Extended Validation Certificates

Mark van Cuijk

February 17, 2009

Abstract

When securely browsing the web, the HTTPS protocol is used between a browser and a web server. The protocol protects the data that is transmitted in both directions against eavesdroppers and man-in-the-middle attacks, as long as proper cryptographic ciphers are used and the end user has verified the server certificate. Today, such certificates are issued to any entity that can demonstrate a certain level of control over the domain name that the certificate is to be bound to. Often, this (virtual) entity can only be connected to a legal entity with a limited degree of certainty, if at all possible. Extended Validation Certificates are introduced to overcome this limitation and bind a certificate to a legal entity.

1 Introduction

One of the main purposes of using the HTTPS protocol [1] for browsing the web is to ensure that the other endpoint of the TCP connection really is the web server the user has intended to communicate with, as opposed to an adversary performing a man-in-the-middle attack. With this goal in mind, the web server can present an SSL Server Certificate [2] to the browser, containing three important pieces of information: validity information, the public key used by the web server and a signature.

The signature on the certificate is a value that has been computed by a Certifying Authority (CA), whereby the CA declares that it agrees with the contents of the other pieces of information in the certificate. If the public key of this CA is installed in the key database of the browser, it can verify the correctness of the signature. If the signature is correct, the user can place a certain amount of trust on the validity of the information on the certificate, based on its trust in the CA that placed the signature.

The validity of the certificate is bound by the validity information that it contains. The validity of the certificate is restrict temporarily, so that the certificate is only deemed valid during a certain period, bounded by a "Not Before" and a "Not After" timestamp. The certificate is also bound to a specific domain name and to specific uses, like document signing or key encipherment.

When the browser has finished the validation procedure — possibly consulting the user — it can initialize the secure connection using the public key extracted from the certificate. Since the value of the signature includes the contents of the public key, the user can place a certain amount of trust in the fact that this key actually belongs to the web server he intends to communicate with.

1.1 The problem with certificates

In practice, CAs exist — that are trusted by major browsers — which only verify the identity of the entity submitting a certificate signing request by sending an email to a specific email address connected to a domain name, e.g. postmaster@*domain*, info@*domain* or the address listed in one of the administrative contact records for the domain name.

This means that the amount of trust that a user can put on the information received over the secure connection can only be determined by his trust on the domain name. When a user does not properly verify the domain name of the web site it is communicating with, HTTPS cannot protect him against attacks like phishing, as anyone can anonymously register a domain name and obtain a server certificate for it that is trusted by all major browsers.

The main problem with standard certificates is that they only bind a certificate to a domain name, but neglect to verifiably bind it to a legal entity, like a private company or a governmental organisation.

2 EV Certificates

Several purposes are established for Extended Validation (EV) Certificates, which are described in the EV Certificate Guidelines [3]. Besides the purposes of any SSL Server Certificate, the additional main

purpose of an EV Certificate is to bind a website to a legal entity. With this purpose in mind, identification information is stored in the certificate. When a CA issues such a certificate, it verifies the supplied identification information and only computes the signature after it successfully validated all details.

Besides the primary purposes, the documents describe certain secondary purposes, mainly targeting at making it more difficult to mount a successful phishing attack[1]. More interesting is the fact that the document explicitly excludes certain purposes by stating that an EV Certificate does not make any statement on the behaviour of the legal entity it is bounded to. For example, it explicitly excludes the intention of providing assurances regarding the trustworthyness, reputability or compliance with applicable laws of the legal entity a certificate is bound to.

2.1 Role of the CA

Compared to the tasks a CA must already perform to issue a standard certificate to an applicant, the role of the CA when issuing an EV Certificate is extended by verifying:

- the legal, physical and operational existence and identity of the applicant;
- that the applicant is a registered holder of the domain name or has the exclusive right to use it; and
- the authorization of the applicant to issue the EV Certificate for the legal entity.

The EV Certificate Guidelines describe several verification requirements that the CA must follow when verifying an applicant. These requirements are set up to provide a high level of assurance on the legal identity of a website.

2.1.1 Identity of the applicant

To verify the legal existence and identity of the applicant, the CA verifies whether the applicant is properly registered as a private organization or other business entity, a government entity or a non-commercial entity, like an international organization. The name of the entity — as stated in the certificate — must exactly match its registered organisation name and the registration number is verified.

