



The CPA. Never Underestimate The Value.SM



Chartered
Accountants
of Canada

Comptables
agr es
du Canada

AICPA/CICA

WebTrust^{SM/TM}

Program for

Certification Authorities

August 25, 2000

Version 1.0

Copyright © 2000 by

American Institute of Certified Public Accountants, Inc. and

Canadian Institute of Chartered Accountants.

Permission is granted to make copies of this work provided that such copies are for personal, intraorganizational, or educational use only and are not sold or disseminated and provided further that each copy bears the following credit line: "Copyright © 2000 by American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. Used with permission."

This document is available on AICPA Online at <http://www.aicpa.org> and on CICA Online at <http://www.cica.ca>.

FOREWORD TO GUIDE

This document, *AICPA/CICA WebTrust Program for Certification Authorities Version 1.0*, was developed with initial and on-going input from a variety of Public Key Infrastructure (PKI) practitioners including both providers and users of PKI. Through the exposure draft process, the AICPA/CICA Electronic Commerce Assurance Task Force received a number of meaningful comments from a variety of international organizations including Certification Authority service providers, users, public accounting firms, national accounting societies, and government entities. Since the Exposure Draft was published in February 2000, the Task Force members have considered each of the comments received. The comments received ranged from general to detailed and are regarded as valuable input. The majority of the comments received resulted in some change to the document, although some did not as they were, in some cases, deemed to be beyond the intended scope of the current document. The Task Force expects the *WebTrust Program for Certification Authorities* to evolve as public key infrastructure technology evolves and looks forward to working with interested parties in the evolution of the *WebTrust Program for Certification Authorities*.

PREFACE

USE OF THE TERM CA IN THIS DOCUMENT

This document describes the **AICPA/CICA *WebTrust Program for Certification Authorities*** which has been developed as part of the WebTrust family of services.

Within the electronic commerce (e-commerce) industry, companies whose main business is to act as certification authorities, or companies who have established a certification authority function to support an e-commerce business activity, are routinely referred to as *CAs* or as performing a *CA function*.

In Canada (and certain other jurisdictions), public accounting professionals, including the practitioner's who are licensed to perform WebTrust assurance services, carry the title of Chartered Accountants, also routinely referred to as *CAs* or as being a *CA*.

In order to avoid confusion in this document, the term *Practitioner*, which is used widely in accounting literature, is used to identify a Chartered Accountant or Certified Public Accountant (CPA), or the equivalent, who is licensed to perform WebTrust assurance services.

The term CA is never used beyond this preface to refer to a Chartered Accountant.

The term CA is only used to denote a Certification Authority (CA) or to refer to the

Certification Authority function (CA function).

The term practitioner is used to denote a properly qualified and licensed Certified Public Accountant (U.S.) or Chartered Accountant (Cdn.).

COMMITTEE AND TASK FORCE MEMBERS

AICPA

Assurance Services Executive Committee

Robert L. Bunting, Chair

Gari Fails

Ted Horne

Everett C. Johnson, Jr.

John Lainhart

George Lewis

Edward F. Rockman

Susan C. Rucker

J. W. Mike Starr

Wendy E. Visconty

Darwin Voltin

CICA

Assurance Services Development Board

John W. Beech, Chair

Douglas C. Isaac

Marilyn Kuntz

Doug McPhie

Steven E. Salterio

David W. Stephen

Doug Timmins

Keith S. Vance

Neal West

Staff Contacts:

Alan Anderson,

Senior Vice President, Technical Services

Anthony J. Pugliese

Director, Assurance Services

AICPA / CICA Electronic Commerce

Staff Contacts:

Cairine M. Wilson,

Vice President, Innovation

Gregory P. Shields,

Director

Assurance Services Development

Staff Contacts:

Assurance Services Task Force

Bryan Walker, CICA

Principal, Assurance Services Development

Everett C. Johnson, Jr., Chair

Sheryl Martin, AICPA

WebTrust Team Leader

Bruce R. Barrick

Jerry R. Devault

Joseph G. Griffin

Christopher J. Leach, Vice Chair

Patrick J. Moriarty

William Powers

Kerry L. Shackelford

Donald E. Sheehy

Christian R. Stormer

Alfred F. Van Ranst, Jr.

Contents
INTRODUCTION

OVERVIEW

Electronic Commerce

Public Key Infrastructure

Digital Signature

Differences Between Encryption Key Pairs and Signing Key Pairs

Certification Authority

Registration Authority

Certification Practice Statements and Certificate Policies

The Difference Between Licensed and Nonlicensed CAs

The Hierarchical and Cross-Certified CA Models

Business Issues Associated With CAs

THE WEBTRUST SEAL OF ASSURANCE FOR CERTIFICATION

AUTHORITIES

Practitioners as Assurance Professionals

Obtaining and Keeping the WebTrust Seal of Assurance for Certification

Authorities

The Assurance Process

Comparison of a WebTrust for Certification Authorities Examination With Service

Auditor Reports

Obtaining the WebTrust Seal

Keeping the WebTrust Seal

The Seal Management Process

WebTrust Seal Authentication

WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES

WebTrust for Certification Authorities Principles

Principle 1: CA Business Practices Disclosure

Principle 2: Service Integrity

Principle 3: CA Environmental Controls

WebTrust for Certification Authorities Criteria

WebTrust Principles and Criteria for Certification Authorities

Appendix A - Illustrative Examples of Practitioner Reports

Appendix B - Illustrative Examples of Management's Assertion

Appendix C - Illustrative Examples of Management's Representation

Appendix D - WebTrust for Certification Authorities Criteria and ANSI X9.79

Cross-Reference

**Appendix E - Comparison of CICA Section 5900, AICPA SAS No. 70, and
AICPA/CICA WebTrust for Certification Authorities Reviews and Reports
Covering the Business Activities of Certification Authority Organizations**

**Appendix F - Practitioner Policies and Guidance for WebTrust for Certification
Authority Engagements**

Suitable Trust Services Criteria and Illustrations for WebTrust for Certification Authorities

Introduction

This document provides a framework for licensed WebTrust[®] practitioners to assess the adequacy and effectiveness of the controls employed by certification authorities (CAs).¹ The importance of this function will continue to increase as the need for third-party authentication to provide assurance with respect to electronic commerce (e-commerce) business activities increases. As a result of the technical nature of the activities involved in securing e-commerce transactions, this document also provides a brief overview of public key infrastructure (PKI) using cryptography, trusted third-party concepts, and their increasing use in e-commerce.

Confidentiality, authentication, integrity, and nonrepudiation are the four most important ingredients required for trust in e-commerce transactions. The emerging response to these requirements is the implementation of PKI technology. PKI uses digital certificates and asymmetric cryptography to address these requirements. PKI provides a means for relying parties (that is, recipients of certificates who act in reliance on those certificates, digital signatures verified using those certificates, or both) to know that another individual's or entity's public key actually belongs to that individual or entity. CA organizations and CA functions have been established to address this need.

Public key cryptography is critical to establishing secure e-commerce. However, it has to be coupled with other secure protocols to provide a comprehensive security solution.

1 Within the electronic commerce (e-commerce) industry, companies whose main business is to act as certification authorities, or companies who have established a certification authority function to support an e-commerce business activity, are routinely referred to as *CAs* or as performing a *CA function*.

In Canada and certain other jurisdictions, public accounting professionals, including the practitioners who are licensed to perform WebTrust[®] assurance services, carry the title of *chartered accountants*, also routinely referred to as *CAs* or as being a *CA*.

To avoid confusion in this document, the term *practitioner*, which is used widely in accounting literature, is used to identify a certified public accountant (CPA) or the equivalent, who is licensed to perform WebTrust assurance services.

In summary:

The term *CA* is *never* used in this standard to refer to a chartered accountant.

The term *CA* is used *only* to denote a certification authority (CA) or to refer to the certification authority function (CA function).

The term *practitioner* is used to denote a properly qualified and licensed certified public accountant.

Several cryptographic protocols require digital certificates (in effect, electronic credentials) issued by an independent, trusted third party (the CA) to authenticate the transaction. CAs have assumed an increasingly important role in secure e-commerce. Although there is a large body of existing national, international, and proprietary standards and guidelines for the use of cryptography, the management of digital certificates, and the policies and practices of CAs, these standards have not been applied or implemented uniformly.

To increase consumer confidence in the Internet as a vehicle for conducting e-commerce and in the application of PKI technology, the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed a set of principles and criteria for CAs, the WebTrust Principles and Criteria for Certification Authorities. Public accounting firms and practitioners who are specifically licensed by the AICPA can provide assurance services to evaluate and test whether the services provided by a particular CA meet these principles and criteria. The posting of the WebTrust seal of assurance for CAs is a symbolic representation of a practitioner's unqualified report. Similar to the WebTrust seal for business-to-consumer e-commerce, the seal of assurance also indicates that those who use the digital certificates (and certificate status information) issued by the CA, subscribers, and relying parties can click on the seal to see the practitioner's report. This seal is displayed on the CA's Web site together with links to the practitioner's report and other relevant information.

This document is designed to benefit users and providers of CA e-commerce assurance services by providing a common body of knowledge that is communicated to such parties. *Suitable Trust Services Criteria and Illustrations for Certification Authorities* is consistent with standards being developed by the American National Standards Institute (ANSI) and the Internet Engineering Task Force (IETF).²

Overview

Electronic Commerce

² The American National Standards Institute (ANSI) X9F5 Digital Signature and Certificate Policy working group is developing the X9.79 *PKI Practices and Policy Framework* (X9.79) standard for the financial services community. This standard includes detailed Certification Authority Control Objectives against which certification authorities may be evaluated. An International Organization for Standardization (ISO) working group has been formed to standardize X9.79 based on international requirements in a new international standard. In addition, the American Bar Association's Information Security Committee (ABA-ISC) is developing the *PKI Assessment Guidelines* (PAG) which address the legal and technical requirements for certification authorities. The PAG makes reference to the Certification Authority Control Objectives that are detailed in the draft X9.79 standard and reflected in the WebTrust Principles and Criteria for Certification Authorities. The Certification Authority Control Objectives referred to in each of these documents were developed based on the existing body of ANSI, ISO, Internet Engineering Task Force (IETF), and other existing standards.

E-commerce involves individuals and organizations engaging in a variety of electronic business transactions, without paper documents, using computer and telecommunication networks. These networks can be either private or public, or a combination of the two. Traditionally, the definition of e-commerce has been focused on electronic data interchange (EDI) as the primary means of conducting business electronically between entities with a preestablished contractual relationship. Commerce has also been conducted electronically for years in the form of credit card transactions authorized at the point of sale, debit card transactions, and cash advances from automatic teller machines. More recently, however, with the development of electronic mail, and separately, the browser and HTML, the definition of e-commerce has broadened to encompass business conducted over the Internet between entities generally not previously known to each other. This is attributable to the Web's surge in popularity and the acceptance of the Internet as a viable transport mechanism for business information. The use of a public network-based infrastructure such as the Internet can reduce costs and "level the playing field" for small and large businesses. This allows companies of all sizes to extend their reach to a broader customer base.

Public Key Infrastructure

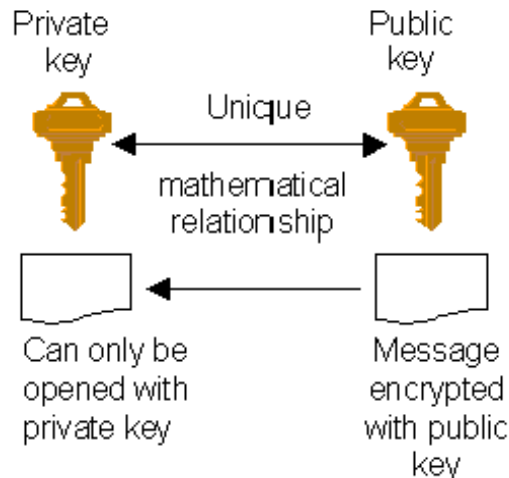
With the expansion of e-commerce, PKI is growing in importance and will probably be the most critical enterprise security investment a company will make in the next several years. PKI enables parties to an e-commerce transaction to identify one another by providing authentication with digital certificates, and allows reliable business communications by providing confidentiality through the use of encryption and authentication, data integrity, and a reasonable basis for nonrepudiation through the use of digital signatures.

PKI uses public/private-key pairs—two mathematically related keys. Typically, one of these keys is made public, by posting it on the Internet for example, while the other remains private. Public-key cryptography works in such a way that a message encrypted with the public key can be decrypted only with the private key, and, conversely, a message signed with a private key can only be verified with the public key. This technology can be used in different ways to provide the four ingredients required for trust in e-commerce transactions, namely confidentiality, authentication, integrity, and nonrepudiation.

Using PKI, a subscriber (that is, an end entity or individual whose public key is cryptographically bound to his or her identity in a digital certificate) has an asymmetric cryptographic key pair (that is, a public key and a private key). The subscriber's private key must be kept secret, whereas the public key may be made widely available, usually presented in the form of a digital certificate to ensure that relying parties know with confidence the identity to which the public key belongs. Using public key cryptography, the subscriber can send a message signed with his or her private key. The signature can be validated by the message recipient using the subscriber's public key. The subscriber can also encrypt a message using the recipient's public key. The message can be decrypted only with the recipient's private key.

A subscriber first obtains a public/private key pair (generated by the subscriber or for the subscriber as a service). The subscriber then goes through a registration process by submitting his or her public key to a certification authority or a registration authority (RA), which acts as an agent for the CA. The CA or RA verifies the identity of the subscriber in accordance with the CA's established business practices (that may be contained in a certification practice statement), and then issues a digital certificate. The certificate includes the subscriber's public key and identity information, and is digitally signed by the CA, which binds the subscriber's identity to that public key. The CA also manages the subscriber's digital certificate through the certificate life cycle (that is, from registration through revocation or expiration). In some circumstances, it remains important to manage digital certificates even after expiry or revocation so digital signatures on stored documents held past the revocation or expiry period can be validated at a later date.

The following diagram illustrates the relationship between a subscriber's public and private keys, and how they are used to secure messages sent to a relying party.



A transaction submitted by a customer to an online merchant via the Internet can be encrypted with the merchant's public key and therefore can only be decrypted by that merchant using the merchant's private key—ensuring a level of confidentiality. Confidentiality can also be achieved through the use of Secure Socket Layer (SSL), Secure/Multipurpose Internet Mail Extensions (S/MIME), and other protocols, such as Secure Electronic Transaction (SET).

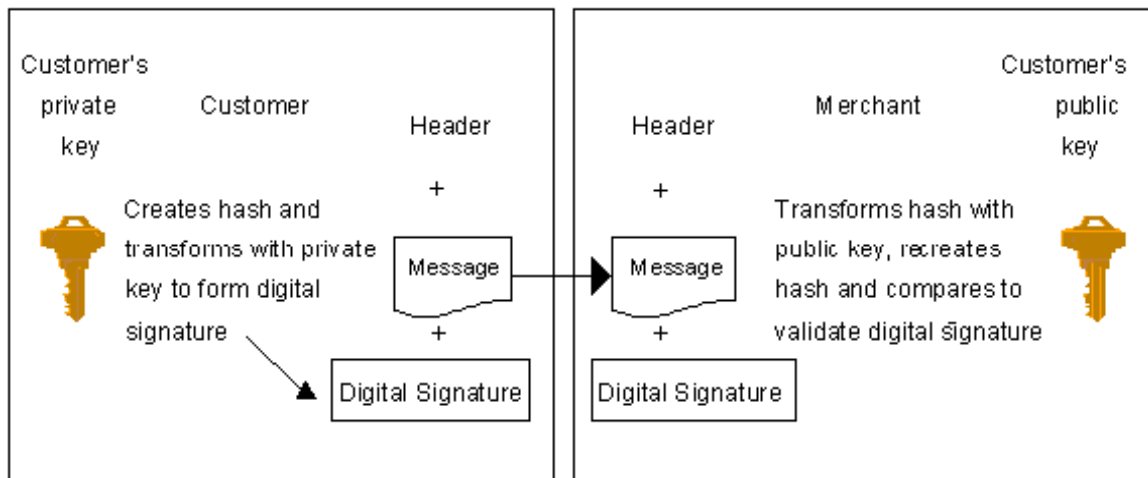
Digital Signature

Digital signatures can be used to provide authentication, integrity, and nonrepudiation. Generally speaking, if a customer sends a digitally signed message to a merchant, the customer's private key is used to generate the digital signature and the customer's public key can be used by the merchant to verify the signature. The mathematical processes employed differ somewhat depending on the kind of asymmetric cryptographic algorithm employed. For example, the processes are slightly different for reversible algorithms (that is, those that can be readily used to support digital signatures as well as encryption), such

as Rivest Shamir Adleman (RSA), and irreversible algorithms, such as the Digital Signature Algorithm (DSA).

The following example illustrates the digital signature generation and verification process for a reversible asymmetric cryptographic algorithm (such as RSA). Suppose a customer wants to send a digitally signed message to a merchant. The customer runs the message through a hash function (that is, a mathematical function that converts a message into a fixed-length block of data—the hash—in such a fashion that the hash uniquely reflects the message; in effect, is the message’s “fingerprint.” The customer then transforms the hash using the algorithm and the customer’s private key to create the digital signature, which is appended to the message. A header is also added, indicating the merchant’s e-mail address, the sender’s e-mail address, and other information such as the time the message is sent. The message header, the message itself, and the digital signature are then sent to the merchant. The customer has the option to send his or her public key certificate to the merchant in the message itself. All of this is usually done by the e-mail software in such a way that the process is transparent to the user.

The following diagram illustrates the process of using a subscriber’s key pair to ensure the integrity and authenticity of a message sent by the customer (subscriber) to a merchant.



To determine whether the message came from the customer (that is, authentication) and to determine whether the message has not been modified (that is, integrity), the merchant validates the digital signature. To do so, the merchant must obtain the customer’s public key certificate. If the customer did not send his or her public key certificate as part of the message, the merchant would typically obtain the customer’s public key certificate from an online repository (maintained by the CA, another party acting as the agent of the CA, or any other source even if unrelated to the CA). The merchant then validates that the customer’s digital certificate (containing the customer’s public key) was signed by a recognized CA to ensure that the binding between the public key and the customer represented in the certificate has not been altered. Next, the merchant extracts the public key from the certificate and uses that public key to transform the digital signature to reveal the original hash. The merchant then runs the message as received through the same hash function to create a hash of the received message. To verify the digital

signature, the merchant compares these two hashes. If they match, the digital signature validates and the merchant knows that the message came from the customer and it was not modified from the time the signature was made. If the hashes do not match, the merchant knows that the message was either modified in transit or the message was not signed with the customer's private key. As a result, the merchant cannot rely on the digital signature.

Digital signatures can also be used to provide a basis for nonrepudiation (that is, that the signer cannot readily deny having signed the message). For example, an online brokerage customer who purchases 1,000 shares of stock using a digitally signed order via the Internet should have a difficult task if he or she later tries to deny (that is, repudiate) having authorized the purchase.

Differences Between Encryption Key Pairs and Signing Key Pairs

As stated earlier, establishing a reasonable basis for nonrepudiation requires that the private key used to create a digital signature (that is, the signing private key) be generated and stored securely under the sole control of the user. In the event a user forgets his or her password or loses, breaks, or destroys his or her signing private key, it is acceptable to generate a new signing key pair for use from that point forward with minimal impact on the subscriber. Previously signed documents can still be verified with the user's old signature verification public key. Documents subsequently signed with the user's new signing private key must be verified with the user's new signature verification public key.

