

Realtime  
publishers

"Leading the Conversation"

*The Shortcut Guide™ To*



# Extended Validation SSL Certificates

*sponsored by*



*Dan Sullivan*

Chapter 3: Authentication and Verification .....	34
Standards-Based Verification Process .....	35
Structure of the CA/Browser Forum.....	35
EV Policies Governing CAs .....	36
Compliance Policies.....	36
Insurance Requirements.....	37
Audit Requirements .....	37
Obtaining an EV SSL Certificate.....	38
Subject Verification Requirements .....	38
Business Verification Requirements.....	38
Government Verification Requirements .....	39
Private Organizations.....	39
Documentation Requirements.....	40
Role Requirements.....	40
Verification Requirements .....	41
Verifying Legal Existence .....	41
Entity Legal Existence .....	41
Principal Legal Existence .....	42
Physical Existence .....	42
Operational Existence .....	42
Domain Name Rights.....	42
Authority to Request an EV SSL Certificate .....	44
Utilizing Existing Trust Models.....	44
Maintaining Certification Status.....	45
Additional Requirements of CAs.....	46
Employee Regulations .....	47
RAs .....	47
Document Management .....	47
Data Security.....	47
Summary .....	48

## Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at [info@realtimepublishers.com](mailto:info@realtimepublishers.com).

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

## Chapter 3: Authentication and Verification


In the first two chapters, we have seen a wide range of threats to Web security, including phishing, loss of privacy and confidentiality. The implications for businesses include fraud, identity theft, damage to brand reputation, and ultimately the reduced potential for online business due to a lack of trust. Clearly, business transactions are dependent on establishing authenticated identities and maintaining the confidentiality and integrity of transactions. SSL has met many of these needs, but changes in phishing and other attacks are pushing the limits of SSL-based protections. Certification Authorities (CAs) and browser vendors have responded with the Extended Validation (EV) SSL certificate.

The EV SSL authentication and verification standard is more demanding on the part of CAs, parties seeking certificates, and has also required feature and functionality updates to web browsers in order to display the unique interface conventions associated with these certificates. This chapter will focus on the CAs and the parties seeking certificates. The use of EV SSL within browsers is the subject of Chapter 4.

The authentication and verification process is best explored by examining several aspects:

- Elements of the standards-based verification process
- Steps to obtaining an EV SSL certificate
- Verification requirements and processes
- Certificate revocation

Together these components provide for a better identification process, which in turn establishes the foundation for greater trust—that is the objective of EV SSL certificates.

 The focus of this chapter is the process and procedures used to authenticate and issue EV SSL Certificates. For details about the business case and cost justification for these enhanced measures, see Chapter 1.


## Standards-Based Verification Process

The additional trust that one places in EV SSL certificates is based largely on the comprehensive verification process. To describe the verification process, it is useful to consider three elements:

- Structure of the CA/Browser Forum
- Extended Validation policies
- Compliance issues

### *Structure of the CA/Browser Forum*


As we have seen with traditional SSL certificates, CAs often have different standards for verification. For this reason CAs, working with browser vendors, have established a governing body known as the CA/Browser Forum to define a standards-based verification process.

 See “Limitations of SSL: Lack of Standards” in Chapter 2 for a discussion of issues related to non-standardized certification processes.

The evolution of standards in the field of information security is similar to that of other disciplines. From the esoteric standards of the Institute of Electrical and Electronics Engineers (IEEE) to the well-known Underwriters Laboratory (UL), technical business disciplines have benefited from objective third parties who are able to create standards that are adopted across an industry. The CA/Browser Forum has filled this role for the digital certification industry.

The CA/Browser Forum includes leading CAs—such as Thawte, VeriSign, and GeoTrust—as well as browser vendors and open source projects, including Microsoft, Opera Software, KDE, and The Mozilla Foundation. The widespread participation is crucial to ensuring that a single set of standards is adopted to prevent confusion and defeat the purpose of EV. For example, if some leading CAs did not adopt this standard and instead proposed their own, there could be confusion in the market about the definition of EV SSLs and possibly concerns that one standard is a “watered down” version of the other.

