Certicom’s own root as limited by the terms and conditions set forth herein.

1.3.3. Subscribers

Subscribers are individuals, companies, or other entities that use Certicom’s PKI services to provide supported transactions and communications. Subscribers are identified in and have the private key corresponding to the public key listed in an issued certificate. Prior to being issued a certificate, an applicant (a potential subscriber) must submit an application accompanied by certain verification information. Certicom will only issue a Certificate to an applicant after the applicant has been approved and verified by Certicom.

In certain circumstances, Certicom may issue a certificate to an individual or entity that is different from the entity which actually applied for the certificate. In such circumstances, the Subject of the certificate will be the entity whose credentials have been submitted, and the term Subscriber shall

apply to the entity which contracted with Certicom for the issuance of the certificate. Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

1.3.4. Relying Parties

Relying parties use Certicom's PKI services to perform certain transactions, communications, or functions and may reasonably rely on issued certificates and/or digital signatures that contain a verifiable reference to a public key that is listed in the subscriber certificate. Not all of Certicom's certificate products are intended to be used in e-commerce transactions or environments, and parties who rely on such certificates do not qualify as a relying party.

Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be an ethical business operation. Relying Parties should always independently examine each certificate holder to determine whether the certificate owner is ethical and trustworthy.

1.3.5. Other Participants

Certicom operates a network of resellers that allows authorized agents of Certicom to integrate Certicom digital certificates into their own product portfolios. Resellers are responsible for referring digital certificate customers to Certicom. Certicom, and not Reseller, maintains full control over the certificate lifecycle process, including application, issuance, renewal and revocation. All Resellers are required to provide proof of organizational status and must enter into a Reseller agreement with Certicom that requires them to comply with this CPS prior to being provided with Reseller status and facilities. Unless otherwise noted, all certificates provided by Certicom are also available through its Reseller program.

1.4. Certificate Usage

A digital certificate is formatted data that cryptographically binds an identified subscriber to a public key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to the other participants in such transaction. Certificates may be issued for individuals, organizations, government entities, educational institutions, or infrastructure components such as firewalls, routers, or other security devices.

1.4.1. Appropriate Certificate Use

Depending on the certificate type, the certificates issued from Certicom may only be used for authentication, encryption, access control, and digital signature purposes.

Low assurance (or Domain Validated) certificates are not used for authentication purposes and are ideal for mail servers and server to server communications. Entities purchasing these certificates receive limited validation by Certicom. These certificates are used to ensure that the data being transmitted from one party to another is secure and are not intended for websites conducting e-commerce or other valued data transactions. A party transmitting data cannot be sure or guaranteed that the receiving party is the party named in the certificate. Due to increased validation speed, the lack of stringent validation, and the intended use of low assurance certificates, the certificates do not carry a warranty.

High assurance certificates are issued to both individuals and organization whose identity has first been verified according to the validation procedures described in section 4.

Extended validation certificates are certificates that have been issued in accordance with Certicom's EV CPS and the EV Guidelines established by the CAB Forum.

Code Signing Certificates are designed for commercial software developers to provide assurance regarding the developer's identity, and are designed to represent the level of assurance provided today by retail channels for software. With a Code Signing Certificate, a digital signature can be appended to the executable code itself, thus providing assurance to recipients that the code or software does indeed come from the signer of the software.

Secure Email Certificate, in combination with an S/MIME compliant email application, allow subscribers to digitally sign email for relying parties, or relying parties to encrypt email for the subscriber.

Certicom uses third party domain name registrars and directories to assist with application validation in order to provide increased speed of issuance. Where possible, Certicom's or a third party's directories will be used to confirm the right to use the domain name used in the application. If the directory cannot be used to sufficiently validate a certificate applicant, further validation processes may be used which may include an out of bands validation of the applicant's submitted information.

See Appendix B for further information on different Certificates issued by Certicom.

1.4.2. Prohibited Certificate Use

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations. Certificates may not be used to complete or assist in performing any transaction that is prohibited by law.

Each party using or relying on a certificate shall be bound by and comply with the terms and conditions set forth in the applicable agreement between the party and Certicom. Low assurance certificates may not be used as proof of identity and may not be held forth as establishing the legitimacy of the certificate holder's business operations. Digital certificates do not guarantee that a certificate holder has good intentions or that the certificate holder will be an ethical business operation.

Certificates may not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause any form of damage.

1.5. Policy Administration

1.5.1. Organization Administering the Document

This CPS and any related documents, agreements, or policy statements referenced herein are maintained and administered by the Certicom Policy Authority.

Certicom Corp.
5520 Explorer Drive, 4th Floor
Mississauga, Ontario L4W 5L1
Canada

1.5.2. Contact Person

Certicom Certification Authority
5520 Explorer Drive, 4th Floor
Mississauga, Ontario L4W 5L1
Canada

1.5.3. Person Determining CPS Suitability for the Policy

The suitability and applicability of Certicom's CPS is reviewed and approved by both Certicom's Policy Authority and Certicom's legal department.

1.5.4. CPS Approval Procedures

Certicom's CPS and any amendments made to it are reviewed and approved by Certicom's policy authority and legal department. Amendments to the CPS may be made by reviewing and updating the entire CPS or by publishing an addendum. The current version of the CPS is always made available to the public through Certicom's repository which can be accessed online at www.Certicom.com/repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in section 5.4 of this CPS.

1.6. Definitions and Acronyms

Acronyms:

| | |
|-------|--|
| CA | Certificate Authority |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| CVC | Content Verification Certificate |
| EPKI | Enterprise Public Key Infrastructure Manager |
| FTP | File Transfer Protocol |
| HTTP | Hypertext Transfer Protocol |
| ITU | International Telecommunication Union |
| ITU-T | ITU Telecommunication Standardization Sector |
| MDC | Multiple Domain Certificate |
| OCSP | Online Certificate Status Protocol |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure (based on X.509 Digital Certificates) |
| PKCS | Public Key Cryptography Standard |
| RA | Registration Authority |
| SGC | Server Gated Cryptography |
| SSL | Secure Sockets Layer |
| TLS | Transaction Layer Security |
| URL | Uniform Resource Locator |
| X.509 | The ITU-T standard for Certificates and their corresponding authentication framework |

Definitions:

| | |
|--------------------------|---|
| Applicant: | The Applicant is an entity applying for a Certificate. |
| Certificate: | A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, and contains a serial number. |
| Subscriber: | The Subscriber is an entity that has been issued a Certificate. |
| Subscriber Agreement: | The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process. |
| Relying Party: | The Relying Party is an entity that relies upon the information contained within the Certificate. |
| Relying Party Agreement: | The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or |

using a Certificate and is available for reference at www.Certicom.com/repository.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

This CPS is only one of a set of documents relevant to the Certicom's certification services. The list of documents below is a list of other documents that this CPS will from time to time mention. The list is not exhaustive. The document name, location of, and status, whether public or private, are detailed below. The Certicom Repository can be found at www.Certicom.com/repository.

| Document Status Location | Status | Location |
|---|--------------|-----------------------------------|
| Certicom Certification Practice Statement | Public | Certicom Repository |
| SSL Subscriber Agreement | Public | Certicom Repository |
| Code Signing Subscriber Agreement | Public | Certicom Repository |
| Email Certificate Subscriber Agreement | Public | Certicom Repository |
| SSL Relying Party Agreement | Public | Certicom Repository |
| SSL Relying Party Warranty | Public | Certicom Repository |
| Reseller Agreement | Confidential | Presented to partners accordingly |

2.1. Repositories

Certicom publishes this CPS, its EV CPS, its subscriber agreements, and the relying party agreement in the official Certicom repository at www.Certicom.com/repository. The Certicom Certificate Policy Authority maintains the Certicom repository. All updates, amendments and legal promotions are logged in accordance with the logging procedures referenced in this CPS.

Certicom makes all reasonable efforts to ensure that parties accessing its Repositories receive accurate, updated, and correct information. However, Certicom cannot accept any liability beyond the limits set forth in this CPS.

Parties accessing the repository agree with the provisions of this CPS and any other conditions of usage that Certicom may make available. Parties demonstrate acceptance this CPS and the other terms and conditions that may apply by using a Certicom issued certificate.

Failure to comply with the conditions herein or posted on the Certicom website may result in the termination of the relationship between Certicom and the party.

2.2. Publication of Certificate Information

Certificate information is published by Certicom's issuance of the Certificate and in accordance with the provisions of this CPS that are relevant to such a certificate. Revoked certificate information is published through Certicom's OCSP operations.

An updated CRL is published on the Certicom website every 24 hours; however, under special circumstances the CRL may be published more frequently. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate.

2.3. Time or Frequency of Publication

Updates to the CPS are published in accordance with Section 9.12. Updates to the Subscriber Agreement, Relying Party Agreements, and other agreements posted on the repository are published as often as necessary. Certificates are published upon issuance.

Certificate information is published in accordance with the provisions of the CPS relevant to such a certificate. CRLs are issued every 24 hours and include a monotonically increasing sequence number for each CRL issued. Under special circumstances, Certicom may publish new CRLs prior to the expiration of the current CRL. Each CRL is valid only for the 24 hours following its publication or until an updated CRL has been published, whichever comes first.

Typically, Certicom updates its OCSP every 24 hours. Under special circumstances the OCSP may be more frequently. All parties are strongly urged to always consult the OCSP prior to relying on information featured in a certificate.

2.4. Access Controls on Repositories

The information published in the Certicom repository (www.Certicom.com/repository) is public information and may be accessed freely by anyone visiting the site, provided they agree to the site's terms and conditions as posted thereon. Read-only access to the information is unrestricted. Certicom has implemented logical and physical security measures to prevent unauthorized additions, modification, or deletions of repository entries.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of Names

Certicom Certificates are issued with an X.501 compliant non-null Distinguished Name (DN) in the Issuer and Subject Fields. Issuer Distinguished Names may consist of a combination of the following Components:

| Attribute | Abbr. | Value |
|---------------------|-------|---|
| Common Name | CN | The CA name or not used |
| Organization | O | Certicom |
| Organizational Unit | OU | Certificates may be multiple OU attributes. The attributes may include: <ul style="list-style-type: none"> Certicom Copyright information References to the terms and conditions of use Description of the Certificate |
| Country | C | DE |
| Locality | L | Not used |
| State or Province | S | Not Used |

Certificate Distinguished Names may consist of a combination of the following Components:

| Attribute | Abbr. | Value |
|---------------------|-------|---|
| Common Name | CN | The Common Name which could be the name of the Subscriber or domain name for which the certificate has been issued |
| Organization | O | The organization or blank |
| Organizational Unit | OU | Certificates may be multiple OU attributes. The attributes may include: <ul style="list-style-type: none"> Organization information or Issuer Information |

| | | |
|-------------------|------------|--|
| | | Copyright information References to the terms and conditions of use |
| | | Description of the Certificate Certificate warranty information Verification or validation information Issuance and/or hosting information Special certificate notes |
| Country | C | The two letter ISO country code or not used |
| Locality | L | Subscriber's locality or not used |
| State or Province | S | State or Providence or not used |
| Street | STREET | Street address or not used |
| Postal code | PostalCode | Postal code or not used |
| Email address | E | Email address for Email certificates |

Enhanced naming is the usage of an extended organization field in an X.509v3 certificate. Information contained in the organizational unit field is also included in the Certificate Policy extension that Certicom may use.

For High assurance certificates, the Common Name (CN) component of the Certificate is verified prior to the Certificate's issuance. The CN is not verified in Low Assurance certificates.

Certicom certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and any disclaimers of warranty that may apply. The lack of such information does not mean it does not apply to that certificate.

To communicate information Certicom may use:

- An organizational unit attribute.
- A Certicom standard resource qualifier to a certificate policy.
- Proprietary or other vendors' Certicom extensions.

3.1.2. Need for Names to be Meaningful

Certicom uses non-ambiguous designations and commonly used semantics to identify both the Issuer of the Certificate and the Subject of the Certificate.

3.1.3. Anonymity or Pseudonymity of Subscribers

Certicom does not intentionally issue anonymous or pseudonymous names. However, low assurance and email certificate subscribers are not validated prior to the certificate's issuance and, as a result, may contain an anonymous or pseudonymous name.

3.1.4. Rules for Interpreting Various name Forms

Distinguished Names in Certificates are X.501 compliant. For information on how X.501 Distinguished names are interpreted, please see RFC 2253 and RFC 2616.

3.1.5. Uniqueness of Names

The Distinguished Name of a Certicom-issued Certificate is unique for each Subscriber. The uniqueness of the Distinguished Name is ensured through an automated process. Also, Certicom assigns certificate serial numbers that appear in Certicom certificates. Assigned serial numbers are unique.

3.1.6. Recognition, Authentication, and Role of Trademarks

Through its subscriber agreements, Certicom prohibits the use of a name or symbol that infringes upon the Intellectual Property Rights of another. However, Certicom does not verify or check the name appearing in a Certificate for non-infringement. Subscribers are solely responsible for ensuring the legality of any information presented for use in a Certicom-issued Certificate. Certicom subscribers represent and warrant that when submitting an application to Certicom and when using a domain and distinguished name (and all other certificate application information) that they are not interfering with or infringing any rights of any third parties in any jurisdiction with respect to their trademarks, service marks, trade names, company names, or any other intellectual property right, and that they are not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

Certicom does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any intellectual property or a domain's use of any infringing material. Certicom, in its sole discretion and without any liability, may reject an application or revoke a certificate, based on any intellectual property infringement claims or ownership disputes.

3.2. Initial Identity Validation

Upon receipt of an application for a digital certificate and based on the submitted information, Certicom confirms the following information:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorized to do so.

