Certificate Policy
For
Access Certificates for Electronic Services

U.S. General Services Administration

Office of Governmentwide Policy

September 3, 1999

TABLE OF CONTENTS

SECTION **PAGE**

SECTION 1 INTRODUCTION 1

1.1 OVERVIEW 1
1.2 POLICY IDENTIFICATION 1
1.3 COMMUNITY AND APPLICABILITY 2
1.3.1 Certification Authorities (CAs) 2
1.3.2 Registration Authorities (RAs) 2
1.3.3 Certificate Manufacturing Authorities (CMAs) 2
1.3.4 Repositories 2
1.3.5 End Entities 3
1.3.6 Policy Authority 3
1.3.7 Applicability and Applications 3
1.4 CONTACT DETAILS 4
1.4.1 Policy Administration Organization 4
1.4.2 Contact Person 4
1.4.3 Person Determining ACES CPS Suitability for the Policy 4

SECTION 2 GENERAL PROVISIONS 6

2.1 OBLIGATIONS 6
2.1.1 Authorized CA Obligations 6
2.1.2 RA Obligations 6
2.1.3 CMA Obligations 6
2.1.4 Repository Obligations 6
2.1.5 Subscriber Obligations 7
2.1.6 Qualified Relying Party Obligations 7
2.1.7 Policy Authority Obligations 7
2.2 LIABILITIES 8
2.2.1 Authorized CA Liability 8
2.2.2 RA, CMA, and Repository Liability 8
2.3 FINANCIAL RESPONSIBILITY 8
2.3.1 Indemnification by Relying Parties 8
2.3.2 Fiduciary Relationships 8
2.3.3 Administrative Processes 8
2.4 INTERPRETATION AND ENFORCEMENT 8
2.4.1 Governing Law 8
2.4.2 Severability, Survival, Merger, Notice 8
2.4.3 Dispute Resolution Procedures 8
2.5 FEES 9
2.5.1 Certificate Issuance, Renewal, Suspension, and Revocation Fees 9
2.5.2 Certificate Access Fees 9

2.5.3 Revocation Status Information Access Fees (Certificate Validation Services) 9
2.5.4 Fees for Other Services such as Policy Information....9
2.5.5 Refund Policy....9
2.6 PUBLICATION AND REPOSITORY....10
2.6.1 Publication of Information....10
2.6.2 Frequency of Publication....10
2.6.3 Access Controls....10
2.6.4 Repositories....10
2.7 QUALITY ASSURANCE INSPECTION AND REVIEW....10
2.7.1 Frequency of Certification Authority Compliance Review....10
2.7.2 Identity/Qualifications of Reviewer....10
2.7.3 Auditor's Relationship to Audited Party....11
2.7.4 Topics Covered by Quality Assurance Inspection and Review....11
2.7.5 Actions Taken as a Result of Deficiency....11
2.7.6 Communication of Results....11
2.8 CONFIDENTIALITY....12
2.8.1 Types of Information to Be Kept Confidential....12
2.8.2 Types of Information Not Considered Confidential....12
2.8.3 Disclosure of Certificate Revocation/Suspension Information....12
2.8.4 Release to Law Enforcement Officials....12
2.8.5 Release as Part of Civil Discover....13
2.8.6 Disclosure upon Owner's Request....13
2.8.7 Other Information Release Circumstances....13
2.9 INTELLECTUAL PROPERTY RIGHTS....13

SECTION 3 IDENTIFICATION AND AUTHENTICATION....14

3.1 INITIAL REGISTRATION....14
3.1.1 Types of Names....14
3.1.2 Name Meanings....14
3.1.3 Rules for Interpreting Various Name Forms....14
3.1.4 Name Uniqueness....14
3.1.5 Name Claim Dispute Resolution Procedures....14
3.1.6 Recognition, Authentication, and Role of Trademarks....14
3.1.7 Verification of Possession of Key Pair....14
3.1.8 Authentication of Sponsoring Organization Identity....14
3.1.9 Authentication of Individual Identity....15
3.2 ROUTINE REKEY (RENEWAL)....16
3.3 REKEY AFTER REVOCATION....16
3.4 REVOCATION REQUEST....16

SECTION 4 OPERATIONAL REQUIREMENTS....17

4.1 CERTIFICATE APPLICATION....17
4.2 CERTIFICATE ISSUANCE....17
4.3 CERTIFICATE ACCEPTANCE....17

4.4 CERTIFICATE SUSPENSION AND REVOCATION 18
4.4.1 Who Can Request Revocation 18
4.4.2 Circumstances for Revocation 18
4.4.3 Procedure for Revocation Request 18
4.4.4 Revocation Request Grace Period 18
4.4.5 Circumstances for Suspension 19
4.4.6 Who Can Request Suspension 19
4.4.7 Procedure for Suspension Request 19
4.4.8 Limits on Suspension Period 19
4.4.9 CRL Issuance Frequency 19
4.4.10 CRL Checking Requirements 19
4.4.11 Online Revocation/Status Checking Availability 19
4.4.12 Online Revocation Checking Requirements 19
4.4.13 Other Forms of Revocation Advertisements Available 19
4.4.14 Checking Requirements for Other Forms of Revocation Advertisements 19
4.4.15 Special Requirements re Key Compromise 20
4.5 COMPUTER SECURITY AUDIT PROCEDURES 20
4.6 RECORDS ARCHIVAL 20
4.6.1 Types of Events Recorded 20
4.6.2 Retention Period for Archive 20
4.6.3 Protection of Archive 20
4.7 KEY CHANGEOVER 20
4.8 COMPROMISE AND DISASTER RECOVERY 20
4.8.1 Computing Resources, Software, and/or Data are Corrupted 20
4.8.2 Authorized CA Public Key Is Revoked 20
4.8.3 Authorized CA Private Key Is Compromised (*Key Compromise Plan*) 20
4.8.4 Secure Facility after a Natural or Other Disaster (*Disaster Recovery Plan*) 21
4.9 AUTHORIZED CA CESSATION OF SERVICES 21
4.10 CUSTOMER SERVICE CENTER 21

SECTION 5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 22

5.1 PHYSICAL SECURITY CONTROLS 22
5.2 PROCEDURAL CONTROLS 22
5.2.1 Trusted Roles 22
5.2.2 Number of Persons Required Per Task 22
5.2.3 Identification and Authentication for Each Role 22
5.3 PERSONNEL SECURITY CONTROLS 22