The founders of the CA/Browser Forum recognized that the value is in being able to demonstrate this high level of authentication to the end user. To be most effective, end users would have to be able to identify sites secured by EV SSL certificates easily. Unlike CAs, browser vendors have more flexibility with how they display EV SSL information. For example, all browsers may change the background color of the URL address line when a site is certified by EV SSL but some may use additional visual cues. IE7 was the first to develop the “green bar”—other browser manufacturers will develop similar methodologies to signal the presence of an EV SSL certificate.

 For example, VeriSign provides a Firefox plug-in to turn the address bar green when an EV SSL certificate is available and provides additional information when the user right-clicks the address bar. The add-on is available at <https://addons.mozilla.org/en-US/firefox/addon/4828>.

## EV Policies Governing CAs

The CA/Browser Forum has issued a set of requirements for CAs to follow when processing EV SSL certificate requests. To be considered a legitimate provider of EV certificates, CAs must follow the requirements that address areas such as:

- Compliance
- Insurance
- Disclosure
- Commitment to guidelines

Each of these areas provides a component of the foundation on which trust in EV SSL certificates is built.

## Compliance Policies

The compliance policies establish the minimum expectations for a CA. Users of EV SSL certificates might even take for granted that the compliance policies are followed. Nonetheless, the CA/Browser Forum has spelled them out directly:

- Implement and make public its own auditable processes for processing requests for EV SSL certificates
- Make known the CA's and Root CA's certification hierarchy
- Incorporate the CA/Browser Forum guidelines in their EV certification process
- Comply with business laws of the jurisdiction in which the CA does business
- Implement the requirements of the WebTrust Program for CAs or the WebTrust EV program

The WebTrust program is a set of principles and policies established by a professional organization from the public accounting field to further boost consumer confidence and trust in e-commerce and the use of PKI technology. Participating public accounting firms assess the services provided by CAs to determine whether they meet the policies and criteria established by the WebTrust Program. In addition to the basic principles established to verify identities, compliance requirements address insurance and auditing. For CAs to have their root included in browsers, they need to complete the WebTrust audit.



It is important to note that if a CA fails its annual WebTrust audit, its certificates will no longer cause compatible browsers to behave as if they were EV SSL certificates. The certificates will still support encrypted communication, but the browser will not show the green bar when displaying a page from a site with an EV SSL certificate from such a CA.



For more information about the WebTrust Program for CAs see [http://www.webtrust.org/CertAuth\\_fin.htm](http://www.webtrust.org/CertAuth_fin.htm).

## Insurance Requirements

Like many businesses providing professional services, CAs are expected to carry general liability and errors and omissions insurance. The general liability insurance must be at least \$2 million and the errors and omissions insurance must be at least \$5 million. The guidelines stipulate additional specifications for CAs that want to self-insure. As one might expect, there are stringent audit requirements imposed on CAs issuing EV certificates.

## Audit Requirements

CAs are required to undergo these types of audits:

- Pre-issuance readiness audits
- Regular self-audits
- Annual independent audits

The pre-issuance readiness audit is conducted before a CA begins issuing EV SSL certificates. This audit is based on the WebTrust EV program and determines at the time of the audit whether the CA is prepared to follow the policies and procedures established by the CA/Browser Forum.

Once the initial pre-issuance audit is completed and the CA begins issuing certificates, the CA must conduct regular self audits. If the CA performed final due diligence and cross validation, then self audits must be performed using at least 3% of the certificates issued. In cases in which the CA depended on another party, known as a registration authority (RA), for the final due diligence and cross validation, the self audit must use at least 6% of certificates issued.

An annual audit is done to ensure that CAs are following all policies and procedures established by the CA/Browser Forum. For commercial CAs, the audit is based on the WebTrust Program for CA audit and the WebTrust EV Auditing Program. Government agencies that issue EV SSL certificates may be audited by government auditing agencies. In both commercial and business audits, the final report must be made public.