Verification of a digital signature is used to determine that:

- the private key corresponding to the public key listed in the signer's certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

In all types of Certicom certificates, the Subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify Certicom of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in the Subscriber Agreement will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber. Subscriber shall still be required to pay any applicable charges and fees as specified in the relevant subscriber agreement.

3.2.1. Method to Prove Possession of Private Key

Every Applicant must demonstrate that it holds the private key corresponding to the public key that will be included in the Certificate. To prove possession, the Applicant must submit a digitally signed PKCS#10 to Certicom or provide another cryptographically equivalent demonstration.

3.2.2. Authentication of Organization Identity

The following elements are critical information elements for a Certicom certificate issued to an organization. Those elements marked with PUBLIC are present within an issued certificate and are therefore within the public domain. Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)

- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Company / DUNS number (if available)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed (if applying out of bands)

Documentation requirements for organizational applicants include any / all of the following:

- Articles of Association
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)

Certicom may accept at its discretion other official organizational documentation supporting an application.

Each certificate is validated according to the level of security required for the issued certificate as explained more fully in Section 4.2

Certicom may use the services of a third party to confirm information on a business entity that applies for a digital certificate. Certicom accepts confirmation from third party organizations, other third party databases and government entities.

Certicom's controls may also include Trade Registry transcripts that confirm the registration of the applicant company and state the members of the board, the management and Directors representing the company.

Subscribers shall solely be responsible for the legality of the information they present for use in certificates issued under this CPS, in any jurisdiction in which such content may be used or viewed.

3.2.3. Authentication of Individual Identity

The following elements are critical information elements for a Certicom certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)

- Organizational unit (PUBLIC)
- Street, city, postal/zip code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Contact information including full name, email address and telephone
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Subscriber agreement, signed (if applying out of bands)

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement

Certicom may accept, in its sole discretion, other official documentation supporting an application.

Each certificate is validated according to the level of security required for the issued certificate as explained more fully in Section 4.2

3.2.4. Non-Verified Subscriber Information

Certicom does not validate any information not listed as being validated under Section 4.2. Subscriber Information in low assurance certificates is not validated.

3.2.5. Validation of Authority

The authority of an individual's authority to issue a certificate is confirmed with a WHOIS check or by a practical demonstration of the agent's authority to act on behalf of the domain owner.

The Subscriber shall control and be responsible for the data that an agent supplies to Certicom. The Subscriber must promptly notify Certicom of any misrepresentations and omissions made by an agent. The duty of this article is continuous.

3.2.6. Criteria for Interoperation

All third party CAs interoperating with Certicom are required to enter into a contractual arrangement with Certicom that requires them to operate under a CPS that meets the verification requirements set forth herein for each certificate that will be issued.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routines Re-key

Renewal application requirements and procedures are the same as those requirements and procedures implemented for the application validation and issuance of new customers.

3.3.2. Identification and Authentication for Re-key After Revocation

Rekey/renewal after revocation is only permitted if the Certificate was not revoked because of (i) a mistake in the party to whom the certificate was issued, (ii) a breach of the subscriber agreement, (iii) a material misrepresentation by the Subscriber, or (iv) any other reason that could potentially cause harm to Certicom's trusted status.

3.4. Identification and Authentication for Revocation Requests

Prior to revoking a certificate, Certicom verifies that the revocation was requested by the Certificate Subscriber. The revocation request must be sent by the administrator contact associated with the certificate application. Certicom may, if necessary, also request that the revocation request be made by either the organizational contact or billing contact. Upon receipt of the revocation request, Certicom will request confirmation of out of bands contact details by telephone or by fax from the known administrator.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

Certicom certificates are issued to organizations and individuals who submit a certificate application and successfully complete the required validation procedures described herein. Prior to the issuance of a certificate, Certicom will validate an application in accordance with this CPS. Validation of the application may involve the request by Certicom for the applicant to provide relevant official documentation supporting the application.

4.1.1. Who Can Submit a Certificate Application

Certificate applications may be submitted by an individual or an authorized representative of an organization or other entity who is the subject of the certificate. An authorized agent of an applicant may submit a certificate on the applicant's behalf.

4.1.2. Enrollment Process and Responsibilities

Generally, applicants will complete the online forms made available by Certicom through its website in order to apply for a certificate. Under special circumstances, the applicant may submit an application via email. Email applications are under the discretion of Certicom and may not be accepted.

All Certificate applicants must complete the enrolment process prior to being issued a certificate. The enrollment process may include:

- Generating a RSA or ECDSA key pair and demonstrate to Certicom ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR). ECC public keys are validated during the vetting process as part of the validation process described in Section 4.2.
- Making all reasonable efforts to protect the integrity the private key half of the key pair
- Submitting to Certicom a certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Providing proof of identity through the submission of official documentation as requested by Certicom during the enrolment process

Additional documentation in support of the application may be required by Certicom in its sole discretion in order to assist Certicom in verifying the identity of the subscriber. Upon verification of identity, Certicom issues the certificate and sends a notice to the applicant. The applicant downloads and installs the certificate to its device. The applicant must notify Certicom of any inaccuracy or defect in a certificate promptly after receipt of the certificate or earlier notice of informational content to be included in the certificate.

The following steps describe the milestones to issue a Secure Server Certificate:

- a) The applicant fills out the online request on Certicom's web site and the applicant submits the required information: Certificate Signing Request (CSR), e-mail address,

common name, organizational information, country code, verification method and billing information.

- b) The applicant accepts the on line subscriber agreement.
- c) The applicant submits the required information to Certicom.
- d) The applicant pays the certificate fees.
- e) Certicom verifies the submitted information using third party databases and Government records
- f) Upon successful validation of the application information, Certicom may issue the certificate to the applicant. Should the application be rejected, Certicom will alert the applicant that the application has been unsuccessful.
- g) Renewal is conducted as per the procedures outlined in this CPS and the official Certicom websites.
- h) Revocation is conducted as per the procedures outlined in this CPS.

4.2. Certificate Application Processing

Prior to the issuance of a certificate Certicom will validate an application in accordance with this CPS which may involve the request by Certicom to the applicant for relevant official documentation supporting the application.

From time to time, Certicom may modify the requirements related to application information for individuals, to respond to Certicom's requirements, the business context of the usage of a digital certificate, or as prescribed by law.

4.2.1. Performing Identification and Authentication Functions

Applications for Certicom certificates are supported by appropriate documentation to establish the identity of an applicant as described in Section 3.2. Certicom may use any means of communication at its disposal to ascertain the identity of an organizational or individual applicant. Certicom reserves the right of refusal in its absolute discretion.

ECC public keys are validated to ensure that the key conforms to the arithmetic requirements of the public key. The validation of this shows that the private key for the public key can logically exist.

Prior to issuing a Certificate, Certicom employs controls to validate the identity of the subscriber information featured in the certificate application. Such controls are indicative of the product type:

4.2.1.1. Low Assurance Certificates

Low assurance certificates receive limited validation by Certicom. Certicom, at its discretion, may establish domain control by utilizing Certicom or third party domain registrars and directories, by verifying control of the domain by practical demonstration of control of the domain, by implementing further validation processes including out of bands validation of the applicant's submitted information, or by relying on the accuracy of the applicant's application and the representations made in the subscriber agreement.

4.2.1.2. High Assurance Certificates

Validation of high assurance certificates involves validating the organization named in the certificate. This process involves Certicom, automatically or manually, reviewing the application information provided by the applicant (as per section 4.1 of this CPS) in order to check that:

1. The applicant has the right to use the domain name used in the application.
 - Validated by reviewing domain name ownership records or (for government and educational institutions associated with a .EDU or .GOV domain only) receiving a letter on official departmental letterhead, with the order details and a statement verifying that the signor (which must be a WHOIS contact or senior member of management) is authorized to act on behalf of the organization.

- Validation may be supplemented through the use of the administrator contact associated with the domain name Certicom record for communication with Certicom validation staff or for automated email challenges.
 - Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@..., postmaster@..., admin@...
2. The applicant is an accountable legal entity, whether an organization or an individual.
- Validated by requesting official company documentation, such as Business License, Articles of Incorporation, Sales License or other relevant documents.
 - For non-corporate (including individual, government, and educational entities) applications, documentation such as bank statement, copy of passport, copy of driving license or other relevant documents.

The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases.

4.2.1.3. EV Certificates

EV Certificates are not covered in this CPS. Interested parties are referred to the Certicom EV CPS for more information about these products.

4.2.1.4. Code Signing

Code Signing Certificates are processed by Certicom in accordance with the process outlined for high assurance certificates. Certicom may employ the data held in its domain databases to expedite the validation process. If the application data matches the records held by Certicom, manual validation intervention is not required.

4.2.1.5. Secure Email/ Client Certificates

Secure Email Certificates and client certificates are *non-validated*. Certicom only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by Certicom. The login details are sent via email to the address submitted during the certificate application.

Once logged into the online certificate collection facilities and prior to the installation of the Secure Email Certificate, Certicom validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, Certicom will release the digital certificate to the Subscriber.

4.2.2. Approval or Rejection of Certificate Applications

Following successful completion of all required validations of a certificate application, Certicom will approve an application for a digital certificate and issue the certificate.

If the validation of a certificate application fails, Certicom will reject the certificate application. Certicom reserves its right to reject applications to issue a certificate to applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of Certicom might get tarnished, diminished, or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently re-apply.

The private key associated with a public key, which has been submitted as part of a rejected certificate application, may not under any circumstances be used to create a digital signature if the effect of the signature is to create conditions of reliance upon the rejected certificate. The private key may also not be resubmitted as part of any other certificate application.

4.2.3. Time to Process Certificate Applications

Certicom makes reasonable efforts to confirm certificate application information and issue a digital certificate within a reasonable time frame. The time frame is greatly dependent on the Subscriber providing the necessary details and / or documentation in a timely manner. Upon the receipt of the necessary details and / or documentation, Certicom aims to confirm submitted application data and to complete the validation process and issue / reject a certificate application within two (2) working days.

From time to time, events outside of the control of Certicom may delay the issuance process. However Certicom will make every reasonable effort to meet issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner.

4.3. Certificate Issuance

Certicom issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.4 of this CPS). Issuing a digital certificate means that Certicom accepts a certificate application. Certicom certificates are issued to organizations or individuals.

4.3.1. CA Actions During Certificate Issuance

Certicom issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 4.4 of this CPS). Issuing a digital certificate means that Certicom accepts a certificate application.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Certicom, directly or through an RA, notifies the Subscriber of the issuance of a certificate within a reasonable amount of time after the certificate is created. Issued certificates may either be downloaded by the Subscriber or may be installed by Certicom directly (depending on the certificate type).

4.4. Certificate Acceptance

An issued certificate is either delivered via email or installed on a subscriber's computer / hardware security module through an online collection method.

4.4.1. Conduct Constituting Certificate Acceptance

A subscriber is deemed to have accepted a certificate when:

- the subscriber uses the certificate, or
- 30 days pass from the date of the issuance of a certificate

4.4.2. Publication of the Certificate by the CA

An issued certificate is published solely by delivering the certificate to the Subscriber.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

RAs and other parties involved in the issuance and approval of the Certificate may receive notification of the issuance of a certificate to their customer or client.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

Use of the Private Key is prohibited until the Subscriber has agreed to a Subscriber agreement. Certificates may only be used for lawful and appropriate purposes as set forth in this CPS. Subscribers are responsible for protecting their private keys from unauthorized use and agree to immediately cease using the Certificate following the expiration or revocation of the Certificate.

4.5.2. Relying Party Public Key and Certificate Usage

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate;
- the relying party has checked the revocation status of the certificate by referring to the relevant OCSP and the certificate has not been revoked;
- the relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile; and
- the digital certificate applied for is appropriate for the application it is used in, e.g. relying parties should not rely on low assurance SSL Certificates for e-commerce uses.

Reliance is accepted as reasonable under the provisions made for the relying party under this CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by Certicom under the provisions made in this CPS, the relying party must obtain additional assurances.

Warranties are only valid if the steps detailed above have been carried out.

4.6. Certificate Renewal

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

Renewal fees are detailed on the official Certicom websites and within communications sent to subscribers approaching the certificate expiration date. Certicom shall make reasonable efforts to notify subscribers via e-mail of the imminent expiration of a digital certificate. Notice shall ordinarily be provided within a 60-day period prior to the expiration of the certificate.

4.6.1. Circumstances for Certificate Renewal

A Subscriber may renew an existing Certificate prior to or after its expiration by submitting a renewal request on line or in writing to Certicom.

4.6.2. Who May Request Renewal

The Subscriber of the certificate or an authorized representative must be the party requesting the certificate's renewal.

4.6.3. Processing Certificate Renewal Requests

Renewal applications and requests undergo the same identity check as detailed for new customers.

4.6.4. Notification of New Certificate Issuance to Subscriber

Notification of a new certificate issuance is performed in accordance with Section 4.4.3.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Conduct constituting acceptance of a renewed certificate is the same as specified in Section 4.4.1.

4.6.6. Publication of the Renewal Certificate by the CA

A renewed certificate is published by delivering the certificate to the Subscriber.

4.6.7. Notification of Certificate Issuance by the CA to other Entities

RAs and resellers may receive notification of its customer's certificate renewal if the party was involved in the issuance of the certificate or performed validation services for the issued certificate.

4.7. Certificate Re-key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

4.7.1. Circumstances for Certificate Re-Key

Sometimes circumstances may dictate that a valid or expired certificate must be rekeyed. Rekeying a certificate prior to its expiration will prevent an interruption in the certificate's usage. A rekey request made more than thirty (30) days from the certificate's date of issuance may be refused.

4.7.2. Who May Request Certificate of a New Public Key

The Subscriber of a Certificate or an authorized representative must be the party requesting a certificate rekey.