Extra care is required to secure the CA's signing private key, which is used for signing user certificates. The trustworthiness of all certificates issued by a CA depends upon the CA protecting its private signing key. CAs often back up their private signing key(s) securely for business continuity purposes. This allows the CA to continue to operate in the event that the CA's private signing key is accidentally destroyed (but not compromised)—as a result of hardware failure, for example. Except for CA business continuity purposes, there are generally no technical or business reasons to back up a signing private key.

On the other hand, and as cited earlier, it is often desirable that a key pair used for encryption and decryption be securely backed up to ensure that encrypted data can be recovered when a user forgets his or her password or otherwise loses access to his or her decryption key. This is analogous to requiring that the combination to a safe be backed up in case the user forgets it or becomes incapacitated. As a result, a PKI typically requires two key pairs for each user: one key pair for encryption and decryption and a second key pair for signing and signature verification.

Certification Authority

For these technologies to enable parties to securely conduct e-commerce, one important question must be answered: How can a user in the digital world know that an individual's public key actually belongs to that individual? A digital certificate, which is an electronic document containing information about an individual and his or her public key, is the

answer. This document is digitally signed by a trusted organization, the CA. The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. The CA provides a level of assurance that the public key contained in the certificate does indeed belong to the entity named in the certificate. The digital signature placed on the public key certificate by the CA provides the cryptographic binding between the entity's public key, the entity's name, and other information in the certificate, such as a validity period. For a relying party to determine whether the certificate was issued by a legitimate CA, the relying party must verify the issuing CA's signature on the certificate by using the CA's public key. The public keys of many common root CAs (defined in the section "The Hierarchical and Cross-Certified CA Models") are preloaded into standard Web browser software (for example, Netscape Navigator and Microsoft Internet Explorer).

The purpose of a CA is to manage the certificate life cycle, which includes generation and issuance, distribution, renewal and rekey, revocation, and suspension of certificates. The CA frequently delegates the initial registration of subscribers to RAs, which act as agents for the CA. In some cases, the CA may perform registration functions directly. The CA is also responsible for providing certificate status information through the issuance of certificate revocation lists (CRLs), the maintenance of an online status-checking mechanism, or both. Typically, the CA posts the certificates and CRLs that it has issued to a repository (such as an online directory) that is accessible to relying parties.

Registration Authority

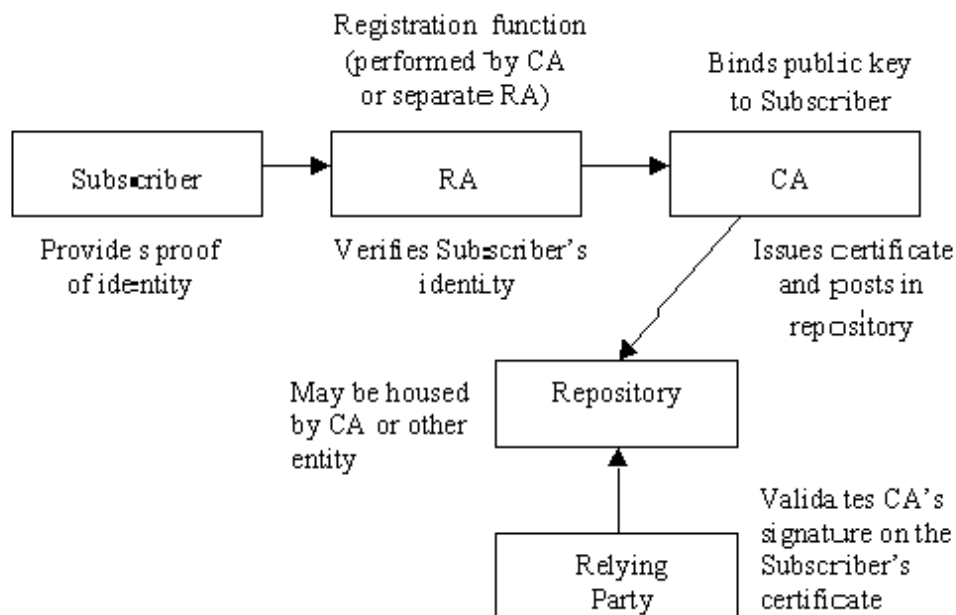
An RA is an entity that is responsible for the identification and authentication of subscribers, but does not sign or issue certificates. In some cases, the CA performs the subscriber registration function internally. In other cases, the CA delegates the RA function to external registration authorities (sometimes referred to as local registration authorities, or LRAs) that may or may not be part of the same legal entity as the CA. In still other cases, a customer of a CA (for example, a company) arranges with that CA to perform the RA function itself or using its agent. These external RAs are required to comply with the relevant provisions of the CA's business practices disclosures, often documented in a certification practice statement (CPS) and applicable certificate policy(s) (CPs). In performing a WebTrust for certification authorities engagement, the practitioner must consider how the CA handles the RA function and whether the RA function is within the scope of the examination. For example, a CA that provides CA services to several banks might delegate the subscriber registration function to RAs that are specifically designated functional groups within each bank. The functions performed by these specific groups would typically be outside the scope of the WebTrust for Certification Authorities examination performed for the CA. In this case management's assertion should specify those aspects of the registration process that are not handled by the CA.

The initial registration process for a subscriber is as follows, although the steps may vary from CA to CA and also depend upon the certificate policy under which the certificate is to be issued. The subscriber first generates his or her own public/private key pair. (In some implementations, a CA may generate the subscriber's key pair and deliver it to the

subscriber securely, but this is normally done only for encryption key pairs, not signature key pairs.) Then, the subscriber produces proof of identity in accordance with the applicable certificate policy requirements and demonstrates that he or she holds the private key corresponding to the public key without disclosing the private key (typically by digitally signing a piece of data with the private key, with the subscriber's digital signature then verified by the CA). Once the association between a person and a public key is verified, the CA issues a certificate. The CA digitally signs each certificate that it issues with its private key to provide the means for establishing authenticity and integrity of the certificate.

The CA then notifies the subscriber of certificate issuance and gives the subscriber an opportunity to review the contents of the certificate before it is made public. Assuming the subscriber approves the accuracy of the certificate, the subscriber will publish the certificate, have the CA publish it and make it available to other users, or both. A repository is an electronic certificate database that is available online. The repository may be maintained by the CA or a third party contracted for that purpose by the subscriber or by any other party. Subscribers may obtain certificates of other subscribers and certificate status information from the repository. For example, if a subscriber's certificate was revoked, the repository would indicate that the subscriber's certificate has been revoked and should not be relied upon. The ability to update the repository is typically retained by the CA. Subscribers and other relying parties have read-only access to the repository. Because the certificates stored in the repository are digitally signed by the CA, they cannot be maliciously changed without detection, even if someone were to hack into the repository.

The following diagram illustrates the relationship between the subscriber and the RA and CA functions.



Certification Practice Statements and Certificate Policies

A CPS is a statement of the practices that a CA employs in issuing and managing certificates. A CP is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular CP might indicate the applicability of a type of certificate to the authentication of EDI transactions for the trading of goods within a given price range.

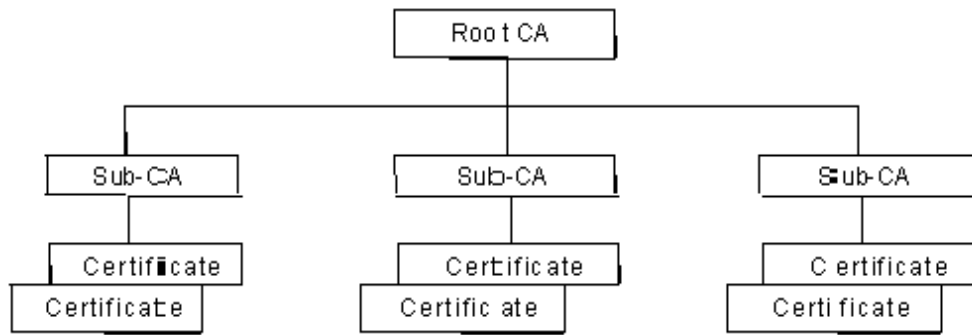
The Difference Between Licensed and Nonlicensed CAs

Many countries, states, and other governmental jurisdictions have enacted or are developing digital signature laws. In those jurisdictions that have digital signature laws and provide for certification authority licensing, certificates issued by licensed CAs typically have a higher level of legal recognition than those issued by nonlicensed CAs. For a number of jurisdictions, the use of certificates issued by licensed CAs is provided specific recognition in those jurisdictions' digital signature laws. In the United States, for example, several state digital signature laws require that audits of CAs be performed as a requirement for licensing. One of the purposes of this document is to provide suitable criteria that would meet the requirements of various governmental jurisdictions and the marketplace.

The Hierarchical and Cross-Certified CA Models

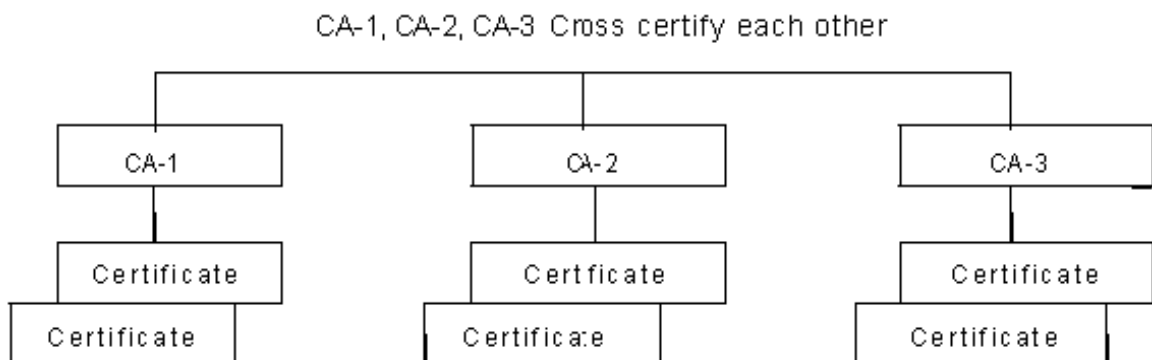
CAs may be linked using two basic architectures, hierarchical and cross-certified (shared trust), or a hybrid of the two. In a hierarchical model, a highest level (or "root") CA is deployed and subordinate CAs may be set up for various business units, domains, or communities of interest. The root CA validates the subordinate CAs, which in turn issue certificates to lower-tier CAs or directly to subscribers. Such a root CA typically has more stringent security requirements than a subordinate CA. Although it is difficult for an attacker to access the root CA (which in some implementations is online only in the rare event that it must issue, renew, or revoke subordinate CA certificates), one drawback to this model is that the root CA represents a single point of failure. In the hierarchical model, the root CA maintains the established "community of trust" by ensuring that each entity in the hierarchy conforms to a minimum set of practices. Adherence to the established policies may be tested through audits of the subordinate CAs and, in a number of cases, the RAs.

The following diagram illustrates the structure and relationships between CAs and subscribers operating in a hierarchical model.



In an alternative model, cross-certified CAs are built on a peer-to-peer model. Rather than deploying a common root CA, the cross-certification model shares trust among CAs known to one another. Cross-certification is a process in which two CAs certify the trustworthiness of the other's certificates. If two CAs, CA1 and CA2, cross-certify, CA1 creates and digitally signs a certificate containing the public key of CA2 (and vice versa). Consequently, users in either CA domain are assured that each CA trusts the other and therefore subscribers in each domain can trust each other. Cross-certified CAs are not subject to the single point of failure in the hierarchical model. However, the network is only as strong as the weakest CA, and requires continual policing. In the cross-certified model, to establish and maintain a community of trust, audits may be performed to ensure that each cross-certified CA conforms to a minimum set of practices as agreed upon by the members of the community of trust.

The following diagram illustrates the structure and relationships between CAs and subscribers operating in a cross-certified (shared trust) model.



In a hybrid model, both a hierarchical structure and cross-certification are employed. For example, two existing hierarchical communities of trust may want to cross-certify each other, so that members of each community can rely upon the certificates issued by the other to conduct e-commerce.

Business Issues Associated With CAs

Unless they are subject to governmental licensing and regulation, CAs may use different

standards or procedures to verify the identity of persons to whom they issue certificates. Thus, a digital signature is only as reliable as the CA is trustworthy in performing its functions. Consequently, a relying party needs some way to gauge how much reliance it should place on a digital signature supported by a certificate issued by a particular CA.

CA topology (for example, use of a hierarchical, a cross-certified, or a hybrid model) is a developing issue. Which model is most appropriate depends on business circumstances. Although it is important that public keys be certified, the issuance of nonstandard certificates can be a concern. For example, if the broadly recognized International Telecommunications Union-Telecommunication Standardization Sector's (ITU-T) X.509 data format standard³ is not used, subscribers and relying parties may be unable to process such certificates. Implementing the cross-certified CA model (discussed previously) would also be very difficult. For these reasons, major entities such as the U.S. and Canadian governments are using or plan to use X.509 certificates for their internal and external activities.

The WebTrust Seal of Assurance for Certification Authorities

The Web has captured the attention of businesses and consumers, causing the number and kinds of electronic transactions to grow rapidly. Nevertheless, many believe that e-commerce will not reach its full potential until customers perceive that the risks of doing business electronically have been reduced to an acceptable level. Customers may have legitimate concerns about confidentiality, authentication, integrity, and nonrepudiation. In e-commerce, participants need the assurance of an objective third party. This assurance can be provided by an independent and objective practitioner and demonstrated through the display of a WebTrust seal for CAs on the CA's Web site.

The WebTrust seal of assurance for CAs symbolizes to potential relying parties that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities, and has issued a report with an unqualified opinion indicating that such principles are being followed in conformity with the WebTrust for Certification Authorities criteria. See Appendix A, "Illustrative Examples of Practitioner Reports." These principles and criteria reflect fundamental rules for the operation of a CA organization or function.

Practitioners as Assurance Professionals

Practitioners are in the business of providing assurance services, the most publicly recognized of which is the audit of financial statements. An audit opinion signed by a qualified practitioner is valued because these professionals are experienced in assurance matters and financial accounting subject matter and are recognized for their

3 International Telecommunications Union-Telecommunication Standardization Sector's (ITU-T) Recommendation X.509 (1997) was also standardized by International Organization for Standardization (ISO) as ISO/IEC 9594-8.

independence, integrity, discretion, and objectivity. Practitioners also follow comprehensive ethics rules and professional standards in providing their services. However, financial statement assurance is only one of the many kinds of assurance services that can be provided by a practitioner. Practitioners also provide assurance about controls and compliance with specified criteria.

In general, the business and professional experience, subject matter expertise (e-commerce information systems security, privacy, auditability, and control), and professional characteristics (independence, integrity, discretion, and objectivity) needed for such projects are the same key elements that enable a practitioner to comprehensively and objectively assess the risks, controls, and business disclosures associated with e-commerce.

Obtaining and Keeping the WebTrust Seal of Assurance for Certification Authorities

The Assurance Process

The CA's management will make assertions along the following lines:

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) Management's opinion, in providing its certification authority (CA) services at [location], ABC-CA, during the period from [Month, day, year] through [Month, day, year]:

Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices

Maintained effective controls to provide reasonable assurance that:

- Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
- The integrity of keys and certificates it managed was established and protected throughout their life cycles

Maintained effective controls to provide reasonable assurance that:

- Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria.

For an initial representation, the historical period covered should be at least two months or more as determined by the practitioner. For established CAs and CA functions, two

months may be quite sufficient, while for new CAs and CA functions, the practitioner may believe that a longer initial period would be more appropriate. For subsequent representations, the period covered should begin with the end of the prior period, to provide continuous representation. Reports should be issued at least every 12 months. In some situations, given the business needs or expectations of relying parties, the practitioner may believe a shorter subsequent period would be more appropriate.

To have a basis for such assertions, the CA's management should have made a risk assessment and implemented appropriate controls for its CA operations. The WebTrust for Certification Authorities criteria and illustrative controls provide a basis for a risk assessment and a minimum set of CA controls.

An independent, objective, and knowledgeable practitioner will perform tests of these representations under AICPA professional standards⁴ and provide a professional opinion, which adds to the credibility of management's representations.

Comparison of a WebTrust for Certification Authorities Examination With Service Auditor Reports

Professional standards currently exist for auditors to report on controls of third-party service providers (a service auditor's engagement). Guidance for these engagements is set out in the AICPA's Statement on Auditing Standards (SAS) No. 70, *Service Organizations* (AICPA, *Professional Standards*, vol. 1, AU sec. 324), as amended. A WebTrust for Certification Authorities engagement differs from a service auditor's engagement in a number of ways, including the following:

Purpose. WebTrust for Certification Authorities provides a new framework for reporting activities of CAs through auditor communication to interested parties, including business partners and existing or potential customers. SAS No. 70 (service auditor reports) was designed for auditor-to-auditor communication to assist the user auditor in reporting on the financial statements of a customer of the service organization.

Target of evaluation. WebTrust for Certification Authorities was designed specifically for the examinations of CA business activities. Service auditor

4 These services are performed in the United States under Chapter 1, "Attest Engagements," of Statement on Standards for Attestation Engagements (SSAE) No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101). Practitioners will need the appropriate skills and experience, training in the WebTrust for Certification Authorities service offering, and a WebTrust business license from the AICPA, CICA, or other authorized national accounting institute to provide the WebTrust for Certification Authorities services to their clients. The practitioner needs to perform an "examination" (audit) level engagement in order to award the WebTrust seal for certification authorities. A review level engagement is not sufficient.

reports were designed for service organizations in general.

Type of engagement. WebTrust for Certification Authorities requires reporting on compliance with the AICPA/CICA WebTrust Principles and Criteria for Certification Authorities. Service auditor reports were designed for reporting on the design and existence of controls and the effective operation of those controls when the report covers a period of time.

Examination standards. WebTrust for Certification Authorities follows the AICPA Statements on Standards for Attestation Engagements (SSAEs). Service auditor reports follow generally accepted auditing standards.

Coverage of activities. WebTrust for Certification Authorities requires coverage of specific areas as defined herein, including CA business practices disclosure, service integrity (including key and certificate life cycle management activities), and CA environmental controls. Service auditor reports were designed for reporting upon controls related to financial information.

Linkage to authoritative standards. WebTrust for Certification Authorities provides uniform rules derived from the draft ANSI X9.79 standard (which is intended to be submitted to the International Organization for Standardization [ISO] for international standardization). Standards underlying service auditor reports do not specify the control objectives that must be covered by the report.

Period of coverage of review. WebTrust for Certification Authorities encourages continuous coverage from the point of initial qualification and requires continuous coverage to retain the seal. Qualification after compliance can be tested over a minimum two-month period, with updates over a specified period (currently one-year maximum). Service auditor reports cover a period of time specified by the service organization, but do not require continuous coverage.

In addition, this approach maintains consistency in the professional standards used for the Suitable Trust Services Criteria and Illustrations. Both WebTrust and SysTrust use Chapter 1, “Attest Engagements,” of SSAE No. 10, *Attestation Standards: Revision and Recodification* (AICPA, *Professional Standards*, vol. 1, AT sec. 101), as amended, as the reporting standards.

A table highlighting the differences between a WebTrust for Certification Authorities engagement and SAS No. 70 and Section 5900 engagements is provided in Appendix E.

Obtaining the WebTrust Seal

To obtain the WebTrust seal of assurance, the CA must meet all the WebTrust for Certification Authorities principles as measured by the WebTrust for Certification Authorities criteria associated with each of these principles. In addition, the entity must (a) engage a practitioner who has a WebTrust business license from the AICPA, CICA,

or other authorized national accounting institute to provide the WebTrust service, and (b) obtain an unqualified report from such practitioner.