SECTION 6 TECHNICAL SECURITY CONTROLS 23

6.1 KEY PAIR GENERATION AND INSTALLATION 23
6.1.1 Key Pair Generation 23
6.1.2 Private Key Delivery to Entity 23
6.1.3 Subscriber Public Key Delivery to Authorized CA 23

6.1.4 Authorized CA Public Key Delivery to Users 23
6.1.5 Key Sizes 23
6.2 AUTHORIZED CA PRIVATE KEY PROTECTION 23
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 23
6.3.1 Public Key Archival 23
6.3.2 Usage Periods for the Public and Private Keys (*Key Replacement*) 24
6.4 ACTIVATION DATA 24
6.5 COMPUTER SECURITY CONTROLS 24
6.7 NETWORK SECURITY CONTROLS 24
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 24

SECTION 7 CERTIFICATE AND CRL PROFILES 25

7.1 CERTIFICATE PROFILE 25
7.2 CRL PROFILE 25

SECTION 8 POLICY ADMINISTRATION 26

8.1 POLICY CHANGE PROCEDURES 26
8.1.1 List of Items 26
8.1.2 Comment Period 26
8.2 PUBLICATION AND NOTIFICATION PROCEDURES 26
8.3 CPS APPROVAL PROCEDURES 26

GLOSSARY 27

SECTION 1

INTRODUCTION

1.1 OVERVIEW

The development of a National Information Infrastructure (NII) centered on the use of the Internet promises:

(a) To improve citizens' access to government services and information;
(b) To facilitate the flow of government information within and among the different branches and agencies; and
(c) To reduce government operating costs through the implementation of electronic business processes.

Fulfilling that promise requires the use of digital signatures to ensure the identity of the senders of electronic messages and the integrity of the messages themselves. This requires the use of public key cryptography and public key certificates to bind a person's public key to his/her/its identity. Because public key certificates and the systems that support their use are major prerequisites for greater federal use of the Internet, it is important to begin by facilitating their implementation. In support of this goal, GSA's Office of Governmentwide Policy (OGP) and Federal Technology Service (FTS) have initiated projects aimed at providing commercial public key certificate services to the public (referred to as "Access Certificates for Electronic Services" or "ACES"). GSA will enter into contracts ("GSA ACES contracts") with service providers to provide the services presented in this policy and the Request for Proposals issued by GSA on January 4, 1999..

This Certificate Policy ("Policy") describes (1) roles, responsibilities, and relationships among the Certification Authorities, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Qualified Relying Parties, and Policy Authority (referred to collectively as "Program Participants") authorized to participate in the public key infrastructure described by this Policy, (2) the primary obligations and operational responsibilities of the Program Participants, and (3) the rules and requirements for the issuance, acquisition, management, and use of ACES Certificates to verify digital signatures.

This Certificate Policy provides a high level description of the policies and operation of the ACES Program. Specific detailed requirements for the services outlined in the document may be found in the GSA ACES contracts. In the event that there is any inconsistency between the GSA ACES contracts and this policy, the GSA ACES contract provisions take precedence

1.2 POLICY IDENTIFICATION

This Policy is registered with the Computer Security Objects Register (CSOR) at the National Institute of Standards and Technology (NIST), and has been assigned the following object identifiers (OIDs) for the ACES Certificates defined in this Policy.

Authorized CA ACES Certificates: { 2 16 840 1 101 3 2 1 1 1 }
Identity ACES Certificates: { 2 16 840 1 101 3 2 1 1 2 }
Business Representative ACES Certificates: { 2 16 840 1 101 3 2 1 1 3 }

Qualified Relying Party Application ACES Certificates: { 2 16 840 1 101 3 2 1 1 4 }

All ACES Certificates issued under this Policy shall reference this Policy by including the appropriate OID for this Policy in the *Certificate Policies* field of the ACES Certificate. The foregoing OIDs may not be used except as specifically authorized by this Policy.

CSOR information is available from 1) http://csrc.nist.gov/csor/csor.html, and 2) csor@nist.gov.

1.3 COMMUNITY AND APPLICABILITY

This Policy describes a bounded public key infrastructure. It describes the rights and obligations of persons and entities authorized under this Policy to fulfill any of the following roles: Certificate Service Provider roles, End Entity roles, and Policy Authority role. Certificate Service Provider roles are Certification Authority, Registration Authority, Certificate Manufacturing Authority, and Repository. End Entity roles are Subscriber and Relying Party. Requirements for persons and entities authorized to fulfill any of these roles are in this Section. A general description of each of these roles and their responsibilities is set forth in Section 2 of this Policy.

1.3.1 Certification Authorities (CAs)

A CA may issue certificates that identify this Policy ("ACES Certificates") only if such CA first qualifies as an "Authorized CA" by:

(a) entering into an appropriate GSA ACES Contract;
(b) documenting the specific practices and procedures it will implement to satisfy the requirements of this Policy in a certificate practice statement ("ACES CPS"); and
(c) successfully completing GSA's ACES Security Certification and Accreditation.

1.3.2 Registration Authorities (RAs)

Each Authorized CA shall perform the role and functions of the Registration Authority (RA). An Authorized CA may subcontract Registration Authority functions to third party RAs who agree to be bound by this Policy, provided that each such subcontractor is approved in advance by the GSA, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its GSA ACES Contract. The only exception is when the Government, pursuant to agreement between GSA, Qualified Relying Parties, and the Authorized CAs provides defined portions of the RA role and function.

1.3.3 Certificate Manufacturing Authorities (CMAs)

Each Authorized CA shall perform the role and functions of the Certificate Manufacturing Authority (CMA). An Authorized CA may subcontract CMA functions to third party CMAs who agree to be bound by this Policy, provided that each such subcontractor is approved in advance by GSA, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its GSA ACES Contract.

1.3.4 Repositories

Each Authorized CA shall perform the role and functions of the Repository. An Authorized CA may subcontract performance of the Repository functions to a third party Repository who agrees to be bound by this Policy, provided that such subcontractor is approved in advance by GSA, but the Authorized CA remains responsible for the performance of those services in accordance with this Policy and the requirements of its GSA ACES Contract.

1.3.5 End Entities

1.3.5.1 Subscribers

An Authorized CA may issue ACES Certificates to the following classes of Subscribers:

(a) Members of the general public ("Unaffiliated Individuals");
(b) Individuals authorized to act on behalf of business entities (i.e., Sponsoring Organizations) recognized by the Authorized CA, such as employees, officers, and agents of a Sponsoring Organization ("Business Representatives"); and
(c) Qualified Relying Parties that choose to use ACES.

