KPMG

DIGITAL CERTIFICATES, AUTHENTICATION, AND TRUST ON THE INTERNET

ASSURANCE

PREFACE

Until recently, substantially all server certificates (SSL or secure socket layer certificates) issued by public certification authorities (CAs) were issued to organizations following a subscriber authentication process that included verification of the organization's existence, the organization's right to use the domain name included in the certificate, and the authority of the requester to obtain a certificate on behalf of the organization. Such certificates afforded a satisfactory level of assurance by enabling three security services—confidentiality, authentication, and integrity.

In recent months, with the rise of a new business model for SSL certificate issuance, some CAs now issue lower-assurance server certificates without authenticating the subscriber, thereby providing only two security services—confidentiality and integrity. Using current browser technology, it is very difficult for an Internet user to distinguish between higher- and lower-assurance server certificates. As a result, consumer confidence in the security of electronic commerce may be at risk. This paper addresses this topic and provides recommendations for addressing related issues through industry and standardization activities.

Abbreviations

certificate policy	CP
certification authority	CA
certification practice statement	CPS
certificate revocation list	CRL
certificate signing request	CSR
hypertext transfer protocol with SSL	HTTPS
identification and authentication	I&A
Internet service provider	ISP
object identifier	OID
online certificate status protocol	OCSP
policy management authority	PMA
public key infrastructure	PKI
registration authority	RA
secure socket layer	SSL
uniform resource locator	URL

CONTENTS

EXECUTIVE SUMMARY

The use of high-assurance SSL certificates is a critical building block for secure electronic commerce and one of the most ubiquitous uses of public key infrastructure (PKI). SSL certificates provide three security services—confidentiality, authentication, and integrity. They enable an Internet user to:

- Securely communicate with a Web site—information provided by the Internet user cannot be intercepted in transit (confidentiality) or altered without detection (integrity)
- Verify that the Internet user is actually at the company's Web site and not an impostor's site (authentication).

For example, an SSL certificate bearing the organization name "XYZ Software, Inc." is intended to convey assurance that the visited Web site (e.g., www.xyzsoftware.com) is an XYZ Software, Inc. Web site (and not another entity's site perhaps intended to trick unsuspecting Web surfers into doing business with someone pretending to be XYZ Software, Inc.).

Why is this point important? A domain name or URL (uniform resource locator) is like a telephone number. It is assigned to a paying customer (organization or individual) for the period of time it is registered.

The domain name system was designed to support open-systems information flow. While there are restrictions on certain types of domains (e.g., *.mil* is restricted to military entities, *.es* is restricted to organizations physically located in Spain), there are no such restrictions on the most common types of domains (including *.com*, *.org*, *.net*, and others). To register for these types of domains, the individual or organization need only pay the annual fee. The applicant is also obligated to provide accurate information, though there is no requirement for registrars to verify the accuracy of the information provided.

Leading browser providers such as Microsoft® and Netscape® recognized the importance of high-assurance SSL certificates and incorporated easy to understand icons (locks and keys) into their browsers to inform Web site visitors when an SSL session was invoked and consequently that their information would be secure in transit. Until recently, this simple approach worked well and facilitated the expansion of online commerce. However, recent changes in the SSL certificate marketplace pose a security risk with a potential threat to consumer confidence in the security of online commerce.

SUBSCRIBER AUTHENTICATION

Until recently, substantially all SSL certificates could be categorized as "medium" to "high" assurance and therefore provided all three security services—confidentiality, authentication, and integrity. However, in recent months emerging providers of SSL certificates have elected to provide lower-assurance SSL certificates (with no authentication of the subscriber) at a reduced cost and with rapid order fulfillment. These lower-assurance SSL certificates provide confidentiality and integrity, but not authentication. This conflicts with generally accepted industry practices and serves as a source of confusion for Internet users. Whereas, in the past, users could reasonably rely on the lock or key, they must now examine and understand the contents of the SSL certificate to distinguish between varying levels of assurance.

Industry standards for subscriber registration require that a certification authority (CA) maintain controls to provide reasonable assurance that:

- Subscribers are properly identified and authenticated
- Subscriber certificate requests are accurate, authorized, and complete.[1]

EXECUTIVE SUMMARY

A certification authority's specific practices for meeting these requirements should be disclosed in the CA's published certificate policy (CP) or certification practice statement (CPS). Fundamental to the process of issuing SSL certificates to an organization for use on its Web site are three basic verification components:

- Confirmation that the organization named in the certificate has the right to use the domain name identified in the certificate
- Confirmation that the organization named in the certificate is a legal entity
- Confirmation that the individual who requested the SSL certificate on behalf of the organization was reasonably authenticated and had proper authorization.[2]

Completion of these verification steps prior to certificate issuance enables Internet users to know they are conducting business with an authenticated organization. In general, an Internet user incurs a higher degree of risk if such verification steps are not performed. The following table provides an overview of some of those risks.

In each scenario, the failure to complete the specified checks could expose:

- Unsuspecting Internet users to direct loss of funds due to fraud
- The legitimate company to direct loss of funds due to fraud, or undue business risk such as loss of productivity, bad public relations, or legal action
- The CA to undue business risk such as loss of productivity, bad public relations, or legal action.

Scenario	Threat
1. No authentication of the organization by the CA. *or* **2.** No check of the applicant's right to use the domain name by the CA.	A malicious individual could masquerade as an existing organization, deceiving users into believing that the malicious individual's Web site is operated under the auspices of an existing organization whose name is included in the site's SSL certificate. A false level of trust is established by associating the malicious individual's domain name with the name of an existing organization.
3. No check of the organization's existence by the CA.	A malicious individual could pretend to be an organization even though no such organization exists (i.e., the organization has not been registered with the appropriate government authority).
4. No check of the applicant's identity and authority to request a certificate for the organization by the CA.	A malicious individual who is not authorized by the organization could obtain an SSL certificate bearing the organization's name, allowing the malicious individual to masquerade as the organization.

EXECUTIVE SUMMARY

RELYING PARTY CONTROL CONSIDERATIONS

Current browsers do not distinguish between higher- and lower-assurance SSL certificates. As long as the SSL certificate is linked to a trusted Root CA and the common name in the certificate matches the domain name of the visited Web site, the browser will not generate an alert and, consequently, the Internet user (relying party) will generally trust the SSL certificate. The "lock" icon in the user's browser will appear exactly the same to the user regardless of whether a particular site has an authenticated high-assurance SSL certificate or a lower-assurance unauthenticated SSL certificate.