Keeping the WebTrust Seal

Once the seal is obtained, the CA will be able to continue displaying it on its Web site provided the following are performed.

1. The CA's WebTrust practitioner updates his or her assurance examination of the assertion on a regular basis. The CA must continue to obtain an unqualified report from such practitioner. The interval between such updates will depend on matters such as the following:
 - a. The nature and complexity of the CA's operations
 - b. The frequency of significant changes to the CA's operations
 - c. The relative effectiveness of the entity's monitoring and change-management controls for ensuring continued conformity with the applicable WebTrust for Certification Authorities criteria as such changes are made
 - d. The practitioner's professional judgment

For example, an update may be required more frequently for a CA that is expanding operations, changing extensively and rapidly, or issuing high-assurance certificates that are used for very sensitive transmissions or high-value transactions, as compared to a CA that issues few certificates and has a relatively stable operation. In no event should the interval between updates exceed 12 months; this interval often may be shorter. For example, in the situation of a start-up CA or CA function, it may be more appropriate that the initial examination period be established at 3 months, with the next review being performed 6 months after the WebTrust seal for CAs is awarded, thereafter moving to a 12-month review cycle. To provide continuous coverage and retain the seal, the period covered for update reports should begin with either the end of the prior period or the start of the period in the initial report.

2. During the period between updates, the CA undertakes to inform the practitioner of any significant changes in its business policies, practices, processes, and controls, particularly if such changes might affect the CA's ability to continue meeting the WebTrust Principles and Criteria for Certification Authorities, or the manner in which they are met. Such changes may trigger the need for an assurance update or, in some cases, removal of the seal until an update examination by the practitioner can be made. If the practitioner becomes aware of such a change in circumstances, he or she determines whether the seal needs to be removed until an update examination is completed and the updated auditor's report

is issued.

The Seal Management Process

The WebTrust seal of assurance for the CA will be managed by a seal manager along the following lines.

- Upon becoming a WebTrust licensee, the WebTrust practitioner obtains a registration number (ID and password) from the WebTrust licensing authority. With this the practitioner can issue a WebTrust seal to the CA.
- When the practitioner is prepared to issue a WebTrust seal, he or she accesses the WebTrust secure server system. Upon payment of the registration fee, the practitioner receives passwords and IDs unique to the engagement. The seal manager issues these to the practitioner in pairs. One set allows the practitioner to read and write to the secure server (see below) and the other permits the CA to preview the presentation.
- The practitioner prepares a draft of the practitioner's report and provides it along with management's assertions for posting to the preview site.
- The seal manager then delivers the seal to the CA with the appropriate links to the preview site. Notification of delivery is provided to the practitioner.
- When the practitioner and CA have agreed that the seal should become active, the practitioner notifies the seal manager to transfer the information from the preview site to the active WebTrust site and provides the appropriate expiration date.
- The seal remains valid for the period provided by the practitioner plus a one-month grace period, unless removed for cause. The one-month period is to allow sufficient time to complete the engagement and other open items. For example, if the seal expires on June 30, 20XX, the practitioner has 30 days to complete open items and prepare new documents for posting with the seal manager. The subsequent examination period begins July 1, 20XX.
- If the practitioner determines that the seal should be removed from the CA's Web site, the practitioner will immediately notify the CA and request that the seal be removed from the CA's site. The practitioner will then notify the seal manager to remove all the relevant information and to replace it with a statement that the WebTrust seal for this site is no longer valid.
- The seal manager will notify the practitioner 30 days prior to expiration that the seal needs to be renewed. The seal manager may revoke seals if the registration fee for the seal is unpaid or for other sufficient cause.

WebTrust Seal Authentication

To verify whether the seal displayed on a CA's Web site is authentic, the customer can:

- Click on the seal, which links the customer through a secure connection to a WebTrust seal verification page hosted by the seal manager. It identifies the CA and confirms that the CA is entitled to display the WebTrust seal. It also provides links to the appropriate principle(s) (that is, the WebTrust for Certification Authorities principles) and other relevant information.
- Access the list of entities that have received a WebTrust seal; the list is maintained by the seal manager at www.webtrust.org/abtseals.htm. A CA is registered on this list when the seal is issued.

WebTrust Principles and Criteria for Certification Authorities

WebTrust for Certification Authorities Principles

To be understandable to the ultimate users—the subscriber and relying party—the following principles have been developed with the relying party in mind, and, as a result, are intended to be practical and nontechnical in nature.

Principle 1: CA Business Practices Disclosure

The first principle is—*The certification authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.*

The CA must disclose its key and certificate life cycle management business and information privacy practices. Information regarding the CA's business practices should be made available to all subscribers and all potential relying parties, typically by posting on its Web site. Such disclosure may be contained in a certificate policy (CP), certification practice statement (CPS), or other informative materials that are available to users (subscribers and relying parties).

Principle 2: Service Integrity

The second principle is—*The certification authority maintains effective controls to provide reasonable assurance that:*

- *Subscriber information was properly authenticated (for the registration activities performed by ABC-CA).*
- *The integrity of keys and certificates it manages is established and protected throughout their life cycles.*

Effective key management controls and practices are essential to the trustworthiness of the public key infrastructure. Cryptographic key management controls and practices

cover CA key generation; CA key storage, backup, and recovery; CA public key distribution (especially when done in the form of self-signed “root” certificates); CA key escrow (optional); CA key usage; CA key destruction; CA key archival; the management of CA cryptographic hardware through its life cycle; and CA-provided subscriber key management services (optional). Strong key life cycle management controls are vital to guard against key compromise that can damage the integrity of the public key infrastructure.

The user certificate life cycle is at the core of the services provided by the CA. The CA establishes its standards and practices by which it will deliver services in its published CPS and CPs. The user certificate life cycle includes the following:

- Registration (that is, the identification and authentication process related to binding the individual subscriber to the certificate)
- The renewal of certificates (optional)
- The rekey of certificates
- The revocation of certificates
- The suspension of certificates (optional)
- The timely publication of certificate status information (through certificate revocation lists or some form of online certificate status protocol)
- The management of integrated circuit cards (ICCs) holding private keys through their life cycle (optional)

Effective controls over the registration process are essential, as poor identification and authentication controls jeopardize the ability of subscribers and relying parties to rely on the certificates issued by the CA. Effective revocation procedures and timely publication of certificate status information are also essential elements, as it is critical for subscribers and relying parties to know when they are unable to rely on certificates that have been issued by the CA.

Principle 3: CA Environmental Controls

The third principle is—*The certification authority maintains effective controls to provide reasonable assurance that:*

- *Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA’s business practices disclosure;*
- *The continuity of key and certificate life cycle management operations is maintained; and*

- *CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.*

The establishment and maintenance of a trustworthy CA environment is essential to the reliability of the CA's business processes. Without strong CA environmental controls, strong key and certificate life cycle management controls are severely diminished in value. CA environmental controls include CPS and CP management, security management, asset classification and management, personnel security, physical and environmental security of the CA facility, operations management, system access management, systems development and maintenance, business continuity management, monitoring and compliance, and event journaling.

WebTrust for Certification Authorities Criteria

To provide more specific guidance on meeting the WebTrust for Certification Authorities principles, the WebTrust for Certification Authorities criteria have been developed. These provide a basis against which a CA can make a self-assessment of its conformity with the criteria, and a consistent set of measurement criteria for practitioners to use in testing and evaluating CA practices.

The WebTrust for Certification Authorities criteria are presented under the three principles listed above (Principle 1, CA Business Practices Disclosure; Principle 2, Service Integrity, including key and certificate life cycle management controls; and Principle 3, CA Environmental Controls). Each principle contains a series of criteria that the CA's management asserts it has achieved. Depending on the scope of services provided by the CA, a number of the criteria may not be applicable. Criteria considered optional, depending on whether the CA provides the related services, are key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards (ICCs), and the provision of subscriber key management services. If any of these services are provided by the CA, the criteria are applicable and must be tested by the practitioner. If any of these services are not provided by the CA, the criteria are not applicable and no modification of the standard report is necessary. In some situations, some RA services may be performed by another party that is not controlled by the CA, and therefore those activities are not included in the examination of the CA. In these circumstances the standard report should be modified to specify the exclusion of the specific RA activities from the scope of the examination, as shown in Appendix A, Example 2. This may be accomplished by reference to the CA's business practice disclosures in which the CA specifies which RA activities it does not control. In all instances some RA activities will be performed by the CA and should be tested by the practitioner for compliance with the controls disclosed under Principle 1 and the criteria specified in Principle 2.⁵

5 As indicated herein, during development of this document, the AICPA/CICA Electronic Commerce Assurance Task Force considered the situations in which subscriber registration is performed by the certification authority (CA) itself or by external registration authorities (RAs). This document has been written such that the RA function

In performing a WebTrust for Certification Authorities engagement, the practitioner must gain an understanding of the CA's business model and services provided to determine which control criteria may not be applicable. For each of the disclosure and control criteria, there is a detailed list of illustrative disclosures and control procedures that might be followed by the CA to meet the related criteria. The illustrative disclosures and controls do not necessarily need to be in place for a criterion to be met in a given business circumstance and alternatives may be sufficient.

The CA Business Practices Disclosure criteria were derived primarily from the Internet Engineering Task Force's (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Request For Comments Draft (RFC 2527), which has been incorporated into Annex A of the draft ANSI X9.79 standard. For specific key and certificate life cycle management (Principle 2) and CA environmental illustrative controls (Principle 3), in which the CA's implemented controls may vary depending on the CA's business practices, such illustrative controls refer to specifically required CA business practices disclosures included in Principle 1.

WebTrust Principles and Criteria for Certification Authorities

Principle 1: CA Business Practices Disclosure

The certification authority discloses its key and certificate life cycle management business and information privacy practices and provides its services in accordance with its disclosed practices.

Criteria

Illustrative Disclosures

1.1 CA Business Practices Disclosure

<p>Identification of each certificate policy (CP) and certification policy statement (CPS) for which the CA issues certificates</p>	<p>1</p>	<p>The certification authority (CA) discloses its business practices, including but not limited to the following: General The CA issues certificates in accordance with the CA's certification policy statement (CPS) dated [date]. The CA issues certificates that support the following certificate policies: CA's Class 1 Certificate Policy, CA's Class 2 Certificate Policy, CA's Class 3 Certificate Policy, and the Bank Consortium's Certificate Policy.</p>
---	----------	---

may be "carved out" or considered outside the scope of the WebTrust for certification authorities examination when registration activities are performed by parties external to the CA. For the purpose of some end users, this approach may not address all requirements for the independent verification of such end users. The Task Force was aware of this situation and concluded that the issuance and use of this document was desirable and that the impact of a third-party registration function was beyond the scope of this document.

<p>Community and applicability, including a description of the types of entities within the public key infrastructure (PKI) and the applicability of certificates issued by the CA</p>	<p>2</p>	<p>The CA is established to provide certificate services for a variety of external customers. The organization operates a single CA, which issues user certificates to all CA customers. The CA makes use of customer designated personnel to act as agents to verify the identity of subscribers, in accordance with the indicated certificate policy. Subscribers include all parties who contract with the CA for digital certificate services. All parties who may rely upon the certificates issued by the CA are considered relying parties.</p> <p>This certification policy statement (CPS) (or other CA business practices disclosure) is applicable to all certificates issued by the CA. The practices described in the CPS (or other CA business practices disclosure) apply to the issuance and use of certificates and certificate revocation lists (CRLs) for users within the CA domain.</p>
<p>Contact details and administrative provisions, including:</p> <ul style="list-style-type: none"> • Contact person • Identification of policy authority • Street address • Version and effective date(s) of each CP and CPS 	<p>3</p>	<p>This CPS (or other CA business practices disclosure) is administered by the CA operations manager. The CA's certificate policies are administered by the CA's policy authority. Contact information is listed below.</p> <p>The contact details for this CPS are: CA Operations Manager</p> <p>[Address] [Telephone] [Fax] [E-mail]</p> <p>The contact details for the CA's certificate policy are: Policy Authority [Address] [Telephone] [Fax] [E-mail]</p>
<p>Any applicable provisions regarding apportionment of liability</p>	<p>4</p>	<p>Except as expressly provided otherwise in this CPS, applicable CP, or by statute or regulation, the CA's total liability per breach of any express warranties made under this CPS and/or applicable CP is limited to direct damages having a maximum dollar amount (that is, a liability cap) of \$10,000. The liability cap set forth in this CPS or applicable CP shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. Additionally, in the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall the CA be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of the liability cap.</p>

<p>Financial responsibility, including: 5</p> <ul style="list-style-type: none"> • Indemnification by relying parties • Fiduciary relationships 	<p>By their applying for and being issued certificates, or otherwise relying upon such certificates, subscribers and relying parties agree to indemnify, defend, and hold harmless the CA, and its personnel, organizations, entities, subcontractors, suppliers, vendors, representatives, and agents from any errors, omissions, acts, failures to act, or negligence resulting in liability, losses, damages, suits, or expenses of any kind, due to or otherwise proximately caused by the use or publication of a certificate that arises from the subscriber's failure to provide the CA with current, accurate, and complete information at the time of certificate application or the subscriber's errors, omissions, acts, failures to act, and negligence.</p> <p>The CA and its registration authorities (RAs) are not the agents, fiduciaries, trustees, or other representatives of subscribers or relying parties.</p>
<p>Interpretation and enforcement, including: 6</p> <ul style="list-style-type: none"> • Governing law • Severability, survival, merger, and notice • Dispute resolution procedures 	<p>Governing Law:</p> <p>The laws of [<i>jurisdiction</i>] shall govern the enforceability and construction of this CPS (or other CA business practices disclosure) to ensure uniform procedures and interpretation for all users.</p> <p>Severability, Survival, Merger, Notice:</p> <p>Severance or merger may result in changes to the scope, management, and/or operations of this CA. In such an event, this CPS may require modification as well. Changes to the operations will occur consistently with the CA's disclosed CPS management processes.</p> <p>Dispute Resolution Procedures:</p> <p>In the event of any dispute involving the services or provisions covered by this CPS (or other CA business practices disclosure), the aggrieved party shall first notify the CA and all other relevant parties regarding the dispute. The CA will involve the appropriate personnel to resolve the dispute.</p>
<p>Fees, including: 7</p> <ul style="list-style-type: none"> • Certificate issuance or renewal fees • Certificate access fees • Revocation or status information access fees • Fees for other services, such as policy information • Refund policy 	<p>The CA may charge subscribers fees for their use of the CA's services. A current schedule of such fees is available from the CA's repository at [<i>URL</i>]. Such fees are subject to change seven (7) days following their posting in the CA's repository.</p>

<p>Publication and repository requirements, including:</p> <ul style="list-style-type: none"> • Publication of CA information • Frequency of publication • Access controls 	8	<p>The CA's CPS (or other CA business practices disclosure) is available at [URL]. The CA's certificate policies can be found at [URL].</p> <p>Upon issuance, all public key certificates and CRLs issued by the CA are published in the CA's directory.</p> <p>All subscribers and relying parties have access to the CA's repository.</p>
<p>Compliance audit requirements, including:</p> <ul style="list-style-type: none"> • Frequency of entity compliance audit • Auditor's relationship to audited party • Topics covered by audit • Actions taken as a result of deficiency • Communication of results 	9	<p>An annual audit is performed by an independent external auditor to assess the adequacy of the CA's business practices disclosure and the effectiveness of the CA's controls over its CA operations.</p> <p>Topics covered by the annual audit include the following:</p> <ul style="list-style-type: none"> • CA business practices disclosure • Service integrity (including key and certificate life cycle management controls) • CA environmental controls <p>Significant deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by the auditor with input from CA management. The CA is responsible for seeing that corrective action is taken within 60 days. Should a severe deficiency be identified that might compromise the integrity of the CA, CA management considers, with input from the auditor, whether suspension of the CA's operation is warranted.</p> <p>Compliance audit results are communicated to the board of directors of the CA, CA management, and the CA's policy authority, as well as others deemed appropriate by CA management.</p>
<p>Description of the conditions for applicability of certificates issued by the CA that reference a specific CP, including:</p> <ul style="list-style-type: none"> • Specific permitted uses for the certificates if such use is limited to specific applications • Limitations on the use of certificates if there are specified prohibited uses for such certificates 	10	<p>Certificates issued under the CA's certificate policy are limited to use in connection with [bank's] Consumer Internet Banking application. Certificates issued by the CA may not be used for any other purpose.</p>

CA and/or registration authority (RA) 11 obligations:

- Notification of issuance of a certificate to the subscriber who is the subject of the certificate being issued
- Notification of issuance of a certificate to others than the subject of the certificate
- Notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended
- Notification of revocation or suspension of a certificate to others than the subject whose certificate is being revoked or suspended

The CA is obligated to:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the CA repository
- Issue and publish certificates in a timely manner in accordance with the relevant certificate policy
- Revoke certificates issued by the CA, upon receipt of a valid request to revoke the certificate from a person authorized to request revocation
- Publish CRLs on a regular basis, in accordance with the applicable certificate policy and with provisions described in the CA's disclosed business practices (Principle 1, item 35)
- Notify subscribers via e-mail (1) that certificates have been generated for them and (2) how the subscribers may retrieve the certificates
- In the event the CA is not successful in validating the subscriber's application in accordance with the requirements for that class of certificate the CA shall notify the subscriber that the application has been rejected
- Notify subscribers via e-mail that the subscriber's certificate has been revoked
- Notify other participants in the PKI of certificate issuance revocation through access to certificates and CRLs in the CA repository

RA obligations, including: 12

- Identification and authentication of subscribers
- Validation of revocation and suspension requests
- Verification of subscriber renewal or rekey requests

The RAs (or the CA's RA function) are obligated to:

- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application, in accordance with the relevant certificate policy.
- Validate and securely send a revocation request to the CA upon receipt of a request to revoke a certificate, in accordance with the relevant certificate policy.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of renewal or rekey, in accordance with the relevant certificate policy.

Repository obligations, including: 13

- Timely publication of certificates and certificate revocation lists (CRLs)

The CA's repository function is obligated to publish certificates and certificate revocation lists in a timely manner.

Subscriber obligations, including: 14

- Accuracy of representations in certificate application
- Protection of the subscriber's private key
- Restrictions on private key and certificate use
- Notification upon private key compromise

Subscribers are obligated to:

- Provide information to the CA that is accurate and complete to the best of the subscribers' knowledge and belief regarding information in their certificates and identification and authentication information and promptly notify the CA of any changes to this information.
- Safeguard their private key from compromise.
- Use certificates exclusively for legal purposes and in accordance with the relevant certificate policy and this CPS (or other CA business practices disclosure).
- Promptly request that the CA revoke a certificate if the subscriber has reason to believe there has been a compromise of their private key corresponding to the public key listed in the certificate.