1.3.5.2 Qualified Relying Parties

Persons and entities authorized to accept and rely upon ACES Certificates for purposes of verifying digital signatures on electronic records and messages are those eligible Federal agencies and entities that enter into a GSA ACES Agreement (i.e., Memorandum of Understanding)to accept ACES Certificates and agree to be bound by the terms of this Policy ("Qualified Relying Parties"). Eligible Federal agencies and entities include all Federal agencies, authorized Federal contractors, agency-sponsored universities and laboratories, other organizations, and, if authorized by law, state, local, and tribal governments. All organizations listed in GSA Order ADM 4800.2D (as updated) are also eligible. The Government has the right to add authorized users in these categories at any time during the term of this Policy.

1.3.6 Policy Authority

The GSA serves as the Policy Authority and is responsible for organizing and administering the ACES Policy and ACES Contract (s).

1.3.7 Applicability and Applications

1.3.7.1 Purpose

Subscribers and Authorized CAs may use ACES Certificates to authenticate Subscribers to Qualified Relying Party applications for individual and/or business purposes, and for authentication of Qualified Relying Party applications. The following table summarizes the functional uses of ACES Certificates:

ACES Certificate Type	Subscriber	Use of Certificate
Unaffiliated Individual	Unaffiliated Individual	To enable an Unaffiliated Individual to authenticate itself to Qualified Relying Parties electronically for information and transactions and to verify digitally signed documents/transactions

ACES Certificate Type	Subscriber	Use of Certificate
Business Representative	Business Representative authorized to act on behalf of a Sponsoring Organization	To enable a Business Representative to authenticate itself to Qualified Relying Parties to conduct business-related activities electronically and to verify digitally signed documents/transactions
Qualified Relying Party Application	Qualified Relying Party	To enable a Qualified Relying Party to authenticate itself to Unaffiliated Individuals, Business Representatives, and Authorized CAs and to verify digitally signed documents/transactions

1.3.7.2 Suitable Applications

Qualified Relying Parties shall specify in their GSA ACES Agreement those applications that they have determined to be suitable for the use of ACES Certificates. Examples of suitable applications include, but are not limited to:

(a) Personal or restricted information retrieval;
(b) Updating personal or restricted information;
(c) Filings with government agencies;
(d) Application processes, such as applying for government licenses, student loans, government benefits, etc.; and
(e) Financial transactions with government agencies.

1.4 CONTACT DETAILS

1.4.1 Policy Administration Organization

GSA, as the Policy Authority and Contract Authority administers this Policy:

General Services Administration
18th and F Streets, NW
Washington, DC 20405-0007

1.4.2 Contact Person

Attn.: Office of Electronic Commerce
Phone: (202) 501-7092
e-mail address: aces.policy@gsa.gov

1.4.3 Person Determining ACES CPS Suitability for the Policy

Attn: Federal Computer Acquisition Center
Phone: (781) 860-7138

e-mail address: aces.contract@gsa.gov

SECTION 2

GENERAL PROVISIONS

2.1 OBLIGATIONS

This Section provides a general description of the roles and responsibilities of the ACES Program Participants operating under this Policy: Authorized CAs, Registration Authorities (RAs), Certificate Manufacturing Authorities (CMAs), Repositories, Subscribers, Qualified Relying Parties, and the Policy Authority. Additional obligations are set forth in other provisions of this Policy, the GSA ACES Contracts, the GSA ACES Agreements with Qualified Relying Parties, and the Subscriber Agreements.

2.1.1 Authorized CA Obligations

This Policy describes the responsibilities on each Authorized CA that issue ACES Certificates (and all of its subcontractor RAs, CMAs, and Repositories) by virtue of its GSA ACES Contract, and governs its performance with respect to all ACES Certificates it issues.

Each Authorized CA is responsible for all aspects of the issuance and management of ACES Certificates, including the application/enrollment process; the identification verification and authentication process; the certificate manufacturing process; dissemination and activation of the certificate; publication of the certificate (if required); renewal, suspension, revocation, and replacement of the certificate; verification of certificate status upon request; and ensuring that all aspects of the Authorized CA Services and Authorized CA operations and infrastructure related to ACES Certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. The only exception is when the Government, pursuant to agreement between GSA, Qualified Relying Parties, and the Authorized CAs provides defined portions of the RA role and function.

2.1.2 RA Obligations

A Registration Authority (RA) is responsible for the applicant registration, certificate application, and authentication of identity functions for Unaffiliated Individuals, Business Representatives, and Qualified Relying Parties. An RA may also be responsible for handling suspension and revocation requests, and for aspects of Subscriber education.

2.1.3 CMA Obligations

A Certificate Manufacturing Authority (CMA) is responsible for the functions of manufacturing, issuance, suspension, and revocation of ACES Certificates.

2.1.4 Repository Obligations

A Repository is responsible for maintaining a secure system for storing and retrieving ACES Certificates, a current copy of this Policy, and other information relevant to ACES Certificates, and for providing information regarding the status of ACES Certificates as valid or invalid that can be determined by a Qualified Relying Party.

2.1.5 Subscriber Obligations

The responsibilities of each applicant for an ACES Certificate are to:

- provide complete and accurate responses to all requests for information made by the Authorized CA (or an authorized RA) during the applicant registration, certificate application, and authentication of identity processes;

- generate a key pair using a reasonably trustworthy system, and take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of the private key;

- upon issuance of an ACES Certificate naming the applicant as the Subscriber, review the ACES Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the ACES Certificate;

- use the ACES Certificate and the corresponding private key exclusively for purposes authorized by this Policy and only in a manner consistent with this Policy; and

- instruct the issuing Authorized CA (or an authorized RA) to revoke the ACES Certificate promptly upon any actual or suspected loss, disclosure, or other compromise of the private key, or, in the case of a Business Representative ACES Certificate, whenever the Subscriber is no longer affiliated with the Sponsoring Organization.

2.1.6 Qualified Relying Party Obligations

This Policy is binding on each Qualified Relying Party by virtue of its GSA ACES Agreement, and governs its performance with respect to its application for, use of, and reliance on ACES Certificates.