Browser providers play an important role in enabling SSL-secured electronic commerce by including and distributing "trusted" Root CA certificates in their browsers. To establish a standard for trusting Root CAs, Microsoft implemented a program in 2001 requiring that Root CAs must complete an annual WebTrust Program for Certification Authorities (WebTrust for CAs) audit for their Root CA certificates to be included in future browser releases and the Microsoft Windows® Update function. Other browser providers such as Netscape and AOL have not formally established a similar requirement. However, this does not address the issues of SSL certificate authentication practices and assurance levels, or the lack of an intuitive or automated mechanism for users to distinguish between higher- and lower-assurance SSL certificates.

In addition, browsers are not configured to check certificate status by default. Many certificates do not contain the extensions that are necessary to enable automated certificate status checking. The time required to automatically check certificate status might vary significantly depending on the certificate status publication technology used by the CA. As a result, it is very difficult for an Internet user to distinguish between a valid SSL certificate and a revoked SSL certificate.

Another scenario that may give Internet users a false sense of security is the situation where a Web site has been implemented in a shared hosting environment using shared SSL to secure the HTTPS pages of multiple customers' Web sites with a single certificate issued to the Internet service provider (ISP). In this scenario, the Internet user may visit a Web page that is secured with an SSL certificate issued to the ISP rather than the organization (e.g., ABC Co.) with which the user believes he is doing business. When the user visits such a secured page via the ABC Co. Web site and sees the lock icon, the user may conclude that ABC Co. has been authenticated when, in reality, only the ISP has been authenticated.

The following sections describe these issues in greater detail and provide recommendations for addressing them through industry and standardization activities.

REQUIREMENTS FOR CA TRUST

OVERVIEW

As the adage goes, trust is difficult to build and easy to lose. This is particularly true in the context of PKI where a relying party must have the confidence and ability to trust a particular certificate. How does a CA ensure the trustworthiness of the certificates it issues? It does this by establishing a Community of Trust through a complex set of technology, procedural, legal, and audit components.

From a technology perspective, the CA must implement a highly secure IT infrastructure and a PKI solution consisting of CA signing servers, database servers, application and Web servers, registration authority (RA) terminals or workstations, backup servers, hardware security modules, firewalls, routers, intrusion detection systems, monitoring systems, a disaster recovery infrastructure, and many other technology components. Each of these elements must be appropriately secured and housed within a physically secure environment protected by multiple levels of security.

From a procedural perspective, the CA performs many functions and has many processes to support the issuance and management of certificates. At the highest level, policy requirements are specified in one or more certificate policies. The CPs are supported by a more detailed description of the CA's practices and procedures (i.e., a CPS). In addition, it is necessary for a CA to establish detailed operating procedures and system configuration standards to enable qualified and trained CA personnel to perform their duties in accordance with the CP, CPS, and operational procedures.

From a legal perspective, in different countries and jurisdictions it may be necessary for a CA to be licensed or accredited to operate or to issue certain types of certificates. Laws and regulations relating to digital and electronic signatures, electronic record keeping, repository requirements, and privacy also will impact the CA.

From an audit and controls perspective, it is critical to ensure the system integrity of the PKI. Internal compliance and quality assurance processes are essential to ensuring that occurrences of noncompliance with policies, procedures, and standards are identified and corrected quickly. In addition, a robust third-party audit can enhance consumer confidence in the CA and the certificates it issues. Toward this end, the WebTrust Program for Certification Authorities was designed to specifically address the needs and requirements of CAs. WebTrust for CAs defines the specific criteria that must be included in the scope of the audit and provides a specific reporting format intended for broad distribution to customers and other relying parties. If the CA successfully completes the audit, the CA may post the WebTrust for CAs seal on its Web site with a link to the audit opinion.

Industry standards, including WebTrust for CAs, ANS X9.79, and ISO CD 21188 (draft), address key elements of a PKI that are critical to enabling an Internet user to rely on the authenticity of a digital certificate. These include the following:

- CA business practices disclosure
  - Published certificate policy
  - Published certification practice statement
- CA environmental controls
- CA key life cycle management
- Certificate life cycle management.

CA CONTROL REQUIREMENTS

To enable trust in the certificates issued by a particular CA, it is necessary to adequately address a number of control areas that are summarized below. See Appendix A for a detailed description of the WebTrust for CAs criteria.

CA Business Practices Disclosure

Certificate policy (CP). A CP is a named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements. Certificate policies are used to define the level of assurance associated with a particular type or class of certificate. See Appendix B for more information on the contents of a CP.

REQUIREMENTS FOR CA TRUST

Certification practice statement (CPS). A CPS is a statement of the practices that a CA employs in issuing certificates. The CPS defines the policies, procedures, and controls the CA uses to satisfy the requirements specified in the certificate policies it supports.

CA Environmental Controls

These controls include those practices and procedures that create a secure and trustworthy environment for the CA. The components of CA environmental controls include CPS and CP 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, and event journaling.

CA Key Life Cycle Management

CA key management is a core function of the CA and the underpinning of the PKI. Maintaining the security and integrity of CA keys throughout their life cycles is critical to maintaining the integrity and trustworthiness of the PKI. The CA key management controls include CA key generation; CA key storage, backup, and recovery; CA public key distribution; CA key usage; CA key destruction; CA key archival; and CA cryptographic hardware life cycle management.

Certificate Life Cycle Management

The certificate life cycle covers the end-to-end process of certificate management and represents the core functions of a CA. The certificate life cycle management controls include subscriber registration, certificate rekey and renewal, certificate issuance, certificate distribution, certificate revocation and suspension, and certificate status information processing [e.g., certificate revocation list (CRL) processing and online certificate status protocol (OCSP)].

Specific certificate life cycle management policies and practices may vary depending on the intended purpose and assurance level of the certificates issued by the CA. This is discussed further in the sections that follow, with an emphasis on SSL server certificates.