<p>Relying party obligations, including: 15</p> <ul style="list-style-type: none"> • Purposes for which certificate is used • Digital signature verification responsibilities • Revocation and suspension checking responsibilities • Acknowledgment of applicable liability caps and warranties 	<p>Relying parties are obligated to:</p> <ul style="list-style-type: none"> • Restrict reliance on certificates issued by the CA to the purposes for those certificates, in accordance with the relevant certificate policy and with this CPS (or other CA business practices disclosure). • Verify the status of certificates at the time of reliance. • Agree to be bound by the provisions of limitations of liability as described in the CPS (or other CA business practices disclosure) upon reliance on a certificate issued by the CA.
<p>Key Life Cycle Management</p>	
<p>Any applicable reliance or financial limits for certificate usage 16</p>	<p>Certificates issued under the CA's certificate policy may only be used in connection with transactions having a dollar value of no more than \$100,000.</p>
<p>CA key pair generation, including: 17</p> <ul style="list-style-type: none"> • What key sizes are required • What key generation algorithm is required • Whether key generation is performed in hardware or software • What standards are required for the module used to generate the keys (for example, the required ISO 15782-1/FIPS 140-1/ANSI X9.66 level of the module) • For what purposes the key may be used • For what purposes usage of the key should be restricted • The usage periods or active lifetimes for the CA public and the private key, respectively 	<p>The CA's signing key pair is 1024 bit using the RSA algorithm.</p> <p>Hardware key generation is used and is compliant to at least FIPS 140-1 level 3.</p> <p>The CA's signing key is used to sign certificates and CRLs.</p> <p>The lifetime of the CA signing key pair is five years.</p>
<p>CA private key protection including: 18</p> <ul style="list-style-type: none"> • What standards are required for the module used to store the CA private signature key (for example, the required ISO 15782-1/FIPS 140-1/ANSI X9.66 level of the module) • Whether the CA private key is maintained under m out of n multiperson control • Whether the CA private signature key is escrowed • Whether the CA private signing key is backed up • Whether the CA private and public signature keys are archived 	<p>Hardware cryptographic modules for generating and storing the CA's root key are certified to FIPS 140-1 level 3.</p> <p>There is a separation of physical and logical access to the CA's root private key. Two individuals provide dual control over physical access to the hardware modules; m of n secret shares held by other, separate custodians on removable media are required for logical activation of the private keys.</p> <p>The CA's private signing key is backed up only on hardware certified to FIPS 140-1 level 3 and is stored with two-person control enforced.</p> <p>Escrow of CA private keys by an external third party is not performed.</p> <p>The CA's private signing key and expired (and revoked) CA public key certificates are archived.</p>

<p>Whether the CA provides subscriber key management services and a description of the services provided</p>	19	<p>The CA provides subscriber key management services including the following:</p> <ul style="list-style-type: none"> • Subscriber key generation • Subscriber key storage, backup, and recovery • Subscriber key archival • Subscriber key destruction
<p>CA public key distribution, including a description of how the CA's public key is provided securely to subscribers and relying parties</p>	20	<p>The CA's public key is delivered in a self-signed certificate to subscribers using an encrypted session between the CA and the subscriber's client software, with an authorization code as a shared secret. Authenticity and integrity protection is based on a MAC key derived from the authorization code.</p>
<p>Key changeover, including a description of the procedures used to provide a new public key to a CA's users</p>	21	<p>The CA root signing private key has a lifetime of two years and the corresponding public key certificate has a lifetime of four years. Upon the end of the private key's lifetime, a new CA signing key pair is generated and all subsequently issued certificates and CRLs are signed with the new private signing key. The corresponding new CA public key certificate is securely provided to subscribers and relying parties.</p>
<p>Subscriber key pair generation (if the CA provides subscriber key pair generation services), including:</p> <ul style="list-style-type: none"> • How the subscriber's private key is provided securely to the subscriber • What key sizes are required • What key generation algorithm is required • Whether key pair generation is performed in hardware or software • What standards are required for the module used to generate the keys (for example, the required ISO 15782-1/FIPS 140-1/ANSI X9.66 level of the module) • For what purposes the key may be used • For what purposes usage of the key should be restricted 	22	<p>For subscribers, the CA creates an encryption key pair and the corresponding encryption public key certificate.</p> <p>For subscribers, the encryption key pair is provided securely to the user via an encrypted session between the CA and the subscriber's client software.</p> <p>Subscriber encryption key pairs are 1024 bit using the RSA algorithm.</p> <p>The CA's process for generating subscriber encryption key pairs uses the CA system software and is designed to comply with FIPS 140-1 level 1.</p>

Subscriber private key protection (if the CA provides subscriber key management services), including:

- Whether the subscriber's decryption private key is backed up
- Whether the subscriber's decryption private key is archived
- Under what conditions a subscriber's private key can be destroyed
- Whether subscriber private decryption keys are escrowed by the CA

Subscriber encryption private keys generated by the CA are backed up in the CA database. The CA database is encrypted and its integrity is protected by master keys. Subscriber signature private keys are generated by the subscriber and are not known or stored by the CA.

The encryption key pair history for all users, including a complete history of all decryption private keys, is stored encrypted in the CA database.

Subscriber encryption private keys stored by the CA are not destroyed.

Escrow of subscriber private keys is not performed by the CA.

Whether certificate suspension is supported 24

The CA does not support suspension of certificates.

Certificate Life Cycle Management

Initial registration, including a description of the CA's requirements for the identification and authentication of subscribers and validation of certificate requests during entity registration or certificate issuance:

25

- Types of names assigned to the subject and rules for interpreting various name forms
- Whether names have to be meaningful or not
- Whether names have to be unique
- How name claim disputes are resolved
- Recognition, authentication, and role of trademarks
- If and how the subject must prove possession of the companion private key for the public key being provided for a certificate
- How the subscriber's public key is provided securely to the CA for issuance of a certificate
- Authentication requirements for organizational identity of subject
- Authentication of individual identity
- Required certificate request data
- How the CA verifies the authority of the subscriber to request a certificate
- How the CA verifies the accuracy of the information included in the subscriber's certificate request
- Whether the CA checks certificate requests for errors or omissions

The CA has established a single naming hierarchy utilizing the X.500 Distinguished Name form.

In all cases, names of subjects must be meaningful. Generally, the name by which a subscriber is commonly known to the CA should be used. The CA does not support the use of pseudonyms in subscriber common names.

All subjects in the CA's PKI are unambiguously identified in the naming hierarchy.

When there is a conflict in distinguished names, such as a second "John Doe," then a middle initial, middle name, or other modification acceptable to the subscriber may be used to make the name unique.

The CA issues certificates within a closed PKI. Trademarks and related naming issues will generally not apply to certificates issued within this space.

Possession of a private key is proved by a certificate applicant by providing check values as defined in the certificate policy.

If organizational identity is considered important based upon the certificate policy, the organization identity is verified using a method approved by the certificate policy.

The requirements for authentication of individual identity are defined by the certificate policy [*hot link to certificate policy*].

In submitting a certificate application, at least the following information must be submitted to the CA: subscriber's public key, subscriber's distinguished name, and other information required on the CA's certificate application form.

If required by the certificate policy, the CA verifies the authority of the subscriber to request a certificate by checking whether the subscriber is an employee of a particular organization or association through inquiry of the organization's HR department or the association's membership department.

The CA verifies the accuracy of the information included in the subscriber's certificate request through validation against a third-party database.

The CA checks certificate requests for errors or omissions.

<p>Registration requirements where external RAs are used, including the CA's procedures for:</p> <ul style="list-style-type: none"> • Validating the identity of external RAs • Authorizing external RAs • Requirements for the external RA to secure that part of the certificate application, certificate renewal, and certificate rekey processes for which the RA assumes responsibility • How the CA verifies the authenticity of certificate request submissions received from an external RA 	<p>26</p>	<p>The CA requires that external registration authorities (RAs) physically present themselves along with two forms of identification to an employee of the CA.</p> <p>The CA authorizes external RAs upon successful identification and authentication, and approval of the external RA enrollment and certificate application forms.</p> <p>External RAs are responsible for identification and authentication of subscribers and must secure their private signing keys used for signing certificate applications, securely forward certificate applications to the CA, and securely store any subscriber information collected.</p> <p>The CA verifies the authenticity of certificate request submissions received from an external RA by validating the RA's digital signature on the submission.</p>
<p>Certificate renewal, including a description of the CA's procedures for the following:</p> <ul style="list-style-type: none"> • Notifying subscribers of the need for renewal • Identification and authentication • Renewal request verification 	<p>27</p>	<p>The certificate renewal process is similar to an application for a new certificate. However, the subscriber needs to provide only information that has changed.</p>
<p>Routine rekey, including a description of the identification and authentication and rekey request verification procedures</p>	<p>28</p>	<p>Authentication of the individual's identity as defined in the CA's identification and authentication requirements for initial registration need not be repeated unless required by the applicable certificate policy. Subscribers will be limited to rekeying no more than twice before repeating the authentication process defined in identification and authentication requirements for initial registration.</p>
<p>Rekey after revocation or expiration, including a description of the identification and authentication and rekey request verification procedures for rekey after the subject certificate has been revoked</p>	<p>29</p>	<p>For subscribers whose certificates have been revoked or have expired, rekey is permitted if the identification and authentication requirements for initial registration are repeated.</p>
<p>Certificate issuance, including a description of the requirements regarding the following:</p> <ul style="list-style-type: none"> • Issuance of a certificate • Notification to the applicant of such issuance • Certificate format requirements • Validity period requirements • Extension field requirements (that is, what extension fields are honored, and how they are to be populated) 	<p>30</p>	<p>Certificates are issued to the subscribers upon successful processing of the application and the acceptance of the certificates by the subscribers. Certificate format, validity period, extension field, and key usage extension field requirements are specified in accordance with the CA's disclosed certificate profile.</p>

Certificate acceptance, including a description of the requirements regarding acceptance of an issued certificate and for consequent publication of certificates	31	Once a certificate has been generated, it is maintained in a secure remote repository until it is retrieved by the subscriber. Upon retrieval of the certificate from the secure remote repository, the certificate status is updated to reflect its status as accepted and valid.
Certificate distribution, including a description of the CA's established mechanism (for example, a repository such as a directory) for making available to relying parties the certificates and CRLs that it issues	32	A single repository is operated for all subscribers and relying parties. All certificates issued by the CA and all certificate revocation lists (CRLs) relating thereto, shall be published in the repository. The repository for this CA is provided by an X.500 directory system. The protocol used to access the directory is the Lightweight Directory Access Protocol (LDAP) version 2.

Certificate revocation, including: 33

- Circumstances under which a certificate may or must be revoked
- Identification and authentication procedures required for revocation requests
- Procedures used for initiation, authorization, and verification of certificate revocation requests
- Revocation request grace period available to the subscriber
- Any variations on the preceding stipulations in the event that the revocation is the result of private key compromise (as opposed to other reasons for revocation)
- Procedures to provide a means of rapid communication to facilitate the secure and authenticated revocation of (1) one or more certificates of one or more entities; (2) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and (3) all certificates issued by a CA, regardless of the public/private key pair used
- Procedures for notifying the subscriber upon revocation of the subscriber's certificate
- Whether the external RA is notified upon the revocation of a subscriber's certificate for which the revocation request was processed by the external RA
- How and when the subscriber's certificate status information is updated upon certificate revocation

A certificate can be revoked for several reasons, including suspected or actual compromise of control of the private key that relates to the public key contained in the certificate, hardware or software failures that render the private key inoperable, or failure of a subscriber to meet the obligations of this certification policy statement (CPS) and the related certificate policy (CP). Other circumstances for revocation may be stipulated in the particular CP and may relate to changes in a subscriber's relationship with the CA, such as a change in customer or employee status or a change in the particular role of an employee.

Revocation may be requested by the subscriber, registration authority, or CA. Requests by RA personnel to revoke a certificate require sufficient RA system access rights. Requests by subscribers to revoke their own certificates require one of the following:

- A digitally signed message from the subscriber to the RA
- Personal presentation of the subscriber to the RA with a personal photo ID card
- Presentation of the pass phrase created by the subscriber at the point of initial application
- Other means as provided in the CP

A subscriber can request a certificate revocation online, via e-mail, or by telephone to the CA. If the request is made online and the end entity supplies the correct pass phrase, the certificate is revoked immediately. Certificate revocation requests made via e-mail or telephone are processed on a daily basis by the CA after the validity of such requests is ascertained. Validation procedures for telephone and e-mail revocation requests are defined in the CP. Validated certificate revocation requests will be processed no more than 24 hours after receipt. The CP may define a shorter time period for the processing of revocation requests.

Revocation requests for reasons other than key compromise must be placed within a maximum of 48 hours of the event necessitating revocation. In the case of suspected or known private key compromise, revocation request should be made immediately upon identification of the event.

The CA's certificate revocation process supports the secure and authenticated revocation of one or more certificates of one or more entities and provides a means of rapid communication of such revocation through the issuance of daily CRLs (or, if necessary, more frequent CRLs). The CA's system and processes provide the capability to revoke (1) the set of all certificates issued by the CA that have been signed with a single CA private signing key or (2) groups of certificates issued by the CA that have been signed with different CA private signing keys.

Upon revocation of the subscriber's certificate, the subscriber is notified via e-mail.

When a revocation request has been processed by an external registration authority, the external RA is also notified upon the revocation of a subscriber's certificate.

Upon the revocation of a subscriber's certificate, the newly revoked certificate is recorded in the next CRL that is issued.

Certificate suspension, including: 34 The CA does not support certificate suspension.

- Circumstances under which a certificate may or must be suspended
- Identification and authentication procedures required for revocation requests
- Procedures used for initiation, authorization, and verification of certificate suspension requests
- How long the suspension may last
- Circumstances under which the suspension of a certificate may or must be lifted
- Authorization criteria to request the lifting of a certificate suspension
- Any variations on the preceding stipulations if the suspension is the result of private key compromise (as opposed to other reasons for suspension)
- Procedures to provide a means of rapid communication to facilitate the secure and authenticated suspension of (1) one or more certificates of one or more entities; (2) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and (3) all certificates issued by a CA, regardless of the public/private key pair used
- Procedures for notifying the subscriber upon suspension of the subscriber's certificate
- Whether the external RA is notified upon the suspension of a subscriber's certificate for which the suspension request was processed or submitted by the external RA
- How and when the subscriber's certificate status information is updated upon certificate suspension and the lifting of a certificate suspension

Provision of certificate status information, including: 35

- What mechanism is used (CRLs, online certificate status protocol [OCSP], other)
- If a CRL mechanism is used, the issuance frequency
- Requirements on relying parties to check CRLs
- Online revocation and status checking availability
- Requirements on relying parties to perform online revocation and status checks
- Other forms of revocation advertisements available
- Requirements on relying parties to check other forms of revocation advertisements
- Any variations on the above stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation)
- The CA's requirements for archival and retention of CRLs or other certificate status information
- Whether copies of all certificates issued (including all expired, revoked, or suspended certificates) are retained and disclosure of the retention period
- If an online status mechanism is used (for example, OCSP), certificate status request content requirements
- If an online status mechanism is used (for example, OCSP), definitive response message data content requirements
- What key is used to digitally sign definitive response messages
- Whether the CA signs error messages when returned in response to certificate status requests

The CA issues CRLs once a day at 11:59 PM. In addition, the CA may issue interim CRLs in the event that personnel of the CA deem it necessary (that is, in the event of a serious private key compromise) or as dictated by certificate policy (CP).

As stated in the CP, CRL checking is required for all relying parties.

A subscriber is notified of the revocation of his or her certificate by e-mail, postal mail, or telephone. The CP may define other forms of revocation advertisements.

The CA archives and retains all certificates and CRLs issued by the CA for a period not less than 10 years.

The CA also supports online certificate revocation checking using OCSP.

The CA requires that OCSP requests contain the following data:

- Protocol version
- Service request
- Target certificate identifier
- Optional extensions which may be processed by the OCSP responder.

Definitive OCSP response messages include the following:

- Version of the response syntax
- Name of the responder
- Responses for each of the certificates in a request (including target certificate identifier, certificate status value, response validity interval, and optional extensions)
- Optional extensions
- Signature algorithm OID
- Signature computed across hash of the response

All definitive response messages are digitally signed with a key belonging to the CA that issued the certificate in question.

When the CA returns an error message in response to a certificate status request, the error message is not digitally signed.

<p>Certificate profile, including:</p> <ul style="list-style-type: none"> • Version number(s) supported • Certificate extensions populated and their criticality • Cryptographic algorithm object identifiers • Name forms (that is, naming hierarchy used to ensure that the certificate subject can be uniquely identified—if required) used for the CA, RA, and subscribers names • Name constraints used and the name forms used in the name constraints • Applicable certificate policy object identifier(s) • Usage of the policy constraints extension • Policy qualifiers syntax and semantics • Processing semantics for the critical certificate policy extension 	36	<p>The following fields in the X.509 certificate format are utilized in the CA's PKI:</p> <ul style="list-style-type: none"> • Version—Set to v3 • Serial number—Unique values for each certificate in the CA domain • Signature algorithm identifier The algorithm used by the CA for signing the certificate • Issuer—Identification of the certificate issuer • Validity—Start date and end date of the validity period are defined • Subject—Certificate subject's distinguished name • Public key information—Algorithm identifier (that is, RSA with SHA-1) and public key • Issuer unique identifier • Subject unique identifier • Extensions
<p>CRL profile, including:</p> <ul style="list-style-type: none"> • Version numbers supported for CRLs • CRL and CRL entry extensions populated and their criticality 	37	<p>The following fields of the X.509 CRL format are utilized by the CA:</p> <ul style="list-style-type: none"> • Version—v2 • Signature—Identifies algorithm used to sign CRL • Issuer—Identification of the CA issuing the CRL • This update—Time of CRL issue • Next update—Time of next anticipated CRL issue • Revoked certificates—Listing of information for revoked certificates <p>The CA may alternatively support online certificate status and revocation checking services.</p>
<p>Integrated circuit card (ICC) life cycle management, including:</p> <ul style="list-style-type: none"> • Whether ICCs are issued by the CA (or RA) • If supported, a description of the CA's ICC life cycle management processes, including a description of the ICC distribution process 	38	<p>The CA does not issue smart cards to subscribers. Subscribers may, at their own discretion, purchase smart cards and readers for purposes of key generation and storage.</p>

CA Environmental Controls

<p>CPS and CP administration:</p> <ul style="list-style-type: none"> • CPS and CP change control procedures • Publication and notification policies • CPS and CP approval procedures 	<p>39</p>	<p>Some revisions to this certification policy statement (CPS) may be deemed by the CA's policy authority to have minimal or no impact on subscribers and relying parties using certificates and CRLs issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS. Revisions to the certificate policies supported by this CPS, as well as revisions to the CPS which are deemed by the CA's policy authority to have significant impact on the users of this CPS, may be made with 45 days notice to the users and a change in version number for this CPS.</p> <p>The CA's policy authority will provide notification of upcoming changes on the CA's Web site 45 days prior to significant revisions to this CPS.</p> <p>This CPS and any subsequent changes are approved by the CA's policy authority.</p>
<p>CA termination, including a description of the CA's procedures for termination and for termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records</p>	<p>40</p>	<p>The CA can only be terminated by the board of directors of the CA. In the event the CA is terminated, all certificates issued under the CA will be revoked and the CA will cease to issue certificates. The CA will provide no less than one month notice to all business units utilizing the services of the CA. Upon termination, the records of the CA will be archived and transferred to a specified custodian.</p>

Confidentiality, including: 41

- Applicable statutory or regulatory requirements to keep information confidential
- Kinds of information to be kept confidential
- Kinds of information not considered confidential
- Disclosure of information concerning certificate revocation and suspension
- Release to law enforcement officials
- Release as part of civil discovery
- Disclosure upon owner's request
- Other information release circumstances

Information which is not considered by the CA to be public domain information is to be kept confidential.

Confidential information includes:

- Subscribers' private signing keys are confidential and are not provided to the CA or RA.
- Information specific to the operation and control of the CA, such as security parameters and audit trails, is maintained confidentially by the CA and is not released outside of the CA organization unless required by law.
- Information about subscribers held by the CA or RAs, excluding that which is published in certificates, CRLs, certificate policies, or this CPS, is considered confidential and shall not be released outside of the CA except as required by certificate policy or otherwise required by law.
- Generally, the results of annual audits are kept confidential, unless disclosure is deemed necessary by CA management.