(a) Acceptance of Certificates. Each Qualified Relying Party will validate ACES Certificates issued by all Authorized CAs;

(b) Certificate Validation. Each Qualified Relying Party will validate every ACES Certificate it requests and receives with the Authorized CA that issued the certificate; and

(c) Reliance. A Qualified Relying Party may rely on an valid ACES Certificate for purposes of verifying the digital signature only if:

- The ACES Certificate was used and relied upon to authenticate a Subscriber's digital signature for an application bound by this Policy;
- Prior to reliance, the Qualified Relying Party (1) verified the digital signature by reference to the public key in the ACES Certificate, and (2) checked the status of the ACES Certificate by generating an online status request to the issuing Authorized CA, and a check of the certificate's status indicated that the certificate was valid; and
- The reliance was reasonable and in good faith in light of all the circumstances known to the Qualified Relying Party at the time of reliance.

2.1.7 Policy Authority Obligations

The Policy Authority is responsible for the terms of this Policy and contract administration.

2.2 LIABILITIES

Nothing in this Policy shall create, alter, or eliminate any other obligation, responsibility, or liability that may be imposed on any Program Participant by virtue of any contract or obligation that is otherwise determined by applicable law.

2.2.1 Authorized CA Liability

Tort liability for transactions involving services under the ACES contract(s) is governed by the Federal Tort Claims Act. The Government Contractor defense is available to the ACES Contractor to the extent that the contractor has met the standard of care spelled out by the contractor's requirements.

2.2.2 RA, CMA, and Repository Liability

See 2.2.1.

2.3 FINANCIAL RESPONSIBILITY

No stipulation.

2.3.1 Indemnification by Relying Parties

No stipulation.

2.3.2 Fiduciary Relationships

No stipulation.

2.3.3 Administrative Processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing Law

The laws of the United States shall govern the enforceability, construction, interpretation, and validity of this Policy.

2.4.2 Severability, Survival, Merger, Notice

No stipulation.

2.4.3 Dispute Resolution Procedures

In the event of any dispute or disagreement between two or more of the Program Participants

("Disputing Parties") arising out of or relating to this Policy or ACES Contracts, CPS, or Agreements, the Disputing Parties shall use their best efforts to settle the dispute or disagreement through negotiations in good faith following notice from one Disputing Party to the other(s). If the Disputing Parties cannot reach a mutually agreeable resolution of the dispute or disagreement within sixty (60) days following the date of such notice, then the Disputing Parties may present the dispute to the GSA ACES Contract Officer for resolution.

Any contract dispute between Authorized CAs and GSA shall be handled under the terms and conditions of the ACES contract.

2.5 FEES

2.5.1 Certificate Issuance, Renewal, Suspension, and Revocation Fees

The Authorized CA will issue, renew, suspend, and revoke Unaffiliated Individual ACES Certificates at no cost to individual members of the general public.

2.5.2 Certificate Access Fees

The Authorized CA shall not impose any certificate access fees on Subscribers with respect to its own ACES Certificate(s) or the status of such ACES Certificate(s).

2.5.3 Revocation Status Information Access Fees (Certificate Validation Services)

Fees may be assessed for certificate validation services as set forth in the Authorized CA's GSA ACES Contract.

2.5.4 Fees for Other Services such as Policy Information

The authorized CA shall not impose fees for access to policy information.

2.5.5 Refund Policy

No stipulation.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of Information

Each Authorized CA shall operate a secure online Repository available to Subscribers and Qualified Relying Parties that shall contain: (1) all ACES Certificates issued by the Authorized CA that have been accepted by the Subscriber; (2) a Certificate Revocation List ("CRL") or online certificate status information; (3) the Authorized CA's ACES Certificate for its signing key; (4) past and current versions of the Authorized CA's ACES CPS; (5) a copy of this Policy; and (6) other relevant information about ACES Certificates.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published promptly after such information is available to the Authorized CA. The Subscriber will publish ACES Certificates issued by the Authorized CA promptly upon acceptance of such ACES Certificates. Information relating to the status of an ACES Certificate will be published in accordance with the Authorized CA's GSA ACES Contract.

2.6.3 Access Controls

The Authorized CA shall not impose any access controls on this Policy, the Authorized CA's ACES Certificate for its signing key, and past and current versions of the Authorized CA's ACES CPS. The Authorized CA may impose access controls on ACES Certificates and ACES Certificate status information, in accordance with provisions of the Authorized CA's GSA ACES Contract.

2.6.4 Repositories

See Section 2.6.1.

2.7 QUALITY ASSURANCE INSPECTION AND REVIEW

The Authorized CA, including all of its RA, CMA, and Repository subcontractor(s), shall undergo ACES Security Certification and Accreditation ("C&A") as a condition of obtaining and retaining approval to operate as an Authorized CA under this Policy and GSA ACES Contract. The purpose of the C&A process shall be to verify that the CA has in place and follows a system that assures that the quality of its Authorized CA Services conforms to the requirements of this Policy and the GSA ACES Contract.

2.7.1 Frequency of Certification Authority Compliance Review

Certification authorities shall undergo C&A from GSA prior to initial approval as an Authorized CA, to demonstrate compliance with this Policy, their ACES CPS, and GSA ACES contracts. Re-certification will be required every 12 months or at any time that a significant change in their operations is made, whichever occurs first, to demonstrate continuing compliance.

2.7.2 Identity/Qualifications of Reviewer

An independent security audit firm acceptable to GSA that is qualified to perform a security audit on a CA shall conduct the C&A process.

2.7.3 Auditor's Relationship to Audited Party

No stipulation.

2.7.4 Topics Covered by Quality Assurance Inspection and Review

The C&A quality assurance inspection shall be conducted pursuant to the guidance provided in the American Institute of Certified Public Accountants' (AICPA's) Statement on Auditing Standards (SAS) Number 70, *Reports on the Processing of Transactions by Service Organizations*, as follows:

(a) Authorized CAs that have been in operation for one year or less shall undergo a SAS 70 Type One Review – A Report of Policies and Procedures in Operation; the Authorized CA must receive an unqualified opinion; and

(b) Authorized CAs that have been in operation for longer than one year shall undergo a SAS 70 Type Two Review – A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

2.7.5 Actions Taken as a Result of Deficiency

GSA will address any identified deficiencies with the ACES CA.

2.7.6 Communication of Results

Results of the C&A review will be made available to GSA, to be used in determining the CA's suitability for initial and continued performance as an Authorized CA.

