HOSTED ENTERPRISE PKI

An SSL.com Whitepaper
June 14, 2019

Enterprises are increasingly turning to hosted solutions for organizational PKI (public key infrastructure) offered by commercial public certificate authorities (CAs). This paper gives an overview of PKI, weighs the advantages of private vs. public trust, and outlines the potential advantages of a hosted solution when setting up a PKI for your organization.

www.ssl.com (877) 775-7328 sales@ssl.com

Table of Contents

EXECUTIVE SUMMARY

Private Certificate Authorities (CAs) are an increasingly important part of enterprise network infrastructure. Digital certificates are commonly used for:

- Secure web browsing.
- Authentication of employees for workstation sign-on and internal web applications.
- Prevention of fraud and phishing through signed and encrypted email.
- Authentication of digital documents and code through digital signatures.
- Single sign-on (SSO).
- Mutual authentication of servers for internal network security.

The primary decisions that must be made before setting up an organizational CA are ***private*** vs. ***public trust*** and ***internal*** vs. ***hosted PKI*** (public key infrastructure):

- A publicly trusted CA can issue certificates that will automatically be trusted by operating systems and application software such as web browsers and email clients, but must conform to specific industry standards. Privately trusted CAs are not subject to these standards, but are not usable for public-facing applications. Publicly trusted and privately trusted CAs each offer distinct advantages and disadvantages which must be taken into account when deciding which to employ for a given application. Many organizations will find having both to be desirable.
- Commercial public CAs, such as SSL.com, now offer hosted PKI as a service, potentially giving significant cost benefits over internal staffing and infrastructure. Hosted PKI can be used to set up both publicly and privately trusted organizational CAs.

After reading this paper, you should have a better idea of the relevant issues surrounding the practical choices to be made when planning an organizational PKI and Certificate Authority for your enterprise.

PKI AND CERTIFICATE AUTHORITIES

What is Public Key Infrastructure?

Public Key Infrastructure* (PKI)** is used to manage pairs of ***public and private keys and bind them to the identities of entities, such as persons and organizations, through the issuance of electronic documents called ***digital certificates***. The mathematics behind PKI ensure that if a certificate is ***signed*** with a given entity's private key, anyone with the public key from the pair can:

- Verify that the entity presenting the signed certificate is in possession of its corresponding private key (***authenticity***).
- Trust that the content of the certificate has not been altered since it was initially generated (***integrity***).
- Use the public key to encrypt a message that can only be decrypted with its associated private key (***encryption***).

Furthermore, when a certificate is used to ***sign*** an electronic document, such as a web page, email message, word processor document, or piece of application code, the signer's private key is used to generate a ***cryptographic hash***, or fixed-length digest, of the document. Like the certificate itself, the authenticity and integrity of the signed document, email, or code can be confirmed by a person in possession of the signer's public key by independently calculating this hash.

By enabling authenticity, integrity, and encryption, PKI and digital certificates permit secure communication over insecure networks, such as the Internet.

What is a Certificate Authority?

A ***Certificate Authority* (CA)** is an organization that maintains a PKI and manages the issuance and revocation of digital certificates. Some CAs, such as SSL.com, are ***publicly trusted*** – they are regularly audited against industry standards such as the CA/Browser Forum's *Baseline Requirements* in order to be included in the public trust stores of operating system and browser suppliers (most notably Microsoft, Apple, Google, and Mozilla). Privately trusted CAs, on the other hand, are typically designed for private PKI use and thus not subject to the same compliance requirements, providing more flexibility to customers. However, private PKI may still be affected by evolving public PKI standards or regulations specific to a particular industry.

Note: The term *CA* is also used as a shorthand for the certificate authority's private key.

PKI Applications

The most well-known use of PKI and digital certificates is for secure web browsing, which is made possible through the SSL/TLS and HTTPS protocols. Secure web browsing is built on the multiple interlocking PKIs of CAs, browsers, and more to protect confidential information sent across the Internet, such as password and credit card numbers. Other important enterprise applications of digital certificates are:

- Signed and/or encrypted email messages via the S/MIME standard.
- Signed and/or encrypted electronic documents and computer code.
- Client authentication for workstation sign-on and application access.
- Identification and security for Internet of Things (IoT) devices.
- Mutual authentication of servers for internal networking.
- Single sign-on (SSO).