4.7.3. Processing Certificate Re-keying Requests

During a 30-day period (beginning when a certificate is first issued) the Subscriber may request a rekey of their certificate and incur no further fees for the reissue. If details other than just the public key require amendment, Certicom reserves the right to revalidate the application in accordance with the validation processes detailed within this CPS. If the rekey request does not pass the validation process, Certicom reserves the right to refuse the rekey application. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant.

4.7.4. Notification of New Certificate Issuance to Subscriber

Notification of a rekeyed certificate is provided in accordance with Section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

Acceptance of a rekeyed certificate is made in the manner specified in Section 4.4.1.

4.7.6. Publication of the Re-keyed Certificate by the CA

A rekeyed certificate is published by its deliver to the Subscriber.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

RAs and other reseller partners may receive notification of a rekeyed certificate's issuance if that party approved the issuance of the certificate or performed validation or verification services for the issued certificate.

4.8. Certificate Modification

4.8.1. Circumstance for Certificate Modification

Certificate information may change during the life of the certificate. In this case, Certicom will issue a new certificate based on the new information rather than modifying an existing certificate. Certificate modification is considered and handled the same as an application for a new certificate.

4.8.2. Who May Request Certificate Modification

See 4.1.1.

4.8.3. Processing Certificate Modification Requests

See 4.1.2.

4.8.4. Notification of New Certificate Issuance to Subscriber

See 4.3.2

4.8.5. Conduct Constituting Acceptance of Modified Certificate

See 4.4.1

4.8.6. Publication of the Modified Certificate by the CA

See 4.4.2.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

See 4.4.3

4.9. Certificate Revocation and Suspension

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated. The serial number of the revoked certificate will be placed within the OCSP and remains on the OCSP until some time after the end of the certificate's validity period.

4.9.1. Circumstances for Revocation

Revocation of a certificate is the permanent end of the operational period of the certificate prior to reaching the conclusion of its stated validity period. Certicom may revoke a digital certificate if any of the following occur:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate;
- The Subscriber or Certicom has breached a material obligation under this CPS or the relevant Subscriber Agreement;
- Either the Subscriber's or Certicom's obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised;
- There has been a modification of the information pertaining to the Subscriber that is contained within the certificate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- A Subscriber's Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The subscriber has used the Subscription Service contrary to law, rule or regulation, or Certicom reasonably believes that the Subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The certificate is being used or is suspected to be used to distribute or sign malware;
- The information contained in the certificate is incorrect or has changed;
- The certificate was issued as a result of fraud or negligence; or
- The certificate, if not revoked, will compromise the trust status of Certicom.

When considering whether or not the certificate should be revoked, Certicom will consider:

- The nature and number of complaints received
- The nature of the complaining party

- Relevant legislation and industry standards
- Additional outside input regarding the trust status of the certificate or the nature of the use of the certificate

4.9.2. Who can Request Revocation

The subscriber or other appropriately authorized parties can request revocation of a certificate. Prior to the revocation of a certificate Certicom will verify that the revocation request has been made by the organization or individual entity that has made the certificate application.

4.9.3. Procedure for Revocation Request

Certicom employs the following procedure for authenticating a revocation request:

- The revocation request must be sent by the Administrator contact associated with the certificate application. Certicom may, if necessary, also request that the revocation request be made by either the organizational contact or the billing contact.
- Upon receipt of the revocation request, Certicom will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- Certicom validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

4.9.4. Revocation Request Grace Period

There is no revocation grace period.

4.9.5. Revocation Checking Requirement for Relying Parties

Relying Parties must always check the status of the Certificate on which they are relying. Relying Parties may check the OCSP and/or CRL or use the applicable web-based repository to confirm that the certificate has not been revoked or expired.

4.9.6. Time Within Which CA Must Process the Revocation Request

Certicom processes all revocation requests without delay. The amount of time required depends on the nature of the revocation request, the party requesting the revocation, and other factors surrounding the revocation request. Certicom will revoke the certificate and place the certificate in the OCSP and/or CRL once it has determined, to Certicom's satisfaction, that the revocation request was proper.

4.9.7. CRL Issuance Frequency

An updated CRL is published on the Certicom website every 24 hours. Under special circumstances the CRL may be published more frequently.

4.9.8. Maximum Latency for CRLs

CRLs are posted to the online repository within a commercially reasonable time after their generation. Usually, this is within a minute of the CRL's generation.

4.9.9. On-line Revocation/Status Checking Availability

Certicom manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs). All CRLs issued by Certicom are X.509v2 CRLs as profiled in RFC3280. Users and relying parties are strongly urged to consult the directories of revoked certificates at all times prior to relying on information featured in a certificate. Certicom updates and publishes a new CRL every 24 hours or more frequently under special circumstances. The CRL for end entity certificates can be accessed via crl.Certicom.com.

Revoked intermediate and higher level certificates are published in the CRL accessed via: <http://certicom.com/Class3SecurityServices.crl>

4.9.10. On-line Revocation Checking Requirements

Relying Parties must confirm the validity of a certificate via the CRL prior to relying on the Certificate.

4.9.11. Other Forms for Revocation Advertisements available

Not applicable.

4.9.12. Special Requirements Re-key Compromise

Certicom uses commercially reasonable efforts to notify Relying Parties if it believes or has reason to believe that one of its private keys have been compromised.

4.9.13. Circumstances for Suspension

Certicom does not utilize certificate suspension.

4.9.14. Who can Request Suspension

Not applicable

4.9.15. Procedure for Suspension Request

Not applicable

4.9.16. Limits on Suspension Period

Not applicable

4.10. Certificate Status Services

4.10.1. Operational Characteristics

Certicom utilizes both CRLS and an OCSP to allow relying parties to verify the validity of a digital signature made using a Certicom issued digital certificate. Each CRL and the OCSP contain information for all of Certicom's revoked or un-expired certificates.

Each CRL contains entries for all revoked un-expired certificates issued and is valid for 24 hours. Certicom issues a new CRL every 24 hours and includes a monotonically increasing sequence number for each CRL issued. Under special circumstances, Certicom may publish new CRLs prior to the expiry of the current CRL. All expired CRLs are archived (as described in section 5.5 of this CPS) for a period of 7 years or longer if applicable.

Individual entries into the OCSP can be requested using the Certicom OCSP responder. Revoked certificates are affected in the OCSP within 24 hours after their revocation.

4.10.2. Service Availability

The OSPC provides access to certificate status information 24x7. CRL's are open to public inspection 24x7.

4.10.3. Optional Features

Not applicable.

4.11. End of Subscription

A Subscriber may terminate a subscription to Certicom's Certificate services by allowing the Certificate to expire without renewal or by requesting that Certicom revoke the issued Certificate.

4.12. Key Escrow and Recovery

Certicom does not escrow subscriber private keys

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Security Controls

Certicom makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

5.1.1. Site Location and Construction

Certicom performs its CA operations in a secure data center located in the United States. The building is a secure structure. The data center is operated under a secure policy to ensure that no unauthorized logical or physical access is allowed.

Most records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.1.2. Physical Access

Access to the secure part of Certicom facilities is limited using physical access control and is only accessible to appropriately authorized individuals (referred to hereon as Trusted Personnel). Card access systems are in place to control, monitor and log access to all areas of the facility. Access to the Certicom CA physical machinery within the secure facility is protected with locked cabinets and logical access control.

5.1.3. Power and Air Conditioning

Certicom secure facilities have a primary and secondary power supply and ensure continuous, uninterrupted access to electric power. Heating / air ventilation systems are used to prevent overheating and to maintain a suitable humidity level.

5.1.4. Water Exposures

Certicom has taken commercially reasonable efforts to ensure that its CA system is secure and protected from flood and water damage.

5.1.5. Fire Prevention and Protection

Fire protection and prevention is made in compliance with local fire regulations

5.1.6. Media Storage

All media storing Certicom data or information, including media containing audit logs, archived records, software, subscriber information, and other information pertinent to the CA's operation is stored in a secure facility that has implemented both logical and physical controls that limit potential harm to the data.

5.1.7. Waste Disposal

Sensitive documents are shredded prior to disposal. Electronic Media is wiped clean by a trusted source upon the expiration of the data. All media is rendered unreadable prior to its disposal and, where possible, is physically destroyed.

5.1.8. Off-site Backup

Certicom performs routine backups of all sensitive information. Offsite backups are stored in a separate secure location using a third party data center.

5.2. Procedural Controls

5.2.1. Trusted Roles

Trusted roles are parties allowed to access the Certicom account management system. Persons acted in a trusted role are granted functional permissions to the account management system. All permissions are applied on an individual basis and are decided by senior members of the management team. All signed authorizations are archived. The roles and responsibilities of each personnel are assigned in such a manner that one person alone cannot circumvent Certicom's security measures.

5.2.2. Number of Persons Required Per Task

Internal policy and operational procedures require multiple trusted personnel to take part in the CA's operations. This provides an added layer of security. All of the CA's most sensitive tasks require the involvement of multiple trusted personnel.

At least two trusted individuals are required to:

- Issue certificates
- Revoke Certificates
- Handle the CA private keys

5.2.3. Identification and Authentication for Each Role

Trusted personnel must identify and authenticate themselves before system access is granted. Identification is via a username, with authentication requiring a password and digital certificate.

5.2.4. Roles Requiring Separation of Duties

Roles requiring the separation of duties include:

- Validation of Certificate Applications, renewals, or rekeys
- Approval or rejection of Certificate Applications
- Certificate Issuance and Revocations
- Management of the CA key, including issuance or destruction of a CA certificate

5.3. Personnel Security Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

Certicom follows personnel and management practices that provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties. All Certicom employees must have the necessary qualifications or experience to fulfill their job descriptions.

5.3.2. Background Check Procedures

Background checks are performed on all trusted personnel before access is granted to Certicom's systems. These checks include, but are not limited to, credit history, employment history (for references), and a Companies House cross-reference to disqualified directors.

5.3.3. Training Requirements

Personnel training occurs via a mentoring process involving senior members of the team to which the employee is attached. Certicom periodically reviews and enhances its training programs as necessary.

Training programs are tailored toward each individual's job responsibilities and include training on PKI concepts, job responsibilities, operational policies and procedures, incident handling and reporting, and disaster recovery procedures.

5.3.4. Retraining Frequency and Requirements

Certicom provides refresher training courses to its personnel in order to ensure that all such personnel can competently and satisfactorily perform their job responsibilities.

5.3.5. Job Rotation Frequency and Sequence

No Stipulation

5.3.6. Sanctions for Unauthorized Actions

Any personnel found violating a Certicom policy or procedure is subject to disciplinary action. The action taken by Certicom depends on the circumstances surrounding the action, the severity

of the violation, and the personnel's past performance. In some cases, disciplinary action may include the personnel's termination.

5.3.7. Independent Contractor Requirements

If an independent contractor or consultant is used, Certicom shall first ensure that each such contractor or consultant is first obligated to abide by the same functional and security criteria that are set forth herein. Contractors and consultants are subject to the same sanctions as other personnel as set forth in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

Certicom supplies its personnel with the training and documentation needed to perform their job responsibilities. Certicom personnel understand and are obligated and required to safe guard and protect all private and confidential information to which they might have access.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recoded

For audit purposes, Certicom maintains electronic or manual logs of the following events for core functions.

CA & Certificate Lifecycle Management

- CA Root signing key functions, including key generation, backup, recovery and destruction
- Subscriber certificate life cycle management, including successful and unsuccessful certificate applications, certificate issuances, certificate re-issuances and certificate renewals
- Subscriber certificate revocation requests, including the reason for the revocation
- Subscriber changes of affiliation that would invalidate the validity of an existing certificate
- Certificate Revocation List updates, generations and issuances
- Custody of keys and of devices and media holding keys
- Compromise of a private key

Security Related Events

- System downtime, software crashes, and hardware failures
- CA system actions performed by Certicom personnel, including software updates, hardware replacements, and upgrades
- Cryptographic hardware security module events, such as usage, de-installation, service, or repair and retirement
- Successful and unsuccessful Certicom PKI access attempts
- Secure CA facility visitor entry and exit

Certificate Application Information

- The documentation and other related information presented by the applicant as part of the application validation process
- Storage locations, whether physical or electronic, of presented documents

An audit log is maintained of each movement of the removable media.

5.4.2. Frequency of Processing Log

Logs are review on a weekly basis by CA management.

5.4.3. Retention Period of Audit Log

Logs are archived by the system administrator on a weekly basis by the system administrator. Logs are thereafter retain as part of the record archive as set forth in Section 5.5.

5.4.4. Protection of Audit Log

All logs are backed up on removable media and the media held at a secure off-site location on a daily basis. These media are only removed by Certicom staff on a visit to the data centre, and when not in the data centre are held either in a safe in a locked office within the development site, or off-site in a secure storage facility.

5.4.5. Audit Log Backup Procedures

Logs are archived by the system administrator on a weekly basis by the system administrator. Both current and archived logs are maintained in a form that prevents unauthorized modification, substitution or destruction. When the removable media reaches the end of its life it is wiped by a third party secure data destruction facility and the certificates of destruction are archived.

5.4.6. Audit Collection System

Audit data is generated both automatically and manually. Automatic logs are computer-generated and are based off of set security protocols, scans, and alerts. Manual audits are recorded and stored by Certicom personnel.

All logs include the following elements:

- Date and time of entry
- Serial or sequence number of entry
- Method of entry
- Source of entry
- Identity of entity making log entry

5.4.7. Notification to Event-Causing Subject

Notice of audited events are confidential information and no notice is given to individuals or organizations unless required by law or agreement.

5.4.8. Vulnerability Assessments

Events in the audit process are logged to monitor vulnerabilities. Certicom periodically reevaluates its security procedures and updates them as may be required.