The CA/Browser Forum has established a standards-based verification process that defines policies governing the issuance of EV SSL certificates and establishes criteria for how CAs perform their business operations to ensure the certification process is not compromised. Audits and public disclosure of audit reports are required to ensure transparency of operations, which is essential to maintaining confidence in the EV SSL certificate authentication process.

## Obtaining an EV SSL Certificate

Obtaining a conventional SSL certificate can be done relatively quickly and depending on the product/CA, with minimal documentation. In some cases, it may just require verification that you have a right to a particular domain name. In other cases, there may be some additional documents required but the specific details of those requirements can vary among CAs.

Obtaining an EV SSL, however, requires a well-defined set of authentication requirements:

- Subject verification requirements
- Document requirements
- Role requirements

The reason for such stringent requirements is to ensure that EV SSL certificates are issued only to legitimate organizations and only in response to valid requests from employees or agents authorized to make such requests.

### **Subject Verification Requirements**

The first step to obtaining an EV SSL certificate is to demonstrate the company's legitimate organizational identity. The CA/Browser guidelines recognize three types of organizations:

- Businesses
- Government agencies
- Private organizations

Each has a specific set of requirements to be eligible to receive an EV SSL certificate.

### **Business Verification Requirements**

The business verification requirements are used to establish that a requestor is a legitimate business and recognized in the jurisdiction in which it has established a presence. The specific requirements include:

- The business has registered with government bodies and received a charter, license, or documented recognition
- The business has established a physical and business presence
- At least one principal in the business is identified
- The identified principal can vouch for the statement and claims made in the certificate request
- The business and the principal are both located in a jurisdiction in which the CA is allowed to conduct business
- The business may not be under any government restrictions established by the government in the CA's jurisdiction

Essentially, these requirements ensure the business actually exists, there is at least one known individual associated with the business, and there are no legal restrictions on the CA conducting business with the organization.



---

## Government Verification Requirements

The requirements on a government agency are a subset of the requirements on business entities and include:

- The government agency must be established by a political subdivision of the jurisdiction in which it operates
- The CA must be allowed to do business in the country in which the government agency operates
- The government agency or the country in which it operates must not be subject to restrictions by the CA's host jurisdiction

## Private Organizations

The requirements on a private organization are similar to those of a business entity. The basic requirements are:

- The organization is recognized as incorporated or has received a charter from a state or federal agency
- It must have an established and legally recognized office or other facility
- The organization must be legally active
- It must have a verifiable physical presence
- The CA must be allowed to do business in the country in which the private organization operates
- The private organization must not be subject to restrictions by the CA's host jurisdiction

In some ways, these requirements may seem obvious. But traditional SSL has lacked standards defining the level to which CA's are required to vet this information, and as a result phishers and other illegitimate operations are able to acquire SSL certificates. Although having an SSL certificate is no guarantee of the reputation of the holder, phishers can and do take advantage of the appearance of legitimacy that has come to be associated with secure Web session.

### **Documentation Requirements**

The documentation requirements in the CA/Browser Forum guidelines consist of several specific items that must be produced before issuing an EV SSL certificate:

- An EV certificate request
- A subscriber agreement
- Documents required to prove the elements of the previous section

CAs have some latitude with regard to the documentation requirements. This is necessary because one cannot reasonably define a fixed list of documents that can support identity verification and business operations. For example, different jurisdictions may issue different documentation to businesses. A multinational company may have different types of business licenses, incorporation papers, and other legal documents for each of its subsidiaries. CAs may have the discretionary power to call for additional documentation when there may be questions about the legitimacy of a request; they might also use discretion to waive common documentation requests when the authenticity of a request is already well established.