ASSURANCE LEVELS

Certificate policies are typically used to define the trust requirements for a particular type or class of certificate. Each type or class of certificate is intended to provide a certain level of assurance. Levels of assurance are typically defined within a particular community. For example, the U.S. Federal Bridge CA has defined five assurance levels—test, rudimentary, basic, medium, and high—each providing an increasing level of assurance. Other CAs classify specific types of certificates as providing a low, medium, or high level of assurance.

See Appendix C for a more detailed description of the Federal Bridge CA classes of certificates.

CAs generally provide different types or classes of digital certificates that have different levels of trustworthiness depending on a variety of factors, including the level of subscriber authentication performed prior to issuance. Relying parties must independently ascertain the sufficiency of these authentication procedures and the appropriateness of reliance on a given type or class of digital certificate for a given application or transaction.

REQUIREMENTS FOR SUBSCRIBER AUTHENTICATION

STANDARDS FOR SUBSCRIBER AUTHENTICATION

AICPA/CICA WebTrust for CAs and ANS X9.79

WebTrust for CAs, which is based on the ANS X9.79 standard, provides a detailed set of criteria and a reporting framework specifically for reporting on the operations of a CA. WebTrust for CAs defines baseline requirements and requires that the CA disclose its business practices (typically through a CP and/or CPS). In the area of subscriber registration, WebTrust for CAs is not prescriptive as to the appropriate identification and authentication (I&A) requirements, but requires the CA to disclose its practices for the different types of certificates it issues. As part of the audit, the CA is audited against the baseline WebTrust for CAs criteria and the CA's disclosed practices. WebTrust for CAs does not define levels of certificates (e.g., low, medium, and high assurance), but allows the CA to establish its own levels or types.

The WebTrust for CAs subscriber registration criteria require that the CA maintains controls to provide reasonable assurance that:

- Subscribers are properly identified and authenticated
- Subscriber certificate requests are accurate, authorized, and complete.

WebTrust for CAs provides illustrative (example) controls that would satisfy the requirements for subscriber registration. The most relevant illustrative controls generally include, but are not limited to, the following:

- 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.
- 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.
- 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.
- 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.

WebTrust for CAs also requires certain disclosures. As it relates to subscriber registration practices, the most relevant disclosure requirements are that the CA disclose a description of the following items:

- The conditions for applicability of certificates issued by the CA that reference a specific certificate policy, including
  - 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[3]
- Certificate life cycle management practices including initial registration, and 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.[4]

As stated in WebTrust for CAs, 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 critical elements, as subscribers and relying parties must know when they are unable to rely on certificates that have been issued by the CA.[5]

REQUIREMENTS FOR SUBSCRIBER AUTHENTICATION

ISO CD 21188 (draft)

The ISO CD 21188 *PKI Policy and Practices Framework* draft standard builds on the criteria identified in X9.79 and WebTrust for CAs. The current draft of the standard includes the same subscriber registration criteria but provides additional (example) controls that would satisfy the requirement for subscriber registration, including the following:[6]

- The CA verifies or requires that the external RA verify the identity of the entity requesting a certificate in accordance with the CA's CPS and the applicable certificate policy.
  - For individual certificates, the CA or external RA verifies the identity of the individual whose name is to be included in the subject distinguished name field of the certificate. An unauthenticated individual name shall not be included in the subject distinguished name.
  - For organizational certificates (including server, network resource, code signing, etc.), the CA or external RA verifies the legal existence of the organization's name to be included in the organization attribute in the subject distinguished name field of the certificate. An unauthenticated organization name shall not be included in a certificate.
  - For organizational certificates containing a domain name, the CA or external RA [also] verifies the organization's ownership of or right to use the domain name included in the common name attribute of the subject distinguished name field of the certificate. An unauthenticated domain name shall not be included in a certificate.
- The CA verifies or requires that the external RA verify the authority of the entity requesting a certificate in accordance with the CA's CPS and the applicable certificate policy.
  - For individual certificates, the CA or external RA verifies the authority of the certificate applicant to obtain a certificate in accordance with the CA's CPS.
  - For organizational certificates, the CA or external RA verifies the authority of the requesting individual to request a certificate on behalf of the organization in accordance with the CA's CPS.

In addition, the criteria for certificate issuance require that the CA maintains controls to provide reasonable assurance that:[7]

- Certificates are generated and issued in accordance with the CA's disclosed business practices
- Unauthenticated individual and organization names are not included in the subject distinguished name field of certificates issued by the CA.

INDUSTRY PRACTICES FOR SUBSCRIBER AUTHENTICATION

Since the use of SSL certificates became prevalent in the mid-1990s, until recently major public CAs have substantially followed similar standards for subscriber identification and authentication. At the core of this standard I&A process are three basic checks:

- Organization's right to use the domain name (domain name registration)
- Legal existence of the organization
- The requester's association with the organization and authority to request a certificate.

As a result, the following assurances are asserted:

- The organization's right to use the domain name that is included in the certificate
- The legal existence (i.e., formal approval by a government body) of the organization named in the certificate
- The fact that the requester is associated with the organization and is authorized to request a certificate on behalf of the organization.

While different CAs have differing procedures for issuing server certificates, they generally perform the three basic checks specified above and their server certificates generally provide a similar level or degree of assurance.[8] The following table summarizes each component, its significance, and the risks associated with non-performance.

REQUIREMENTS FOR SUBSCRIBER AUTHENTICATION

Component	Description	What Is Verified?	Significance	Risks/Threats
Domain Name Check	The certificate applicant (i.e., requesting organization) has the right to use the domain name.	The organization name in the certificate signing request (CSR) must match the registrant name per the domain registration.	When coupled with the "authentication of organization" step, the organization applying for a certificate has the legal right to use the domain to which the certificate is being issued. This prevents an entity from obtaining a certificate that associates an organization with a domain that it is not legally authorized to use.	Without this step, an organization could potentially obtain a certificate for another organization's domain.
Authentication of Organization	The requesting organization has the legal right to use the organization name listed in the subject distinguished name field of the certificate.	The certificate applicant is an organization that is: • Registered with the appropriate government entity based on the type and location of the organization. • An active organization. • Based in the location (e.g., city, state, country) included in the certificate.	This confirms that: • The organization enrolling for the certificate exists. • The organization enrolling for the certificate is still in business (i.e., is currently operating).	A certificate could be issued to an organization that does not exist, and the certificate could be used to mislead relying parties. The wrongly issued certificate could be used by the requesting entity to masquerade as an existing organization.
Authorization of Requester	The certificate request is made by an authorized representative of the organization.	The certificate request must be authorized by an employee of the authenticated organization (i.e., the corporate contact).	This ensures that the certificate was in fact requested by someone within the organization who is authorized to do so. The purpose of this step is to confirm: • The corporate contact works for the organization. • The technical contact (i.e., requester) is authorized to receive the certificate. • The corporate contact is aware and approves of the certificate request.	A certificate could be issued and provided to an individual who is not authorized to request a certificate. The certificate could be used for malicious purposes.