5.5. Records archival

5.5.1. Types of records archived

The following information may be archived:

- Information or documentation submitted by Subscribers in support of a certificate application.
- Copies of certificates, regardless of their status (such as expired or revoked). Such records may be retained in electronic, in paper-based format or any other format that Certicom may see fit.
- Audit logs
- Other records deemed important and valuable to the Certicom business operations

5.5.2. Retention period for archive

Certicom retains the records of Certicom digital certificates and the associated documentation for a term of than 7 years, or as necessary to comply with applicable laws. The retention term begins on the date of expiration or revocation.

5.5.3. Protection of archive

Records are archived at a secure off-site location and are maintained in a form that prevents unauthorized modification, substitution or destruction.

5.5.4. Archive backup procedures

Certicom regularly backs up electronic archives. Copies are maintained of paper files.

5.5.5. Requirements for time-stamping of records

Certificates, CRLs, and other archived information shall contain time and date information that may or may not be cryptographic-based.

5.5.6. Archive collection system

The Certicom archive collection system is an internal system.

5.5.7. Procedures to obtain and verify archive information

Only authorized trusted personnel are permitted access to the archive. Subscribers may obtain copies of archived information related to their Certificate upon written request and payment of any associated costs.

5.6. Key changeover

Towards the end of each private key's lifetime, a new CA signing key pair is commissioned and all subsequently issued certificates are signed with the new private signing key. Both keys may be concurrently active. The corresponding new CA public key certificate is provided to subscribers and relying parties through the delivery methods detailed in section 6.1 of this CPS.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

To maintain its CA operations when an incident occurs, Certicom makes a backup of critical CA software is performed weekly and is stored offsite. Certicom also performs a backup of critical business information is performed daily and is stored offsite. Further, Certicom operations are distributed across several sites world wide. All sites offer facilities to manage the lifecycle of a certificate, including but not limited to the application, issuance, revocation and renewal of such certificates.

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

Certicom operates a fully redundant CA system. The backup CA is readily available in the event that the primary CA should cease operation. All of Certicom's critical computer equipment is housed in a co-location facility run by a commercial data-centre, and all of the critical computer equipment is duplicated within the facility. Incoming power and connectivity feeds are duplicated. The duplicate equipment is ready to take over the role of providing the implementation of the CA, and allows Certicom to specify a maximum system outage time (in case of critical systems failure) of 1 hour.

As well as a fully redundant CA system, Certicom maintains provisions for the activation of a backup CA and a secondary site should the primary site suffer a total loss of systems. This disaster recovery plan states that Certicom will endeavor to minimize interruptions to its CA operations.

5.7.3. Business continuity capabilities after a disaster

To maintain the integrity of its services Certicom implements, documents and periodically tests appropriate contingency and disaster recovery plans and procedures. Such plans are revised and updated as may be required at least once a year.

5.8. CA or RA termination

In the event that it is necessary for a CA or RA of Certicom to cease operation, Certicom shall make a commercially reasonable effort to notify Participants of such termination in advance of the effective date of the termination. Should Certicom cease its CA operations, Certicom shall develop a termination plan to minimize the disruption of services to its customers, Subscribers, and Relying Parties. The plan shall provide for:

- Revocation of Certificates issued to the CA
- Revocation of unexpired and unrevoked Certificates as may be necessary
- Preservation of the CA's archives and records as required by this CPS
- Continuation of customer support services
- Providing to affected parties and how to address the cost of such notice
- Transition of the services to the CA's successor
- Disposition of the CA's private key
- Refunds (if necessary)
- Continuation of revocation services

6. TECHNICAL SECURITY CONTROLS

Certicom's operational sites operate under a security policy designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section of the CPS outlines the security policy, physical and logical access control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

6.1. Key pair generation and installation

6.1.1. Key pair generation

Certicom securely generates and protects its own private key(s), using a trustworthy system (nCipher accredited to FIPS PUB 140-1 level 3), and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The Certicom CA Root key was generated in accordance with the guidelines detailed in the Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

The Subscriber is solely responsible for the generation of the private key used in the certificate request. Certicom does not provide key generation, escrow, recovery or backup facilities.

Upon making a certificate application, the Subscriber is solely responsible for the generation of an RSA or ECDSA key pair appropriate to the certificate type being applied for. During application, the Subscriber will be required to submit a public key and other personal / corporate details in the form of a Certificate Signing Request (CSR).

Secure Server Certificate requests are generated using the key generation facilities available in the Subscriber's webserver software.

Code Signing Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in Microsoft Internet Explorer.

Secure Email Certificate requests are generated using the FIPS 140-1 Level 1 cryptographic service provider module software present in popular browsers.

6.1.2. Private key delivery to subscriber

Certicom provides the full certificate chain to the Subscriber upon issuance and delivery of the Subscriber certificate. Certicom incorporates by reference the following information in every digital certificate it issues:

- Terms and conditions of the digital certificate.
- Any other applicable certificate policy as may be stated on an issued Certicom certificate, including the location of this CPS.
- The mandatory elements of the standard X.509v3.
- Any non-mandatory but customized elements of the standard X.509v3.
- Content of extensions and enhanced naming that are not fully expressed within a certificate.
- Any other information that is indicated to be so in a field of a certificate.

Delivery of Subscriber certificates to the associated Subscriber is dependent on the certificate product type:

6.1.2.1. Secure Server Certificate

If Certicom's domain databases hold sufficient validation information, an automatic validation of the Certificate Application may take place. In the event of such an automated validation the Certificate is delivered to commonly used generic email addresses ordinarily belonging to authorized personnel at the domain name used in the application, such as webmaster@... admin@... postmaster@... Confirmation of the certificate delivery location is provided to the administrator contact provided during the application process. If the Certificate is validated outside of Certicom's databases, then the secure server certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

6.1.2.2. Code Signing Certificates

Code Signing Certificates are delivered via email to the Subscriber using the administrator contact email address provided during the application process.

6.1.2.3. Delivery of other Certificates

Unless otherwise specified through an amendment to this CPS, all other Certificates shall be delivered to the relevant party through email using a Subscriber-provided email address.

6.1.2.4. Secure Email Certificate

Upon issuance of a Secure Email Certificate, the Subscriber is emailed a collection link using the email provided during the application. The Subscriber must visit the collection link using the same computer from which the original certificate request was made. The Subscriber's cryptographic service provider software is initiated to ensure the Subscriber holds the private key corresponding to the public key submitted during application. Pending a successful challenge, the issued certificate is installed automatically onto the Subscriber's computer.

6.1.3. Public key delivery to certificate issuer

Secure Server Certificate requests are generated using the Subscriber's webserver software and the request is submitted to Certicom in the form of a PKCS #10 Certificate Signing Request (CSR). Submission is made electronically via the Certicom website or through a Certicom approved RA.

Secure Email Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted to Certicom in the form of a

PKCS#10 Certificate Signing Request (CSR). The Subscriber's browser generally makes submission automatically.

Code Signing Certificate requests are generated using the Subscriber's cryptographic service provider software present in the Subscriber's browser and submitted automatically to Certicom in the form of a PKCS#10 Certificate Signing Request (CSR).

The private key may either be allowed to remain in the cryptographic service provider, or may be exported to the subscriber's hard drive.

6.1.4. CA public key delivery to relying parties

Certicom makes all its CA Root Certificates available in online repositories at www.Certicom.com/repository.

The UTN USERFirst Hardware certificate is present in Explorer 5.01 and above, Netscape 8.1 and above, Opera 8.0 and above, Mozilla 1.76 and above, Konqueror 3.5.2 and above, Safari 1.2 and above, FireFox 1.02 and above, Camino and SeaMonkey and is made available through these browsers.

The AddTrust External CA Root certificate is present in Netscape 4.x and above, Opera 8.00 and above, Mozilla .06 and above, Konqueror, Safari 1.0 and above, Camino and SeaMonkey and is made available to relying parties through these browsers.

The Certicom CA Root Certificates are cross-signed by the UTN USERFirst Hardware certificate and AddTrust External CA Root certificates and are trusted by Explorer 5.01 and above, Safari 1.0 and above, Opera 8.00 and above, Mozilla .06 and above, Firefox 1.02 and above, Konqueror, Camino, and SeaMonkey through this cross-signing.

6.1.5. Key sizes

Key pairs are of sufficient length to prevent unauthorized determination or reverse engineering of the private key. Certicom keys are either RSA 2048 bit or ECC 256 or 384 bit keys. See Appendix A for the size of each issued key.

6.1.6. Public key parameters generation and quality checking

Certicom securely generates and protects its own private key(s), using a trustworthy system and takes necessary precautions to prevent the compromise or unauthorized usage of it.

The Certicom CA Root keys were generated in accordance with the guidelines detailed in the Certicom's Root Key Generation Ceremony Reference. The activities undergone and the personnel involved in the Root Key Generation Ceremony are recorded for audit purposes. Subsequent Root Key Generation Ceremonies are to follow the documented reference guide also.

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

The key usage field extension in Certicom Certificates specifies the purpose for which the Certificate may be used. Enforcement of the limitations of use found in this field are beyond Certicom's control as its correct use is highly dependant on having the correct software.

6.2. Private Key Protection and Cryptographic Module Engineering Controls

Certicom protects its CA Root key pairs in accordance with this CPS.

6.2.1. Cryptographic module standards and controls

Certicom protects its Root Certificates in accordance with its AICPA/CICA WebTrust program compliant infrastructure and CPS. Details of Comodo's WebTrust compliancy are available at its official website (www.comodogroup.com).

The Certicom root certificates are cross signed to the UTN and AddTrust CA Root Key pairs which are protected within the Comodo CA Limited PKI.

Certicom private keys are generated and store on an nCipher accredited to FIPS PUB 140-1 level 3.

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

For CA Root key recovery purposes, the Root CA signing keys are encrypted and stored within a secure environment. The decryption key is split across **m** removable media and requires **n** of **m** to reconstruct the decryption key. Custodians in the form of two or more authorized Certicom officers are required to physically retrieve the removable media from the distributed physically secure locations.

6.2.3. Private key escrow

Certicom does not escrow private keys.

6.2.4. Private key backup

Certicom's CA keys are generated and stored inside cryptographic hardware. The keys are backed up and transferred in an encrypted form.

The Subscriber is solely responsible for protection of their private keys. Certicom maintains no involvement in the generation, protection or distribution of such keys.

Certicom strongly urges Subscribers to use a password or equivalent authentication method to prevent unauthorized access and usage of the Subscriber private key.

6.2.5. Private key archival

When any CA Root Signing Key pair expires, they will be archived for at least 7 years. The keys will be archived in a secure cryptographic hardware module, as per their secure storage prior to expiration.

6.2.6. Private key transfer into or from a cryptographic module

Where CA Root signing keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

6.2.7. Private key storage on cryptographic module

Certicom private keys are generated and store on an nCipher accredited to FIPS PUB 140-1 level 3.

6.2.8. Method of activating private key

Certicom's private keys are activated according to the specifications of the cryptographic hardware manufacturer. Subscriber's are responsible for protecting their own private keys and should take commercially reasonable steps to prevent physical or logical unauthorized access to a private key. This might include using a windows logon or screensaver password.

6.2.9. Method of deactivating private key

All deactivated private keys should be kept in an encrypted form only. Keys are deactivated by logging off their system. Root keys are further deactivated by removing them from their storage partition.

6.2.10. Method of destroying private key

Private keys are destroyed by deleting them from all known storage partitions and then by zeroizing or by physically destroying the hardware on which they were stored. All CA key destruction activities are logged.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. Other aspects of key pair management

Certicom conducts the overall certification management within the Certicom PKI. Certicom is not involved in functions associated with the generation, issuance, decommissioning or destruction of a Subscriber key pair.

6.3.1. Public key archival

Certicom retains copies of all Public Keys in its archive via its routine backup procedures and as described in Section 5.5.

6.3.2. Certificate operational periods and key pair usage periods

The operational period of each Certificate generated ends upon its revocation or expiration. The operational period of each CA key is set forth in Appendix A.

The validity period of Certicom certificates varies dependent on the certificate type, but typically, a certificate will be valid for 1 to 5 years. Certicom reserves the right to, at its discretion, issue certificates that may fall outside of these set periods.

6.4. Activation data

6.4.1. Activation data generation and installation

Certicom activates the cryptographic module containing its private keys according to the specifications set forth by the hardware manufacturer and meets the requirements of FIPS 140-2 Level 3. All cryptographic hardware is under two-personnel control.

All Certicom personnel are required to use strong passwords (non-dictionary alphanumeric passwords with a minimum length that are changed on a regular basis) to protect sensitive information.

6.4.2. Activation data protection

Data is protected using strong passwords as described in 6.4.1.

6.4.3. Other aspects of activation data

All activation is transmitted, stored, and destroyed using methods and procedures that protect against loss, theft, modification, or any other unauthorized access, loss, or use.

6.5. Computer security controls

The Certicom CA Infrastructure uses trustworthy systems to provide certificate services. A trustworthy system is computer hardware, software and procedures that provide an acceptable resilience against security risks, provide a reasonable level of availability, reliability and correct operation, and enforce a security policy.

6.5.1. Specific computer security technical requirements

Certicom computer systems are set up and maintained in a secure manner that prevents unauthorized access. Certicom uses software and hardware that constitute the industry's best practice in security measures.

Computers are password protected and require a strong password for access. All passwords are changed on a regular basis. Computers are firewalled and scanned regularly for viruses, spyware, Trojans, and other malware.

6.5.2. Computer security rating

No Stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

Certicom closely controls and monitors its CA systems and software development. All systems and software are developed and implemented in accordance with industry standards. All systems and software are routinely checked for malware and security issues.

6.6.2. Security management controls

Certicom controls and monitors the configuration and operation of its CA systems. Changes in Security-related changes are logged and processed. Certicom periodically reviews and updates its security policy and controls to ensure that no unauthorized access is allowed.

