Enterprise SSL Solutions

A BUYERS GUIDE

SECURITY BOULEVARD

Having SSL certificates, or what are now officially known as TLS certificates, has always been a requirement for corporate IT organizations. Certificates encrypt data as it is being transferred between servers and web-facing browsers as well as protect data as it moves between servers.

Certificates also play a critical role in making sure that only authorized users are accessing data they have permissions to see and share.

Unfortunately, it's become too tempting to consider certificates that are based on widely accepted standards just another commodity product. In principle, every Certificate Authority (CA) provides the same level of encryption and cryptographic functions. Certificates, however, are not all the same. There are different classes of certificates that provide significantly different levels of protection, which IT teams need to know how best to employ based on their requirements.

It also worth noting that how a CA manages the certificate lifecycle process from deployment to renewal can make a critical difference, especially at a time when an unplanned outage can generate the type of headlines no organization wants. In the wake of the COVID-19 pandemic, organizations are depending on digital business processes more than ever. That means they have never been more dependent on CAs to ensure those processes won't be disrupted simply because someone forgot to, for example, renew a certificate.

There is, of course, no shortage of free SSL certificates available. However, as tempting as those offers might be, like most free things they can wind up being more trouble than they're worth.

Certificate Authentication Levels

Today all SSL certificates offer the same level of encryption. The fundamental difference is the level of authentication being provided across three main classes of certificates:

Domain Validation (DV): The only information authenticated by a DV certificate is who controls the domain. Potential methods of authentication include email, inclusion of a file on the website or a change to a DNS record.

Organization Validation (OV): Before issuing an OV SSL certificate, a certificate authority is likely to require:

- A legal existence record
- An attestation letter
- A government license
- An article of incorporation
- A bank statement
- A letter confirming relation between the individual asking for the certificate and an organization
- A listing on a third-party database

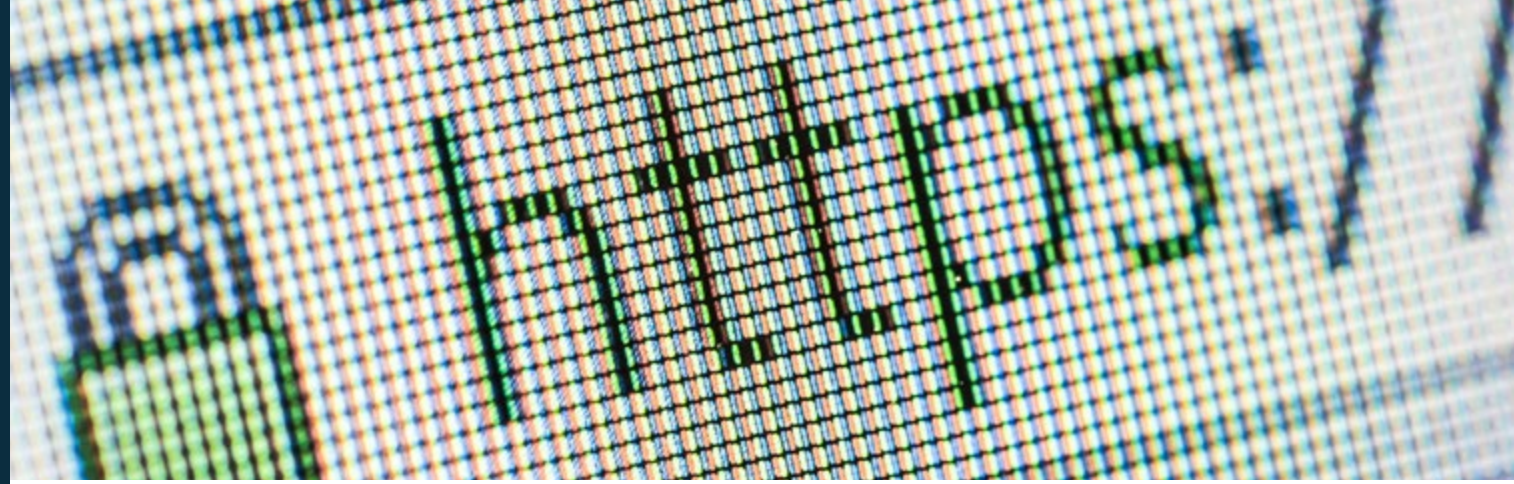
Authenticated information will be included in the body of the certificate. Users viewing OV certificates in their browsers are able to see this information.

