Public Key Certificate

In cryptography, a **public key certificate** (also known as a **digital certificate** or **identity certificate**) is an electronic document that uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, the address, and the email address. 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.

For provable security, this reliance on something external to the system has the consequence that any public key certification scheme has to rely on some special setup assumption, such as the existence of a certificate authority.[1]

Operating systems

Certificates can be created for Unix-based servers with tools such as OpenSSL's ca command, [2] or SuSE's gensslcert. These may be used to issue unmanaged certificates, certification authority (CA) certificates for managing other certificates, and user or computer certificate requests to be signed by the CA, as well as a number of other certificate related functions.

Similarly, Windows Server contains a CA as part of Certificate Services for the creation of digital certificates. In Windows Server 2008 and later the CA may be installed as part of Active Directory Certificate Services. The CA is used to manage and centrally issue certificates to users or computers. Microsoft also provides a number of different certificate utilities, such as SelfSSL.exe for creating unmanaged certificates, and Certreq.exe for creating and submitting certificate requests to be signed by the CA, and certutil.exe for a number of other certificate related functions.

Mac OS X comes with the Keychain Access program, which is able to perform various certificate-related services.

Contents of a typical digital certificate

- **Serial Number**: Used to uniquely identify the certificate.
- **Subject**: The person, or entity identified.
- **Signature Algorithm**: The algorithm used to create the signature.
- **Signature**: The actual signature to verify that it came from the issuer.
- **Issuer**: The entity that verified the information and issued the certificate.
- **Valid-From**: The date the certificate is first valid from.
- **Valid-To**: The expiration date.
- **Key-Usage**: Purpose of the public key (e.g. encipherment, signature, certificate signing...).
- **Public Key**: The public key.
- **Thumbprint Algorithm**: The algorithm used to hash the public key certificate.
- **Thumbprint** (also known as fingerprint): The hash itself, used as an abbreviated form of the public key certificate.

Classification

Vendor defined classes

VeriSign uses the concept of classes for different types of digital certificates:[3]

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

Other vendors may choose to use different classes or no classes at all as this is not specified in the PKI standards.

Usage in the European Union

The EU Directive 1999/93/EC on "a Community framework for electronic signatures" defines the term *qualified certificate* as a certificate which meets the requirements of Annex I and is provided by a certification service provider who fulfills the requirements of Annex II.[4]

According to Annex I, qualified certificates must contain:

1. An indication that the certificate is issued as a qualified certificate
2. The identification of the certification service provider and the state in which it is established
3. The name of the signatory or a pseudonym, which shall be identified as such
4. Provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended
5. Signature verification data which correspond to signature creation data under the control of the signatory
6. An indication of the beginning and end of the period of validity of the certificate
7. The identity code of the certificate
8. The advanced electronic signature of the certification service provider issuing it
9. Limitations on the scope of use of the certificate, if applicable
10. Limits on the value of transactions for which the certificate can be used, if applicable

Annex II requires certification service providers to:

1. Demonstrate the reliability necessary for providing certification services
2. Ensure the operation of a prompt and secure directory and a secure and immediate revocation service
3. Ensure that the date and time when a certificate is issued or revoked can be determined precisely
4. Verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued
5. Employ personnel who possess the expert knowledge, experience, and qualifications necessary for the services provided, in particular competence at managerial level, expertise in electronic signature technology and familiarity with proper security

procedures. They must also apply administrative and management procedures which are adequate and correspond to recognized standards.
6. Use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them
7. Take measures against forgery of certificates, and, in cases where the certification service provider generates signature creation data, guarantee confidentiality during the process of generating such data
8. Maintain sufficient financial resources to operate in conformity with the requirements laid down in the Directive, in particular to bear the risk of liability for damages, for example, by obtaining appropriate insurance
9. Record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings. Such recording may be done electronically.
10. Not store or copy signature creation data of the person to whom the certification service provider provided key management services
11. Before entering into a contractual relationship with a person seeking a certificate to support their electronic signature, inform that person by a durable means of communication of the precise terms and conditions regarding the use of the certificate, including any limitations on its use, the existence of a voluntary accreditation scheme and procedures for complaints and dispute settlement. Such information, which may be transmitted electronically, must be in writing and in readily understandable language. Relevant parts of this information must also be made available on request to third parties relying on the certificate.
12. Use trustworthy systems to store certificates in a verifiable form so that:
    - Only authorized persons can make entries and changes
    - Information can be checked for authenticity
    - Certificates are publicly available for retrieval in only those cases for which the certificate holder's consent has been obtained
    - Any technical changes compromising these security requirements are apparent to the operator