2.8 CONFIDENTIALITY

2.8.1 Types of Information to Be Kept Confidential

Subscriber Information. The Authorized CA shall protect the confidentiality of personal information regarding Subscribers that is collected during the applicant registration, ACES Certificate application, authentication, and certificate status checking processes in accordance with the *Privacy Act of 1974*, and *Appendix III to Office of Management and Budget (OMB) Circular A-130*. Such information shall be used only for the purpose of providing Authorized CA Services and carrying out the provisions of this Policy and the GSA ACES Contract, and shall not be disclosed in any manner to any person without the prior consent of the Subscriber, unless otherwise required by law, except as may be necessary for the performance of the Authorized CA Services in accordance with the ACES Contract. In addition, personal information submitted by Subscribers:

(a) must be made available by the Authorized CA to the Subscriber involved following an appropriate request by such Subscriber;

(b) must be subject to correction and/or revision by such Subscriber;

(c) must be protected by the Authorized CA in a manner designed to ensure the data's integrity; and

(d) cannot be used or disclosed by the Authorized CA for purposes other than the direct operational support of ACES unless such use is authorized by the Subscriber involved.

Under no circumstances shall the Authorized CA (or any authorized RA, CMA, or Repository) have access to the private keys of any Subscriber to whom it issues an ACES Certificate.

GSA and Other Government Information. The Authorized CA shall take reasonable steps to protect the confidentiality of any GSA, Qualified Relying Party, or other Government information provided to the Authorized CA. Such information shall be used only for the purpose of providing Authorized CA Services and carrying out the provisions of this Policy and GSA ACES Contract, and shall not be disclosed in any manner to any person except as may be necessary for the performance of the Authorized CA Services in accordance with the GSA ACES contract.

2.8.2 Types of Information Not Considered Confidential

Information contained on a single ACES Certificate or related status information shall not be considered confidential, when the information is used in accordance with the purposes of providing Authorized CA Services and carrying out the provisions of this Policy and the GSA ACES contract and in accordance with the *Privacy Act of 1974*, and *Appendix III to Office of Management and Budget (OMB) Circular A-130*. However, a compilation of such information shall be treated as confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

See 2.8.2.

2.8.4 Release to Law Enforcement Officials

No stipulation.

2.8.5 Release as Part of Civil Discover

No stipulation.

2.8.6 Disclosure upon Owner's Request

See 2.8.1.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in an ACES Certificate. This Policy is the property of GSA. "Access Certificates for Electronic Services," "ACES", and the ACES OIDs are the property of GSA, which may be used only by Authorized CAs in accordance with the provisions of this Policy and the Authorized CA's GSA ACES Contract. Any other use of the above without the express written permission of GSA is expressly prohibited.

SECTION 3

IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

Subject to the requirements noted below, applications for ACES Certificates may be communicated from the applicant to an Authorized CA or an authorized RA, and authorizations to issue ACES Certificates may be communicated from an authorized RA to an Authorized CA, (1) electronically, provided that all communication is secure, (2) by U.S. Postal Service first-class mail, or (3) in person.

3.1.1 Types of Names

The subject name used for ACES Certificate applicants shall be the Subscriber's authenticated common name.

3.1.2 Name Meanings

In the case of Unaffiliated Individuals, the authenticated common name should be a combination of first name and/or initials and surname. In the case of Business Representatives, the authenticated common name should be the combination of first name and/or initials and surname and reflect the legal name of the organization and/or unit. In the case of Qualified Relying Parties, the common name should be the authenticated name of the Qualified Relying Party application.

3.1.3 Rules for Interpreting Various Name Forms

No stipulation.

3.1.4 Name Uniqueness

Name uniqueness is not required.

3.1.5 Name Claim Dispute Resolution Procedures

No stipulation.

3.1.6 Recognition, Authentication, and Role of Trademarks

Not applicable.

3.1.7 Verification of Possession of Key Pair

The Authorized CA shall verify that the applicant possesses the private key corresponding to the public key submitted with the application.

3.1.8 Authentication of Sponsoring Organization Identity

If the applicant is requesting a Business Representative ACES Certificate, in addition to verifying the applicant's individual identity and authorization to represent the Sponsoring Organization, the Authorized CA shall also verify that the Sponsoring Organization exists and conducts business at the address listed in the ACES Certificate application. In conducting its review and investigation, the

Authorized CA shall provide validation of information concerning the Sponsoring Organization, including legal company name, type of entity, year of formation, names of directors and officers, address (number and street, city, ZIP code), and telephone number.

3.1.9 Authentication of Individual Identity

3.1.9.1 Unaffiliated Individual ACES Certificates

Unaffiliated Individuals may be authenticated through an electronically submitted application or by personal presence. In accordance with the ACES Contract requirements the Authorized CA shall verify all of the following identification information supplied by the applicant: first name, middle initial, and last name, , current address (number and street, city, ZIP code), and telephone number. Subscriber identification must be confirmed via a GSA-approved identity-proofing process that incorporates the following factors:

a) Submission by the applicant of at least three individual identity items, which must be verified through reference to multiple independent data sources along with cross-checks for consistency, for example:

- Currently-valid credit card number;
- Alien Registration Number;
- Passport number;
- Current employer name, address (number and street, city, ZIP code), and telephone number;
- Currently valid state-issued driver's license number or state-issued identification card number; and
- Social Security Number
- date of birth
- place of birth.

b) At least one of the above data sources must be based on an antecedent in-person or the equivalent identity verification process;

c) The use of an out-of-band notification process that is linked to the requesting individual's physical U.S. postal mail address; or equivalent, and

Verification that the information contained in the Certificate Application is correct.

3.1.9.2 Business Representative ACES Certificates

If the applicant is requesting a certificate for a Business Representative, the Authorized CA shall verify:

(a) that the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association; and

(b) the Sponsoring Organization's identity as specified in section 3.1.8.

3.1.9.3 Qualified Relying Party ACES Certificates

If the applicant is requesting a Qualified Relying Party ACES Certificate, The Authorized CA shall verify:

(a) that the applicant is authorized to act on behalf of the Qualified Relying Party;

and

(b) the affiliation of the ACES Certificate applicant with the Qualified Relying Party.