Extended Validation (EV): An EV SSL certificate goes one step further by displaying the business name at the top adjacent to the URL in some browsers. For users of these browers, the organization's brand effectively becomes attached to the EV SSL certificate, which serves to provide the end user more confidence in the site.

CAs authenticating EV certificates must follow uniform authentication rules defined by the CA/Browser Forum. These rules represent a set of best practices for authenticating business identity, considered to be the most reliable authentication techniques available. After more than a decade of use, these EV authentication processes have not been defeated

Certificate Domain Coverage

Just as SSL certificates come in different authentication levels, likewise they are available in different forms that allow them to work on different sets of domain names.



SINGLE-DOMAIN

As the name suggests, a single-domain certificate is minted to work on precisely one domain or subdomain. For example a single-domain certificate for *www.sample.com* would not work on *shop.sample.com*, just as the certificate for *shop.sample.com* would not work on *login.sample.com*.

The only exception to this rule is for the www and "bare" versions of a top level domain. Most CAs will take advantage of SSL's Subject Alternative Name (SAN) capability to allow the same certificate to work on both these treatments, as they are so often treated as identical by companies and users alike.

Single-domain certificates offer the most precise control over server security by limiting the footprint of any given certificate. In the event of a key compromise or other security problem, the scope of affected systems is minimized when using single-domain SSL certificates.

MULTI-DOMAIN

Multi-domain certificates add SAN fields to allow the same certificate to work on more than one domain, not only subdomains of the same main domain but even entirely different domain names. Therefore a multi-domain certificate for *www.sample.com* could also work for *shop.sample.com* and also for *www.different.com*. Although the majority of multi-domain certificates only contain a few SAN fields, they can, in principle, serve hundreds of domain names.

Multi-domain certificates offer greater flexibility than single-domain certificates, as the same server can provide content or functionality for more than one domain name. And by potentially reducing the total number of certificates in use, administrators may reduce overhead for deploying, managing, and renewing certificates.

The downside of multi-domain certificates is that any problem that does occur with the certificate is magnified across multiple sites and systems, which, other than the certificate, may have little to do with each other. Any outage owing itself to certificate revocation or unexpected expiration will affect all systems dependent on the multi-domain certificate.

A specific subset of the multi-domain SSL certificate is called a Unified Communications Certificate, or UCC. Often referred to as an “Exchange certificate,” UCC is a specific configuration of multi-domain certificate for use on Microsoft Outlook or Exchange servers. While many CAs will sell UCC certificates by name, any multi-domain certificate for the correct set of domains will do the job correctly.

WILDCARD

A wildcard certificate secures a single main domain name and all subdomains under it. Therefore, a wildcard certificate for *.sample.com would secure *sample.com, www.sample.com, shop.sample.com, login.sample.com* and any other legal subdomain of sample.com.

For scenarios where all pages and services fall under a single main domain name, wildcards offer the most flexibility of all certificate types, as they can secure any number of subdomains and can be used for new subdomains that weren't thought of when the certificate was issued. Of course, that also means the risk of breach or outage increases in cases of certificate compromise, revocation, or expiration.

Furthermore, according to the CA/Browser Forum EV Guidelines, public CAs are not allowed to issue wildcard Extended Validation certificates. Therefore, for use cases that require or benefit from EV, wildcards are not a good option.

Root Ubiquity

Not all SSL certificates are recognized as trusted by all client systems. While modern browsers and operating systems contain root update functionality to allow the addition and removal of trusted roots, personal computers and mobile devices lacked that capability for many years. Older systems and devices still in use might not recognize any given CA's most current roots.

To address this issue, CAs cross-sign their certificates to older "legacy" roots. These are roots that were created long ago and are still valid because they were embedded in old client systems. Cross-signing allows modern systems to chain up to the modern root while allowing old systems to chain up to the legacy root.

Not all legacy roots are the same because each was created at a different time. The exact set of operating systems and devices covered will vary from one to another. Legacy roots also have expiration dates, at which point they will stop providing trust for older systems.