Nonconfidential information includes:

- Information included in certificates and CRLs issued by the CA is not considered confidential.
- Information in the certificate policies supported by this CA is not considered confidential.
- Information in the CA's disclosed CPS (or other CA business practices disclosure) is not considered confidential.
- When the CA revokes a certificate, a revocation reason is included in the CRL entry for the revoked certificate. This revocation reason code is not considered confidential and can be shared with all other subscribers and relying parties. However, no other details concerning the revocation are normally disclosed.

The CA will comply with legal requirements to release information to law enforcement officials.

The CA may disclose to another party information pertaining to the owner of such information upon the owner's request.

Intellectual property rights 42

Public key certificates and CRLs issued by the CA are the property of the CA. This CPS and the related certificate policies are the property of the CA.

Physical security controls, including: 43

- Site location and construction
- Physical access controls, including authentication controls to control and restrict access to CA facilities
- Power and air conditioning
- Water exposures
- Fire prevention and protection
- Media storage
- Waste disposal
- Off-site backup

All critical CA operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Such systems are physically separated from the organization's other systems so that only authorized employees of the CA can access them.

Physical access to the CA systems is strictly controlled. Only trustworthy individuals with a valid business reason are provided such access. The access control system is always functional and utilizes proximity cards and biometrics for access.

All CA systems have industry standard power and air conditioning systems to provide a suitable operating environment.

All CA systems have reasonable precautions taken to minimize the impact of water exposure.

All CA systems have industry standard fire prevention and protection mechanisms in place.

Media storage at the CA third-party processor is subject to the same degree of protection as the CA hardware. Media storage under the control of the CA is subject to the normal media storage requirements of the company.

Waste is disposed of in accordance with the organization's normal waste disposal requirements. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal.

Off-site backups are stored in a physically secure manner by a bonded third-party storage facility.

Business continuity management controls, including: 44

- Whether the CA has business continuity plans to maintain or restore the CA's business operations in a reasonably timely manner following interruption to or failure of critical business processes
- Whether the CA's business continuity plans define an acceptable system outage and recovery time and disclosure of the defined time period(s)
- How frequently backup copies of essential business information and software are taken
- Proximity of recovery facilities to the CA's main site

The CA has a business continuity plan to restore the CA's business operations in a reasonably timely manner following interruption to, or failure of, critical business processes. The CA's business continuity plan defines 24 hours as an acceptable system outage time in the event of a major natural disaster or CA private key compromise.

Copies of essential business information and CA system software are performed daily.

The CA maintains a recovery site which is located approximately 50 miles from the CA's primary site.

<p>Event logging, including the following:</p> <ul style="list-style-type: none"> • How frequently the CA archives event journal data • How frequently event journals are reviewed 	45	<p>As part of the CA’s scheduled system backup procedures, audit trail files are backed up to media on at least a daily basis. Audit trail files are archived by the system administrator on a weekly basis.</p> <p>Event journals are reviewed at least on a weekly basis by CA management.</p>
--	----	--

Principle 2: Service Integrity

The certification authority maintains effective controls to provide reasonable assurance that:

- Subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and
- The integrity of keys and certificates it manages is established and protected throughout their life cycles.

Criteria

*Illustrative Controls
(Based on the CA Control Procedures
Detailed in the Draft ANS8.79 Standard)*

2.1 Key Life Cycle Management Controls

2.1.1 CA Key Generation

The certification authority (CA) maintains controls to provide reasonable assurance that CA key pairs are generated in accordance with industry standards.

Such controls generally include but are not limited to the following:

- | | |
|---|---|
| 1 | CA key generation occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA’s business practices (see Principle 1, item 18). |
| 2 | CA key generation by the CA requires dual control by properly authorized personnel. |
| 3 | The CA generates its own key pair in the same cryptographic device in which it will be used or the key pair is injected directly from the device where it was generated into the device in which it will be used. |
| 4 | Key generation uses a random number generator (RNG) or pseudo random number generator (PRNG) as specified in an ANSI X9 or ISO standard. |
| 5 | Key generation uses a prime number generator as specified in an ANSI X9 or ISO standard. |
| 6 | Key generation uses a key generation algorithm as specified in an ANSI X9 or ISO standard as disclosed in the CA’s business practices (Principle 1, item 18). |
| 7 | Key generation results in key sizes as disclosed in the CA’s business practices (Principle 1, item 18). |

- 8 The integrity of the hardware and software used for key generation and the interfaces to the hardware and software are tested before usage.

2.1.2 CA Key Storage, Backup, and Recovery

The CA maintains controls to provide 1 reasonable assurance that CA private keys remain confidential and maintain their integrity.

Such controls generally include but are not limited to the following:

- The CA’s private signing key is stored within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA’s business practices (Principle 1, item 17).
- 2 If the CA private key is not exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the CA private key is generated and used within the same cryptographic module and is never exported outside of the cryptographic module.
- 3 If the CA private key is exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the private key is exported in a secure key management scheme including any of the following:
 - a. As ciphertext using dual control
 - b. As encrypted key fragments using dual control and split knowledge/ownership
 - c. In another secure cryptographic module such as a key transportation device using dual control
- 4 The CA private key is backed up, stored, and recovered by authorized personnel using dual control in a physically secured environment.
- 5 If the CA’s private signing key is backed up, backup copies of the CA private keys are subject to the same or greater level of security controls as keys currently in use.
- 6 If the CA’s private signing key is backed up, recovery of the CA private key is conducted in the same secure schema used in the backup process, using dual control.

2.1.3 CA Public Key Distribution

The CA maintains controls to provide 1 reasonable assurance that the integrity and authenticity of the CA public key and any associated parameters are maintained during initial and subsequent distribution.

Such controls generally include but are not limited to the following:

- The CA provides a mechanism for detecting the modification of the CA’s public key during the initial distribution process (for example, using a self-signed certificate).
- 2 The initial distribution mechanism for the CA’s public key is controlled as disclosed in the CA’s business practices (Principle 1, item 20).
- 3 CA public keys are initially distributed using one of the following methods as disclosed in any one of the following CA’s business practices (Principle 1, item 20)
 - a. Machine readable media (for example, smart card)
 - b. Embedding in an entity’s cryptographic module
 - c. Other secure means

- 4 The CA's public key is changed (rekeyed) periodically as disclosed in the CA's business practices (Principle 1, item 21).
- 5 The subsequent distribution mechanism for the CA's public key is controlled as disclosed in the CA's business practices (Principle 1, item 21).
- 6 If an entity already has an authenticated copy of the CA's public key, a new CA public key is distributed using one of the following methods as disclosed in the CA's business practices (Principle 1, item 21):
 - a. Direct electronic transmission from the CA
 - b. Placing into a remote cache or directory
 - c. Loading into a cryptographic module
 - d. Any of the methods used for initial distribution

2.1.4 CA Key Escrow (Optional)

The CA maintains controls to provide reasonable assurance that escrowed CA private signing keys remain confidential.

Such controls generally include but are not limited to the following:

If a third party provides CA private key escrow services, a contract outlining the liabilities and remedies between the parties exists.

- 2 If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys are subject to the same or greater level of security controls as keys currently in use.

2.1.5 CA Key Usage

The CA maintains controls to provide reasonable assurance that CA keys are used only for their intended functions in their intended locations.

Such controls generally include but are not limited to the following:

The activation of the CA private signing key is performed using multiparty control (that is, *m of n*).

- 2 If necessary based on a risk assessment, the activation of the CA private signing key is performed using multi-factor authentication (for example, smart card and password, biometric, and password).
- 3 The CA ceases to use a key pair at the end of the cryptoperiod or when the compromise of the private key is known or suspected.

2.1.6 CA Key Destruction

The CA maintains controls to provide reasonable assurance that CA keys are completely destroyed at the end of the key pair life cycle.

Such controls generally include but are not limited to the following:

Authorization to destroy a CA private key and how the CA's private key is destroyed (for example, token surrender, token destruction, or key overwrite) are limited as disclosed in the CA's business practices (Principle 1, item 17).

- 2 All copies and fragments of the CA's private key are destroyed at the end of the key pair life cycle.
- 3 If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed.

- 4 If a CA cryptographic device is being permanently removed from service, any key contained within the device that has been used for any cryptographic purpose is erased from the device.
- 5 If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, the case is destroyed.

2.1.7 CA Key Archival

The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential and are never put back into production.

Such controls generally include but are not limited to the following:

Archived CA keys are subject to the same or greater level of security controls as keys currently in use.

- 2 All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site.
- 3 Archived keys are never put back into production.
- 4 Archived keys are recovered for the shortest time period technically permissible.
- 5 Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.

2.1.8 CA Cryptographic Hardware Life Cycle Management

The CA maintains controls to provide reasonable assurance that access to CA cryptographic hardware is limited to properly authorized individuals.

For purposes of this section, CA cryptographic hardware refers to devices containing CA private signing keys.

Such controls generally include but are not limited to the following:

- 1 Policies and procedures require that CA cryptographic hardware be sent from the manufacturer via registered mail using tamper-evident packaging.
- 2 Upon the receipt of CA cryptographic hardware from the manufacturer, authorized CA personnel inspect the tamper-evident packaging to determine whether the seal is intact.
- 3 To prevent tampering, CA cryptographic hardware is stored in a secure site, with access limited to authorized personnel, having the following characteristics:
 - a. Inventory control processes and procedures to manage the origination, arrival, condition, departure, and destination of each device
 - b. Access control processes and procedures to limit physical access to authorized personnel
 - c. All successful or failed access attempts to the CA facility and device storage mechanism (for example, a safe) recorded in an event journal
 - d. Incident processes and procedures to handle abnormal events, security breaches, and investigation and reports
 - e. Audit processes and procedures to verify the effectiveness of the controls

- 4 CA cryptographic hardware is stored in tamper-resistant packages.
- 5 The handling of CA cryptographic hardware is performed in the presence of no less than two trusted employees.
- 6 The installation of CA cryptographic hardware is performed in the presence of no less than two trusted employees.
- 7 The removal of CA cryptographic hardware from production is performed in the presence of no less than two trusted employees.
- 8 The process whereby CA cryptographic hardware is serviced or repaired with new hardware, firmware, or software is performed in the presence of no less than two trusted employees.
- 9 The service or repair site is a secure site with inventory control and access limited to authorized personnel.
- 10 The process whereby CA cryptographic hardware is disassembled and permanently removed from use is performed in the presence of no less than two trusted employees.

The CA maintains controls to provide 11 reasonable assurance that CA cryptographic hardware is functioning correctly.

Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed.

- 12 Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings is performed.
- 13 Devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.
- 14 Correct processing of CA cryptographic hardware is verified on a periodic basis.
- 15 Diagnostic support is provided during troubleshooting of CA cryptographic hardware in the presence of no less than two trusted employees.

2.1.9 CA-Provided Subscriber Key Management Services (Optional)

For purposes of this section, subscriber includes external registration authorities (RAs).

Such controls generally include but are not limited to the following:

The CA maintains controls to provide 1 reasonable assurance that subscriber keys generated by the CA (or registration authority [RA]) are generated in accordance with industry standards.

Subscriber key generation performed by the CA (or RA) occurs within a secure cryptographic device meeting the appropriate ISO 15782-1/FIPS 140-1/ANSI X9.66 level requirement as disclosed in the CA’s business practices (Principle 1, item 18).

- 2 Subscriber key generation performed by the CA (or RA) uses a random number generator (RNG) or pseudo random number generator (PRNG) as specified in an ANSI X9 or ISO standard.
- 3 Subscriber key generation performed by the CA (or RA) uses a prime number generator as specified in an ANSI X9 or ISO standard.
- 4 Subscriber key generation performed by the CA (or RA) uses a key generation algorithm as specified in an ANSI X9 or ISO standard as disclosed in the CA's business practices (Principle 1, item 18).
- 5 Subscriber key generation performed by the CA (or RA) results in key sizes as disclosed in the CA's business practices (Principle 1, item 18).
- 6 Subscriber key generation performed by the CA (or RA) is performed by authorized personnel as disclosed in the CA's business practices (Principle 1, item 18).
- 7 When subscriber key generation is performed by the CA (or RA), the CA (or RA) securely (confidentially) delivers the key pair(s) generated by the CA (or RA) on behalf of the subscriber to the subscriber as disclosed in the CA's business practices (Principle 1, item 18).

The CA maintains controls to provide reasonable assurance that subscriber private keys stored by the CA remain confidential and maintain their integrity.

Subscriber private keys stored by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the business requirements of the CA.

- 9 If the CA generates key pair(s) on behalf of a subscriber, the CA ensures that subscriber's private keys are not disclosed to any entity other than the owner of the keys.
- 10 If the CA generates public/private digital signature key pair(s), the CA does not maintain a copy of any digital signature private key, once that key is delivered to the subscriber.
- 11 If the CA provides subscriber key storage, backup, and recovery, subscriber private key backup and recovery is performed only by authorized personnel.
- 12 If the CA provides subscriber key storage, backup, and recovery, controls exist to ensure that the integrity of the subscriber's private key is maintained throughout its life cycle.

The CA maintains controls to provide reasonable assurance that subscriber keys stored by the CA are completely destroyed at the end of the key pair life cycle.

If the CA provides subscriber key storage, authorization to destroy a subscriber's private key and the means to destroy the subscriber's private key (for example, key overwrite) are limited as disclosed in the CA's business practices (Principle 1, item 22).

- 14 If the CA provides subscriber key storage, all copies and fragments of the subscriber's private key are destroyed at the end of the key pair life cycle.

The CA maintains controls to provide reasonable assurance that subscriber keys archived by the CA remain confidential.

Subscriber private keys archived by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the business requirements of the CA.

16 If the CA provides subscriber key archival, all archived subscriber keys are destroyed at the end of the archive period.

The CA maintains controls to provide reasonable assurance that subscriber keys escrowed by the CA remain confidential.

Subscriber private keys escrowed by the CA are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the business requirements of the CA.

2.2 Certificate Life Cycle Management Controls

2.2.1 Subscriber Registration

Note: A requesting entity may be a subscriber requesting a certificate from an RA or CA, an RA requesting a certificate from a CA, or a subordinate CA requesting a certificate from a root CA or superior CA.

Such controls generally include but are not limited to the following:

The CA maintains controls to provide reasonable assurance that subscribers are properly identified and authenticated.

The CA verifies or requires that the external RA verify the identity of the entity requesting a certificate as disclosed in the CA's business practices (Principle 1, item 25).

2 The CA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data (registration request) to an RA (or the CA) as disclosed in the CA's business practices (Principle 1, item 25).

3 The CA verifies or requires that the external RA verify the authority of the entity requesting a certificate as disclosed in the CA's business practices (Principle 1, item 25).

4 The CA verifies or requires that the external RA verify the accuracy of the information included in the requesting entity's certificate request as disclosed in the CA's business practices (Principle 1, item 25).

5 If external RAs are used, the CA validates the identity of external RAs as disclosed in the CA's business practices (Principle 1, item 26).

6 If external registration authorities are used, the CA authorizes external RAs as disclosed in the CA's business practices (Principle 1, item 26).

The CA maintains controls to provide reasonable assurance that subscriber certificate requests are accurate, authorized, and complete.

The CA requires that an entity requesting a certificate prepare and submit the appropriate certificate request data to the CA or an external RA as disclosed in the CA's business practices (Principle 1, item 25).

- 8 The CA requires that the requesting entity submit its public key in a signed message to the CA for certification. The CA requires that the requesting entity digitally sign the registration request using the private key that relates to the public key contained in the registration request in order to:
 - a. Allow the detection of errors in the certificate application process.
 - b. Prove possession of the companion private key for the public key being registered.
- 9 The CA uses the public key contained in the requesting entity's certificate request to verify the requesting entity's signature on the certificate request submission.
- 10 If an external RA is used, the CA requires that the external RA submits the requesting entity's certificate request data to the CA in a message (certificate request) signed by the RA.
- 11 If an external RA is used, the CA requires that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility as disclosed in the CA's business practices (Principle 1, item 26).
- 12 If an external RA is used, the CA requires that the external RA records its actions in an event journal.
- 13 If an external RA is used, the CA verifies the authenticity of the submission by the RA as disclosed in the CA's business practices (Principle 1, item 26).
- 14 If an external RA is used, the CA verifies the RA's signature on the certificate request.
- 15 The CA or RA checks the certificate request for errors or omissions as disclosed in the CA's business practices (Principle 1, item 25).
- 16 The CA verifies the uniqueness of the requesting entity's distinguished name within the CA's domain.
- 17 The CA accepts the certificate request from the requesting entity whose identity has been validated.
- 18 When the CA detects duplicate public keys, the certificate request is rejected and the original certificate is revoked.

2.2.2 Certificate Renewal (Optional)

The CA maintains controls to provide 1 reasonable assurance that certificate renewal requests are accurate, authorized, and complete.

Such controls generally include but are not limited to the following:

- 1 The subscriber's certificate renewal request includes at least the subscriber's distinguished name, the serial number of the certificate (or other information that identifies the certificate), and the requested validity period to allow the CA or the RA to identify the certificate to renew.
- 2 The CA requires that the requesting entity digitally sign the certificate renewal request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.

- 3 The CA or the RA processes the certificate renewal data to verify the identity of the requesting entity and identify the certificate to be renewed.
- 4 The CA or the RA validates the signature on the certificate renewal request.
- 5 The CA or the RA verifies the existence and validity of the certificate to be renewed.
- 6 The CA or the RA verifies that the request, including the extension of the validity period, meets the requirements as disclosed in the CA's business practices (Principle 1, item 28).
- 7 If an external RA is used, the CA requires that the external RA submits the requesting entity's certificate request data to the CA in a message (certificate renewal request) signed by the RA.
- 8 When an external RA is used, the RA secures that part of the certificate renewal process for which it (the RA) assumes responsibility as disclosed in the CA's business practices (Principle 1, item 26).
- 9 If an external RA is used, the CA requires that the external RAs record its actions in an event journal.
- 10 If an external RA is used, the CA verifies the authenticity of the submission by the RA.
- 11 If an external RA is used, the CA verifies the RA's signature on the certificate renewal request.
- 12 The CA or RA checks the certificate renewal request for errors or omissions.
- 13 The CA or RA notifies subscribers prior to the expiration of their certificate of the need for renewal as disclosed in the CA's business practices (Principle 1, item 27).
- 14 Prior to certificate generation and issuance of renewed certificates, the CA or RA verifies the following:
 - a. The signature on the certificate renewal data submission
 - b. The existence and validity of the certificate to be renewed
 - c. That the request, including the extension of the validity period, meets the requirements as disclosed in the CA's business practices (Principle 1, item 27)

2.2.3 Certificate Rekey

The CA maintains controls to provide 1 reasonable assurance that certificate rekey requests are accurate, authorized, and complete.

Such controls generally include but are not limited to the following:

- 1 The subscriber's certificate rekey request includes at least the subscriber's distinguished name, the serial number of the certificate, and the requested validity period to allow the CA or the RA to identify the certificate to rekey.
- 2 The CA requires that the requesting entity digitally sign the certificate rekey request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.