3.2 ROUTINE REKEY (RENEWAL)

In accordance with the ACES contract the Authorized CA shall accept ACES Certificate renewal requests from their Subscribers within 90 days from the scheduled end of the operational period (expiration date) of the ACES Certificate, provided the ACES Certificate is not revoked, suspended, or expired. ACES Certificates shall be renewed in 2-year increments. In the event that subject information and/or the key pair change, the Authorized CA shall require the Subscriber to request a new ACES Certificate. The Authorized CA shall renew ACES Certificates issued to Qualified Relying Parties only after completing successful identity proofing verification in accordance with the requirements for identity proofing specified in Section 3.1.9.1

3.3 REKEY AFTER REVOCATION

In accordance with the ACES Contract suspended, revoked, or expired ACES Certificates shall not be renewed. Applicants without a valid ACES Certificate shall be re-authenticated by the Authorized CA or an authorized RA through a new ACES Certificate application, just as with an initial applicant registration, and shall be issued a new ACES Certificate.

3.4 REVOCATION REQUEST

In accordance with the ACES contract an ACES Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the ACES Certificate's associated key pair. The identity of the person submitting a revocation request in any other manner shall be authenticated in accordance with Section 3. Revocation requests authenticated on the basis of the ACES Certificate's associated key pair shall always be accepted as valid. Other revocation request authentication mechanisms may be used as well, including a request in writing signed by the Subscriber and sent via U.S. Postal Service first-class mail, or equivalent. These authentication mechanisms must balance the need to prevent unauthorized revocation requests against the need to quickly revoke certificates.

SECTION 4

OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Application Initiation. The following persons may initiate the ACES Certificate application process:

Potential Subscriber	Authorized Initiator
Unaffiliated Individual	Potential Subscriber only
Business Representative	Sponsoring Organization; or potential Subscriber
Qualified Relying Party	Duly authorized representative of the Qualified Relying Party

(a) Application Form. An applicant for an ACES Certificate shall complete an ACES Certificate application and provide requested information in a form prescribed by the Authorized CA and this Policy.

(b) Applicant Education and Disclosure. At the time of ACES Certificate application, the Authorized CA shall inform applicants of the advantages and potential risks associated with using ACES Certificates to access Qualified Relying Parties electronically and provide information to Subscribers regarding the use of private keys and digital signatures created with such keys, and Subscriber obligations.

4.2 CERTIFICATE ISSUANCE

Upon successful completion of the Subscriber identification and authentication process in accordance with the GSA ACES contract, the Authorized CA shall create the requested ACES Certificate, notify the applicant thereof, and make the ACES Certificate available to the applicant. The Authorized CA shall use an out-of-band notification process linked to the ACES Certificate applicant's physical U.S. postal mail address, or equivalent, and deliver the ACES Certificate only to the Subscriber. Upon issuance of an ACES Certificate, the Authorized CA warrants to all Program Participants that:

(a) The Authorized CA has issued, and will manage, the ACES Certificate in accordance with the requirements in this Policy;
(b) The Authorized CA has complied with all requirements in this Policy when identifying the Subscriber and issuing the ACES Certificate;
(c) There are no misrepresentations of fact in the ACES Certificate known to the Authorized CA and the Authorized CA has verified the information in the ACES Certificate;
(d) Information provided by the Subscriber for inclusion in the ACES Certificate has been accurately transcribed to the ACES Certificate; and
(e) The ACES Certificate meets the material requirements of this Policy.

4.3 CERTIFICATE ACCEPTANCE

As described in the ACES contract a condition to issuing the ACES Certificate, the Subscriber shall indicate acceptance or rejection of the ACES Certificate to the Authorized CA and acknowledge the Subscriber obligations under Section 2.1.5. By accepting the ACES Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the ACES

Certificate are true.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Who Can Request Revocation

The only persons permitted to request revocation of an ACES Certificate issued pursuant to this Policy are the Subscriber, the Sponsoring Organization (where applicable), and the issuing Authorized CA.

4.4.2 Circumstances for Revocation

4.4.2.1 Permissive Revocation

As described in the ACES contract a Subscriber may request revocation of his/her/its ACES Certificate at any time for any reason. A Sponsoring Organization may request revocation of an ACES Certificate issued to its Business Representative at any time for any reason.

4.4.2.2 Required Revocation

A Subscriber, or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of an ACES Certificate:

(a) When any of the information on the ACES Certificate changes or becomes obsolete;

(b) When the private key, or the media holding the private key, associated with the ACES Certificate is, or is suspected of having been, compromised;

(c) When the individual named as a Business Representative no longer represents, or is no longer affiliated with, the Sponsoring Organization;

(d) If an Authorized CA learns, or reasonably suspects, that the Subscriber's private key has been compromised; or

(e) If the issuing Authorized CA determines that the ACES Certificate was not properly issued in accordance with this Policy and/or the Authorized CA's ACES CPS.

Failure to do is at the subscriber's risk.

4.4.3 Procedure for Revocation Request

As described in the ACES Contract an ACES Certificate revocation request should be promptly communicated to the issuing Authorized CA, either directly or through the RA authorized to accept such notices on behalf of the Authorized CA. An ACES Certificate revocation request may be communicated electronically if it is digitally signed with the private key of the Subscriber or the Sponsoring Organization (where applicable). Alternatively, the Subscriber, or Sponsoring Organization (where applicable), may request revocation by contacting the issuing Authorized CA or its RA in person and providing adequate proof of identification in accordance with this Policy.

4.4.4 Revocation Request Grace Period

No stipulation.

4.4.5 Circumstances for Suspension

A certificate may be placed in suspended status following an unsigned request for certificate revocation, pending authentication of the revocation request.

4.4.6 Who Can Request Suspension

See Section 4.4.1.

4.4.7 Procedure for Suspension Request

See Section 4.4.3.

4.4.8 Limits on Suspension Period

No Stipulation.

4.4.9 CRL Issuance Frequency

Not applicable.

4.4.10 CRL Checking Requirements

Not applicable.

4.4.11 Online Revocation/Status Checking Availability

Authorized CAs shall validate online, near-real-time the status of the ACES Certificate indicated in an ACES Certificate validation request message.

4.4.12 Online Revocation Checking Requirements

Each Qualified Relying Party will validate every ACES Certificate it receives in connection with a transaction.

4.4.13 Other Forms of Revocation Advertisements Available

No Stipulation.

4.4.14 Checking Requirements for Other Forms of Revocation Advertisements

No Stipulation.

4.4.15 Special Requirements re Key Compromise

No Stipulation.

4.5 COMPUTER SECURITY AUDIT PROCEDURES

All significant security events on each Authorized CA's system shall be automatically recorded in audit trail files. Such files shall be securely archived in accordance with Section 4.6.

4.6 RECORDS ARCHIVAL

4.6.1 Types of Events Recorded

The data and files which must be archived by or on behalf of each Authorized CA include ACES certificate application information, certificate issuance and transaction data.