6.6.3. Life cycle security controls

No Stipulation.

6.7. Network security controls

Certicom performs all of its CA functions on secured networks to prevent unauthorized access and other malicious activity.

6.8. Time-stamping

Certificates, CRLs, and OCSP entries shall contain time and date information about the Certificate, CRL, or OCSP information. Such information may not be cryptographic based.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Certicom currently offers a portfolio of digital certificates and related products that can be used in a way that addresses the needs of users for secure personal and business communications.

Certicom offers a range of distinct certificate types. The different certificate types have differing intended usages and differing policies. Pricing and subscriber fees for the certificates are made available on the relevant official Certicom websites. The maximum warranty associated with each certificate is set forth in Appendix E of this CPS.

As the suggested usage for a digital certificate differs on a per application basis, Subscribers are urged to appropriately study their requirements for their specific application before applying for a specific certificate.

Certicom may update or extend its list of products, including the types of certificates it issues, as it sees fit. The publication or updating of the list of Certicom products creates no claims by any third party. If necessary, Certicom shall amend this CPS upon the inclusion of a new certificate product in the Certicom hierarchy. The CPS shall usually be made public on the official Certicom websites at least seven (7) days prior to the offering such new product.

Suspended or revoked certificates are appropriately referenced in the CRL and/or OCSP.

7.1. Certificate profile

Certicom certificates are general purpose and may be used without restriction on geographical area or industry. In order to use and rely on a Certicom certificate, the relying party must use X.509v3 compliant software.

7.1.1. Version number(s)

All Certicom certificates are X.509 version 3 certificates.

7.1.2. Certificate extensions

Certicom uses the standard X.509, version 3 to construct digital certificates for use within the Certicom PKI. X.509v3 allows a CA to add certain certificate extensions to the basic certificate structure. Certicom uses a number of certificate extensions for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. X.509v3 is the standard of the International Telecommunications Union for digital certificates.

7.1.2.1. Key Usage Extension field

Certicom certificates include key usage extension fields to specify the purposes for which the certificate may be used and to technically limit the functionality of the certificate when used with

X.509v3 compliant software. Reliance on key usage extension fields is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Certicom. Certicom assumes that user software that is claimed to be compliant with X.509v3 and other applicable standards enforces the requirements set out in this CPS. Certicom cannot warrant that any such user software will support and enforce the controls required by Certicom. All software use is left to the user's sole discretion.

The possible key purposes identified by the X.509v3 standard are the following:

- a) Digital signature, for verifying digital signatures that have purposes other than those identified in b), f) or g), that is, for entity authentication and data origin authentication with integrity
- b) Non-repudiation, for verifying digital signatures used in providing a nonrepudiation service which protects against the signing entity falsely denying some action (excluding certificate or CRL signing, as in f) or g) below)
- c) Key encipherment, for enciphering keys or other security information, e.g. for key transport
- d) Data encipherment, for enciphering user data, but not keys or other security information as in c) above
- e) Key agreement, for use as a public key agreement key
- f) Key certificate signing, for verifying a CA's signature on certificates, used in CA certificates only
- g) CRL signing, for verifying a CA's signature or CRLs
- h) Encipher only, public key agreement key for use only in enciphering data when used with key agreement
- i) Decipher only, public key agreement key for use only in deciphering data when used with key agreement

7.1.2.2. Extension Criticality Field

The Extension Criticality field denotes two separate uses for the Key Usage field. If the extension is noted as critical, then the key in the certificate is only to be applied to the stated uses. To use the key for another purpose in this case would break the issuer's policy. If the extension is not noted as critical, the Key Usage field is simply there as an aid to help applications find the proper key for a particular use.

7.1.2.3. Basic Constraints Extension

The Basic Constraints extension specifies whether the subject of the certificate may act as a CA or only as an end-entity. Reliance on basic constraints extension field is dependent on correct software implementations of the X.509v3 standard and is outside of the control of Certicom.

7.1.3. Algorithm object identifiers

Certicom has its own self-signed root certificates which have been cross-signed with the UTN-USERFIRST-Hardware and AddTrust External CA Root for ubiquity. This cross-signing allows Certicom to issue its own certificates that inherit the trust level associated with the UTN root certificate (named "UTN-USERFIRST-Hardware") and the AddTrust root certificate (named "AddTrust External CA Root"). The high-level representation of the Certicom PKI set forth in Appendix C is used to illustrate the hierarchy utilized.

7.1.4. Name forms

Certicom Certificates following the naming policy set forth in Section 3.1.1.

7.1.5. Name constraints

No Stipulation

7.1.6. Certificate policy object identifier

Certificate Policy (CP) is a statement of the issuer that corresponds to the prescribed usage of a digital certificate within an issuance context. A policy identifier is a number unique within a specific domain that allows for the unambiguous identification of a policy, including a certificate policy.

Specific Certicom certificate profiles are provided in Appendix D.

7.1.7. Usage of Policy Constraints extension

No Stipulation

7.1.8. Policy qualifiers syntax and semantics

Certicom usually includes information in the Policy Qualifier field of the Certificate Policy extension that puts Relying Parties on notice of the location of its CPS. This field usually includes a URL that points the Relying Party to the CPS where they can find out more about the limitations on liability and other terms and conditions governing the use of the Certificate.

7.1.9. Processing semantics for the critical Certificate Policies extension

No Stipulation.

7.2. CRL profile

Certicom manages and makes publicly available directories of revoked certificates using Certificate Revocation Lists (CRLs).. All CRLs issued by Certicom are X.509v2 CRLs, in particular as profiled in RFC3280.

7.2.1. Version number(s)

CRLs conform to RFC 3280 and contain the basic fields listed below:

| Field | Content |
|--|--|
| Version | v2 |
| Signature Algorithm | <Same Signature Algorithm used to sign certificates> |
| Issuer | <Same Issuer name included in certificates> |
| Validity Period | 96 hours, but refreshed every 24 hours |
| | |
| Extensions: | |
| Authority Key Identifier (non-critical) | <Same Authority Key Identifier included in certificates> |
| CRL Number (non-critical) | <A monotonically increasing integer> |
| | |
| For each Revoked Certificate: | |
| Serial Number | <Copied from the revoked certificate> |
| Revocation Date | <Date/time at which this certificate was revoked> |

7.2.2. CRL and CRL entry extensions

No Stipulation.

7.3. OCSP profile

OCSP is way for users to obtain information about the revocation status of a Certicom issued Certificate. Certicom uses OCSP to provide information about all of its certificates. OCSP responders conform to RFC 2560.

7.3.1. Version Number(s)

Certicom uses Version 1 of the OCSP specification as defined by RFC2560.

7.3.2. OCSP Extensions

Certicom’s uses timestamp and validity periods to establish the accuracy of each OCSP response. Certicom does not use a cryptographic nonce in connection with its OCSP services. Instead, local time should be used by participants to ensure the freshness of the OCSP response.

| Field | Content |
|--------------------|--|
| Version | v1 |
| Responder ID | byKey: <SHA-1 Hash of the Issuing CA's Public Key> (OCSP Responses are always signed directly by the Issuing CA, rather than by a delegated OCSP Responder Certificate) |
| Produced At | <Date/Time that this OCSP Response was produced> |
| | There is always precisely 1 “SingleResponse” in each OCSP Response: |
| Hash Algorithm | <Same Hash algorithm used in the certificate's signature> |
| Issuer Name Hash | <Hash of the Issuing CA's Name> |
| Issuer Key Hash | <Hash of the Issuing CA's Public Key> |
| Serial Number | <Copied from the certificate> |
| Certificate Status | “good” when the certificate is unrevoked “revoked” when the certificate is revoked “unknown” when the OCSP Request contained an invalid Serial Number |
| Validity Period | 96 hours, but refreshed every 24 hours |
| Revocation Time | <Date/Time when the certificate was revoked, if applicable> |

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards including the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79:2001 PKI Practices and Policy Framework, and other industry standards related to the operation of CAs.

8.1. Frequency or Circumstances of Assessment

An annual audit is performed by an independent external auditor to assess Certicom's compliancy with the AICPA/CICA WebTrust program for Certification Authorities.

8.2. Identity/Qualifications of Assessor

Certicom’s audits are performed by a public accounting firm that:

- Is a highly reputable accredited accounting firm that is a member of the American Institute of Certified Public Accountants (AICPA)
- Has significant quality assurance mechanisms, including peer review, competency testing, and other measures.

- Abides by and conforms with the applicable standards and best practices as set forth by the relevant standards committees.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology, data centers, personnel controls, and other relevant fields of interest.
- Is knowledgeable about the operations of the CA and has an expertise in public key security technology.

8.3. Assessor's Relationship to Assessed Entity

The Assessor is independent of Certicom and does not have any financial interest or course of dealings with Certicom that could foreseeably create a significant bias in the Assessor's evaluation.

8.4. Topics Covered by Assessment

Topics covered by the annual audit include but are not limited to the following:

- CA business practices disclosure
- Service integrity
- CA environmental controls

8.5. Actions Taken as a Result of Deficiency

If any material noncompliance or deficiencies are discovered during an audit, then Certicom shall create and implement a plan to cure such deficiencies or noncompliance. The plan shall be created by Certicom management with input from the auditing agent. In the event that the deficiency cannot be resolved, Certicom may revoke any certificates affected by deficiency or noncompliance.

8.6. Communication of Results

The results of each audit are reported directly to Certicom management and any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement. Audit results may also be published by Certicom in Certicom's sole and absolute discretion.

9. OTHER BUSINESS AND LEGAL MATTERS

This part of the CPS describes the business matters of Certicom and legal representations, warranties and limitations associated with Certicom digital certificates.

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Certicom charges Subscriber fees for some of the certificate services it offers, including issuance, and renewal. Such fees are detailed on the official Certicom websites (www.Certicom.com). Certicom retains its right to affect changes to such fees.

9.1.2. Certificate Access Fees

Currently, Certicom does not charge a fee for Certificate Access, but reserves the right to establish and charge a reasonable fee for access to its database of certificates. Charges may be incurred for extensive or time consuming searches. Fees for such extensive used are negotiated on an individual basis.

9.1.3. Revocation or Status Information Access Fees

Certicom does not charge fees for the revocation of a certificate or for a Relying Party to check the validity status of a Certicom issued certificate using its OCSP.

9.1.4. Fees for Other Services

Fees for other services offered by Certicom are set either within the individual agreements with the parties or are detailed on the official Certicom websites (www.Certicom.com) depending on the Services required. Fees may be discussed for other services by contacting Certicom at sales@certicom.com.

9.1.5. Refund Policy

Certicom offers a 30-day refund policy. During a 30-day period (beginning when a certificate is first issued), the Subscriber may request a full refund for their certificate. Under such circumstances, the original certificate may be revoked and a refund provided to the applicant. Certicom is not obliged to refund a certificate after the 30-day reissue policy period has expired.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

Certicom maintains errors and omissions insurance coverage.

9.2.2. Other Assets

No Stipulation

9.2.3. Insurance or Warranty Coverage for End-Entities

If Certicom was negligent in issuing a digital certificate that resulted in a loss to a Relying Party, Relying Party may be eligible under Certicom's certificate warranty to receive reimbursement for any damages caused, subject to the limitations of Certicom's insurance policy. Except to the extent of willful misconduct, the liability of Certicom is limited to the negligent issuance of certificates. The cumulative maximum liability of Certicom to all applicants, subscribers and relying parties for each certificate is set forth in the table in Appendix E.

Under Certicom's warranty a covered person may only receive the maximum payment per online transaction listed in Schedule E ("Incident Limit") for which the Covered Person claims there was a breach of the Certicom Warranty (each an "Incident"). If multiple Covered Persons are affiliated as to a common entity, then those multiple Covered Persons collectively are eligible to receive the maximum amount per Incident. Any payments to Covered Persons shall decrease by an amount equal to the sum of such payments the relevant Aggregate Limit available to any party for future payments for any claims relating to that Digital Certificate. For example, if a Digital Certificate carries a Payment Limit of \$10,000 and a per incident limit of \$1,000, then Covered Persons can receive payments in accordance with this warranty for up to \$1,000 per Incident until a total of \$10,000 has been paid in the aggregate for all claims by all parties related to that Digital Certificate. Upon renewal of any Digital Certificate, the total claims paid for such Digital Certificate shall be reset to zero dollars.

Certicom certificates may only be used in connection with data transfer and transactions having a US dollar (US\$) value no greater than the max transaction value associated with the certificate and detailed in the table in Appendix E of this CPS.

Certicom also provides assurance to its network of RAs that operate under Certicom practices and procedures. Certicom warrants the integrity of certificates issued under its own root within the limits of the Certicom insurance policy and in accordance with this CPS.

9.3. Confidentiality of Business Information

Certicom observes applicable rules on the protection of personal data deemed by law or the Certicom privacy policy to be confidential.

9.3.1. Scope of Confidential Information

Certicom keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- Executed Subscriber agreements.
- Certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records and financial audit records.
- External or internal audit trail records and reports, except for WebTrust audit reports that may be published at the discretion of Certicom.
- Contingency plans and disaster recovery plans.
- Internal tracks and records on the operations of Certicom infrastructure, certificate management and enrolment services and data.

9.3.2. Information Not Within the Scope of Confidential Information

Subscribers acknowledge that revocation data of all certificates issued by the Certicom CA is public information. Subscriber application data marked as “Public” in the relevant subscriber agreement and submitted as part of a certificate application is published within an issued digital certificate in accordance with this CPS.

9.3.3. Responsibility to Protect Confidential Information

All personnel in trusted positions handle all information in strict confidence. Certicom is not required to and does not release any confidential information, unless otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom Certicom owes a duty to keep information confidential.
- The party requesting such information.
- A court order, if any.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

Certicom has implemented a privacy policy, which complies with this CPS. The Certicom privacy policy is published at the Certicom repository at www.Certicom.com/repository.