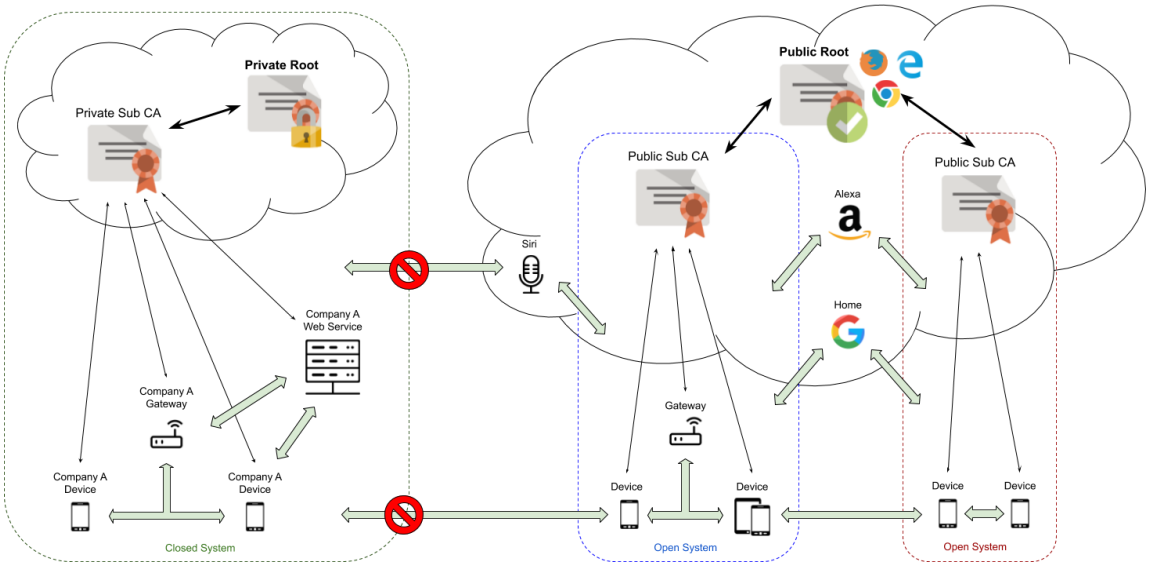
As businesses and government organizations become increasingly aware of the potential effects of security breaches through high-profile examples like the 2016 Democratic National Committee email leak, PKI is becoming a standard part of enterprise infrastructure. Through establishing its own PKI and CAs, an organization can control the issuance of digital certificates for internal and external applications and issue branded certificates in its own name.

PUBLIC VS. PRIVATE VS. INTERNAL VS. HOSTED PKI

When describing how PKI works, the terms "public" and "private" are used frequently, and often in subtly different ways. To reduce confusion, let's use these definitions in this paper:

- **Public PKI**: Publicly trusted PKI, in which issued certificates lead back to a publicly trusted root CA such as SSL.com. The CA that issues end-entity certificates is part of a ***chain of trust***; that is, a series of digital certificates, each signed by the previous one in the chain, leading back to public CA's trusted root certificate.
- **Private PKI**: Privately trusted PKI, in which certificates chain to a private root CA and are trusted within an organization. **Note**: Certificates issued by a private CA are not trusted by browsers and other applications and usually cause warnings and/or prevent connections outside of the private network they are created to operate within.

- **Internal PKI**: Locally hosted PKI infrastructure, managed in-house by a business or other organization. While internal PKI is usually privately trusted, it is also possible for an organization to arrange to have its locally hosted CA signed by a publicly trusted CA, resulting in the ability to issue publicly trusted certificates (this usually adds security and auditing requirements beyond those needed for a purely private PKI).
- **Hosted PKI**: PKI as a service (PKIaaS). With hosted PKI, the relevant infrastructure is maintained externally by a third party on behalf of an organization, and may be either privately or publicly trusted. This is often the more cost-effective choice whether or not public trust is required.



Hosted PKI: Private Trust (left) vs. Public Trust (right)

PUBLIC, PRIVATE, OR BOTH?

An important consideration for an organizational CA is whether or not public trust is required for its intended business purposes. Public trust is not always essential (or even desirable), since it can impose additional operational requirements. The following subsections outline some of the potential advantages of public versus private trust:

Advantages of Public Trust

There are multiple reasons why an enterprise may choose to issue publicly trusted certificates. For example,

- If an organization wishes to issue publicly trusted end-entity certificates for websites or email, code, and document signing, its issuing CA **must** have a chain of trust that leads back to a publicly trusted root CA. There is really no other secure option for public-facing websites or other public information.
- Publicly trusted certificates are automatically trusted by client software such as operating systems, web browsers, and email clients, eliminating the need to manually install private certificates on company workstations and devices.
- For IoT manufacturers, publicly trusted SSL/TLS certificates allow unfettered access to device admin and settings pages via a web browser.
- Publicly trusted CAs are held strictly accountable to industry standards for the generation and handling of certificates and keys. This will often be considered a security advantage for an organization's PKI even if public trust is not absolutely required for business purposes.

Advantages of Private Trust

Industry standards like the CA/B Forum Baseline Requirements are a double-edged sword; while they effectively enforce what the industry regards as the current best practices for public CAs, they also mandate conditions that may or may not be optimal for private PKI. For example, under the Baseline Requirements:

- Public CAs may not generate or handle private keys, while a private CA may.
- Public CAs may not issue certificates for internal domains (e.g., `example.local`), while private CAs may do so at will.
- Publicly trusted certificates must include specific information and be strictly formatted according to the X.509 standard for public certificates. A private CA, on the other hand, can issue certificates customized to an organization's specific needs and purposes
- The validity period for publicly trusted SSL/TLS certificates is currently 825 days. Private PKI does not face this restriction.