### **Role Requirements**

EV certificates require the identification of three roles:

- **Certificate requestor**—The certificate requestor is the person or agent for a business or government agency who submits the EV Certificate Request on behalf of the business or government agency. In general, the requestor is a person employed or contracted by the organization or a third party who submits the request on behalf of a customer, as in the case of Internet service providers (ISPs).
- **Certificate approver**—The certificate approver is a person or third party who has the authority to approve requests made by the requestor.
- **Contract signer**—The contract signer is a person who has been granted the authority to sign subscriber agreements on behalf of the requesting business or government agency.

An organization can assign a single person to all these roles or have one or more persons assigned to each role.

## Verification Requirements

When a business or organization applies for an EV SSL certificate, it is the responsibility of the applicant to provide suitable documentation to authenticate their identity. The previous section reviewed the types of documentation that are required as well as other constraints on when CAs are allowed to issue EV SSL certificates, such as when the CA's home government restricts trade with business in the applicant's country.

Once the requestor has provided the necessary documentation, the CA is then required to verify the validity of the information in those documents. Needless to say, we can assume that a phisher willing to defraud thousands with email scams would be willing to forge a few documents to acquire an EV SSL certificate.

There are several specific verifications that CAs have to carry out, and these include verifying:

- Legal existence
- Physical existence
- Operational existence
- Domain name rights
- Requestor's authority to request an EV SSL certificate

### **Verifying Legal Existence**

Verifying legal existence applies to both the entity requesting a certificate and the principal individual representing the entity.

### **Entity Legal Existence**

A business' legal existence is verified by establishing that the company is engaged in business. For private organizations, the CA must verify that the company is legally established as a corporation or other legal entity and that it has not been categorized as inactive. A search of public records can establish legal existence of companies. For government entities, the CA must verify that the entity is a legitimate sub-division of the government established in its area.

In all cases, the legal existence check also includes verifying that the formal legal name of the entity matches that on the certificate request. This is an important step to ensure phishers do not obtain certificates with "cousin domains"—names that are similar enough to possibly confuse customers, such as Paypa1.com where the number one is substituted for the letter "l".

In addition, to these requirements, the CA must also obtain the unique registration number assigned to a business or private organization by the registering authority in the jurisdiction governing the entity. This information must be obtained directly from the registering agency or through a government agency that consolidates and distributes this information. In the case of government entities, the Secretary of State in a U.S. state or similar administrative division should provide the information.

## Principal Legal Existence

Individuals representing a business or private entity must be verified in a face-to-face meeting. The CA can do this or can depend on an RA if that agency's procedures include face-to-face verification. When establishing identity, the person must provide his or her full legal name, address, and date of birth. Identifying documents, such as a driver's license, passport, or military ID are also required. Two forms of secondary identification, one from a financial institution, must be presented as well. These could be copies of bank statements, mortgage documents, utility bill, birth certificate, tax bill, or similar documents.

## Physical Existence

The physical existence check ensures that the entity has an established physical presence in a location that conducts business. The business' physical address cannot be a post office box, for example.

In most cases, this requirement can be met by checking tax records or other government sources. The business main telephone number is also independently verified.

The legal existence verification ensures that an entity is a legitimate, legal establishment; the physical existence check ensures that it is established enough to conduct business. The next requirement, operational existence, verifies that the entity actually is conducting business.

## Operational Existence

The operational existence checks are relatively simple. If the entity has a verifiable bank account with a regulated financial institution, the requirement is satisfied. For companies that have not been in existence at least 3 years and are not listed on government tax records, additional verification is required to satisfy this requirement. The other verification requirements focus on the use of a domain name and the authority to request a certificate.

## Domain Name Rights

CAs are required to meet a few verification requirements with regards to the domain name listed in the request for the certificate:

- The domain name must be registered with an Internet naming authority such as the Internet Corporation for Assigned Names and Numbers (ICANN) or a registry listed by the Internet Assigned Numbers Authority (IANA).
- The WHOIS database should have a public listing of the entity requesting the certificate showing the name, physical address, and contact information. (See Listing 3.1 for an example WHOIS database entry).
- The entity requesting the certificate has exclusive rights to the domain name.