4.6.2 Retention Period for Archive

No stipulation.

4.6.3 Protection of Archive

The archive media must be protected at least at the level required to maintain and protect all Subscriber information and data from disclosure, modification, or destruction.

4.7 KEY CHANGEOVER

No stipulation.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing Resources, Software, and/or Data are Corrupted

No stipulation.

4.8.2 Authorized CA Public Key Is Revoked

No stipulation.

4.8.3 Authorized CA Private Key Is Compromised (*Key Compromise Plan*)

As required by the ACES contract each Authorized CA must have in place an appropriate key compromise plan that addresses the procedures that will be followed in the event of a compromise of the private signing key used by an Authorized CA to issue ACES Certificates. Such plan shall include

procedures for revoking all affected ACES Certificates and promptly notifying all Subscribers and all Qualified Relying Parties.

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

An Authorized CA must have in place an appropriate disaster recovery/business resumption plan. Such plan shall be detailed within the Authorized CA's ACES CPS. or other appropriate documentation made available to and approved by GSA.

4.9 AUTHORIZED CA CESSATION OF SERVICES

In the event that an Authorized CA ceases operation or its participation as an Authorized CA in ACES or is otherwise terminated,

(a) all Subscribers, sponsoring organizations, and Qualified Relying Parties must be promptly notified of the cessation;
(b) all ACES Certificates issued by an Authorized CA shall be revoked no later than the time of cessation; and
(c) all current and archived ACES identity proofing, certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data shall be transferred to GSA within 24 hours of cessation and in accordance with this Policy. Transferred data shall not include any non-ACES data.

4.10 CUSTOMER SERVICE CENTER

As described in the ACES contract each Authorized CA shall implement and maintain an ACES Customer Service Center to provide assistance and services to Subscribers and Qualified Relying Parties, and a system for receiving, recording, responding to, and reporting ACES problems within its own organization and for reporting such problems to GSA.

SECTION 5

PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

Each Authorized CA, and all associated RAs, CMAs, and Repositories, shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing Authorized CA Services. Access to such hardware and software shall be limited to those personnel performing in a Trusted Role as described in Section 5.2.1.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

No Stipulation.

5.2.2 Number of Persons Required Per Task

An Authorized CA shall utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.3 PERSONNEL SECURITY CONTROLS

Each Authorized CA and its RA, CMA, and Repository subcontractors shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this Policy.

SECTION 6

TECHNICAL SECURITY CONTROLS

The Authorized CA, and all authorized RAs, CMAs, and Repositories, shall implement appropriate technical security controls in accordance with protection under 15 U.S.C. 278g(3) and (4), the responding regulations relating to protection of these systems as set forth in Appendix III (*Security of Federal Automated Information Resources)* to Office of Management and Budget (OMB) Circular Number A-130 (*Management of Federal Information Resources),* and the GSA ACES Contract.

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

(a) General. Key pairs for all Program Participants must be generated in such a way that the private key is not known by other than the authorized user of the key pair. Authorized CA, RA, CMA, and Qualified Relying Party application keys must be generated in hardware tokens. Key pairs for Subscribers can be generated in either hardware or software.

6.1.2 Private Key Delivery to Entity

See Section 6.1.1.

6.1.3 Subscriber Public Key Delivery to Authorized CA

As part of the ACES Certificate application process, the Subscriber's public key must be transferred to the Registration Authority or Authorized CA in a way that ensures that (1) it has not been changed during transit; (2) the sender possesses the private key that corresponds to the transferred public key; and (3) the sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 Authorized CA Public Key Delivery to Users

No stipulation.

6.1.5 Key Sizes

Key sizes and algorithms shall be specified in the GSA ACES contract and applicable certificate profile.

6.2 AUTHORIZED CA PRIVATE KEY PROTECTION

Each Authorized CA, RA, and CMA shall each protect its private key(s) in accordance with the provisions of the GSA ACES contract and this Policy.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

No stipulation.

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

Subscriber key pair must be replaced in accordance with the validity periods specified in the applicable certificate profile.

6.3.3 Restrictions on CA's Private Key Use

The private key used by Authorized CAs for issuing ACES Certificates shall be used only for signing such Certificates and, optionally, CRLs or other validation services responses.

A private key held by a CMA, if any, and used for purposes of manufacturing ACES Certificates is considered the Authorized CA's signing key, is held by the CMA as a fiduciary, and shall not be used by the CMA for any other purposes, except as agreed by GSA and the Authorized CA.[1] Any other private key used by a CMA for purposes associated with its CMA function shall not be used for any other purpose without the express permission of the CA.

The private key used by each RA employed by an Authorized CA in connection with the issuance of ACES Certificates shall be used only for communications relating to the approval or revocation of such certificates.

6.4 ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

No stipulation.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No stipulation.

SECTION 7

CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

ACES Certificates shall contain public keys used for authenticating the sender of an electronic message and verifying the integrity of such messages, i.e., public keys used for digital signature verification.

The Authorized CA shall create and maintain ACES Certificates that conform to the ITU-T Recommendation X.509, “The Directory: Authentication Framework,” June 1997.
All ACES Certificates must include a reference to an OID for this Policy within the appropriate field, and contain the required certificate fields according to the Authorized CA's CPS and the GSA ACES Contract:

7.2 CRL PROFILE

No stipulation.

SECTION 8

POLICY ADMINISTRATION

8.1 POLICY CHANGE PROCEDURES

8.1.1 List of Items

Notice of all proposed changes to this Policy under consideration by GSA that may materially affect users of this Policy (other than editorial or typographical corrections, changes to the contact details, or other minor changes) will be provided to Authorized CAs and Qualified Relying Parties, and will be posted on the GSA World Wide Website.. The Authorized CA shall post notice of such proposed changes and shall advise their Subscribers of such proposed changes.

8.1.2 Comment Period

Any interested person may file comments with GSA within 45 days of original notice. If the proposed change is modified as a result of such comments, a new notice of the modified proposed change shall be given.

8.2 PUBLICATION AND NOTIFICATION PROCEDURES

A copy of this Policy is available in electronic form on the Internet at *http://csrc.nist.gov/csor/csor.html*, or http://gsa.gov/aces, and via e-mail from the Policy Authority. The Authorized CA shall also make available copies of this Policy both online and in hard copy form.

8.3 CPS APPROVAL PROCEDURES

GSA must approve an Authorized CA's ACES CPS prior to its incorporation into the Authorized CA's operational procedures.