- 3 The CA or the RA processes the certificate rekey request to verify the identity of the requesting entity and identify the certificate to be rekeyed.
- 4 The CA or the RA validates the signature on the certificate rekey request.
- 5 The CA or the RA verifies the existence and validity of the certificate to be rekeyed.
- 6 The CA or the RA verifies that the certificate rekey request meets the requirements as disclosed in the CA's business practices (Principle 1, item 28).
- 7 If an external RA is used, the CA requires that the external RA submits the requesting entity's certificate rekey request to the CA in a message signed by the RA.
- 8 If an external RA is used, the CA requires that the RA secure that part of the certificate rekey process for which it (the RA) assumes responsibility as disclosed in the CA's business practices (Principle 1, item 26).
- 9 If an external RA is used, the CA requires that the external RA records its actions in an event journal.
- 10 If an external RA is used, the CA verifies the authenticity of the submission by the RA.
- 11 If an external RA is used, the CA verifies the RA's signature on the certificate rekey request.
- 12 The CA or the RA checks the certificate rekey request for errors or omissions.
- 13 The CA or RA notifies subscribers prior to the expiration of their certificate of the need for rekey.
- 14 Prior to the generation and issuance of rekeyed certificates, the CA or RA verifies the following:
 - a. The signature on the certificate renewal data submission
 - b. The existence and validity of the certificate to be renewed
 - c. That the request, including the extension of the validity period, meets the requirements as disclosed in the CA's business practices (Principle 1, item 28)

The CA maintains controls to provide reasonable assurance that certificate rekey requests following certificate revocation or expiration are accurate, authorized, and complete.

Following the revocation or expiration of a subscriber's existing certificate, the subscriber is required to follow the CA's subscriber registration procedures to obtain a new rekeyed certificate (as specified in §2.2.1, Subscriber Registration) as disclosed in the CA's business practices (Principle 1, item 29).

2.2.4 Certificate Issuance

The CA maintains controls to provide reasonable assurance that new, renewed, and rekeyed certificates are generated and issued in accordance with the CA's disclosed business practices.

Such controls generally include but are not limited to the following:

The CA generates certificates using the appropriate certificate format as disclosed in the CA's business practices (Principle 1, item 30).

- 2 The CA generates certificates in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30).
- 3 Validity periods are set in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30).
- 4 Extension fields are set in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30).
- 5 Key usage extension fields are set in accordance with ISO 9594/X.509 as disclosed in the CA's business practices (Principle 1, item 30).
- 6 The CA signs the requesting entity's certificate with the CA's private signing key.
- 7 The CA issues the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices (Principle 1, item 31).
- 8 When an RA is used, the CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.
- 9 For certificate renewals, the CA generates and signs a new instance of the certificate, differing from the previous certificate only by the validity period and the CA signature, only if the CA has approved the certificate renewal request as specified in §2.2.2, Certificate Renewal.
- 10 For rekeyed certificates, the CA generates and signs a new certificate only if the CA has approved the certificate rekey request as specified in §2.2.3, Certificate Rekey.
- 11 The CA issues an out-of-band notification to the requesting entity when a certificate is issued.

2.2.5 Certificate Distribution

The CA maintains controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to subscribers and relying parties in accordance with the CA's disclosed business practices.

Such controls generally include but are not limited to the following:

The CA makes the certificates issued by the CA available to relying parties using an established mechanism (for example, a repository such as a directory) as disclosed in the CA's business practices (Principle 1, item 32).

- 2 Upon certificate issuance, the CA posts certificates to the repository or alternative distribution mechanism as disclosed in the CA's business practices (Principle 1, item 32).
- 3 Only authorized CA personnel may administer the CA's repository or alternative distribution mechanism.
- 4 The performance of the CA's repository or alternative distribution mechanism is monitored and managed.
- 5 The integrity of the repository or alternative distribution mechanism is maintained.

2.2.6 Certificate Revocation

Such controls generally include but are not limited to the following:

The CA maintains controls to provide reasonable assurance that certificates are revoked based on authorized and validated certificate revocation requests.

As disclosed in the CA's business practices (Principle 1, item 33), the CA provides a means of rapid communication to facilitate the secure and authenticated revocation of the following:

- a. One or more certificates of one or more entities
- b. The set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates
- c. All certificates issued by a CA, regardless of the public/private key pair used

2 The CA verifies or requires that the external RA verify the identity and authority of the entity requesting revocation of a certificate as disclosed in the CA's business practices (Principle 1, item 33).

3 If an external RA accepts revocation requests, the CA requires that the RA submit certificate revocation requests to the CA in an authenticated manner as disclosed in the CA's business practices (Principle 1, item 33).

4 If an external RA accepts and forwards revocation requests to the CA, the CA provides an authenticated acknowledgement of the revocation to the requesting RA as disclosed in the CA's business practices (Principle 1, item 33).

5 The CA updates the certificate revocation list (CRL) and other certificate status mechanisms upon certificate revocation as disclosed in the CA's business practices (Principle 1, item 33).

6 The CA records all certificate revocation requests and their outcome in an event journal.

7 The CA or RA provides an authenticated acknowledgement of the revocation to the entity whose certificate has been revoked as disclosed in the CA's business practices (Principle 1, item 33).

8 Where certificate renewal is supported, when a certificate is revoked all valid instances of the certificate are also revoked.

2.2.7 Certificate Suspension (Optional)

The CA maintains controls to provide reasonable assurance that certificates are suspended based on authorized and validated certificate suspension requests.

Such controls generally include but are not limited to the following:

As disclosed in the CA's business practices (Principle 1, item 34), the CA provides a means of rapid communication to facilitate the secure and authenticated suspension of the following:

- a. One or more certificates of one or more entities
- b. The set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates
- c. All certificates issued by a CA, regardless of the public/private key pair used

2 The CA verifies or requires that the external RA verify the identity and authority of the entity requesting suspension of a certificate as disclosed in the CA's business practices (Principle 1, item 34).

3 If an external RA accepts suspension requests, the RA submits certificate suspension requests to the CA in an authenticated manner as disclosed in the CA's business practices (Principle 1, item 34).

4 The CA or RA notifies the end entity in the event of a certificate suspension as disclosed in the CA's business practices (Principle 1, item 34).

- 5 Certificate suspension requests are processed and validated as disclosed in the CA's business practices (Principle 1, item 34).
- 6 The CA updates the certificate revocation list (CRL) and other certificate status mechanisms upon certificate suspension as disclosed in the CA's business practices (Principle 1, item 34).
- 7 Certificates are suspended only for the allowable length of time as disclosed in the CA's business practices (Principle 1, item 34).
- 8 Once a certificate suspension (hold) has been issued, the suspension is handled in one of the following three ways:
- a. An entry for the suspended certificate remains on the CRL with no further action, causing users to reject transactions issued during the hold period
 - b. The CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate
 - c. The suspended certificate is explicitly released and the entry removed from the CRL
- 9 A certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first.
- 10 The CA updates the CRL and other certificate status mechanisms upon the lifting of a certificate suspension as disclosed in the CA's business practices (Principle 1, item 34).
- 11 The CA verifies or requires that the external RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.
- 12 Certificate suspensions and the lifting of certificate suspensions are recorded in an event journal.

2.2.8 Certificate Status Information Processing

The CA maintains controls to provide 1 reasonable assurance that timely, complete, and accurate certificate status information (including certificate revocation lists [CRLs] and other certificate status mechanisms) is made available to subscribers and relying parties.

Such controls generally include but are not limited to the following:

Certificate status information is made available to all relevant entities as disclosed in the CA's business practices (Principle 1, item 35).

- 2 The CA makes each certificate revocation list (CRL) issued by the CA available to relying parties using an established mechanism (for example, a repository such as a directory) as disclosed in the CA's business practices (Principle 1, item 35).
- 3 The CA digitally signs each CRL that it issues so that entities can validate the integrity of the CRL and the date of issuance.

- 4 The CA issues CRLs at regular intervals, even if no changes have occurred since the last issuance, as disclosed in the CA's business practices (Principle 1, item 35).
- 5 At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period.
- 6 If certificate suspension is supported, a certificate suspension (hold) entry with its original action date and expiration date remains on the CRL until the normal expiration of the certificate.
- 7 CRLs are archived as disclosed in the CA's business practices (Principle 1, item 35).
- 8 CAs include a monotonically increasing sequence number for each CRL issued by that CA (for example, 1, 2, 3).
- 9 The CRL contains entries for all revoked unexpired certificates issued by the CA.
- 10 Old CRLs are retained for the appropriate period of time as disclosed in the CA's business practices (Principle 1, item 35).
- 11 Whether certificates expire, are revoked, or are suspended, copies of certificates are retained for the appropriate period of time as disclosed in the CA's disclosed business practices (Principle 1, item 35).
- 12 If an online certificate status mechanism (for example, OCSP) is used, the CA requires that certificate status inquiries (for example, OCSP requests) contain all required data as disclosed in the CA's business practices (Principle 1, item 35).
- 13 Upon the receipt of a certificate status request (for example, an OCSP request) from a relying party, the CA returns a definitive response to the relying party if:
- a. The request message is well formed;
 - b. The responder is configured to provide the requested service; and
 - c. The request contains the information needed by the responder as disclosed in the CA's business practices (Principle 1, item 35).
- 14 All definitive response messages are digitally signed as disclosed in the CA's business practices (Principle 1, item 35).
- 15 Definitive response messages include all required data as disclosed in the CA's business practices (Principle 1, item 35).
- 16 If any of the three conditions (specified in item 13) are not met, the CA produces a signed or unsigned error message as disclosed in the CA's business practices (Principle 1, item 35).

2.2.9 Integrated Circuit Card (ICC) Life Cycle Management (Optional)

Note: For purposes of this section, integrated circuit cards (for example, smart cards) include devices that may hold a subscriber's private key(s) and certificate(s).

Such controls generally include but are not limited to, the following:

The CA maintains controls to provide 1 reasonable assurance that ICC preparation is securely controlled by the CA (or RA).	The CA (or RA), as the card issuer, controls ICC personalization (the loading of common data file (CDF) data and its related cryptographic keys).
2	Common data that identify the ICC, the card issuer, and the cardholder are stored by the card issuer in the ICC CDF). CDF activation is performed by the CA (or RA), as the card issuer, using a securely controlled process.
3	After CDF activation, the ICC indicates a CDF activated status.
4	The CA (or RA) logs ICC personalization and CDF activation.
The CA maintains controls to provide 5 reasonable assurance that ICC application data file (ADF) preparation is securely controlled by the CA (or RA).	Specific application supplier data stored in the ICC is located in the application data file (ADF). ADF allocation (the allocation of memory areas in an integrated circuit) is securely controlled by the CA, as the card issuer.
6	The CA, as the application supplier, controls ADF personalization (the loading of ADF related keys and data).
7	The CA, as the card issuer, controls ADF activation (preparation of an ADF for use by the cardholder) using a securely controlled process.
8	An ADF can only be activated when the CDF is either in an activated or a reactivated state.
9	After ADF activation, the ICC indicates an ADF activated status.
10	The CA logs ADF allocation, personalization, and activation.
The CA maintains controls to provide 11 reasonable assurance that ICC usage is enabled by the CA (or RA) prior to ICC issuance.	An ICC is not issued unless the card has been personalized.
12	An ICC is unusable unless the CDF is in an activated or a reactivated state.
The CA maintains controls to provide 13 reasonable assurance that ICCs are securely stored and distributed by the CA (or RA).	ICCs are securely stored prior to distribution.
14	Receipt, activation, and distribution of ICCs are logged in an event journal. An inventory of ICCs and their status is maintained.
15	ICCs are securely distributed as disclosed in the CA's business practices (Principle 1, item 38).
The CA maintains controls to provide 16 reasonable assurance that ICC deactivation and reactivation are securely controlled by the CA (or RA).	ADF deactivation can be performed only by the CA, as the application supplier.
17	CDF deactivation can be performed only by the CA, as the card issuer.
18	CDF reactivation is conducted under the control of the CA, as the card issuer.

	19	ADF reactivation is conducted under the control of the CA, as the application supplier.
	20	ADF deactivation, CDF deactivation, CDF reactivation, and ADF reactivation are logged.
The CA maintains controls to provide reasonable assurance that the use of ICCs is securely terminated for ICCs returned to the CA (or RA).	21	The CA, as the application supplier, controls ADF termination.
	22	CDF termination is controlled by the CA, as the card issuer.

Principle 3: CA Environmental Controls

The certification authority maintains effective controls to provide reasonable assurance that:

- Subscriber and relying party information is restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations is maintained; and
- CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.

Criteria

*Illustrative Control
(Based on the CA Control
Procedures Detailed in
the Draft ANSI
X9.79 Standard)*

3.1 Certification Practice Statement and Certificate Policy Management

The CA maintains controls to provide reasonable assurance that the CA's certification policy statement (CPS) and certificate policy (CP) management controls are effective.

Such controls generally include but are not limited to the following:

The CA organization has a management group with final authority and responsibility for specifying and approving the CA's certification practice statement (CPS).

- | | |
|---|--|
| 2 | There is a policy management authority with final authority and responsibility for specifying and approving certificate policy(s) (CPs). |
| 3 | The policy management authority (or equivalent group) has performed an assessment to evaluate business risks and determine the security requirements and operational procedures to be included in the applicable CP and/or CPS for the following: <ul style="list-style-type: none"> a. Key life cycle management controls b. Certificate life cycle management controls c. CA environmental controls |

- 4 The CA's CPS is approved and modified in accordance with a defined review process, including responsibilities for maintaining the CPS.
- 5 The CA makes available its public CPS to all appropriate subscribers and relying parties.
- 6 Revisions to the CA's CPS are made available to subscribers and relying parties.
- 7 CPs are approved and modified in accordance with a defined review process, including responsibilities for maintaining the CPs.
- 8 A defined review process exists to ensure that CPs are supported by the CA's CPS.
- 9 The CA makes available the CPs supported by the CA to all appropriate subscribers and relying parties.
- 10 Revisions to CPs supported by the CA are made available to subscribers and relying parties.

3.2 Security Management

The CA maintains controls to provide reasonable assurance that management direction and support for information security is provided.

- Such controls generally include but are not limited to the following:**
- 1 An information security policy document (*security policy*) is approved by management, published, and communicated, as appropriate, to all employees.
 - 2 The security policy contains a definition of information security, its overall objectives and scope, and the importance of security as an enabling mechanism for information sharing.
 - 3 The security policy contains a statement of management intent, supporting the goals and principles of information security.
 - 4 The security policy contains an explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization, including the following:
 - a. Compliance with legislative and contractual requirements
 - b. Security education requirements
 - c. Prevention and detection of viruses and other malicious software
 - d. Business continuity management
 - e. The consequences of security policy violations

	5	The security policy contains a definition of general and specific responsibilities for information security management, including reporting security incidents.
	6	The security policy contains references to documentation which supports the policy.
	7	There is a defined review process, including responsibilities and review dates, for maintaining the security policy.
The CA maintains controls to provide reasonable assurance that information security is properly managed within the organization.	8	Senior management and/or a high level management information security committee ensures there is clear direction and visible management support for security initiatives.
	9	A management group or security committee exists to coordinate the implementation of information security measures.
	10	Responsibilities for the protection of individual assets and for carrying out specific security processes are clearly defined.
	11	A management authorization process for new information processing facilities exists and is followed.
The CA maintains controls to provide reasonable assurance that the security of CA facilities, systems, and information assets accessed by third parties is maintained.	12	Procedures exist and are followed to control physical and logical access to CA facilities and systems by third parties including on-site contractors and trading partners or joint ventures.
	13	If there is a business need for the CA to allow third-party access to CA facilities and systems, a risk assessment is performed to determine security implications and specific control requirements.
	14	Arrangements involving third-party access to CA facilities and systems are based on a formal contract containing all necessary security requirements.
The CA maintains controls to provide reasonable assurance that the security of information is maintained when the responsibility for CA functions has been outsourced to another organization or entity.	15	If the CA outsources the management and control of all or some of its information systems, networks, or desktop environments, the security requirements of the CA are addressed in a contract agreed to by the parties.

	16	A CA service provider may choose to delegate a portion of the CA roles and respective functions, and the CA service provider is ultimately responsible for the completion of the identified functions that it performs and the definition and maintenance of a statement of its certification practices (that is, certification practice statement).
3.3 Asset Classification and Management		Such controls generally include but are not limited to the following:
The CA maintains controls to provide reasonable assurance that CA assets and information receive an appropriate level of protection.	1	Owners are identified for all major CA assets and assigned responsibility for the maintenance of appropriate controls.
	2	Inventories of important CA assets are maintained.
	3	The CA has implemented information classification and associated protective controls for information that take account of business needs for sharing or restricting information, and the business impacts associated with such needs.
	4	Procedures are defined to ensure that information labeling and handling is performed in accordance with the CA's information classification scheme.
3.4 Personnel Security		Such controls generally include but are not limited to the following:
The CA maintains controls to provide reasonable assurance that personnel and hiring practices enhance and support the trustworthiness of the CA's operations.	1	Security roles and responsibilities, as specified in the organization's security policy, are documented in job descriptions.
	2	Verification checks on permanent staff are performed at the time of job application. The CA's policies and procedures specify the background checks and clearance procedures required for the personnel filling the trusted roles, and other personnel, including janitorial staff.
	3	Employees sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment.

- 4 Contracting personnel controls include the following:
 - a. Bonding requirements on contract personnel
 - b. Contractual requirements including indemnification for damages due to the actions of the contractor personnel
 - c. Audit and monitoring of contractor personnel

- 5 All employees of the organization and, where relevant, third-party users, receive appropriate training in organizational policies and procedures. The CA's policies and procedures specify the following:
 - a. The training requirements and training procedures for each role
 - b. Any retraining period and retraining procedures for each role

- 6 Periodic reviews occur to verify the continued trustworthiness of personnel involved in the activities related to key management and certificate management.

- 7 A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. The CA's policies and procedures specify the sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems.

- 8 Appropriate and timely actions are taken when an employee is terminated so that controls and security are not impaired by such an occurrence.

3.5 Physical and Environmental Security

The CA maintains controls to provide reasonable assurance that physical access to CA facilities is limited to properly authorized individuals and CA facilities are protected from environmental hazards.

- 1 **Such controls generally include but are not limited to the following:** Physical protection is achieved through the creation of clearly defined security perimeters (meaning, physical barriers) around the business premises and CA facilities.
- 2 The perimeter of the building or site containing the CA facility is physically sound (that is, there should be no gaps in the perimeter where a break-in could easily occur).

- 3 A manned reception area or other means to control physical access is in place to restrict access to the building or site housing CA operations to authorized personnel only.
- 4 To prevent unauthorized entry and environmental contamination, proper physical barriers are in place (for example, extended from real floor to real ceiling as opposed to raised floor to suspended ceiling) as disclosed in the CA's business practices (Principle 1, item 43).
- 5 All fire doors on security perimeters around the CA facilities are alarmed and slam shut.
- 6 Intruder detection systems are installed and regularly tested to cover all external doors of the building housing the CA facility and the CA facility itself.
- 7 The CA facility is alarmed when unoccupied.
- 8 The CA facility is physically locked and periodically checked when vacant.
- 9 Unsupervised working in secure CA facilities is not allowed both for safety reasons and to prevent opportunities for malicious activities.
- 10 All personnel are required to wear visible identification and are encouraged to challenge anyone not wearing visible identification.
- 11 Access to CA facilities is controlled and restricted to authorized persons through the use of authentication controls as disclosed in the CA's business practices (Principle 1, item 43).
- 12 All personnel entering and leaving the CA facility are logged (that is, an audit trail of all access is securely maintained).
- 13 Visitors to the CA facility are supervised and their date and time of entry and departure recorded.
- 14 Third-party support services personnel are granted restricted access to secure CA facilities only when required and such access is authorized and monitored.
- 15 Access rights to the CA facility are regularly reviewed and updated.