 For details about ICANN and IANA, see <http://www.icann.org/registrars/> and <http://www.iana.org/>, respectively.

```
Registrant:
Realtimedpublishers.com
  300 Montgomery Street
  Suite 1121
  San Francisco, CA 94104
  US

Domain Name: REALTIMEPUBLISHERS.COM

Administrative Contact, Technical Contact:
  Daily, Sean                sean@DAILY.S.ORG
  PO BOX 9161
  SANTA ROSA, CA 95405-1161
  US
  707-539-5280 fax: 707-537-8098

Record expires on 14-Feb-2009.
Record created on 14-Feb-2000.
Database last updated on 9-Nov-2007 18:36:32 EST.

Domain servers in listed order:

NS1.REALTIMEPUBLISHERS.COM  209.204.184.130
NS2.REALTIMEPUBLISHERS.COM  64.142.73.209
```

**Listing 3.1:** A typical WHOIS database entry contains both administrative and technical data on a domain and its owner.

Domain verification is generally done through WHOIS queries but may be done by contacting a certificate requestor in cases in which the domain registration information is private.

It should be noted that mixed character sets are allowed in domain names. Mixing character sets has been used in the past by phishers to create phishing sites with addresses that appear legitimate. In cases in which a mixed character set domain name is used, the CA must visually compare the domain name with domains that have high risks of attack, such as financial institutions. If the mixed character set domain name is similar to one of these high-risk sites, the CA must verify beyond reasonable doubt that the requestor is a legitimate business and the domain name is used for legitimate purposes. The last significant task in the verification process is to establish the authority of the contracting agent to request an EV SSL.

### **Authority to Request an EV SSL Certificate**

The authority of the person or persons filling the roles of certificate requestor and certificate approver has to be established by the CA before issuing a certificate. This process includes several steps:

- The CA has to verify the identity of the certificate requestor and the certificate approver. The CA must also verify that these people have the authority to act as agents of the entity seeking the certificate.
- The CA verifies the contract signer is authorized to execute agreements between the entity seeking the certificate and the CA.
- The CA, working with parties other than the certificate approver, verifies that the certificate approver is authorized to request a certificate, to provide information through the certificate requestor to the CA, and to approve of requests made by the requestor.

These requirements can be met in several ways:

- Contacting the Human Resource department and verifying personal information and authority of certificate requestor and certificate approver
- Obtaining a verified legal opinion
- Obtaining a verified accountant letter
- Receiving notice of a corporate resolution appointing individuals as certificate requestor and certificate approver

The CA/Browser Forum guidelines include detailed descriptions of what constitutes a verified legal opinion and verified accountant letter.

### **Utilizing Existing Trust Models**

Throughout this section on verification, we have seen that the CA/Browser Forum has defined in fine detail acceptable methods for verifying requests, the legitimacy of an organization, and the identity and authority of those who represent requesting entities. Although there are variations in these methods to accommodate different types of entities—such as business, government agencies, and private organizations—as well as multiple ways to verify identities and roles, they all build on existing methods used in business and government.

The goal of EV certification is to ensure that individuals and businesses are not tricked into mistaking a bogus operation for a legitimate business. This requires well-established technical applications, such as encryption, as well as a dependence on long-established practices that are regularly used in business and government operations for verifying identity and authority.

Once the authentication and verification requirements are met, an EV certificate may be issued. That, however, is not the end of the CA's responsibility. Like so many areas of IT, maintenance is a substantial part of EV certification.

## Maintaining Certification Status

EV certificates may be valid for as long as 27 months. There are many events that can occur within that period that would render the business or other organization out of compliance with the requirements for an EV certificate. Therefore, part of the CA/Browser Forum guidelines dictate what CAs must do to allow browser users to validate the status of an EV certificate.

These requirements include:

- CAs must maintain a repository for verifying the status of certificates at all times.
- Certificate revocation lists (CRLs) must be updated every 7 days.
- If the Online Certificate Status Protocol (OCSP) is used, information must be updated at least every 4 days.
- CAs must maintain reasonable response times.
- Records of revoked certificates must remain in the repository until at least the expiration date of the certificate.