REQUIREMENTS FOR SUBSCRIBER AUTHENTICATION

LEGAL PERSPECTIVE

From a legal perspective, authentication of the organization is equally as important. As stated in the American Bar Association (ABA) Information Security Committee's PKI Assessment Guidelines:

> ***Validation of Organization Identity*** [9]
>
> To the extent the public key of a device or application is certified, procedures in [the CP or CPS] would also include validation of the identity of the organization controlling the device or application.
>
> The validation of organization identity generally has two purposes. First, the CA or RA performing the validation must be sure that the name in the certificate application, or other application, corresponds to an organization in the real world. In other words, does the organization really exist? Validation procedures seek to prevent fraudulent applications submitted on behalf of non-existent organizations. Second, assuming that the application refers to a real organization, a CA's or RA's validation procedures must ensure that the people presenting a public key for certification, controlling a device that does so, or applying on behalf of an organization wishing to become a CA or RA actually represent the organization and are authorized to submit the certificate or other kind of application. In other words, is the application in fact originating from and authorized by the organization named in the application? Validation procedures, in this case, attempt to prevent fraud based on the impersonation of another organization.
>
> Assessors should determine, based on the assurances provided by the certificates issued within a PKI, whether both of these purposes must be met by the PKI's validation procedures. For lower assurance certificates, the expenditures involved with accomplishing both of these purposes may not be cost effective in light of a relatively modest risk of fraud. With respect to higher assurance certificates, however, assessors will want to determine whether validation procedures meet both purposes.
>
> PKIs may use a number of ways to identify an organization listed in a certificate application, an organization controlling a device or application, or an organization applying to become a CA, RA, or another kind of PKI participant. The methods for validation of the identity of an organization are necessarily different from those used to validate the identity of individuals. Examples of validation methods include, but are not limited to:
>
> - Comparing information in a certificate application or other application to documentation and/or certifications evidencing valid formation and/or recognition (as a corporation, partnership, nonprofit organization, etc.) in a particular jurisdiction.
> - Comparing information in a certificate application or other application with information available from third-party sources to confirm that the organization named in the application does in fact exist.
> - CA or RA personnel initiating an investigation of the organization, for example through face-to-face discussions with organizational representatives or visits to the organization's site.
> - Communications with personnel at the organization who are able to corroborate the organization's identity and the fact that the organization or one of its representatives has in fact submitted a certificate application or application to become a CA or RA.

REQUIREMENTS FOR SUBSCRIBER AUTHENTICATION

The need for rigor in validation procedures will vary from PKI to PKI. A PKI should use validation procedures commensurate with the level of assurances purportedly offered by the certificates. Determining which procedures are appropriate will depend on the risk, sensitivity, and consequence of the transactions, communications, or other applications supported by the certificate. Validation procedures should be sufficiently robust to match the level of assurances provided by the certificates and the business needs underlying the PKI.

Non-Verified Subscriber Information[10]

Certificates issued to corporate representatives for business conducted on behalf of the corporation may provide insufficient assurances if the corporate affiliation listed in the certificate application is not checked by the CA or RA.

If certificates purportedly support e-commerce activities by corporate representatives, a certificate is unlikely to provide sufficient assurances if corporate affiliation is non-verified subscriber information. Determining which information should be validated will depend on the risk, sensitivity, and consequence of the transactions, communications, or other applications supported by the certificate. PKIs should ensure that enough information is validated and critical information is not placed within the non-verified category to match the level of assurances provided by the certificates and the business needs underlying the PKI.

The ABA's PKI Assessment Guidelines support the concept of assurance levels for certificates, the need to perform subscriber authentication procedures commensurate with the assurance level of the certificate, and the need for relying parties to assess the appropriateness of a certificate for a particular use. For high-assurance certificates, robust authentication procedures are necessary to mitigate the risk of fraud.

RISKS OF INSUFFICIENT SUBSCRIBER AUTHENTICATION

The use of high-assurance SSL certificates is very important for electronic commerce in an online environment. This section describes some of the related threats stemming from using lower-assurance SSL certificates. In all of these scenarios, the failure of a CA to perform any of the three basis checks (domain name check, authentication of organization, and authorization of requester) may result in the loss of customer confidence; bad public relations through diminished trust in PKI, SSL, and the ubiquitous lock icon used by common browser software; and potential legal action.

SCENARIO 1: No authentication of the organization by the CA

Suppose ABC Global Bank registers a domain, www.abcbank.com, and implements a legitimate online banking Web site using an SSL certificate. This certificate includes the following in the subject distinguished name:

Organization (O)	**=**	**ABC Global Bank**
Common name (CN)	**=**	**abcbank.com**

Now suppose that "Bad Bob" registers www.abcbankonline.com, mimics ABC Global Bank's site, obtains an unauthenticated SSL certificate, and lures unsuspecting customers to his site. Bad Bob's certificate includes one of the sets of values described in the following table in the subject distinguished name. None of these values contains an authenticated organization name.

RISKS OF INSUFFICIENT SUBSCRIBER AUTHENTICATION

	Option 1	Option 2	Option 3	Option 4
Organization (O) =	ABC Global Bank	abcbankonline.com	abcbankonline.com	
Common Name (CN) =	abcbankonline.com	abcbankonline.com	abcbankonline.com	abcbankonline.com
Disclaimer[11]	Organization not authenticated	Organization not authenticated		

When a customer visits Bad Bob's site, he has no easy way to know the site is not legitimate. If he sees the lock icon, he will get a false sense of security. He will likely think that he is at ABC Global Bank's Web site, but really is connecting to Bad Bob's counterfeit site. Seeing the lock icon on an information submission page will make the user more likely to enter his user ID and password, account information, or other personal information. Alternatively, Bad Bob might capture the user ID and password, divert the user to the legitimate site, and automatically resubmit the user ID and password to the valid site—all without the knowledge of the unsuspecting customer.