The CA maintains controls to provide reasonable assurance that loss, damage, or compromise of assets and interruption to business activities are prevented.	16	Equipment is sited or protected such as to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
	17	Equipment is protected from power failures and other electrical anomalies.
	18	Power and telecommunications cabling carrying data or supporting CA services is protected from interception or damage.
	19	Equipment is maintained in accordance with the manufacturer's instructions and/or other documented procedures to ensure its continued availability and integrity.
	20	All items of equipment containing storage media (that is, fixed hard disks) are checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information are physically destroyed or securely overwritten prior to disposal or reuse.
The CA maintains controls to provide reasonable assurance that compromise or theft of information and information processing facilities are prevented.	21	Sensitive or critical business information is locked away when not required and when the CA facility is vacated.
	22	Personal computers and workstations are not left logged on when unattended and are protected by key locks, passwords, or other controls when not in use.
	23	Equipment, information, and software belonging to the organization cannot be taken off-site without authorization.

3.6 Operations Management

The CA maintains controls to provide reasonable assurance that the correct and secure operation of CA information processing facilities is ensured.	1	CA operating procedures are documented and maintained.
	2	Formal management responsibilities and procedures exist to control all changes to CA equipment, software, and operating procedures.
	3	Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.

	4	Development and testing facilities are separated from operational facilities.
	5	Prior to using external facilities management services, risks are identified and appropriate controls are agreed upon with the contractor and incorporated into the contract.
The CA maintains controls to provide reasonable assurance that the risk of CA systems failure is minimized.	6	Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.
	7	Acceptance criteria for new information systems, upgrades, and new versions are established and suitable tests of the system are carried out prior to acceptance.
The CA maintains controls to provide reasonable assurance that the integrity of CA systems and information is protected against viruses and malicious software.	8	Detection and prevention controls to protect against viruses and malicious software and appropriate user awareness procedures are implemented.
The CA maintains controls to provide reasonable assurance that damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures.	9	A formal reporting procedure exists and is followed, together with an incident response procedure, setting out the action to be taken on receipt of an incident report.
	10	Users of CA systems are required to note and report observed or suspected security weaknesses in or threats to systems or services.
	11	Procedures exist and are followed for reporting software malfunctions.
	12	Procedures exist and are followed to ensure that faults are reported and corrective action is taken.
	13	The types, volumes, and costs of incidents and malfunctions are quantified and monitored.
	14	Incident management responsibilities and procedures exist and are followed to ensure a quick, effective, and orderly response to security incidents.

The CA maintains controls to provide reasonable assurance that media are securely handled to protect media from damage, theft, and unauthorized access.

15

Procedures for the management of removable computer media require the following:

- a. If no longer required, the previous contents of any reusable media that are to be removed from the organization are erased.
- b. Authorization is required for all media removed from the organization and a record of all such removals is kept, to maintain an audit trail.
- c. All media are stored in a safe, secure environment, in accordance with manufacturers' specifications.

16

Media is disposed of securely and safely when no longer required.

17

Procedures for the handling and storage of information exist and are followed in order to protect such information from unauthorized disclosure or misuse.

18

System documentation is protected from unauthorized access.

3.7 System Access Management

Such controls generally include but are not limited to the following:

User access management

The CA maintains controls to provide reasonable assurance that CA system access is limited to properly authorized individuals.

1

Business requirements for access control are defined and documented in an access control policy which includes at least the following:

- a. Roles and corresponding access permissions
- b. Identification and authentication process for each user
- c. Segregation of duties
- d. Number of persons required to perform specific CA operations (that is, *m of n* rule)

2

A formal user registration and deregistration procedure for granting access to CA information systems and services is followed.

3

The allocation and use of privileges is restricted and controlled.

- 4 The allocation of passwords is controlled through a formal management process.
- 5 Users' access rights are reviewed at regular intervals.
- 6 Users are required to follow defined policies and procedures in the selection and use of passwords.
- 7 Users are required to ensure that unattended equipment has appropriate protection.
- 8 Network access control
Users are provided direct access only to the services that they have been specifically authorized to use.
- 9 The path from the user terminal to computer services is controlled.
- 10 If permitted, access by remote users is subject to authentication.
- 11 Connections to remote computer systems are authenticated.
- 12 Access to diagnostic ports is securely controlled.
- 13 Controls (for example, firewalls) are in place to protect the CA's internal network domains from external network domains accessible by third parties.
- 14 Controls are in place to limit the services (for example, HTTP, FTP) available to users in accordance with the CA's access control policies.
- 15 Routing controls are in place to ensure that computer connections and information flows do not breach the access control policy of the organization's business applications.
- 16 The security attributes of all network services used by the organization are documented by the CA.
- 17 Operating system access control
Automatic terminal identification is used to authenticate connections to specific locations and to portable equipment.
- 18 Access to CA systems uses a secure logon process.
- 19 All users have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual.
- 20 A password management system is in place to provide an effective, interactive facility which ensures quality passwords.

- 21 Use of system utility programs is restricted and tightly controlled.
- 22 If required based on a risk assessment, duress alarms are provided for users who might be the target of coercion.
- 23 Inactive terminals serving CA systems time out after a defined period of inactivity to prevent access by unauthorized persons.
- 24 Restrictions on connection times are used to provide additional security for high-risk applications.
- 25 Application access control
Access to information and application system functions is restricted in accordance with the access control policy.
- 26 Sensitive systems require a dedicated (isolated) computing environment.

3.8 Systems Development and Maintenance

The CA maintains controls to provide reasonable assurance that CA systems development and maintenance activities are properly authorized to maintain CA system integrity.

Such controls generally include but are not limited to the following:

- 1 Business requirements for new systems or enhancements to existing systems specify the requirements for controls.
- 2 Change control procedures exist and are followed for the implementation of software on operational systems.
- 3 Change control procedures exist and are followed for scheduled software releases and modifications.
- 4 Change control procedures exist and are followed for emergency software fixes.
- 5 Test data is protected and controlled.
- 6 Strict control is maintained over access to program source libraries.
- 7 The implementation of changes is strictly controlled by the use of formal change control procedures to minimize the risk of corruption of information systems.
- 8 Application systems are reviewed and tested when operating system changes occur.
- 9 Modifications to software packages are discouraged and essential changes strictly controlled.
- 10 The purchase, use, and modification of software is controlled and checked to protect against possible covert channels and Trojan code.

3.9 Business Continuity Management

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster.

- 11 Controls are in place to secure outsourced software development. **Such controls generally include but are not limited to the following:**
- 1 The CA has a managed process for developing and maintaining its business continuity plans.
- 2 The CA has a business continuity planning strategy based on an appropriate risk assessment.
- 3 The CA has business continuity plans to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes as disclosed in the CA's business practices (Principle 1, item 44).
- 4 The CA has a business continuity planning framework which requires that business continuity plans address the following:
- a. The conditions for activating the plans
 - b. Emergency procedures
 - c. Fallback procedures
 - d. Resumption procedures
 - e. A maintenance schedule
 - f. Awareness and education requirements
 - g. The responsibilities of the individuals
- 5 Business continuity plans are tested regularly to ensure that they are up-to-date and effective.
- 6 Business continuity plans are maintained by regular reviews and updates to ensure their continuing effectiveness.
- 7 Business continuity plans define an acceptable system outage time, recovery time, and the average time between failures as disclosed in the CA's business practices (Principle 1, item 44).
- 8 The CA's business continuity plans include disaster recovery processes for all critical components of a CA system, including the hardware, software, and keys, in the event of a failure of one or more of these components.

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of the compromise of the CA's private signing key.

- 9 The CA's business continuity plans address the recovery procedures used if computing resources, software, or data are corrupted or suspected to be corrupted.
- 10 The CA's business continuity plans include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is reestablished either at the original site or a remote hot site.
- 11 Back-up copies of essential business information and software are regularly taken as disclosed in the CA's business practices (Principle 1, item 44). The security requirements of these copies are consistent with the controls for the information backed up.
- 12 Fallback equipment and backup media are sited at a safe distance to avoid damage from disaster at the main site as disclosed in the CA's business practices (Principle 1, item 44).
- 13 The CA's business continuity plans address the compromise or suspected compromise of a CA's private signing key as a disaster.
- 14 In the event of the compromise or suspected compromise of a CA's private key, disaster recovery procedures include the revocation and reissuance of all certificates that were signed with the CA's private key.

	15	The recovery procedures used if the CA's private key is compromised and the CA's public key is revoked include the following:
		<ul style="list-style-type: none"> a. How a secure environment is reestablished b. How the CA's old public key is revoked c. How the CA's new public key is provided to the users d. How the subjects are recertified
	16	In the event that the CA has to replace its CA root private key, procedures are in place for the secure and authenticated revocation of the following: <ul style="list-style-type: none"> a. The old CA root public key b. The set of all certificates issued by a CA based on the compromised private key c. Any subordinate CA private keys and corresponding certificates
	17	The CA's business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data.
The CA maintains controls to provide reasonable assurance that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services.	18	The CA maintains procedures for the termination and notification of affected entities, and for transferring relevant archived CA records to a custodian as disclosed in the CA's business practices (Principle 1, item 40). Such controls generally include but are not limited to the following:
3.10 Monitoring and Compliance		
The CA maintains controls to provide reasonable assurance that the CA complies with legal requirements.	1	All relevant statutory, regulatory, and contractual requirements are explicitly defined and documented for each information system.
	2	Appropriate procedures are implemented to ensure compliance with legal restrictions on the use of material in respect of intellectual property rights, and on the use of proprietary software products as disclosed in the CA's business practices (Principle 1, item 42).
	3	Important records of an organization are protected from loss, destruction, and falsification.

	4	Controls are applied to protect personal information in accordance with relevant legislation.
	5	Management authorizes the use of information processing facilities and controls are applied to prevent the misuse of such facilities.
	6	Controls are in place to ensure compliance with national agreements, laws, regulations, or other instruments to control the access to or use of cryptographic controls.
	7	As disclosed in the CA's business practices (Principle 1, item 41), the CA's confidentiality policies and procedures address the following: <ul style="list-style-type: none"> a. The kinds of information that must be kept confidential by the CA or RA b. The kinds of information that are not considered confidential c. Who is entitled to be informed of reasons for revocation and suspension of certificates d. The policy on release of information to law enforcement officials e. Information that can be revealed as part of civil discovery f. The conditions upon which the CA or RA may disclose information upon the owner's request g. Any other circumstances under which confidential information may be disclosed
The CA maintains controls to provide reasonable assurance that compliance with the CA's security policies and procedures is ensured.	8	Managers are responsible for ensuring that security procedures within their area of responsibility are carried out correctly.
	9	The CA's operations are subject to regular review to ensure compliance with security policies and standards.
	10	CA systems are periodically checked for compliance with security implementation standards.
The CA maintains controls to provide reasonable assurance that the effectiveness of the system audit process is maximized and interference to and from the system audit process is minimized.	11	Audits of operational systems are planned and agreed to such as to minimize the risk of disruptions to business processes.

The CA maintains controls to provide reasonable assurance that unauthorized CA system usage is detected.	12	Access to system audit tools is protected to prevent possible misuse or compromise.
3.11 Event Journaling	13	Procedures for monitoring the use of CA systems are established and the results of the monitoring activities are reviewed regularly.
The CA maintains controls to provide reasonable assurance that significant CA environmental, key management, and certificate management events are logged accurately and completely.		Such controls generally include but are not limited to the following:
	1	The CA generates automatic (electronic) and manual event journals as appropriate.
	2	<p>All journal entries include the following elements:</p> <ul style="list-style-type: none"> <i>a.</i> Date and time of the entry <i>b.</i> Serial or sequence number of entry (for automatic journal entries) <i>c.</i> Kind of entry <i>d.</i> Source of entry (for example, terminal, port, location, customer) <i>e.</i> Identity of the entity making the journal entry

- 3 The CA logs the following key life cycle management related events:
- a.* CA (and subscriber, if applicable) key generation
 - b.* Installation of manual cryptographic keys and its outcome (with the identity of the operator)
 - c.* CA (and subscriber, if applicable) key backup
 - d.* CA (and subscriber, if applicable) key storage
 - e.* CA (and subscriber, if applicable) key recovery
 - f.* CA (and subscriber, if applicable) key escrow activities (optional)
 - g.* CA key usage
 - h.* CA (and subscriber, if applicable) key archival
 - i.* Withdrawal of keying material from service
 - j.* CA (and subscriber, if applicable) key destruction
 - k.* Identity of the entity authorizing a key management operation
 - l.* Identity of the entity handling any keying material (such as key components or keys stored in portable devices or media)
 - m.* Custody of keys and of devices or media holding keys
 - n.* Compromise of a private key
- 4 The CA logs the following certificate life cycle management related events:
- a.* Receipt of requests for certificate(s)—including initial certificate requests, renewal requests, and rekey requests
 - b.* Submissions of public keys for certification
 - c.* Change of affiliation of an entity
 - d.* Generation of certificates
 - e.* Distribution of the CA's public key
 - f.* Certificate revocation requests
 - g.* Certificate suspension requests (if applicable)
 - h.* Generation and issuance of certificate revocation lists
 - i.* Actions taken upon expiration of a certificate

- 5 The CA logs the following cryptographic device life cycle management related events:
 - a. Device receipt
 - b. Entering or removing a device from storage
 - c. Device usage
 - d. Device deinstallation
 - e. Designation of a device for service and repair
 - f. Device retirement

- 6 The CA logs (or requires that the RA log) the following certificate application information:
 - a. Kind of identification document(s) presented by the applicant
 - b. Record of unique identification data, numbers, or a combination thereof (for example, applicant's driver's license number) of identification documents, if applicable
 - c. Storage location of copies of applications and identification documents
 - d. Identity of entity accepting the application
 - e. Method used to validate identification documents, if any
 - f. Name of receiving CA or submitting RA, if applicable

	7	The CA logs the following security-sensitive events: <ul style="list-style-type: none"> a. Security-sensitive files or records read or written, including the event journal b. Deletion of security-sensitive data c. Security profile changes d. Use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication) e. System crashes, hardware failures, and other anomalies f. Actions taken by computer operators, system administrators, and system security officers g. Change of affiliation of an entity h. Decisions to bypass encryption or authentication processes or procedures i. Access to the CA system or any component thereof
	8	Event journals do not record the plain text values of any private keys.
	9	CA computer system clocks are synchronized for accurate recording.
The CA maintains controls to provide reasonable assurance that the confidentiality and integrity of current and archived event journals are maintained.	10	Current and archived event journals are maintained in a form that prevents unauthorized modification or destruction.
	11	Current and archived automated event journals are protected from modification or substitution.
	12	The private key used for signing event journals is not used for any other purpose.
The CA maintains controls to provide reasonable assurance that event journals are archived completely and confidentially in accordance with disclosed business practices.	13	The CA archives event journal data on a periodic basis as disclosed in the CA's business practices (Principle 1, item 45).
	14	A risk assessment has been performed to determine the appropriate length of time for retention of archived event journals.
	15	The CA maintains archived event journals at a secure off-site location for a predetermined period.
The CA maintains controls to provide reasonable assurance that event journals are reviewed periodically by authorized personnel.	16	Current and archived event journals may only be retrieved by authorized individuals for valid business or security reasons.

- 17 Event journals are reviewed periodically as disclosed in the CA's business practices (Principle 1, item 45).
- 18 The review of current and archived event journals includes a validation of the event journals' integrity, and the identification and follow-up of exceptional, unauthorized, or suspicious activity.

Appendix A

Illustrative Examples of Practitioner Reports

This appendix presents three illustrative reports for WebTrust® for Certification Authorities engagements, all prepared in accordance with the American Institute of Certified Public Accountants' (AICPA's) attestation standards.

Under the attestation standards, the first paragraph of the practitioner's report will state that the practitioner has performed an examination of management's assertion about disclosures of its business practices and effectiveness of its controls in conformity with the WebTrust Principles and Criteria for Certification Authorities. The practitioner may opine (1) on management's assertion or (2) directly on the subject matter. Samples of both kinds of reports are provided.

Example 1

The following is an example of a practitioner report for use when all WebTrust for Certification Authorities criteria are applicable.

Report of Independent Certified Public Accountant

To the Management of ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [*hot link to management's assertion*] that in providing its certification authority (CA) services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices [*hot link to CA business practices disclosure*] and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;

- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, for the period [*Month, day, year*] through [*Month, day, year*], ABC-CA management's assertion, as set forth in the first paragraph, is fairly stated, in all material respects, based on the AICPA/CICA WebTrust for Certification Authorities criteria.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for certification authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no

procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Example 2

The following is an example of a practitioner report for use when external registration authorities are used and the certification authority (CA) does not support key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards, or the provision of subscriber key management services.

Report of Independent Certified Public Accountant

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion by the management of ABC Certification Authority, Inc. (ABC-CA) [*hot link to management's assertion*] that in providing its certification authority (CA) services at [*location*], ABC-CA, during the period from _____ through _____:

- Disclosed its key and certificate life cycle management business and information privacy practices [*hot link to CA business practices disclosure*] and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;

- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*].

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our examination.

ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practice disclosures. Our examination did not extend to the controls of external registration authorities.

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for certification authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at external registration authorities and individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Example 3

The following is an example of a direct report for use when all criteria are applicable.

Report of Independent Certified Public Accountant

To the Management of
ABC Certification Authority, Inc.:

We have examined the assertion [*hot link to management's assertion*] by the management of ABC Certification Authority, Inc. (ABC-CA) regarding the disclosure of its key and certificate life cycle management business and information privacy practices on its Web site and the effectiveness of its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity, based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*], during the period [*Month, day, year*] through [*Month, day, year*].

These disclosures and controls are the responsibility of ABC-CA's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and accordingly, included (1) obtaining an understanding of ABC-CA's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the authenticity and privacy of subscriber and relying party information, over the continuity of key and certificate life cycle management operations, and over development, maintenance, and operation of systems integrity; (2) selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices; (3) testing and evaluating the operating effectiveness of the controls; and (4) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, during the period from [*Month, day, year*] through [*Month, day, year*], ABC-CA, in all material respects:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that subscriber information was properly authenticated (for the registration activities performed by ABC-CA) and the integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that

subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure; the continuity of key and certificate life cycle management operations was maintained; and CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*].

Because of inherent limitations in controls, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, (3) changes required because of the passage of time, or (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

The WebTrust seal of assurance for Certification Authorities on ABC-CA's Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

The relative effectiveness and significance of specific controls at ABC-CA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

This report does not include any representation as to the quality of ABC-CA's services beyond those covered by the WebTrust for Certification Authorities criteria, nor the suitability of any of ABC-CA's services for any customer's intended purpose.

[*Name of CPA firm*]
Certified Public Accountants
[*City, State*]
[*Date*]

Appendix B

Illustrative Examples of Management's Assertion

Example 1

The following is an example of management's assertion for use when all criteria are applicable.

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from [Month, day, year] through [Month, day, year]

[Date]

ABC Certification Authority, Inc. operates as a certification authority (CA) known as ABC-CA. ABC-CA, as a root CA [*or as a subordinate CA of DEF Certification Authority, Inc.*], provides the following CA services:

- Subscriber key management services
- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate suspension
- Certificate status information processing (using an online repository)
- Integrated circuit card life cycle management

Management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure [*hot link to CA business practices disclosure*], service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective controls can provide only reasonable assurance with respect to ABC-CA's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) management's opinion, in providing its CA services at [location], ABC-CA, during the period from [Month, day, year] through [Month, day, year]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
 - The continuity of key and certificate life cycle management operations was maintained; and
 - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*], including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Escrow

CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management
CA-Provided Subscriber Key Management Services

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Renewal
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Suspension
Certificate Status Information Processing
Integrated Circuit Card Life Cycle Management

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Event Journaling

[Name]

[Title]

Example 2

The following is an example of management's assertion for use when external registration authorities are used and the certification authority (CA) does not support key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards, or the provision of subscriber key management services.