### Tracking Revoked Certificates: CRLs and OCSP

When depending upon a certificate to authenticate an entity, it is best to verify the status of the certificate each time it is referenced. To do so, CAs must maintain a list of certificates that have been revoked and the reason for the revocation.

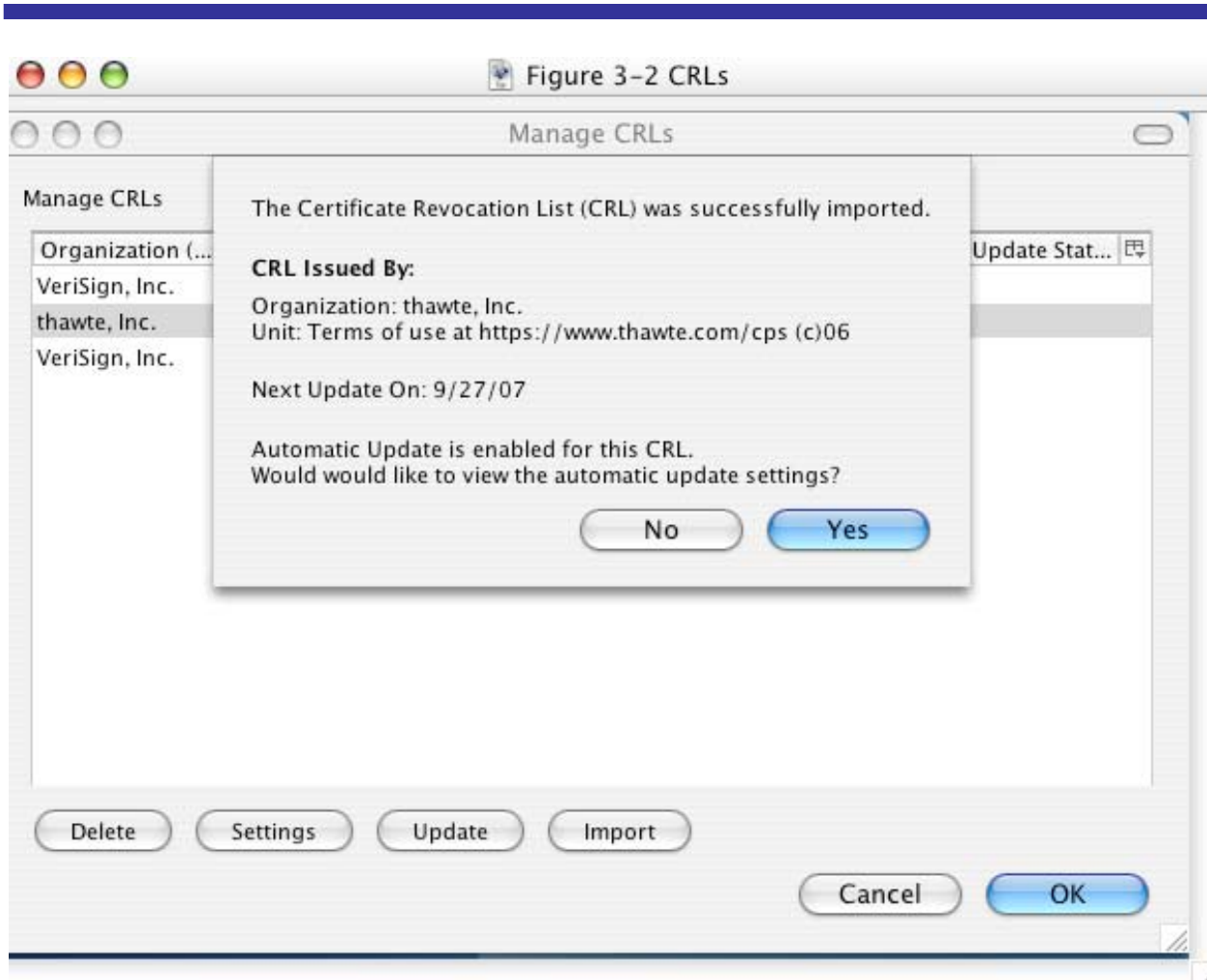
The first widely used method for this was Certificate Revocation Lists (CRLs), which were lists of certificates and related metadata about the certificate that was made available to anyone who depended on certificates issued by that CA. These lists met basic needs but there were drawbacks. The lists had to be updated and downloaded frequently to minimize the chance of accepting an invalid certificate.