Perhaps the customer will look at the SSL certificate and see an "organization not authenticated" disclaimer or see that ABC Global Bank was not named in the certificate, but this assumes that the user will take these additional steps before entering his user ID and password.

This scenario is equally applicable to an online retail site, online medical records site, tax return filing site, etc. In any of these cases, having an unauthenticated SSL certificate could enable a malicious individual to enhance the appearance of legitimacy for his counterfeit site and facilitate the capture of personal or sensitive information.

Requiring authentication of the organization guards against the possibility that a malicious individual or entity can obtain a certificate containing another organization's name. Including an authenticated organization name in the SSL certificate provides assurance to users that the organization that implemented the certificate on its Web site exists.

SCENARIO 2:
No check of the applicant's right to use the domain name by the CA

Suppose Bad Bob registers a domain (abcbankonline.com) to a nonexistent entity (Internet Bank Corp.). He then requests an SSL certificate with the organization name ABC Global Bank and the common name abcbankonline.com. If the CA does not verify ABC Global Bank's right to use the domain name abcbankonline.com, a malicious individual could obtain an SSL certificate for a counterfeit site but include another organization's real organization name in the certificate.

This would enable a malicious individual who established a counterfeit site (abcbankonline.com) to install an SSL certificate on information entry pages and include the real organization's name (ABC Global Bank) in the certificate. As a result, if a user were to examine the certificate to authenticate the organization, he could falsely believe that this was ABC Global Bank's Web site.

Alternatively, Bad Bob might register a domain (abcinvestments.com) and request an SSL certificate that includes the organization name ABC Global Bank. Bad Bob then publicizes ABC Investments as a subsidiary of ABC Global Bank, establishes a fraudulent Web site, and uses the lock icon and ABC Global Bank SSL certificate to deceive users into providing personal and financial information.

The purpose of a certificate is to bind a user's identity and other information to a public key. If the correctness of that information is not verified, the trustworthiness of legitimate certificates is diminished.

RISKS OF INSUFFICIENT SUBSCRIBER AUTHENTICATION

SCENARIO 3: No check of organization's existence by the CA

Suppose Bad Bob registers a domain for Internet Bank Corp. (which does not exist), perhaps using a stolen credit card as the method of payment. Bad Bob creates a Web site and obtains an unauthenticated SSL certificate. When a customer visits the site, he will see the browser's lock icon and think that his information will be secure. Having an SSL certificate helps Bad Bob give the appearance of legitimacy to his Web site. If Bad Bob offers higher than average interest rates on deposits or attractive financing, he may be able to entice users into providing personal information.

Requiring verification of the organization's existence guards against the possibility of an individual pretending to be an organization.

SCENARIO 4: No check of the applicant's authority to request a certificate for the organization by the CA

Bad Bob requests an SSL certificate for ABC Global Bank for use with a certain ABC Global Bank domain, even though he is not an authorized agent for ABC Global Bank. If the CA does not verify Bad Bob's authority to request an SSL certificate, a certificate could be inadvertently issued. Bad Bob might set up a Web server that mimics the ABC Global Bank Web site. On his Web server, Bad Bob might install the SSL certificate giving the appearance (through display of the lock icon) to unsuspecting users that they are dealing with ABC Global Bank and that their information will be secure. Furthermore, if certificates can be issued to unauthorized parties, the trustworthiness of legitimate certificates is diminished.

Requiring verification of the certificate applicant's authority to request a certificate (e.g., employment with the organization named in the certificate) guards against the threat of issuing a certificate to a malicious individual who is not associated with the organization.

RELYING PARTY CONTROL CONSIDERATIONS

In addition to the functions that must be employed by the CA, there are several requirements that are the responsibility of the Internet user and impact his browser software. These include consideration of:

- The appropriateness of a specific certificate for a particular application or transaction
- Trusted Root CAs whose certificates are pre-installed in browser software
- Subordinate CAs (Sub-CAs) that are automatically trusted if they chain to a trusted Root CA
- Browser security settings related to checking certificate status
- The use of "shared SSL" by Web sites implemented in a shared hosting environment.

APPROPRIATENESS FOR USE

One of the core assumptions of PKI implementations is that relying parties (i.e., Internet users) are expected to assess the appropriateness of a particular type or class of certificate relative to its intended use. Certificate policies, certification practice statements, subscriber agreements, relying party agreements, and PKI disclosure statements are the vehicles to convey this responsibility.

In closed communities (such as an internal corporate PKI) or in a membership community (e.g., the Identrus PKI hierarchy) there is typically a policy management authority (PMA) that specifies the trust requirements for the community. The PMA is obligated to understand and specify the intended and acceptable uses for certificates within the community.

However, this poses a problem in an open PKI environment such as the Internet, where there is no designated PMA. As a result, it is necessary for participating CAs to implement policies and practices that meet the needs of the user community and meet or exceed industry norms.

RELYING PARTY CONTROL CONSIDERATIONS

In this open environment, it is unreasonable to expect each user to assess the appropriateness of a particular certificate for use, the appropriateness of a particular certificate policy, or the trustworthiness of a CA without appropriate user education and user-friendly tools for doing so. It is incumbent on CAs and other technology providers (i.e., browser providers) to provide user-friendly automated mechanisms for users to determine whether or not they should rely on a specific certificate. Interested parties (including browser providers, audit standards organizations, industry bodies, and users) should act to define standards, where necessary, to preserve the trustworthiness of the community.

ROOT CA AND SUBORDINATE CA TRUST ISSUES

In the current Internet model, some Root CA certificates are pre-installed in browser software. Users' browsers automatically trust the Root CA certificates that have been included in their browsers, unless the user specifically changes default security settings. As a result, certificates issued by these trusted Root CAs are automatically trusted by user browsers. In addition, certificates issued by Sub-CAs that chain to trusted Root CAs are also automatically trusted by user browsers. Accordingly, it is essential that there be a basis for trusting these Root CAs.

Major browser providers such as Microsoft and Netscape established procedures for accepting new roots into their browsers, although these procedures did not include a formal assessment of the CA's policies and practices.