In addition, web browsers such as Google Chrome now mandate that certificates issued by public CAs must be published to a public database, a practice known as ***certificate transparency***. Private enterprises may wish to avoid exposing internal services to competitors (or network attackers) in this way. A private CA is *not* required to observe certificate transparency:

Do You Need Both?

In reality, most enterprises requiring a private PKI will also need publicly trusted certificates for public websites, publicly distributed code, and any other context in which public trust is either desirable or required. An organization's need for both public and private PKI may also affect the desirability of hosted vs. internal PKI infrastructure.

INTERNAL VS. HOSTED PKI

Once an organization has decided that it needs a private PKI, there is nothing preventing it from simply starting up its own self-signed private CA and issuing certificates. On the surface, this may appear to have practical advantages. Software for issuing digital certificates is widely available at low or no cost; Windows Server, for example, includes a certificate authority, and other commonly used tools, such as OpenSSL and EJBCA, are free and open-source. However, despite the "free" nature of CA software, any analysis of the costs and challenges of running an internal PKI infrastructure must consider:

- **The cost of employing staff qualified to securely and effectively run an internal enterprise CA (including the tasks of managing certificate lifecycle and expiry).** Furthermore, if an enterprise is running both an internal private CA and hosted public CA, these two PKIs may well have entirely different interfaces and systems for user authentication and privileges, adding an additional layer of complexity for IT staff.
- **The hardware and networking costs associated with running and securing an enterprise PKI.** Furthermore, attempts to scale internal PKI often require additional expertise and hardware, leading to more staffing and hardware costs.

By arranging to set up a hosted private PKI with a *public* CA such as SSL.com, enterprises can have the best of both worlds and leverage the public CA's expertise and infrastructure:

- **A public CA has effective systems in place to manage PKI operations, including certificate issuance, lifecycle maintenance, and expiration, and can provide automated notifications of impending certificate expiry.** SSL.com makes its web-based PKI tools and web services API available to our enterprise customers for both public *and* private PKI, eliminating the need to develop these capabilities in-house.
- **A public CA has, by definition, already solved the problem of operating a secure PKI with high availability at a global scale.** To operate globally as a public CA, SSL.com has multiple datacenters and its own content delivery network (CDNify) for distribution of certificate revocation lists (CRLs).
- **A public CA's operations and infrastructure are subject to frequent, detailed audits for adherence to industry standards, and the CA is thus required to continuously stay abreast of best practices.** Aside from the obvious security benefits of intense third-party scrutiny, evolving industry standards for *public* PKI typically also affect *private* PKI. For example, while nothing prevents a private CA from issuing weak SHA-1 SSL certificates for internal websites, all reputable public CAs no longer use the deprecated, easily cracked SHA-1 algorithm for any purpose, and any certificates generated using SHA-1 are either unsupported or deprecated by major web browsers. A hosted PKI solution with a public CA significantly reduces your exposure to existing security pitfalls and will help you deal with new ones as they inevitably arise.

When balancing the above considerations against the staffing and hardware costs associated with installing, maintaining, and scaling private PKI, all but the largest or most specialized businesses will likely find that a hosted solution is more cost-effective, easier to implement, and ultimately more secure.

HOSTED CA OPTIONS FROM SSL.COM

SSL.com offers hosted PKI solutions with both public and private trust to our Enterprise customers and can customize a unique CA to meet our clients' security requirements. If public trust is required, we can generate a customer's organizational CA from our own Enterprise intermediate CA or our offline root itself (more labor-intensive and expensive, but possible). For private trust, SSL.com can generate a new root CA from scratch, from a customer's root or intermediate CA, or the customer can generate their own issuing CA and send it to SSL.com. CA generation can be done on- or offline as an organization's security policies dictate.

CONCLUSION

We hope that this overview has been useful for you in understanding the basic differences between private and public PKI, and the potential advantages of a hosted PKI solution. If you would like to talk to a staff expert about any of your organization's PKI needs, please do not hesitate to contact us by email at Sales@SSL.com or Support@SSL.com, or by phone at 1-877-SSL-SECURE (1-877-775-7328).

ABOUT SSL.COM

SSL.com is a globally trusted certificate authority expanding the boundaries of encryption and authentication relied upon by users worldwide. Founded in 2002, we have grown to be used in over 120 countries by leading organizations and governments of all sizes. We provide a wide range of digital certificates to fit any need, including SSL/TLS server certificates, code signing, document signing, and S/MIME email certificates. As a full member of the CAB Forum, we provide unique, insightful preparation for our clients and partners into the future development of digital certificate technologies and policies.

CONTACT US

3100 Richmond Avenue, Suite 503
Houston, TX 77098

P: (877) 775-7328 **F: (832) 201-7706**

sales@ssl.com **www.ssl.com**