The Online Certificate Status Protocol (OCSP) was developed to improve certificate status checking, and it has a number of advantages over the older CRL method. First, with OCSP, clients do not need to regularly download revocation lists from CAs. There is less processing demanded of client devices with OCSP than with CRLs.

Just as there is a need to standardize the rules for issuing EV certificates, there is a need to standardize the rules governing how and when certificates are revoked. The CA/Browser Forum guidelines define several events that can trigger the revocation of a certificate:

- The subscriber requests that the certificate be revoked
- The certificate requestor was not authorized by the subscriber to request the certificate
- The subscriber's private key is disclosed or the certificate has been misused in some way
- The subscriber commits a material breach of contract with the CA
- The subscriber's right to use the domain has been revoked or has expired
- There is a material change in the information contained in the certificate
- The information in the certificate is incorrect
- The certificate was not issued in compliance with its policies

To ensure that interested third parties can report abuse or false information on a certificate, CAs are also required to establish procedures to receive and respond to complaints.



*Figure 3.1: When CRLs are used, they must be downloaded to clients on a regular basis.*

## Additional Requirements of CAs

The authentication and verification defined by the CA/Browser Forum focus, for the most part, on the process of requesting and issuing EV certificates. In addition to those, there are a number of general requirements on the CAs business operations that address:

- Employees
- RAs
- Document management
- Data security

Each of these areas, at least indirectly, affects the quality of the certification process.



### **Employee Regulations**

CAs are expected to ensure that their employees are trustworthy and competent. Most employers would probably have similar expectations for their staff, but CAs are expected to perform specific checks:

- Identity verification
- Confirming past employment
- Check professional references
- Verify educational level
- Conduct criminal background checks

Employees are expected to receive training in PKI technologies, authentication and verification practices, and other areas relevant to issuing EV certificate. CAs are also required to maintain separation of duties among employees.

### **RAs**

CAs may use subcontractors and RAs to perform some or all the authentication and verification processes, but these third parties must comply with the CA/Forum Browser guidelines just as the CAs do.

### **Document Management**

CAs must maintain an auditable paper trail of all steps taken when issuing or revising EV certificates. This includes events related to

- Certificate requests and revocations
- Key pair generation and management
- Generation of CLR and OCSP entries
- System security events

There are also regulations regarding document retention defined in the guidelines.

### **Data Security**

CAs are expected to maintain information security programs to uphold the confidentiality, integrity, and availability of relevant information and applications. These requirements include the need for risk assessments and security plans to mitigate identified risks.

## Summary

The CA/Browser Forum has established a set of standards governing the policies and procedures for issuing EV certificates. The standards are designed to reduce the risk of phishing attacks by preventing phishers from exploiting characteristics of traditional SSL certification processes:

- Phishers cannot count on an online presence alone to qualify for an EV SSL certificate; the physical and legal existence of the business must be verified.
- Unauthorized individuals cannot successfully request EV SSL certificates on behalf of a business because of additional verification required.
- Phishing sites that employ tricks such as using similar-looking site names or mixed character sets are not likely to receive an EV SSL certificate because of the extensive checks done for domains similar to high-value target domains.

The well-defined authentication and verification policies and procedures help to ensure that only legitimate organizations will receive EV SSL certificates. In the next chapter, we will see how browsers can take advantage of EV SSL certificates to help mitigate the threat of phishing attacks.

## Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.