Recognizing the need to enforce baseline standards on CAs who include or wish to include their Root CA certificates in Microsoft browsers, Microsoft now requires that a CA successfully complete an annual WebTrust for CAs audit. Failure to do so will cause the exclusion of the CA's root certificate in future browser releases and the Windows Update function. Other browser providers such as Netscape and AOL have not formally established a similar requirement. However, this requirement alone is not a complete solution.

For example, a new CA is free to contract with another CA who has one or more trusted roots in browser software to have its Sub-CA certificate signed by the trusted Root CA, enabling certificates issued by the Sub-CA to chain to the Root CA and therefore automatically be trusted by end users. In this scenario, the Root CA generally should have a CP that specifies required baseline policies and practices for Sub-CAs. The Sub-CA also should have a CPS that defines its practices. The Root CA should also have a process to verify that the Sub-CA's CPS complies with the Root CA's CP (e.g., through an assessment of the Sub-CA's practices prior to signing the Sub-CA's certificate and periodic audits of the Sub-CA's compliance with its CP and CPS). In addition, the Sub-CA should be audited at least on an annual basis to assess its compliance with the CPS and the operating effectiveness of its control procedures.

Currently, browser providers have not specified any requirements for the types of certificates that may be issued by Root CAs or Sub-CAs or specific policy and practice requirements (such as minimum subscriber authentication requirements). For the Internet user to assess the trustworthiness of a particular certificate issued by the Sub-CA, the user would need to examine the Sub-CA's CPS and/or CP.

Internet users rely on the browser providers to include trustworthy Root CA certificates in their browsers (unless the user elects to manually remove pre-installed Root CA certificates based on his own assessment of the Root CAs). Browser providers should implement technical mechanisms that enable Internet users to make informed decisions regarding the trustworthiness of a particular certificate that chains to a trusted root.

RELYING PARTY CONTROL CONSIDERATIONS

CERTIFICATE STATUS CHECKING

Before relying on a certificate, relying parties are expected to check the status of the certificate, as well as the status of all the certificates in its certificate chain to ensure that none of the certificates in the chain have expired or been revoked. The CA typically publishes certificate status information using CRLs or other mechanisms such as OCSP. However, most versions of browser software disable certificate status checking by default, and the use of certificate extensions that facilitate automated status checking is inconsistent.

To rely on a particular certificate, Internet users are required to understand the importance of certificate status checking, configure their browsers to check certificate status, and manually consult a CRL where automated certificate status checking is not possible. As a result, certificate status checking is routinely not performed by Internet users.

SHARED HOSTING

Internet users also need to be aware of specific requirements for Web sites that are implemented in an ISP's shared hosting environment (i.e., where a company's Web site is hosted on a server shared with other companies). In a shared hosting environment, a company's Web site might be hosted using the company's own domain name (e.g., www.abcco.com), a directory within the ISP's domain (e.g., www.isp.com/abcco), or a sub-domain within the ISP's domain (e.g., www.abcco.isp.com).

ISPs often obtain an SSL certificate in the ISP's name for the ISP's domain and share the SSL certificate among its hosted customers, a practice known as "shared SSL." As a result, when an Internet user accesses a Web page secured with the ISP's SSL certificate, the user can authenticate the ISP but not the company that is providing the Web site (e.g., ABC Co.). Where the customer's Web site has its own domain name, the user is often transferred from an abcco.com HTTP page to an isp.com HTTPS page for entry of personal or order information. Where the customer's Web site is hosted within a directory or sub-domain in the ISP's domain, the user would access an isp.com HTTPS page for this purpose.

In each of these cases, unless ABC Co. discloses on its Web site that it is using shared SSL, the Internet user would not know whether he was doing business with ABC Co. or the ISP. When the user visits a Web page secured by the ISP's SSL certificate and sees the lock icon, he may conclude that ABC Co. has been authenticated when, in reality, only the ISP has been authenticated.

OTHER TYPES OF HIGH-ASSURANCE CERTIFICATES

There are several types of high-assurance certificates issued to organizations. These generally fall into two categories: server certificates and code signing certificates. There are several types of server certificates, including standard SSL certificates; server gated cryptography (SGC)–enabled SSL certificates, which are configured to enable the use of 128-bit encryption; electronic data interchange (EDI) certificates; online financial exchange (OFX) certificates; and other special-purpose certificates. Discussion of the specific purposes and requirements of these specific types of certificates is beyond the scope of this paper.

Code signing certificates are used for digital signing of software, macros, objects, and other types of code. Even more so than with SSL certificates, it is important that the CA authenticate the organization to which the certificate is issued and the authority of the individual to request a certificate on behalf of the organization. Unlike SSL certificates, the use of a code signing certificate is not tied to a specific domain name or Web site. As a result, a malicious individual who obtains a fraudulently issued code signing certificate can more easily use that certificate for malicious purposes (e.g., by digitally signing viruses, other malicious code, or pirated software).

RECOMMENDATIONS AND FUTURE REQUIREMENTS

Many are familiar with the cartoon[12] depicting a dog sitting at a computer with the caption, "Nobody knows you're a dog on the Internet." The point being that it is difficult to know who you are dealing with in an online environment. Similarly, it can be difficult to ascertain whether a Web site belongs to an existing organization. To this end, high-assurance server certificates have played an important role.

For SSL-secured business-to-business (B2B), business-to-consumer (B2C), government-to-consumer (G2C), and other electronic commerce, the use of high-assurance server certificates is a critical success factor for the continued growth of electronic commerce on the Internet.

Traditionally, Internet users have relied on their browsers' lock icon as an indication that they could trust the authenticity of a Web site. Microsoft and Netscape have described the lock to consumers as providing assurance as to Web site identity and security (see Appendix D). However, these assurances were based on a model in which high-assurance SSL server certificates are issued to authenticated organizations and provide three security services—confidentiality, authentication, and integrity. In recent months, this model has changed and emerging CAs are now issuing unauthenticated low-assurance SSL server certificates that provide only two security services—confidentiality and integrity.

To the Internet user, there is no easy way to distinguish between a Web site that uses a high-assurance SSL server certificate and one that uses a lower-assurance SSL server certificate. As a result, Internet users may have a false sense of security when they visit a Web site that uses the low-assurance variety. Furthermore, removing authentication of the organization from the SSL server certificate issuance process introduces a variety of security threats and may serve to diminish the trustworthiness of SSL certificates in general.