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period from [Month, day, year] through [Month, day, year]

[Date]

ABC Certification Authority, Inc. operates as a certification authority (CA) known as ABC-CA. ABC-CA, as a root CA [or as a subordinate CA of DEF Certification Authority, Inc.], provides the following CA services:

- Certificate rekey
- Certificate issuance
- Certificate distribution (using an online repository)
- Certificate revocation
- Certificate status information processing (using an online repository)

ABC-CA makes use of external registration authorities for specific subscriber registration activities as disclosed in ABC-CA's business practice disclosures.

Management of ABC-CA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure [*hot link to CA business practices disclosure*], service integrity (including key and certificate life cycle management controls), and CA environmental controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error and the circumvention or overriding of controls. Accordingly, even effective internal controls can provide only reasonable assurance with respect to ABC-CA's CA operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) management's opinion, in providing its CA services at [*location*], ABC-CA, during the period from [*Month, day, year*] through [*Month, day, year*]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:

- Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria [*hot link to WebTrust for Certification Authorities criteria*], including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Status Information Processing

CA Environmental Controls

Certification Practice Statement and Certificate Policy Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management

Monitoring and Compliance
Event Journaling

[*Name*]

[*Title*]

Appendix C

Illustrative Examples of Management's Representation

Example 1

The following is an example of a management representation for use when all criteria are applicable.

[Date]

[Name of CPA firm]

[Address]

Dear Members of the Firm:

Management confirms its understanding that your examination of our assertion related to ABC Certification Authority, Inc.'s (ABC-CA) business practices disclosure and controls over its certification authority (CA) operations during the period from [Month, day, year] through [Month, day, year] was made for the purpose of expressing an opinion as to whether our assertion is fairly presented, in all material respects, and that your opinion is based on criteria for effective controls as stated in our assertion document. We are responsible for our assertion. In connection with your examination, management:

1. Acknowledges its responsibility for establishing and maintaining effective controls over its CA operations at [location], including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls.
2. Has performed an assessment and believes that ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls met the minimum requirement of the criteria described in our assertion document during the period from [Month, day, year] through [Month, day, year].
3. Believes the stated criteria against which our assertion has been assessed are reasonable and appropriate.
4. Has disclosed to you that there are no significant deficiencies in the design or operation of the controls which could adversely affect the Company's ability to comply with the control criteria related to ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental

controls, consistent with the assertions of management.

5. Has made available to you all significant information and records related to our assertion.
6. Has responded fully to all inquiries made to us by you during your examination.
7. Has disclosed to you any changes occurring or planned to occur subsequent to _____, in controls or other factors that might significantly affect the controls, including any corrective actions taken by management with regard to significant deficiencies.

In management's opinion, ABC-CA, in providing its CA services at [location] during the period from [Month, day, year] through [Month, day, year]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
 - The continuity of key and certificate life cycle management operations was maintained; and
 - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria, including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Escrow
- CA Key Usage
- CA Key Destruction
- CA Key Archival
- CA Cryptographic Hardware Life Cycle Management
- CA-Provided Subscriber Key Management Services

Certificate Life Cycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Status Information Processing
- Integrated Circuit Card Life Cycle Management

CA Environmental Controls

- Certification Practice Statement and Certificate Policy Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event Journaling

Very truly yours,

[Name]

[Title]

Example 2

The following is an example of a management representation for use when external registration authorities are used and the certification authority (CA) does not support key escrow, certificate renewal, certificate suspension, the use of integrated circuit cards, or

the provision of subscriber key management services.

[Date]

[Name of CPA]

[Address]

Dear Members of the Firm:

Management confirms its understanding that your examination of our assertion related to ABC Certification Authority, Inc.'s (ABC-CA) business practices disclosure and controls over its certification authority (CA) operations during the period from [Month, day, year] through [Month, day, year] was made for the purpose of expressing an opinion as to whether our assertion is fairly presented, in all material respects, and that your opinion is based on criteria for effective controls as stated in our assertion document. ABC-CA makes use of external registration authorities for specific subscriber registration activities, as disclosed in ABC-CA's business practice disclosures. We are responsible for our assertion. In connection with your examination, management:

1. Acknowledges its responsibility for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls.
2. Has performed an assessment and believes that ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, met the minimum requirement of the criteria described in our assertion document during the period from [Month, day, year] through [Month, day, year].
3. Believes the stated criteria against which our assertion has been assessed are reasonable and appropriate.
4. Has disclosed to you that there are no significant deficiencies in the design or operation of the controls which could adversely affect the Company's ability to comply with the control criteria related to ABC-CA's CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental controls, consistent with the assertions of management.
5. Has made available to you all significant information and records related to our assertion.
6. Has responded fully to all inquiries made to us by you during your examination.
7. Has disclosed to you any changes occurring or planned to occur

subsequent to [Month, day, year], in controls or other factors that might significantly affect the controls, including any corrective actions taken by management with regard to significant deficiencies.

In management's opinion, ABC-CA, in providing its CA services at [location], ABC-CA, during the period from [Month, day, year] through [Month, day, year]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
 - The continuity of key and certificate life cycle management operations was maintained; and
 - CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria, including the following:

CA Business Practices Disclosure

Service Integrity

Key Life Cycle Management Controls

CA Key Generation
CA Key Storage, Backup, and Recovery
CA Public Key Distribution
CA Key Usage
CA Key Destruction
CA Key Archival
CA Cryptographic Hardware Life Cycle Management

Certificate Life Cycle Management Controls

Subscriber Registration
Certificate Rekey
Certificate Issuance
Certificate Distribution
Certificate Revocation
Certificate Status Information Processing

CA Environmental Controls

Certification Practice Statement and Certificate Policy
Management
Security Management
Asset Classification and Management
Personnel Security
Physical and Environmental Security
Operations Management
System Access Management
Systems Development and Maintenance
Business Continuity Management
Monitoring and Compliance
Event Journaling

Very truly yours,

[Name]

[Title]

Appendix D

Comparison of WebTrust for Certification Authorities Criteria and ANSI X9.79

<u>WebTrust for Certification Authorities Criteria</u>		Draft¹ <u>ANSI X9.79 (Draft) PKI Practices and Policy Framework Standard's Certification Authority Control Objectives (CACO)</u>	
§1	CA Business Practices Disclosure	§7, §A, & §B	General Requirements—CP and Certification Practice Statements; PKI Practices and Policy Elements; and Certification Authority Control Objectives
§2	Service Integrity	§B.2 & B.3	Key and Certificate Life Cycle Management Controls
§2.1	Key Life Cycle Management Controls	§B.2	Key Life Cycle Management Controls
§2.1.1	CA Key Generation	§B.2.1	CA Key Generation
§2.1.2	CA Key Storage, Backup, and Recovery	§B.2.2	CA Key Storage, Backup and Recovery
§2.1.3	CA Public Key Distribution	§B.2.3	CA Public Key Distribution
§2.1.4	CA Key Escrow	§B.2.4	CA Key Escrow
§2.1.5	CA Key Usage	§B.2.5	CA Key Usage
§2.1.6	CA Key Destruction	§B.2.6	CA Key Destruction
§2.1.7	CA Key Archival	§B.2.7	CA Key Archival
§2.1.8	CA Cryptographic Hardware Life Cycle Management	§B.2.8	CA Cryptographic Hardware Life Cycle Management

1. The American National Standards Institute (ANSI) X9F5 Digital signature and Certificate Policy working group is developing the X9.79 *PKI Practices and Policy Framework (X9.79)* standard for the financial services community. This standard includes detailed Certification Authority Control Objectives against which certification authorities may be evaluated. An International Organization for Standardization (ISO) working group has been formed to standardize X9.79 based on international requirements in a new international standard.

§2.1.9	CA-Provided Subscriber Key Management Services	§B.2.9	CA-Provided Subscriber Key Management Services
§2.2	Certificate Life Cycle Management Controls	§B.3	Certificate Life Cycle Management Controls
§2.2.1	Subscriber Registration	§B.3.1	Subscriber Registration
§2.2.2	Certificate Renewal	§B.3.2	Certificate Renewal
§2.2.3	Certificate Rekey	§B.3.3	Certificate Rekey
§2.2.4	Certificate Issuance	§B.3.4	Certificate Issuance
§2.2.5	Certificate Distribution	§B.3.5	Certificate Distribution
§2.2.6	Certificate Revocation	§B.3.6	Certificate Revocation
§2.2.7	Certificate Suspension	§B.3.7	Certificate Suspension
§2.2.8	Certificate Status Information Processing	§B.3.8	Certificate Status Information Processing
§2.2.9	Integrated Circuit Card (ICC) Life Cycle Management	§B.3.9	Integrated Circuit Card (ICC) Life Cycle Management
§3	CA Environmental Controls	§B.1	CA Environmental Controls
§3.1	Certification Practice Statement and Certificate Policy Management	§B.1.1	Certification Practice Statement and Certificate Policy Management
§3.2	Security Management	§B.1.2	Security Management
§3.3	Asset Classification and Management	§B.1.3	Asset Classification and Management
§3.4	Personnel Security	§B.1.4	Personnel Security
§3.5	Physical and Environmental Security	§B.1.5	Physical and Environmental Security
§3.6	Operations Management	§B.1.6	Operations Management
§3.7	System Access Management	§B.1.7	System Access Management
§3.8	Systems Development and Maintenance	§B.1.8	Systems Development and Maintenance
§3.9	Business Continuity Management	§B.1.9	Business Continuity Management
§3.10	Monitoring and Compliance	§B.1.10	Monitoring and Compliance
§3.11	Event Journaling	§B.1.11	Event Journaling

Appendix E

Comparison of CICA Section 5900, AICPA SAS No. 70, and AICPA/CICA WebTrust for Certification Authorities Reviews and Reports Covering the Business Activities of Certification Authority Organizations

This document analyzes the form and content of reviews and reports performed under the indicated regulations indicating appropriate similarities and differences. For third-party reporting with respect to certification authorities (CAs), the most appropriate and relevant approach is to use the AICPA/CICA Certification Authority Trust approach wherever possible since it has been developed specifically around the reportable business activities of an organization acting as a CA.

<i>SA Standards for Assurance Engagements, Section 5900 "Opinions Control Procedures at a Service Organization"</i>	<i>Statement on Auditing Standards No. 70, Service Organizations (AICPA, Professional Standards, vol. 1, AU sec. 324), as amended</i>	<i>AICPA/CICA WebTrust for Certification Authorities</i>
<ul style="list-style-type: none"> — Auditor to auditor communication for obtaining reliance for audit purposes — Covers specified applications, functions, and processing environments — Practical usage now results in business activity coverage — Defined by each engagement — Report on design and existence of control procedures — Report on design, effective operation, and continuity of control procedures — Generally accepted auditing standards — No mandatory coverage — Coverage must be formulated for each engagement and defined in report scope. 	<ul style="list-style-type: none"> — Auditor to auditor communication for obtaining reliance for audit purposes — Covers specified applications, functions, and processing environments — Practical usage now results in business activity coverage — Defined by each engagement — Report on controls placed in operation — Report on controls placed in operation and tests of operating effectiveness — Generally accepted auditing standards — No mandatory coverage — Coverage must be formulated for each engagement and defined in report scope. 	<ul style="list-style-type: none"> — Auditor communication to interested parties including business partners and existing and potential customers — Mandatory coverage as noted below — New criteria and illustrations for reporting activities of certification authorities — Certification authority business activities pre-defined in principles and criteria — Report on compliance with WebTrust for Certification Authorities Principles and Criteria — Statements on Standards for Attestation Engagements (U.S.) — Standards for Assurance Engagements (Canada) — Areas of coverage defined by principles and criteria, including: <ul style="list-style-type: none"> — CA business practice disclosure (including the privacy of subscriber and relying party information) — Service integrity <ul style="list-style-type: none"> — Key life cycle management controls — Certificate life cycle management controls — CA environmental controls

linkage would need to be established as part of a specific review.

Adequacy of control objectives and procedures subjectively determined by auditor based on the engagement.

Acceptable alternatives:

— Point in time (for design and existence)

— Period of time (determined by client)

Any linkage would need to be established as part of a specific review.

Adequacy of control objectives and procedures subjectively determined by auditor based on engagement.

Acceptable alternatives:

— Point in time (controls placed in operation)

— Period of time (determined by client)

Principles and criteria linked to ANSI X9.79 standard which is intended to be submitted to the International Organization for Standardization (ISO) for international standardization.

AICPA/CICA provides uniform rules which are linked to industry accepted standards. Continuous coverage from the point of qualification. Qualification after compliance can be tested over a minimum 90-day period, followed by updates within a specified period (currently under debate whether this would be six months, annual, or some other).

Appendix F

Practitioner Policies and Guidance for WebTrust for Certification Authority Engagements

This appendix includes practitioner policies which set forth practices that practitioners must follow when conducting a WebTrust engagement. These policies are in *italic* typeface. This section also includes additional practitioner guidance on implementing these policies. This guidance is in normal typeface.

Client/Engagement Acceptance

The practitioner should not accept an engagement where the awarding of a WebTrust seal would be misleading.

The WebTrust seal implies that the entity is a reputable site that has reasonable disclosures and controls in a broad range of areas. Accordingly, the practitioner would avoid accepting a WebTrust engagement when the entity's disclosures outside the scope of the engagement are known by the practitioner to be misleading, when there are known major problems with controls not directly affecting the scope of the engagement, or when the entity is a known violator of laws or regulations.

Procedures to provide WebTrust services resulting in the awarding of a WebTrust seal should be performed at a high level of assurance (i.e., audit or examination level).

Although a practitioner can provide a variety of services related to WebTrust, such as a preliminary review of a certification authority (CA) to identify potential areas of nonconformity with the WebTrust for Certification Authorities criteria, any engagement leading to a WebTrust Seal would need to include procedures to provide a high level of assurance (that is, audit or examination level) as a basis for an unqualified opinion.

Initial Period of Coverage

The period of coverage for an initial WebTrust for Certification Authorities engagement should be at least two months or more as determined by the practitioner.

In determining the initial period of coverage, the practitioner would consider what length of period would be required to obtain sufficient competent evidential matter as a basis for his or her opinion. For example, for established CAs and CA functions, two months may be quite sufficient, while for new CAs and CA functions, the practitioner may believe that a longer initial period would be more appropriate.

Frequency of Updates

The interval between updates for the WebTrust for Certification Authorities seal should not exceed 12 months and this interval often may be considerably shorter.

In determining the interval between updates, the practitioner would consider:

- The nature and complexity of the CA's operations.
- The frequency of significant changes to the CA's operations.

- The relative effectiveness of the entity’s monitoring and change management controls for ensuring continued conformity with the applicable WebTrust for Certification Authorities criteria as such changes are made.
- The practitioner’s professional judgment.

For example, in the situation of a start-up CA or CA function, it may be more appropriate that the initial examination period be established at 3 months, with the next review being performed 6 months after the WebTrust seal for Certification Authorities is awarded, thereafter moving to a 12-month review cycle. In order to provide continuous coverage and retain the seal, the period covered for update reports should either begin with the end of the prior period or the start of the period in the initial report.

If the entity notifies the practitioner of a significant change potentially affecting conformance with the applicable WebTrust for Certification Authorities criteria included in the scope of the engagement during the period between updates, the practitioner should determine whether:

1. *An update examination would need to be performed,*
2. *The seal would need to be removed until an update examination is completed and an updated auditor’s report is issued, or*
3. *No action is required at that time because of the nature of the change and/or the effectiveness of the entity’s monitoring and change management controls.*

Management Assertions

Management should provide an appropriate written assertion on its Web site. Management’s assertion would ordinarily identify the specific CA covered, the period covered (which ordinarily would be the same as that covered by the practitioner’s report), and include a statement along the following lines, for example for the CA model:

Management has assessed the controls over its CA operations. Based on that assessment, in ABC Certification Authority, Inc. (ABC-CA) management’s opinion, in providing its certification authority (CA) services at [location], ABC-CA, during the period from [Month, day, year] through [Month, day, year]:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber information was properly authenticated (for the registration activities performed by ABC-CA); and
 - The integrity of keys and certificates it managed was established and protected throughout their life cycles
- Maintained effective controls to provide reasonable assurance that:
 - Subscriber and relying party information was restricted to

authorized individuals and protected from uses not specified in the CA's business practices disclosure;

- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance, and operations were properly authorized and performed to maintain CA systems integrity based on the AICPA/CICA WebTrust for Certification Authorities criteria.

Example management assertions are provided in Appendix B.

Changes in Client Policies and Disclosures

Changes in an entity's disclosed policies need to be disclosed on its Web site. If the client appropriately discloses such changes, no mention of such change needs to be made in the practitioner's report.

Sufficient Criteria for Unqualified Opinion

In order to obtain an unqualified opinion, the entity should meet, in all material respects, all of the applicable WebTrust for Certification Authorities Criteria included in the scope of the engagement during the period covered by the report and each update period.

Subsequent Events

The practitioner should consider the effect of subsequent events up to the date of the practitioner's report. When the practitioner becomes aware of events that materially affect the subject matter, and the practitioner's conclusion, the practitioner should consider whether the disclosed practices reflect those events properly or whether those events are addressed properly in the practitioner's report.

Representation Letter

Prior to conclusion of the engagement and before the practitioner issues a report, the client will be required to provide to the practitioner a representation letter.

Example representation letters are provided in Appendix C.

AICPA

Assurance Services Executive Committee

ROBERT L. BUNTING, *Chair*
GARI FAILS
TED HORNE
EVERETT C. JOHNSON, Jr
JOHN LAINHART
GEORGE LEWIS

EDWARD F. ROCKMAN
SUSAN C. RUCKER
J. W. MIKE STARR
WENDY E. VISCONTY
DARWIN VOLTIN
NEAL WEST

AICPA Staff

ALAN ANDERSON
Senior Vice President, Technical Services

ANTHONY J. PUGLIESE
Director, Assurance Services

CICA

Assurance Services Development Board

JOHN W. BEECH, *Chair*

STEPHEN E. SALTERIO

DOUGLAS C. ISAAC
MARILYN KUNTZ
DOUG McPHIE

DAVID W. STEPHEN
DOUG TIMMINS
KEITH S. VANCE

CICA Staff

CAIRINE M. WILSON,
Vice President, Innovation

GREGORY P. SHIELDS,
Director, Assurance Services Development

AICPA / CICA Electronic Commerce Assurance Services Task Force

EVERETT C. JOHNSON, Jr, *Chair*
BRUCE R. BARRICK
JERRY R. DEVAULT
JOSEPH G. GRIFFIN
CHRISTOPHER J. LEACH, *Vice Chair*

WILLIAM POWERS
KERRY L. SHAKELFORD
DONALD E. SHEEHY
CHRISTIAN R. STORMER
ALFRED F. VAN RANST, Jr
PATRICK J. MORIARTY

Staff Contacts

BRYAN WALKER, CICA
Principal, Assurance Services Development

KARYN WALLER, AICPA
Senior Technical Manager, Trust Services
(replaced Sheryl Martin in 2001)
SHERYL MARTIN, AICPA
WebTrust Team Leader

For issues related to this release, please e-mail assure@aicpa.org.