The CA is also obligated to verify the physical existence of the applicant. Therefore it has to check whether the address listed on the certificate is not a maildrop or P.O. box and that the applicant actually conducts business operations at the stated address. Besides this, the CA must verify that the main telephone number provided by the applicant actually reaches the applicant.

2.1.2 Domain name

As the EV Certificate is going to bind a website — identified by its domain name — to a legal entity, not only the identification of the legal entity has to be verified, but also the connection between the domain name and this legal entity. The EV Certificate Guidelines [3] obligates the CA to verify that the applicant is either the registered domain holder or has the exclusive rights to use the domain name.

2.1.3 Authorization for EV Certificate

To verify that the application for an EV Certificate is authorized by the legal entity the certificate is going to be bound to, the applicant is required to provide three roles: a certificate requester, a certificate approver and a contract signer. The three roles may be filled by seperate persons or by a single person; an applicant may authorize more than one person to fill each of these roles.

A CA may only issue EV Certificates when an applicable subscriber agreement is signed by an authorized contract signer. The contract signer is a natural person that is legally allowed to sign subscriber agreements on behalf of the applicant. The certificate approver is a natural person who is allowed to approve EV Certificate requests submitted by a certificate requester. The certificate requester is a natural person that completes and submits an EV Certificate request on behalf of the applicant, like an employee or a third party such as an ISP or a hosting company.

The identity of the persons that fill these roles must be verified in a face-to-face setting, while these persons must prove their identity using government-issued legal identification documents. The roles and authorizations claimed by these persons must be verified by the CA.

The signatures on the subscriber agreement and on each individual EV Certificate request must be verified by the CA. The signature must always be a legally valid and enforeable seal, handwritten signature or electronic signature. The EV Certificate Guidelines [3] describe acceptable methods of signature verification.

[1] From wikipedia [4]: phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

2.1.4 Other tasks of the CA

There are several other tasks the CA must perform that are described in the EV Certificate Guidelines [3]. One of these tasks is the obligation to maintain a certificate repository that can be used by browsers to automatically check the current status of a certificate. The CA is obligated to regularly update the status information.

The document also obligates the CA to revoke certificates when certain events occur. Among others, the CA must revoke a certificate when:

- the private key corresponding to the public key in the certificate has been compromised, or the one used by the CA;
- the identification information on the certificate is not correct anymore; or
- the subscriber's right to use the domain name listed in the certificate is revoked.

2.2 EV Certificate warranties

By following the guidelines described in the EV Certificate Guidelines document [3], a CA can make several warranties for EV Certificates. Anyone that is using a browser to visit a website that is protected by such an EV Certificate can therefore rely on the correctness of the information stated in the certificate. In particular, the CA makes warranties about the identity and legal existence of the entity that publishes the website, its right to use the domain name and that this entity has correctly authorized the CA to issue the EV Certificate. The CA also warrants the accuracy of the information contained on the certificate and will revoke the certificate when any of the other warranties cannot be preserved anymore.

3 Conclusion

Existing SSL Server Certificates already do a great job on binding a cryptographic public key to a domain name in such a way that a user can be assured that the web server it is communicating with is actually the one that it is supposed to communicate with. However, the scope of this assurance is limited to identification by domain name. In particular, existing SSL Server Certificates are not bound to a legal entity and only limited warranties are given on the information listed in the certificate.

EV Certificates extend the scope of the assurance, by binding a certificate to a specific legal entity. The CA that issues the certificate follows certain obligated verification procedures to verify the accuracy of the information in the certificate, like the identity and legal existence of the entity that applies for the certificate, the proper authorization for the issuance and the right to use the domain name listed in the certificate. By doing these verifications, an EV Certificate introduces warranties on the accuracy of the information and therefore can extend the trust of end users in communication with web sites that are protected by an EV Certificate.

References

[1] *E. Rescorla* RFC 2818 - HTTP Over TLS

[2] *R. Housley, et al.* RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile

[3] *The CA / Browser Forum* EV Certificate Guidelines - V1.1

[4] *Wikipedia* Phishing `http://en.wikipedia.org/wiki/Phishing` Accessed on: 17/02/2009