

## Certificate Authorization

### CERTIFICATE AUTHORITY

In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CAs are characteristic of many public key infrastructure (PKI) schemes.

There are many commercial CAs that charge for their services. Institutions and governments may have their own CAs, and there is also CAs which is free of charge [citation needed]

### Issuing a certificate

A CA issues digital certificates which contain a public key and the identity of the owner. The CA also attests that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates.

If the user trusts the CA and can verify the CA's signature, then they can also verify that a certain public key does indeed belong to whoever is identified in the certificate. If the CA can be subverted, then the security of the entire system is lost.

Suppose an attacker, Mallory (to use the Alice and Bob convention), manages to get a CA to issue a false certificate tying Alice to the wrong public key; the corresponding private key is known to Mallory. If Bob subsequently obtains and uses Alice's public key in this (bogus) certificate, the security of his communications to her could be compromised by Mallory - since Bob's messages could be decrypted by Mallory, or Bob could be tricked into accepting signatures which are forged to appear to be from Alice.

### Security

The problem of assuring correctness of match between data and entity when the data are presented to the CA (perhaps over an electronic network), and when the credentials of the person/company/program asking for a certificate are likewise presented, is difficult. This is why commercial CAs often use a combination of authentication techniques including leveraging government bureaus, the payment infrastructure, third parties' databases and services, and custom heuristics. In some enterprise systems, local forms of authentication such as Kerberos can be used to obtain a certificate which can in turn be used by external relying parties. Notaries are required in some cases to personally know the party whose signature is being notarized; this is a higher standard than can be reached for many CAs. According to the American Bar Association outline on Online Transaction Management the primary points of federal and state statutes that have been enacted regarding digital signatures in the United States has been to "prevent conflicting and overly burdensome local regulation and to establish that electronic writings satisfy the traditional requirements associated with paper documents." Further the E-Sign and UETA code help ensure that:

A signature, contract or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and a contract relating to such transaction may not be denied legal effect, validity or enforceability solely because an electronic signature or electronic record was used in its formation.

In large-scale deployments, Alice may not be familiar with Bob's certificate authority (perhaps they each have a different CA), so Bob's certificate may also include his CA's public key signed by a different CA2, which is presumably recognizable by Alice. This process typically leads to a hierarchy or mesh of CAs and CA certificates.

### Providers

## Certificate Authorization

Worldwide, the certificate authority business is fragmented, with national or regional providers dominating their home market. This is because many uses of digital certificates, such as for legally binding digital signatures, are linked to local law, regulations, and accreditation schemes for certificate authorities.

However, the market for SSL certificates (used for website security) is largely held by a small number of multinational companies. This market has significant barriers to entry since new providers must convince web browser developers to include them in the list of trusted authorities in future versions of the browser, and there is no automated means to add trusted authorities to older versions. Thus there is an effective oligopoly of approximately 20 root certificates that are already trusted in the most popular versions of the most popular web browsers. Most entrants into the market attempt to acquire an already included certificate rather than wait. A 2007 market share report from Security Space as of September of that year determined that VeriSign and its acquisitions (which include Thawte and more recently Geotrust) have a 57.6% share of the certificate authority market, followed by Comodo (8.3%), and GoDaddy (6.4%).

### PUBLIC KEY CERTIFICATE

In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity — information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

### Principles

Certificates are useful for large-scale public-key cryptography. Securely exchanging secret keys amongst users becomes impractical to the point of effective impossibility for anything other than quite small networks. Public key cryptography provides a way to avoid this problem. In principle, if Alice wants others to be able to send secret messages to her, she needs only to publish her public key. Anyone who wishes to send her secure information can encrypt the information using Alice's public key, knowing that only Alice can decrypt the information with her corresponding private key. Unfortunately, David could publish a different public key (for which he knows the related private key) claiming that it is Alice's public key. In so doing, David could intercept and read at least some of the messages meant for Alice. But if Alice builds her public key into a certificate and has it digitally signed by a trusted third party (Trent), anyone who trusts Trent can merely check the certificate to see whether Trent thinks the embedded public key is Alice's. In typical public-key infrastructures (PKIs), Trent will be a CA, who is trusted by all participants. In a web of trust, Trent can be any user, and whether to trust that user's attestation that a particular public key belongs to Alice will be up to the person wishing to send a message to Alice.