9.4.2. Information Treated as Private

Any information about Subscribers that is not publicly accessible or available through the content of the issued certificate, a CRL, or the OCSP is treated as private information.

9.4.3. Information Not Deemed Private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered private.

9.4.4. Responsibility to Protect Private Information

All Certicom employees receiving private information are responsible to protect such information from compromise and disclosure to third parties. Each party shall use the same degree of care that it exercises with respect to its own information of like importance, but in no event shall the degree of care be less than a reasonable degree of care.

9.4.5. Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, the applicable privacy policy, or by agreement, a party will not use private information without the subject’s express written consent.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

Certicom shall be entitled to disclose any confidential or private information, if Certicom believes, in good faith, that the disclosure is necessary in response to subpoenas and search warrants or if disclosure is necessary in response to a pending legal proceeding.

9.4.7. Other Information Disclosure Circumstances

No Stipulation.

9.5. Intellectual Property Rights

Certicom or its partners or associates own all intellectual property rights associated with its databases, web sites, Certicom digital certificates and any other publication originating from Certicom including this CPS.

9.5.1. Certificates

Certificates are the property of Certicom. Certicom gives permission to reproduce and distribute certificates on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. Certicom reserves the right to revoke the certificate at any time. Private and public keys are property of the subscribers who rightfully issue and hold them. All secret shares (distributed elements) of the Certicom private key remain the property of Certicom.

Subscribers represent and warrant that when submitting to Certicom and using a domain and distinguished name (and all other certificate application information), they do not interfere with or infringe any rights of any third parties in any jurisdiction with respect to the third party's trademarks, service marks, trade names, company names, or any other intellectual property right, and that the subscriber is not seeking to use the domain and distinguished names for any unlawful purpose, including, without limitation, tortious interference with contract or prospective business advantage, unfair competition, injuring the reputation of another, and confusing or misleading a person, whether natural or incorporated.

9.5.2. Copyright

This CPS is copyrighted by Certicom 2008. All rights reserved.

No part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written permission of Certicom. Requests for any other permission to reproduce this Certicom document (as well as requests for copies from Certicom) must be addressed to:

Certicom Corp.
Attn: General Counsel
5520 Explorer Drive, 4th Floor
Mississauga, ON, Canada L4W 5L1

9.5.3. Trademarks

"Certicom" and other terms in this CPS are trademarks of Certicom and may only be used by permission.

9.5.4. Infringement

Although Certicom will provide all reasonable assistance, certificate subscribers shall defend, indemnify, and hold Certicom harmless for any loss or damage resulting from any such interference or infringement and shall be responsible for defending all actions on behalf of Certicom.

9.6. Representations and Warranties

Subscribers, relying parties and any other parties shall not interfere with or reverse engineer the technical implementation of Certicom PKI services, including, but not limited to, the key generation process, the public web site, and the Certicom repositories except as explicitly permitted by this CPS or upon prior written approval of Certicom. Failure to comply with this as a subscriber will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber, and the Subscriber shall pay any Charges payable but that have not yet been paid under this Agreement. Failure to comply with this as a Relying Party will result in the

termination of the agreement with the Relying Party, the removal of permission to use or access the Certicom repository and any Digital Certificate or Service provided by Certicom.

Parties are solely responsible for having exercised independent judgment and employed adequate training in choosing security software, hardware, and encryption/digital signature algorithms, including their respective parameters, procedures, and techniques as well as PKI as a solution to their security requirements.

9.6.1. CA Representations and Warranties

To the extent specified in the relevant sections of the CPS, Certicom promises to:

- Comply with this CPS and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services, including but not limited to the establishment and operation of the Certicom Repository and web site for the operation of PKI services.
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make publicly available.
- Issue digital certificates in accordance with this CPS and fulfill its obligations presented herein.
- Upon receipt of a request from an RA operating within the Certicom network; act promptly to issue a Certicom certificate in accordance with this CPS.
- Publish accepted certificates in accordance with this CPS.
- Provide support to subscribers and relying parties as described in this CPS.
- Revoke certificates according to this CPS.
- Provide for the expiration and renewal of certificates according to this CPS.
- Make available a copy of this CPS and applicable policies to requesting parties.
- Warrant the accuracy of information published on a Qualified Certificate issued pursuant to the requirements of the European Directive 99/93.
- Warrant that the signatory held the private key at the time of issuance of a certificate issued pursuant to the requirements for Qualified Certificates as in the European Directive 99/93.

The subscriber also acknowledges that Certicom has no further obligations under this CPS.

9.6.2. RA Representations and Warranties

A Certicom RA operates under the policies and practices detailed in this CPS and also the associated RA agreement. The RA is bound under contract to:

- Receive applications for Certicom certificates in accordance with this CPS.
- Perform all verification actions prescribed by the Certicom validation procedures and this CPS.
- Receive, verify and relay to Certicom all requests for revocation of a Certicom certificate in accordance with the Certicom revocation procedures and the CPS.
- Act according to relevant Law and regulations.

9.6.3. Subscriber Representations and Warranties

Upon accepting a certificate, the subscriber represents to Certicom and to relying parties that at the time of acceptance and until further notice:

- Digital signatures created using the private key corresponding to the public key included in the certificate is the digital signature of the subscriber and the certificate has been accepted and is properly operational at the time the digital signature is created.
- No unauthorized person has ever had access to the subscriber's private key.
- All representations made by the subscriber to Certicom regarding the information contained in the certificate are accurate and true.
- All information contained in the certificate is accurate and true to the best of the subscriber's knowledge or to the extent that the subscriber had notice of such information whilst the subscriber shall act promptly to notify Certicom of any material inaccuracies in such information.
- The certificate is used exclusively for authorized and legal purposes, consistent with this CPS.
- It will use a Certicom certificate only in conjunction with the entity named in the organization field of a digital certificate (if applicable).
- The subscriber retains control of her private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use.
- The subscriber is an end-user subscriber and not a CA, and will not use the private key corresponding to any public key listed in the certificate for purposes of signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise, unless expressly agreed in writing between subscriber and Certicom.
- The subscriber agrees with the terms and conditions of this CPS and other agreements and policy statements of Certicom.
- The subscriber abides by the laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.
- The subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

Unless otherwise stated in this CPS, subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring adequate knowledge and training on PKI is provided internally.
- To generate their own private / public key pair to be used in association with the certificate request submitted to Certicom.
- Ensure that the public key submitted to Certicom corresponds with the private key used.
- Ensure that the public key submitted to Certicom is the correct one.
- Provide correct and accurate information in its communications with Certicom.
- Alert Certicom if at any stage whilst the certificate is valid, any information originally submitted has changed since it had been submitted to Certicom.
- Generate a new, secure key pair to be used in association with a certificate that it requests from Certicom.

- Read, understand and agree with all terms and conditions in this Certicom CPS and associated policies published in the Certicom Repository at www.Certicom.com/repository.
- Refrain from tampering with a Certicom certificate.
- Use Certicom certificates for legal and authorized purposes in accordance with the suggested usages and practices in this CPS.
- Cease using a Certicom certificate if any information in it becomes misleading, obsolete or invalid.
- Cease using a Certicom certificate if such certificate is expired and remove it from any applications and/or devices it has been installed on.
- Refrain from using the subscriber's private key corresponding to the public key in a Certicom issued certificate to issue end-entity digital certificates or subordinate CAs.
- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a Certicom certificate.
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a Certicom certificate.
- For acts and omissions of partners and agents, they use to generate, retain, escrow, or destroy their private keys.

9.6.4. Relying Party Representations and Warranties

A party relying on a Certicom certificate accepts that in order to reasonably rely on a Certicom certificate they must:

- Minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; the relying party must have reasonably made the effort to acquire sufficient knowledge on using digital certificates and PKI.
- Study the limitations to the usage of digital certificates and be aware through the Relying Party agreement the maximum value of the transactions that can be made using a Certicom digital certificate.
- Read and agree with the terms of the Certicom CPS and relying party agreement.
- Verify a Certicom certificate by examining the information available through Certicom's OCSP.
- Trust a Certicom certificate only if it is valid and has not been revoked or has expired.
- Rely on a Certicom certificate, only as may be reasonable under the circumstances listed in this section and other relevant sections of this CPS.

9.6.5. Representations and Warranties of Other Participants

Partners of the Certicom network shall not undertake any actions that might imperil, put in doubt or reduce the trust associated with the Certicom products and services. Certicom partners shall specifically refrain from seeking partnerships with other root authorities or apply procedures originating from such authorities. Failure to comply with this will result in the termination of the agreement with the relying party, the removal of permission to use or access the Certicom repository and any Digital Certificate or Service provided by Certicom.

9.7. Disclaimers of Warranties

Certicom disclaims all warranties and obligations of any type, including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law.

Except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93 Certicom does not warrant:

- The accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of Certicom except as it may be stated in the relevant product description below in this CPS and in the Certicom insurance policy.
- The accuracy, authenticity, completeness or fitness of any information contained in Certicom Personal certificates class 1, free, trial or demo certificates.
- In addition, shall not incur liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CPS.
- Does not warrant the quality, functions or performance of any software or hardware device.
- Although Certicom is responsible for the revocation of a certificate, it cannot be held liable if it cannot execute it for reasons outside its own control.
- The validity, completeness or availability of directories of certificates issued by a third party (including an agent) unless specifically stated by Certicom.

Notwithstanding limitation warranties under the product section of this CPS, Certicom shall not be responsible for non-verified subscriber information submitted to Certicom, or the Certicom directory or otherwise submitted with the intention to be included in a certificate, except as it may have otherwise been stated in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93.

In no event (except for fraud or willful misconduct) shall Certicom be liable for:

- Any indirect, incidental or consequential damages.
- Any loss of profits.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CPS.
- Any other damages except for those due to reliance, on the information featured on a certificate, on the verified information in a certificate.
- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CPS or the intended use of the ordered certificate as described on the Certicom website or elsewhere.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or on the CPS.
- Any liability that arises from security, usability, integrity of products, including hardware and software a subscriber uses.
- Any liability that arises from compromise of a subscriber's private key.

9.8. Limitations of Liability

In no event (except for fraud or willful misconduct) will the aggregate liability of Certicom to all parties including without any limitation a subscriber, an applicant, a recipient, or a relying party for all digital signatures and transactions related to such certificate exceed the cumulative maximum liability for such certificate as stated in the Certicom insurance plan detailed in section 9.2.3 and Appendix E of this CPS.

Parties relying on a digital certificate must verify a digital signature at all times by checking the validity of a digital certificate through the OCSP services provided by Certicom. Relying parties are alerted that an unverified digital signature cannot be assigned as a valid signature of the subscriber.

Relying on an unverifiable digital signature may result in risks that the relying party, and not Certicom, assumes in whole.

By means of this CPS, Certicom has adequately informed relying parties on the usage and validation of digital signatures through this CPS and other documentation published in its public repository available at www.Certicom.com/repository or by contacting via out of bands means via the contact address as specified in the Document Control section of this CPS.

Certicom reserves its right to refuse to issue a certificate to any party as it sees fit, without incurring any liability or responsibility for any loss or expenses arising out of such refusal. Certicom reserves the right not to disclose reasons for such a refusal.

Certicom does not limit or exclude liability for death or personal injury.

9.9. Indemnities

9.9.1. Subscriber Indemnity to Certicom

By accepting a certificate, the subscriber agrees to indemnify and hold Certicom, as well as its agent(s) and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that Certicom, and the above mentioned parties may incur, that are caused by the use or publication of a certificate, and that arises from:

- Any false or misrepresented data supplied by the subscriber or agent(s).
- Any failure of the subscriber to disclose a material fact, if the misrepresentation or omission was made negligently or with intent to deceive the CA, Certicom, or any person receiving or relying on the certificate.
- Failure to protect the subscriber's confidential data including their private key, or failure to take reasonable precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's confidential data.
- Breaking any laws applicable in his/her country or territory including those related to intellectual property protection, viruses, accessing computer systems etc.

For certificates issued at the request of a subscriber's agent, both the agent and the subscriber shall jointly and severally indemnify Certicom, and its agents and contractors.

9.9.2. Subscriber Indemnity to Relying Parties

Without limiting other subscriber obligations stated in this CPS, subscribers are liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein and have verified one or more digital signatures with the certificate.

9.10. Term and Termination

9.10.1. Term

This CPS and any amendments hereto shall become effective seven days after being published to the Repository and shall remain effective until terminate in accordance with this Section 9.10.

9.10.2. Termination

This CPS and any amendments hereto shall remain effective until replaced with a newer version.

9.10.3. Effect of Termination and Survival

In case of termination of CA operations for any reason whatsoever, Certicom will provide timely notice and transfer of responsibilities to succeeding entities, maintenance of records, and remedies. Before terminating its own CA activities, Certicom will take the following steps, where possible:

- Providing subscribers of valid certificates with ninety (90) days notice of its intention to cease acting as a CA.
- Revoking all certificates that are still un-revoked or un-expired at the end of the ninety (90) day notice period without seeking subscriber's consent.
- Giving timely notice of revocation to each affected subscriber.
- Making reasonable arrangements to preserve its records according to this CPS.
- Reserving its right to provide succession arrangements for the re-issuance of certificates by a successor CA that has all relevant permissions to do so and complies with all necessary rules, while its operation is at least as secure as Certicom's.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

9.11. Individual notices and Communications with Participants

Certicom accepts notices related to this CPS by means of digitally-signed messages or in paper form. Upon receipt of a valid digitally-signed acknowledgment of receipt from Certicom, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or Certicomed mail, postage prepaid, return receipt requested, addressed as follows:

Certicom Corp.
Attn: General Counsel
5520 Explorer Drive, 4th Floor
Mississauga, ON, Canada L4W 5L1

9.12. Amendments

The Certicom Certificate Policy Authority is responsible for determining the suitability of certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

9.12.1. Procedure for Amendment

Amendments to this CPS may be made from time to time by Certicom. Amendments shall either be in the form of an amended form of the CPS or made available as a supplemental document on Certicom's repository. Updates supersede any designated or conflicting provisions of the referenced version of the CPS and shall be indicated through appropriate revision numbers and publication dates. Revisions that are not deemed significant by Certicom (those amendments or additions that have minimal or no impact on Subscribers or Relying Parties), shall be made without notice and without changing the version number of this CPS.