RECOMMENDATIONS AND FUTURE REQUIREMENTS

A combination of policy and technology enhancements is necessary to enable Internet users to assess the trustworthiness of an SSL certificate. From a policy perspective, browser providers control the primary mechanism for trusting SSL certificates—the inclusion of trusted Root CA certificates in their browsers. However, a model certificate policy that includes the requirements for SSL certificate issuance has not been established. Such a CP should be established within the industry, perhaps under the auspices of a security standards organization such as the American National Standards Institute (ANSI), an industry group such as the PKI Forum, or browser providers. A process would also be required to assess a given CA's compliance with the CP.

From a technology perspective, CAs and browser providers have not fully implemented the technical capabilities of certificates. Browsers are configured to verify that a certificate chains to a trusted Root CA. However, certificates can also contain a certificate policies extension that specifies the certificate policy(ies) under which a particular certificate was issued. Browsers should be preconfigured to require the presence of specific values in the certificate policies extension field to enable the use of SSL and the appearance of the lock icon. For example, browsers could be configured to provide a warning message to the user when a certificate (e.g., an unauthenticated SSL certificate) is presented that does not contain the appropriate values in the certificate policies extension field.

In addition, CAs and browser providers have not fully implemented automated certificate status checking capabilities. Most browser releases are preconfigured with SSL certificate status checking disabled. Many SSL certificates do not contain the CRL distribution points extension, which enables automated certificate status checking. In addition, certificate status checking using CRLs is not an instantaneous process. As a result, most Internet users do not check certificate status when visiting a Web site. CAs and browser providers should focus on consistently using the CRL distribution points extension, implementing efficient certificate status checking mechanisms such as OCSP, and enabling browsers to check certificate status by default.

In summary, to maintain a high level of assurance in SSL certificates used in electronic commerce, several action steps are required:

- A model certificate policy for SSL certificates should be established, adopted, and assigned an OID (object identifier).
- Baseline criteria for SSL certificate subscriber authentication should be incorporated into WebTrust for CAs (this could be in the form of additional criteria added to WebTrust for CAs or required compliance with a specific SSL certificate policy).
- Browser providers should require the use of the certificate policies extension.
- Browser providers should require that SSL certificates used on the Internet comply with the model SSL certificate policy.
- Browser providers should incorporate functionality into their browsers to alert the Internet user if a presented SSL certificate does not contain the appropriate OID for the SSL CP in the certificate policies extension field, enabling the user to differentiate between higher- and lower-assurance SSL certificates.
- CAs should consistently use the CRL distribution points extension in SSL certificates to enable automated certificate status checking.
- Browser providers should work with CAs to effectively implement efficient certificate status checking mechanisms (such as OCSP) and configure browsers to check certificate status by default.
- CAs and browser providers should educate Internet users as to the meaning of the browser's lock icon, Web site identity, and the importance of authentication.
- In a shared hosting environment where shared SSL is used, automated mechanisms are necessary to enable the user to distinguish between an SSL certificate issued to an ISP and an SSL certificate issued to an organization for its Web site. CAs should also specify in their CP, CPS, and subscriber agreements whether or not their certificates may be used for this purpose. ISPs that provide shared SSL as part of their hosting services should ensure that the use of this practice is disclosed to Web site visitors.

APPENDIX A:
WEBTRUST FOR CAS— PRINCIPLES AND CRITERIA

WebTrust for CAs has established three principles that must be achieved by a CA as part of a WebTrust for CAs examination.[13]

Principle	Description
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.
Service Integrity	The certification authority maintains effective controls to provide reasonable assurance that: • Subscriber information was properly authenticated (for the registration activities performed by that CA). • The integrity of keys and certificates it manages is established and protected throughout their life cycles.
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. • CA systems development, maintenance, and operation are properly authorized and performed to maintain CA systems integrity.

APPENDIX A:
WEBTRUST FOR CAS— PRINCIPLES AND CRITERIA

These principles are supported by the detailed WebTrust for CAs criteria, which include the following:

Principle	Specific Criteria Topics
Disclosure of CA Business Practices (e.g., CPS and CP)	Required disclosures of the CA's general, key management, certificate life cycle management, and CA environmental control policies and practices.
Service Integrity: Key Life Cycle Management	• CA key generation • CA key storage, backup, and recovery • CA public key distribution • CA key escrow (if supported) • CA key usage • CA key archival and destruction • CA cryptographic hardware life cycle management • CA-provided subscriber key management services (if supported)
Service Integrity: Certificate Life Cycle Management	• Subscriber registration • Certificate renewal (if supported) • Certificate rekey • Certificate issuance • Certificate distribution • Certificate revocation • Certificate suspension (if supported) • Certificate status information processing • Integrated circuit card life cycle management (if supported)
CA Environmental Controls	• CPS and CP management • Security management • Asset classification and management • Personnel security • Physical and environment security • Operations management • System access management • Systems development and maintenance • Business continuity management • Monitoring and compliance • Event journaling

See http://webtrust.org/certauth_fin.htm to download the WebTrust Program for Certification Authorities document, which describes these criteria in detail.

APPENDIX B:
CERTIFICATE POLICY CONTENTS

Among other things, certificate policies include the following elements:

- Description of the conditions for applicability of the certificates issued by the CA that reference a specific certificate policy, including
  - 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
- Disclosure of governing law
- Identification of subscriber obligations and liabilities to
  - Provide information in certificate requests that is accurate and that the act of accepting the certificate guarantees that the information contained in the certificate request is accurate
  - Protect access to the private key associated with the certificate
  - Notify the issuer of private key compromise or change of status
  - Restrict the use of the certificate to the use specified
- Identification of issuer obligations and liabilities to
  - Notify the subscriber who is the subject of the certificate that the certificate has been issued
  - Notify participating subscribers and relying parties of certificate issuance in accordance with the CA's CPS (e.g., by posting certificates issued in a repository available to other participating subscribers and relying parties)
  - Notify any subscriber whose certificate is being revoked or suspended
  - Notify participating subscribers and relying parties of certificate status in accordance with the CA's CPS (e.g., by posting certificate status information in a repository available to participating subscribers and relying parties)
  - Comply with the CP identified and its CPS
  - Provide a disclaimer of liability for misuse of a certificate for disallowed applications
  - Provide confidentiality of nonpublic subscriber and relying party information that is collected
- Identification of relying party obligations and liabilities to
  - Restrict use to applications identified and disallow a claim of liability for misuse of the certificate on excluded applications
  - Verify digital signature
  - Validate certificate content and status
  - Acknowledge applicable liability caps and warranties
- Identification of any applicable reliance or financial limits for certificate usage.[14]