Certificates and web site security

The most common use of certificates is for HTTPS-based web sites. A web browser validates that a TLS (Transport Layer Security) web server is authentic, so that the user can feel secure that his/her 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 (a CA that presents as a commercial retailer of certificates) with a certificate signing request. The certificate request is an electronic document that contains the web site name, contact email address, company information and the public key (for security reasons the private key is not part of the request and is not sent to the certificate authority). The certificate provider signs the request, thus producing a public certificate. During web browsing, this public certificate is served to any web browser that connects to the web site and proves to the web browser that the provider believes it has 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 who registered the domain name.

As an example, when a user connects to https://www.example.com/ with their browser, if the browser does not give any certificate warning message, then the user can be theoretically 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.

Extended Validation

Certificate providers issue "higher security" certificates that require further security checks, and incur higher fees. This is called an Extended Validation (EV). These security checks cross reference the owner of the domain name with the owner of the legal entity that claims to operate under it. (These checks may involve the presentation of utility bills, passports, etc.). The difference between these higher security certificates and regular certificates are that the browser URL bar changes to a different color, usually green. This improved security assumes the user knows the meaning of the colors, and would choose to navigate away from the site if the color code was not commensurate with the purpose of the web site. To be clear, for a https:// web site URL, the difference between having no certificate, and having a regular certificate is that the browser will *refuse* to access the site without confirming with the user. By comparison, the difference between a regular certificate and an extended validation certificate is merely a change in color.

Weaknesses

A web browser will give no warning to the user if a web site suddenly presents a different certificate, even if that certificate has a lower number of key bits, even if it has a different provider, and even if the previous certificate had an expiry date far into the future. However a change from an EV certificate to a non-EV certificate will be apparent as the green bar will no longer be displayed. Where certificate providers are under the jurisdiction of governments, those governments may have the freedom to order the provider to generate any certificate, such as for the purposes of law enforcement. Subsidiary wholesale certificate providers also have the freedom to generate any certificate.

All web browsers come with an extensive built-in list of trusted root certificates, many of which are controlled by organizations that may be unfamiliar to the user.[5] Each of these organizations is free to issue any certificate for any web site and have the guarantee that web browsers that include its root certificates will accept it as genuine. In this instance, end users must rely on the developer of the browser software to manage its built-in list of certificates and on the certificate providers to behave correctly and to inform the browser developer of problematic certificates. While uncommon, there have been incidents, in which fraudulent certificates have been issued: in some cases, the browsers have detected the fraud; in others,

some time passed before browser developers removed these certificates from their software.[6] [7]

The list of built-in certificates is also not limited to those provided by the browser developer: users (and to a degree applications) are free to extend the list for special purposes such as for company intranets.[8] This means that if someone gains access to a machine and can install a new root certificate in the browser, that browser will recognize websites that use the inserted certificate as legitimate.

Usefulness versus unsecured web sites

In spite of the limitations described above, certificate-authenticated SSL is considered mandatory by all security guidelines whenever a web site hosts confidential information or performs material transactions. This is because, in practice, in spite of the serious flaws described above, web sites secured by public key certificates are still more secure than unsecured http:// web sites.

References

1. Ran Canetti: Universally Composable Signature, Certification, and Authentication. CSFW 2004, http://eprint.iacr.org/2003/239
2. OpenSSL: Documentation ca(1)
3. VeriSign Class definitions
4. "Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures". *Official Journal L 013 , 19/01/2000 P. 0012 - 0020*. Annex II. Retrieved 2010-02-17.
5. "List of certificates included by Mozilla". Mozilla.org. Retrieved 30 July 2012.
6. "DigiNotar removal by Mozilla". Mozilla.org. Retrieved 30 July 2012.
7. "DigitNotar removal by Google". Google.com. Retrieved 30 July 2012.
8. "Using certificates article at Mozilla.org". Mozilla.org. Retrieved 30 July 2012.