Controls are in place to reasonably ensure that the Certicom CPS is not amended and published without the prior authorization of the Certificate Policy Authority.

9.12.2. Notification Mechanism and Period

Upon the Certificate Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the Certicom repository (available at www.Certicom.com/repository), with seven (7) days notice given of upcoming changes and suitable incremental version numbering used to identify new editions.

9.12.3. Circumstances Under Which OID Must be Changed

If Certicom decides that a change in Certicom's Certificate Policy of Certificate Practices warrants a change in the currently specified OID for a particular Certificate type, then the revised CPS or amendment thereto will contain a revised OID for that type of certificate.

9.13. Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, binding expert's advice, co-operation monitoring and normal expert's advice) parties agree to notify Certicom of the dispute with a view to seek dispute resolution.

9.14. Governing Law

This CPS is governed by, and construed in accordance with the laws of the state of New York, USA. This choice of law is made to ensure uniform interpretation of this CPS, regardless of the place of residence or place of use of Certicom digital certificates or other products and services. New York law applies in all Certicom commercial or contractual relationships in which this CPS may apply or quoted implicitly or explicitly in relation to Certicom products and services where Certicom acts as a provider, supplier, beneficiary receiver or otherwise.

9.15. Compliance with Applicable Law

Each party, including Certicom partners, subscribers and relying parties, irrevocably agrees that the Court of Manhattan District, New York has exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CPS or the provision of Certicom PKI services.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

This CPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances and intended usage of a product or service. In interpreting this CPS, parties shall also take into account the international scope and application of the services and products of Certicom and its international network of Registration Authorities as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CPS.

Appendices and definitions to this CPS are for all purposes an integral and binding part of the CPS. When this CPS conflicts with other rules, guidelines, or contracts, this CPS shall prevail and bind the subscriber and other parties except as to other contracts either:

- Predating the first public release of the present version of this CPS.
- Expressly superseding this CPS for which such contract shall govern as to the parties thereto, and to the extent permitted by law.

9.16.2. Assignment

This CPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties. The rights and obligations detailed in this CPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such

assignment is undertaken consistent with this CPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.

9.16.3. Severability

If any provision of this CPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4. Enforcement

This CPS shall be enforced as a whole, whilst failure by any person to enforce any provision of this CPS shall not be deemed a waiver of future enforcement of that or any other provision. Agreements between Certicom and the parties detailed in this CPS may contain additional provisions governing enforcement and shall be enforced according to the terms and conditions set forth within each respective agreement.

Certicom may seek indemnification and attorneys' fees from any party that violates their individual agreements with Certicom or whose conduct is in violation of this CPS. Except where an express time frame is set forth in this CPS any delay or omission by any party shall not impair or be construed as a waiver of such right, remedy or power.

9.16.5. Force Majeure

Certicom shall not be liable for any breach of its obligations, representations, warranties, or for its failure to perform where such failure or breach is as a result of a Force Majeure Event., including, but not limited to, fire, flood, earthquake, storm, hurricane or other natural disaster), war, invasion, act of foreign enemies, hostilities (whether war is declared or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation, terrorist activities, nationalization, government sanction, blockage, embargo, labor dispute, strike, lockout or interruption or failure of electricity or telephone service or any other system operated by any other party over which Certicom has no control, or other similar causes beyond Certicom's reasonable control where Certicom is without fault or negligence.

9.17. Other Provisions

No Stipulation

APPENDIX A

CA KEYS

| CA Number | Certicom CA Name | Usage | Lifetime | Type/Size |
|-----------|---|---|-------------------|-----------|
| 1.1 | Certicom RSA Public Primary CA | Self-signed root certificate for RSA intermediates | December 31, 2029 | RSA 2048 |
| 2 | Certicom ECC Public Primary CA | Self signed ECC 384-bit root for ECC 256 and 384 bit intermediates | January 18, 2038 | ECC 384 |
| 3 | RESERVED | | | |
| 4 | RESERVED | | | |
| 5 | RESERVED | | | |
| 6 | Certicom RSA Extended Validation SSL CA | Intermediate certificate for all RSA Extended Validation SSL certificates | December 31, 2026 | RSA 2048 |
| 7 | Certicom RSA Secure Server CA | Intermediate certificate for RSA SSL and server certificates | December 31, 2026 | RSA 2048 |
| 8 | Certicom RSA Code and Object CA | Intermediate certificate for code and object signing certificates | December 31, 2026 | RSA 2048 |
| 9 | Certicom RSA Client Authentication and Email CA | Intermediate RSA certificate for email and identity certificates | December 31, 2026 | RSA 2048 |
| 10 | Certicom ECC 256 Extended Validation SSL CA | Intermediate certificate for 256 bit ECC Extended Validation SSL certificates | January 18, 2035 | ECC 256 |
| 11 | Certicom ECC 256 Secure Server CA | Intermediate certificate for 256-bit ECC SSL and server certificates | January 18, 2035 | ECC 256 |
| 12 | Certicom ECC 384 Extended Validation SSL CA | Intermediate certificate for 384-bit ECC Extended Validation SSL certificates | January 18, 2035 | ECC 384 |
| 13 | Certicom ECC 384 Secure Server CA | Intermediate certificate for 384-bit ECC SSL and server certificates | January 18, 2035 | ECC 384 |
| 14 | Certicom ECC 384 Code and Object Signing CA | Intermediate certificate for code and object signing | January 18, 2035 | ECC 384 |
| 15 | Certicom ECC 384 Secure ID CA | Intermediate ECC certificate for email and identity certificates | January 18, 2035 | ECC 384 |
| 16 | RESERVED | | | |
| 17 | RESERVED | | | |
| 18 | RESERVED | | | |

APPENDIX B

CERTIFICATE TYPES

Certicom Certificate offerings may include the following types of certificates:

1. Secure Server SSL/ Suite B 256 SSL / ECC 256 SSL / Suite B 384 SSL / ECC 384 SSL

Professional level high assurance certificates issued to both individuals and organizations for use on websites conducting high value transactions.

2. Wildcard Secure Server SSL Certificates / ECC 256 Wildcard SSL / ECC 384 Wildcard SSL / Suite B 256 Wildcard SSL / Suite B 384 Wildcard SSL

Professional level high assurance certificates issued to both individuals and organizations for use on websites conducting high value transactions to secure multiple sub-domains with a single certificate.

3. Extended Validation SSL / Suite B 256 Extended Validation SSL / Suite B 384 Extended Validation SSL

Professional level certificates issued to websites conducting high value transactions. All EV Certificates are validated and issued only in accordance with the EV Guidelines and covered separately through the EV CPS.

4. Unified Communications Certificates

Low assurance Microsoft-approved SSL certificates that are specifically designed for use with Microsoft Exchange Server 2007, office Communications Server 2007, and Microsoft Live Communications Server.

5. Intranet SSL / ECC 256 Intranet / ECC 384 Intranet

Low assurance certificates used exclusively on internal private IP networks.

6. Code Signing Certificate / ECC Code Signing / ECC 384 Code Signing

Code Signing Certificates are issued to commercial software developers to provide assurance regarding the developer's identity. With a Code Signing Certificate, a digital signature can be appended to the executable code itself, thus providing assurance to recipients that the code or software does indeed come from the signer of the software.

7. Email and Authentication Certificate / Suite B 256 Email and Authentication Certificate / Suite B 384 Email and Authentication Certificate / ECC 256 Email and Authentication Certificate / ECC 384 Email and Authentication Certificate

Email and Authentication Certificates are issued to natural persons that, in combination with an S/MIME compliant email application, allow subscribers to digitally sign email for relying parties, or relying parties to encrypt email for the subscriber.

Email and Authentication Certificates are *non-validated* certificates provided to individuals. Certicom only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by Certicom. The login details are sent via email to the address submitted during the certificate application.

Once logged into the online certificate collection facilities and prior to the installation of the Secure Email Certificate, Certicom validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, Certicom will release the digital certificate to the subscriber.

APPENDIX C
PKI HEIRARCHY

1. Secure Server SSL / Wildcard Secure Server SSL

Certicom RSA Public Primary CA (*serial number = 44 20 79 44 3F B8 89 FD AD 3B FB BA A5 49 9B 51, expiry = 31 December 2029 23:59:59*)

- ↳ Certicom RSA Secure Server CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)
 - ↳ End Entity SSL Certificate (*serial number = x, expiry = 1 month or up to 5 years from issuance*)

Cross signed as follows:

UTN-DATACorp SGC (*serial number = 44 be 0c 8b 50 00 21 b4 11 d3 2a 68 06 a9 ad 69, expiry = 24 June 2019 20:06:40*)

- ↳ Certicom RSA Public Primary CA (*serial number = TBA, expiry = 30 May 2020 10:48:38*)
 - ↳ Certicom RSA Secure Server CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)
 - ↳ End Entity SSL Certificate (*serial number = x, expiry = 1 month or up to 5 years from issuance*)

2. Code Signing Certificate

Certicom RSA Public Primary CA (*serial number = 44 20 79 44 3F B8 89 FD AD 3B FB BA A5 49 9B 51, expiry = 31 December 2029 23:59:59*)

- ↳ Certicom RSA Code and Object Signing CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)
 - ↳ End Entity Code Signing Certificate (*serial number = x, expiry = 1 month or up to 3 years from issuance*)

Cross signed as follows:

UTN-USERFirst-Object (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 2d e0 b3 5f 1b, expiry = 09 July 2019 19:40:36*)

- ↳ Certicom RSA Public Primary CA (*serial number = TBA, expiry = 30 May 2020 10:48:38*)
 - ↳ Certicom RSA Code and Object Signing CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)
 - ↳ End Entity Code Signing Certificate (*serial number = x, expiry = 1 month or up to 3 years from issuance*)

3. Email and Authentication Certificate

Certicom RSA Public Primary CA (*serial number = 44 20 79 44 3F B8 89 FD AD 3B FB BA A5 49 9B 51, expiry = 31 December 2029 23:59:59*)

- ↳ Certicom RSA Client Authentication and Email CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)
 - ↳ End Entity SSL Email Certificate (*serial number = x, expiry = 1 month or up to 3 years from issuance*)

Cross signed as follows:

UTN-USERFirst-Client Authentication and Email (*serial number = 44 be 0c 8b 50 00 24 b4 11 d3 36 25 25 67 c9 89, expiry = 09 July 2019 18:36:58*)

- ↳ Certicom RSA Public Primary CA (*serial number = TBA, expiry = 30 May 2020 10:48:38*)
 - ↳ Certicom RSA Client Authentication and Email CA (*serial number = TBA, expiry = 31 December 2026 23:59:59*)
 - ↳ End Entity Email Certificate (*serial number = x, expiry = 1 month or up to 3 years from issuance*)

4. Suite B 256 SSL / Suite B 256 Wildcard SSL / ECC 256 SSL / ECC 256 Wildcard SSL

Certicom ECC Public Primary CA (*serial number = 45 AC 56 5D 72 EA A2 16 01 90 64 34 0B C1 B3 B2, expiry = 18 January 2038 23:59:59*)

- ↳ Certicom ECC 256 Secure Server CA (*serial number = TBA, expiry = 18 January 2035 23:59:59*)
 - ↳ End Entity SSL Certificate (*serial number = x, expiry = 1 month or up to 5 years from issuance*)

5. Suite B 384 SSL / Suite B 384 Wildcard SSL / ECC 384 SSL / ECC 384 Wildcard SSL

Certicom ECC Public Primary CA (*serial number = 45 AC 56 5D 72 EA A2 16 01 90 64 34 0B C1 B3 B2, expiry = 18 January 2038 23:59:59*)

- ↳ Certicom ECC 384 Secure Server CA (*serial number = TBA, expiry = 18 January 2035 23:59:59*)
 - ↳ End Entity SSL Certificate (*serial number = x, expiry = 1 month or up to 5 years from issuance*)

6. ECC 256 Code Signing / ECC 384 Code Signing

Certicom ECC Public Primary CA (*serial number = 45 AC 56 5D 72 EA A2 16 01 90 64 34 0B C1 B3 B2, expiry = 18 January 2038 23:59:59*)

- ↳ Certicom ECC 384 Code and Object Signing CA (*serial number = TBA, expiry = 18 January 2035 23:59:59*)
 - ↳ End Entity Code Signing Certificate (*serial number = x, expiry = 1 month or up to 3 years from issuance*)

7. Suite B 256 Email and Authentication Certificate / Suite B 384 Email and Authentication Certificate / ECC 256 Email and Authentication Certificate / ECC 384 Email and Authentication Certificate

Certicom ECC Public Primary CA (*serial number = 45 AC 56 5D 72 EA A2 16 01 90 64 34 0B C1 B3 B2, expiry = 18 January 2038 23:59:59*)

- ↳ Certicom ECC 384 Client Authentication and Email CA (*serial number = TBA, expiry = 18 January 2035 23:59:59*)
 - ↳ End Entity Email Certificate (*Serial number = x, expiry = 1 month or up to 3 years from issuance*)