APPENDIX C:
EXAMPLE ASSURANCE LEVELS

The U.S. Federal Bridge CA has defined five assurance levels as described in the table below.[15]

Class	Description
Test	This level is used for interoperability testing between the FBCA and principal CAs. It is used solely for this purpose and conveys no assurance information.
Rudimentary	This level provides the lowest degree of assurance concerning identity of the individual. One of the primary functions of this level is to provide data integrity to the information being signed. This level is relevant to environments in which the risk of malicious activity is considered to be low. It is not suitable for transactions requiring authentication and is generally insufficient for transactions requiring confidentiality, but may be used for the latter where certificates having higher levels of assurance are unavailable.
Basic	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise that are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.
Medium	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
High	This level is appropriate for use where the threats to data are high, or the consequences of the failure of security services are high. This may include very high-value transactions or high levels of fraud risk.

APPENDIX D:
WHAT DOES AN SSL CERTIFICATE MEAN?

Browser providers emphasize the importance of the security services provided by SSL certificates in the materials contained in their Web sites and help screens.

INTERNET EXPLORER

Microsoft Internet Explorer 5.0 Help indicates:

> A "Web site certificate" states that a specific Web site is secure and genuine. It ensures that no other Web site can assume the identity of the original secure site.[16]

The IE 5.0 informational text accessible when a user attempts to access an SSL-secured Web page indicates:

> You are attempting to make a secure connection to this Web site. This Web site provides secure communication and has a valid certificate. Secure communication means that information you provide, such as your name or credit-card number, is encrypted so that it can't be read or intercepted by other people. The certificate is a statement guaranteeing the security of this Web site. A certificate contains information that a specific Web site is authentic. This ensures that no other site can assume the identity of the original site.

The IE 5.0 informational text accessible when a user attempts to leave an SSL-secured Web page indicates:

> However, the Web site you are going to does not use a security protocol, so information you send and receive will not be protected. And since the site does not have a certificate, you cannot be sure that the site is who it says it is. Given what you know about this Web site and your computer, you must decide whether to view this site. If you do not feel confident about viewing this site, click "No."[17]

NETSCAPE NAVIGATOR®

Netscape's Web site describes the purpose and use of SSL certificates as follows:

> Server certificates are designed to protect you and visitors to your site. Installing a digital certificate on your server lets you:
> – Authenticate your site. A digital certificate on your server automatically communicates your site's authenticity to visitors' Web browsers, confirming that the visitor is actually communicating with you, and not with a fraudulent site stealing credit card numbers or personal information.
> – Keep private communications private. Digital certificates encrypt the data visitors that exchange with your site to keep it safe from interception or tampering using SSL (secure sockets layer) technology, the industry-standard method for protecting Web communications.[18]

Netscape's Web site describes the lock icon as follows:

> For many people, the lock icon provides sufficient information about a page's encryption status. If you want additional warnings, you can select one or more of the warning checkboxes in the SSL preferences panel. Think carefully about whether you want such warnings, since they can be annoying.[19]

In Netscape 6.2, clicking on the lock icon produces a window that states whether the "Web site identity has been verified" and which CA issued the site's SSL certificate. This window also allows the user to view the site's SSL certificate.

APPENDIX D:
WHAT DOES AN SSL CERTIFICATE MEAN?

AOL BROWSER

America Online's version 7.0 browser users are further encouraged to rely on the lock icon as assurance. For example:

- When an AOL version 7.0 browser user using the default settings and a Windows machine accesses an HTTPS page, a gold lock appears in the bottom right corner of the screen. However, the user cannot click on the lock or intuitively obtain any additional information. The user also does not receive an alert that he is connecting to a secure page. When leaving a secure site, the disappearance of the lock icon is apparently the only notification to the user.
- It is possible for the user to examine the server certificate, but not through an AOL browser function. By right-clicking on the Web page and clicking on the certificates button, the user is able to view the certificate. However, this is considerably less intuitive than clicking on the lock (as is the standard for Microsoft Internet Explorer and Netscape Navigator).
- The AOL Help section informs the user that browser security settings can be changed through the AOL Preferences section. However, following these instructions, the user is directed to Windows Internet Options where security settings can be modified. The AOL browser apparently relies on the user's operating system for security configurations and does not contain any specific security capabilities. As a result, the AOL browser user is unable to easily view a server certificate, look at the organization name, and so on.

NOTES

[1] AICPA/CICA WebTrust Program for Certification Authorities (WebTrust for CAs), ANS X9.79-1:2000 *PKI Policy and Practices Framework* (X9.79).

[2] ISO CD 21188 DRAFT, *PKI Policy and Practices Framework*, dated June 2002, §B.

[3] WebTrust for CAs, pp. 33–34.

[4] WebTrust for CAs, p. 37.

[5] WebTrust for CAs, p. 27.

[6] ISO CD 21188 DRAFT, dated June 2002, §B.4.1.

[7] ISO CD 21188 DRAFT, dated June 2002, §B.4.4.

[8] Based on an analysis of disclosed subscriber authentication practices as of 12/01.

[9] American Bar Association, Information Security Committee (ABA-ISC), PKI Assessment Guidelines (PAG), Public Draft for Comment, dated June 18, 2001, §C.3.2.3

[10] ABA-ISC, PAG §C.3.2.6

[11] Such a disclaimer might, for example, be included in an informational organization unit (OU) field.

[12] Peter Steiner, *The New Yorker*, July 5, 1993.

[13] See the AICPA/CICA WebTrust Program for Certification Authorities Version 1.0, dated August 25, 2000, for more information.

[14] ANS X9.79.

[15] X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA), dated February 11, 2002, §13.4.

[16] "Protecting your identity over the Internet," Microsoft Explorer 5.0 Help.

[17] Internet Explorer security alert "Entering a non-secure Web site from a secure Web site."

[18] www.netscape.com/security/techbriefs/servercerts/index.html?cp=sciln

[19] "SSL Warnings," Netscape 6.2 Help.