GLOSSARY

ACES. Access Certificates for Electronic Services. This is a project of GSA's Office of Governmentwide Policy (OGP) and Federal Technology Service (FTS) that is aimed at providing commercial public key certificate services to the American public.

ACES Certificates. Certificates issued by an Authorized CA in accordance with this Policy, which certificates reference, this Policy by inclusion of the ACES OID.

ACES CPS. An ACES CPS is a certification practice statement of the practices that an Authorized CA employs in issuing, suspending, and revoking ACES Certificates and providing access to the same.

Agency. A term used to identify all federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, and, when authorized by law or regulation, state, local, and tribal Governments.

Agency Applications. See "Qualified Relying Party."

Authenticate. Relates to a situation where one party has presented an identity and claims to be that identity. Authentication enables another party to gain confidence that the claim is legitimate.

Authorized CA. A certification authority that has been authorized by GSA to issue ACES Certificates and provide Authorized CA Services under the Policy.

Authorized CA Services. The services relating to ACES Certificates to be provided by Authorized CAs under this Policy (See section 2.1.1).

CA. See "certification authority."

Certificate. A data record that, at a minimum: (a) identifies the Authorized CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a public key that corresponds to a private key under the control of the Subscriber; (d) identifies its operational period; and (e) contains an ACES Certificate serial number and is digitally signed by the Authorized CA issuing it. As used in this Policy, the term of "Certificate" refers to certificates that expressly reference the OID of this Policy in the "*CertificatePolicies*" field of an X.509 v.3 certificate.

Certificate Manufacturing Authority (CMA). An entity that is responsible for the manufacturing and delivery of ACES Certificates signed by an Authorized CA, but is not responsible for identification and authentication of certificate subjects (i.e., a CMA is an entity that is delegated or outsourced the task of actually manufacturing the Certificate on behalf of an Authorized CA).

Certification Authority. A certification authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. See "Authorized CA."

Certification Practice Statement. A "certification practice statement" is a statement of the practices that a certification authority employs in issuing, suspending, revoking, and renewing certificates and providing access to same, in accordance with specific requirements (i.e., requirements specified in this Policy, requirements specified in a contract for services).

CMA. See "Certificate Manufacturing Authority".

CPS. See "Certification Practice Statement".

CRL. Certificate Revocation List

CSOR. Computer Security Objects Register operated by the National Institute of Standards and Technology.

Digital Signature. A digital signature is a string of bits associated with a collection of data (e.g., a file, document, message, transaction); this string of bits can only be generated by the holder of a private key, but can be verified by anyone with access to the corresponding public key. Note that some algorithms include additional steps (e.g., one-way hashes, timestamps) in this basic process.

DSA. Digital Signature Algorithm

DSS. Digital Signature Standard

FAR. Federal Acquisition Regulation

FED-STD. Federal Standard

FIPS. Federal Information Processing Standards. These are Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance to agency waiver procedures.

FIPS PUB Federal Information Processing Standards Publication

Government. Federal Government and authorized agencies and entities.

GSA. The United States General Services Administration.

GSA ACES Contract.

GSA ACES Operating Agreement.

IETF. See "Internet Engineering Task Force."

Internet Engineering Task Force (IETF). The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.

ISO. International Standards Organization

ITU. International Telecommunications Union

ITU-T. International Telecommunications Union – Telecommunications Sector

ITU-TSS. International Telecommunications Union – Telecommunications Systems Sector

Key Changeover (CA). The procedure used by a Authorities to replace its own private key (e.g., due to compromise) and replace current valid certificates issued with old key.

Key pair. Means two mathematically related keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.

Mutual Authentication. Parties at both ends of a communication activity authenticate each other (see authentication).

NIST. National Institute of Standards and Technology.

Object Identifier. An object identifier is a specially formatted number that is registered with an internationally-recognized standards organization.

OID. See "Object Identifier".

Operating Rules. See "ACES Operating Rules".

Operational Period of an ACES Certificate. The operational period of an ACES Certificate is the period of its validity. It would typically begin on the date the certificate is issued (or such later date as specified in the certificate), and ends on the date and time it expires as noted in the certificate or is earlier revoked or suspended.

Out-of-band. Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party using U.S. Postal mail to communicate with another party where current communication is online communication).

PKI. Public Key Infrastructure

PIN. Personal Identification Number

Policy. Means this Certificate Policy.

Policy Authority. The entity specified in Section 1.4 (the General Services Administration).

Private Key. The key of a key pair used to create a digital signature. This key must be kept a secret.

Program Participants. Collectively, the Authorized CAs, Registration Authorities, Certificate Manufacturing Authorities, Repositories, Subscribers, Qualified Relying Parties, and Policy Authority authorized to participate in the public key infrastructure defined by this Policy.

Public Key. The key of a key pair used to verify a digital signature. The public key is made freely available to anyone who will receive digitally signed messages from the holder of the key pair. The public key is usually provided via an ACES Certificate issued by an Authorized CA and is often obtained

by accessing a repository. A public key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding private key.

Qualified Relying Party. A recipient of a digitally signed message who is authorized by this Policy to rely on an ACES Certificate to verify the digital signature on the message.

RA. See "Registration Authority."

Registration Authority. An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an Authorized CA).

Repository. A database containing information and data relating to certificates, and an Authorized CA, as specified in this Policy.

Responsible Individual. A trustworthy person designated by a Sponsoring Organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor.

Revoke a Certificate. Means to prematurely end the operational period of a Certificate from a specified time forward.

Sponsoring Organization. A business entity, government agency, or other organization with which a Business Representative is affiliated (e.g., as an employee, agent, member, user of a service, business partner, customer, etc.).

Subject. A person whose public key is certified in an ACES Certificate. Also referred to as a "Subscriber".

Subscriber. A Subscriber is a person who (1) is the subject named or identified in an ACES Certificate issued to such person and (2) holds a private key that corresponds to a public key listed in that certificate, and (3) the person to whom digitally signed messages verified by reference to such certificate are to be attributed. See "subject."

Suspend a Certificate. Means to temporarily suspend the operational period of a Certificate for a specified time period or from a specified time forward.

Trustworthy System. Means computer hardware, software, and procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

U.S.C. United States Code

Valid Certificate. Means an ACES Certificate that (1) an Authorized CA has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, an ACES Certificate is not "valid" until it is both issued by an Authorized CA and has been accepted by the Subscriber.

WWW. World Wide Web