APPENDIX D
CERTIFICATE POLICIES

RSA Organization-Validated (OV) SSL Server Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | sha1WithRSAEncryption |
| Issuer | CN=Certicom RSA Secure Server CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | Trial: 30 days Paid: 1, 2, 3, 4 or 5 years |
| Subject | (Required) CN=<Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | rsaEncryption |
| Size | 512-bit or higher (1024-bit or higher recommended if expiring <= 2010-12-31) (2048-bit or higher recommended if expiring > 2010-12-31) |
| Modulus | <Supplied by customer> |
| Public Exponent | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: E742136315D67D9F8091EFB5B1FF50CA75CD77D7 |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied RSA Public Key> |
| Key Usage | Digital Signature, Key Encipherment |

| | |
|--|--|
| (critical) | |
| Basic Constraints (critical) | Subject Type=End-entity |
| Extended Key Usage (non-critical) | Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomRSA SecureServerCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomRSA SecureServerCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | DNS Name: <Fully-Qualified Domain Name> |
| | |
| Other Information: | |
| Common Name Requirements | For "RSA Standard SSL" Certificates, the CN field may contain an Internet-accessible Domain Name or IP Address, or an Intranet Server Name or IP Address. For "RSA Wildcard SSL" Certificates, the CN field should contain an Internet-accessible Domain Name prefixed with "*". For "RSA Intranet SSL" Certificates, the CN field must contain an Intranet Server Name or IP Address. |

RSA Unified Communications Certificates (UCCs)

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | sha1WithRSAEncryption |
| Issuer | TBA |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) CN=<Primary Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | rsaEncryption |
| Size | 512-bit or higher (1024-bit or higher recommended if expiring <= 2010-12-31) (2048-bit or higher recommended if expiring > 2010-12-31) |
| Modulus | <Supplied by customer> |
| Public Exponent | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: TBA |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied RSA Public Key> |
| Key Usage (critical) | Digital Signature, Key Encipherment |
| Basic Constraints (critical) | Subject Type=End-entity |
| Extended Key Usage (non-critical) | TBA |

| | |
|--|---|
| Certificate Policies (non-critical) | OID: TBA CPS URL: TBA |
| CRL Distribution Points (non-critical) | URI: TBA |
| Authority Info Access (non-critical) | CA Issuer: TBA OCSP: TBA |
| Subject Alternative Name (non-critical) | DNS Name: <Fully-Qualified Domain Name> (this may appear multiple times) |

RSA Code Signing Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | sha1WithRSAEncryption |
| Issuer | CN=Certicom RSA Code and Object Signing CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) CN=<Organization Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | rsaEncryption |
| Size | 512-bit or higher (1024-bit or higher recommended if expiring <= 2010-12-31) (2048-bit or higher recommended if expiring > 2010-12-31) |
| Modulus | <Supplied by customer> |
| Public Exponent | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: 9AF66E0DA4E95D3848046DF109B8FF6CA56438FA |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied RSA Public Key> |
| Key Usage (critical) | Digital Signature |

| | |
|--|---|
| Basic Constraints (critical) | Subject Type=End-entity |
| Extended Key Usage (non-critical) | Code Signing |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomRSACodeandObjectCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomRSACodeandObjectCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: <Contact Email Address> |

RSA Individual Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | sha1WithRSAEncryption |
| Issuer | CN=Certicom RSA Client Authentication and Email CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) E=<Individual's Email Address> (Required) CN=<Individual's Common Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | rsaEncryption |
| Size | 512-bit or higher (1024-bit or higher recommended if expiring <= 2010-12-31) (2048-bit or higher recommended if expiring > 2010-12-31) |
| Modulus | <Supplied by customer> |
| Public Exponent | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: FD20E267B942E9D2A750B18A8953E378608E6457 |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied RSA Public Key> |
| Key Usage (critical) | Digital Signature, Key Encipherment |

| | |
|--|--|
| Basic Constraints (critical) | Subject Type=End-entity |
| Extended Key Usage (non-critical) | Secure Email, Client Authentication |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomRSAClientAuthenticationandEmailCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crl.certicom.com/CerticomRSAClientAuthenticationandEmailCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: <Individual's Email Address> |

Suite B 256 Organization-Validated (OV) SSL Server Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA256 |
| Issuer | CN=Certicom Suite B 256 Secure Server CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2, 3, 4 or 5 years |
| Subject | (Required) CN=<Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp256r1 |
| ECPPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: 994417AD44EEC08791E6DA384C0EF67D6126D66A |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature |
| Basic Constraints (critical) | Subject Type=End-entity |

| | |
|--|---|
| Extended Key Usage (non-critical) | Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC256SecureServerCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC256SecureServerCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | DNS Name: <Fully-Qualified Domain Name> |
| | |
| Other Information: | |
| Common Name Requirements | For "Suite B 256 Standard SSL" Certificates, the CN field may contain an Internet-accessible Domain Name or IP Address, or an Intranet Server Name or IP Address. For "Suite B 256 Wildcard SSL" Certificates, the CN field should contain an Internet-accessible Domain Name prefixed with "*". |

ECC 256 Organization-Validated (OV) SSL Server Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA256 |
| Issuer | CN=Certicom ECC 256 Secure Server CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | Trial: 30 days Intranet: 1, 2, 3, 4 or 5 years |
| Subject | (Required) CN=<Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp256r1 |
| ECPPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: 994417AD44EEC08791E6DA384C0EF67D6126D66A |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature, Key Agreement |
| Basic Constraints | Subject Type=End-entity |

| | |
|--|---|
| (critical) | |
| Extended Key Usage (non-critical) | Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC256SecureServerCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC256SecureServerCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | DNS Name: <Fully-Qualified Domain Name> |
| | |
| Other Information: | |
| Common Name Requirements | For "ECC 256 Intranet SSL" Certificates, the CN field must contain an Intranet Server Name or IP Address. For "ECC 256 Wildcard SSL" Certificates, the CN field should contain an Internet-accessible Domain Name prefixed with "*". |

ECC 256 Code Signing Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Code and Object Signing CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) CN=<Organization Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp256r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: 4DB0A26C1DF18A98671E654DC437C0C16389328C |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature |
| Basic Constraints (critical) | Subject Type=End-entity |
| Extended Key Usage (non-critical) | Code Signing |

| | |
|--|--|
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384CodeandObjectSigningCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384CodeandObjectSigningCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: < <i>Contact Email Address</i> > |

Suite B 256 Individual Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Client Authentication and Email CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) E=<Individual's Email Address> (Required) CN=<Individual's Common Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp256r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: D7271ADBF6E704C0F83DE78BD07906EBAAA08B3E |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature OR Key Agreement |
| Basic Constraints (critical) | Subject Type=End-entity |

| | |
|--|---|
| Extended Key Usage (non-critical) | Secure Email, Client Authentication (<i>when Key Usage = Digital Signature</i>) OR Secure Email (<i>when Key Usage = Key Agreement</i>) |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384SecureIDCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384SecureIDCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: < <i>Individual's Email Address</i> > |

ECC 256 Individual Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Client Authentication and Email CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) E=<Individual's Email Address> (Required) CN=<Individual's Common Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp256r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: D7271ADBF6E704C0F83DE78BD07906EBAAA08B3E |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature, Key Agreement |
| Basic Constraints (critical) | Subject Type=End-entity |

| | |
|--|---|
| Extended Key Usage (non-critical) | Secure Email, Client Authentication |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384SecureIDCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384SecureIDCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: < <i>Individual's Email Address</i> > |

Suite B 384 Organization-Validated (OV) SSL Server Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom Suite B 384 Secure Server CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2, 3, 4 or 5 years |
| Subject | (Required) CN=<Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp384r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: C0F10A0E9C165FDF653285E832874F217C3E4192 |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature |
| Basic Constraints (critical) | Subject Type=End-entity |

| | |
|--|---|
| Extended Key Usage (non-critical) | Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384SecureServerCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384SecureServerCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | DNS Name: <Fully-Qualified Domain Name> |
| | |
| Other Information: | |
| Common Name Requirements | For "ECC 384 Standard SSL" Certificates, the CN field may contain an Internet-accessible Domain Name or IP Address, or an Intranet Server Name or IP Address. For "ECC 384 Wildcard SSL" Certificates, the CN field should contain an Internet-accessible Domain Name prefixed with "*". |

ECC 384 Organization-Validated (OV) SSL Server Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Secure Server CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | Trial: 30 days Intranet: 1, 2, 3, 4 or 5 years |
| Subject | (Required) CN=<Domain Name> (Optional) OU=<Product Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp384r1 |
| ECPPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: C0F10A0E9C165FDF653285E832874F217C3E4192 |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature, Key Agreement |
| Basic Constraints | Subject Type=End-entity |

| | |
|--|---|
| (critical) | |
| Extended Key Usage (non-critical) | Server Authentication, Client Authentication, Microsoft SGC, Netscape SGC |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384SecureServerCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384SecureServerCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | DNS Name: <Fully-Qualified Domain Name> |
| | |
| Other Information: | |
| Common Name Requirements | For "ECC 384 Intranet SSL" Certificates, the CN field must contain an Intranet Server Name or IP Address. For "Suite B 384 Wildcard SSL" Certificates, the CN field should contain an Internet-accessible Domain Name prefixed with "*". |

ECC 384 Code Signing Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Code and Object Signing CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) CN=<Organization Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp384r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: 4DB0A26C1DF18A98671E654DC437C0C16389328C |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature |
| Basic Constraints (critical) | Subject Type=End-entity |
| Extended Key Usage (non-critical) | Code Signing |

| | |
|--|--|
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384CodeandObjectSigningCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384CodeandObjectSigningCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: < <i>Contact Email Address</i> > |

Suite B 384 Individual Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Client Authentication and Email CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) E=<Individual's Email Address> (Required) CN=<Individual's Common Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp384r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: D7271ADBF6E704C0F83DE78BD07906EBAAA08B3E |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature OR Key Agreement |
| Basic Constraints (critical) | Subject Type=End-entity |

| | |
|--|---|
| Extended Key Usage (non-critical) | Secure Email, Client Authentication (<i>when Key Usage = Digital Signature</i>) OR Secure Email (<i>when Key Usage = Key Agreement</i>) |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384SecureIDCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384SecureIDCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: < <i>Individual's Email Address</i> > |

ECC 384 Individual Certificates

| Field | Content |
|--|---|
| Version | v3 |
| Serial Number | <a 16-byte integer> |
| Signature Algorithm | ecdsa-with-SHA384 |
| Issuer | CN=Certicom ECC 384 Client Authentication and Email CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US |
| Validity Period | 1, 2 or 3 years |
| Subject | (Required) E=<Individual's Email Address> (Required) CN=<Individual's Common Name> (Optional) OU=<Organizational Unit Name> (Required) O=<Organization Name> (Required) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Required) L=<Locality Name> (Required) ST=<State or Province Name> (Required) PostalCode=<Postal Code> (Required) C=<Country Name> |
| Public Key: | |
| Algorithm Identifier | id-ecPublicKey |
| ECPParameters (namedCurve) | secp384r1 |
| ECPoint | <Supplied by customer> |
| Extensions: | |
| Authority Key Identifier (non-critical) | Key ID: D7271ADBF6E704C0F83DE78BD07906EBAAA08B3E |
| Subject Key Identifier (non-critical) | <SHA-1 hash of customer-supplied ECC Public Key> |
| Key Usage (critical) | Digital Signature, Key Agreement |
| Basic Constraints (critical) | Subject Type=End-entity |

| | |
|--|---|
| Extended Key Usage (non-critical) | Secure Email, Client Authentication |
| Certificate Policies (non-critical) | OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps |
| CRL Distribution Points (non-critical) | URI: http://crl.certicom.com/CerticomECC384SecureIDCA.crl |
| Authority Info Access (non-critical) | CA Issuer: http://crt.certicom.com/CerticomECC384SecureIDCA.crt OCSP: http://ocsp.certicom.com |
| Subject Alternative Name (non-critical) | Email: < <i>Individual's Email Address</i> > |

APPENDIX E
INSURANCE LIMITS

| <u>Certicom Certificate Type</u> | <u>Max Transaction Value</u> | <u>Cumulative Max Liability</u> |
|--------------------------------------|------------------------------|---------------------------------|
| Secure Server SSL | \$10,000 | \$500,000 |
| Wildcard Secure Server SSL | \$10,000 | \$500,000 |
| Extended Validation SSL | \$10,000 | \$250,000 |
| Unified Communications | \$0 | \$0 |
| Intranet SSL | \$0 | \$0 |
| Code Signing | \$0 | \$50,000 |
| Email and Authentication | \$0 | \$0 |
| Suite B 256 SSL | \$10,000 | \$500,000 |
| Suite B 256 Wildcard SSL | \$10,000 | \$500,000 |
| Suite B 256 Extended Validation SSL | \$10,000 | \$250,000 |
| Suite B 256 Email and Authentication | \$0 | \$0 |
| ECC 256 SSL | \$10,000 | \$500,000 |
| ECC 256 Wildcard SSL | \$10,000 | \$500,000 |
| ECC 256 Secure Server Trial | \$0 | \$0 |
| ECC 256 Intranet SSL | \$0 | \$0 |
| ECC 256 Code Signing | \$0 | \$50,000 |
| ECC 256 Email and Authentication | \$0 | \$0 |
| Suite B 384 SSL | \$10,000 | \$500,000 |
| Suite B 384 Wildcard SSL | \$10,000 | \$500,000 |
| Suite B 384 Extended Validation SSL | \$10,000 | \$250,000 |
| ECC 384 SSL | \$10,000 | \$500,000 |
| ECC 384 Wildcard SSL | \$10,000 | \$500,000 |
| ECC 384 Secure Server Trial | \$0 | \$0 |
| ECC 384 Intranet SSL | \$0 | \$0 |
| ECC 384 Code Signing | \$0 | \$50,000 |
| ECC 384 Email and Authentication | \$0 | \$0 |