In another example, Alice and Bob need to share a message, but Alice may not be familiar with Bob's certificate authority. This scenario is common when Alice and Bob have different employers and their certificates were issued by their employer's CA. In this case, Bob's certificate may also include his CA's public key signed by a "higher level" CA2, which might be recognized by Alice. This process leads to a hierarchy of certificates, and to even more complex trust relationships. Public key infrastructure mostly refers to the software that manages certificates in a large-scale setting. In X.509 PKI systems, the hierarchy of certificates is always a top-down tree, with a root certificate at the top, representing a CA that is so central to the scheme that it does not need to be authenticated by some trusted third party.

A certificate may be revoked if it is discovered that its related private key has been compromised, or if the relationship embedded in the certificate (between an entity and a public key) changes or is discovered to be incorrect. This might occur if a person changes jobs or names. Although certificate revocation is usually rare, trusted certificates should always be checked for validity. This can be accomplished by comparing the certificate to a certificate revocation list (CRL), which

## Certificate Authorization

a list of revoked or cancelled certificates. Ensuring that such a list is up-to-date and accurate is a core function in a centralized PKI. To be effective, CRLs must always be readily available to anyone who needs them, and they must be updated frequently. Online Certificate Status Protocol (OCSP) is another means for checking the validity of a certificate. OCSP uses a third-party server to parse the CRLs, and returns an answer to the client, rather than requiring the client itself to retrieve and interpret the CRLs.

### A certificate typically includes:

1. The public key being signed.
2. A name, which can refer to a person, a computer or an organization.
3. A validity period.
4. The location (URL) of a revocation center.
5. The digital signature of the certificate produced by the CA's private key.

The most common certificate standard is the ITU-T X.509. X.509 is being adapted to the Internet by the IETF PKIX working group.

### Classes

VeriSign introduced the concept of classes of digital certificates:

1. Class 1 for individuals, intended for email.
2. Class 2 for organizations, for which proof of identity is required.
3. Class 3 for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority.
4. Class 4 for online business transactions between companies.
5. Class 5 for private organizations or governmental security.

### Certificates and web site security

The most common use of certificates is for https web sites. A Web browser validates that an SSL (Transport Layer Security) Web server is authentic; so that the user can feel secure that their interaction with the Web site has no eavesdroppers and that the web site is who it claims to be. This security is important for electronic commerce. In practice, a web site operator obtains a certificate by applying to a certificate provider with a certificate signing request. The certificate request is an electronic document that contains the web site name, contact email address, and company information. The certificate provider signs the request, thus producing a public certificate. This public certificate is served to any web browser that connects to the web site and proves to the web browser that the provider believed that the provider issued a certificate to the owner of the web site. Before issuing a certificate, the certificate provider will request the contact email address for the web site from a public domain name registrar, and check that published address against the email address supplied in the certificate request. Therefore, an https web site is only secure to the extent that the end user can be sure that the web site is operated by someone in contact with the person that registered the Domain name.

As an example, when a user connects to <https://www.example.com/> with their browser, if the browser gives no certificate warning message, then the user can be sure that interacting with <https://www.example.com/> is equivalent to interacting with the entity in contact with the email address listed in the public registrar under "example.com", even though that email address may not be displayed anywhere on the web site. No other surety of any kind is implied. Further, the relationship between the purchaser of the certificate, the operator of the web site, and the generator of the web site content may be tenuous and is not guaranteed. At best, the certificate guarantees uniqueness of the web site, provided that the web site itself has not been compromised (hacked) or the certificate issuing process subverted.

## Certificate Authorization

### Certificate providers

A 2005 Netcraft survey determined that VeriSign and its acquisitions such as Thawte have a 53% share of the certificate authority market, followed by GeoTrust (25%), Comodo (12%), GoDaddy (4%) and Entrust (2%). GeoTrust was subsequently acquired by VeriSign.

An April 2007 market share report from Security Space determined that VeriSign and its acquisitions (including GeoTrust) have a 59.6% share of the certificate authority market, followed by Comodo (8.3%), GoDaddy (5.3%), DigiCert (2.1%), Entrust (1.3%) and Network Solutions (1.1%).

CAcert.org is a community-driven certificate authority that issues free public key certificates.