Organizations such as online banks, e-commerce sites, and media outlets should consider the available legacy root support, including expiration dates for these roots, before selecting an SSL provider.

Speed to Issuance

It's critical that organizations have access to the full range of potential certificate types so they can mix-and-match them as circumstances warrant. Even if your organization is not using a particular type of certificate today, the CA relied on should be capable of issuing any type of certificate whenever needed.

Most CAs can issue a DV SSL certificate in minutes. However, in organizations that have adopted agile development and best DevOps practices, that's usually not fast enough. DevOps implementations and other high-capacity environments can require delivery of requested certificates in seconds to meet their performance needs. Organizations that have adopted DevOps generally prefer to automate the process of certificate requests from within their continuous integration/continuous delivery (CI/CD) platform.

For DevOps teams, the actual speed at which a new certificate can be generated and issued is critical. Containers, the atomic unit on which modern applications are now more commonly built, are being created in near real-time. That means each certificate needs to be created on-demand. Each task also requires its own certificate, so the total number of TLS certificates the enterprise needs can increase dramatically as more containers are invoked.

OV and EV certificates also require additional verification beyond the domain name. A CA can facilitate issuance of additional OV or EV certificates for the same enterprise by creating an enterprise authentication account. Enterprise authentication is the practice of maintaining authentication records for a subscriber who repeatedly orders certificates through the same account. Information that already has been authenticated may not need to be authenticated again in every instance of a new certificate, which can speed issuance considerably. In a best-case scenario, EV and OV issuance can rival DV in speed to delivery.

Service and Support

More organizations need to have domains and other services available to new and existing customers on a 24x7 basis. That means their certificate authority must offer 24x7 phone support.

Certificate authorities should make available access to technical account managers as well as experts who can help automate the certificate issuance, lifecycle management, and renewal. A single, dedicated support team for the customer can minimize problems and speed recovery times. These support teams should also be able to help organizations migrate from one certificate authority to another at the lowest cost possible.

When entering into an agreement with a CA, many enterprises are unaware of clauses in the contract that call for the revocation of all outstanding certificates on termination of the contract—in essence holding production certificates hostage to force contract renewal. This hidden lock-in technique severely restricts the customer's agility and removes accountability for performance from the CA. Be sure any volume certificate agreement you enter into includes a guarantee that your deployed certificates will continue for the duration of their issued terms.

Automation and Certificate Management

Before standardizing on a certificate authority, consider these operational issues:

DISCOVERY

A certificate authority needs to make it easy to discover all deployed certificates and bring them under management. A common occurrence is for certificates previously unknown to the central IT department to expire unexpectedly, causing an outage that is difficult to diagnose and, therefore, fix. These "rogue" certificates are often installed by contractors or custom development agencies that are no longer associated with the company, and as more IT responsibilities shift to lines of business (LOB) or other departments, the numbers of rogue certificates or even entire rogue private CAs in the enterprise are growing by leaps and bounds.

In addition to creating expiration risk, rogue certificates are problematic for governance. Compliance officers who cannot account for the certificates used to provide security for critical systems are ultimately unable to provide auditability and true knowledge of compliance with relevant requirements.

Finally, certificate discovery enables true measurement of the certificates in use throughout the organization and facilitates planning, accounting, and IT resource management.

NOTIFICATIONS

There may be nothing more aggravating than your website becoming inaccessible because a certificate wasn't renewed. Notification prior to expiration needs to be shared with multiple recipients to make sure certificates remain valid and your site remains available.

Even with automated certificate renewal, it is still essential to know which certificates are coming up for renewal and how many new certificates will be issued from your available pool. IT teams can then decide whether to renew these certifications, change the type of certificate issued, or discontinue renewals for any service that has been sunsetted.

REPORTING

Compliance audits are a fact of IT life. Certificate authorities must be able to generate reports that associate the certificate with the owner of that resource. That's one less monotonous task IT teams shouldn't have to perform manually. Reports need to identify clearly what cryptography is used, who the issuer is, and when certificates expire.

That visibility is critical when it comes time to audit certificates.

WORKFLOW

Organizations using an IT service management (ITSM) platform from vendors such as ServiceNow must have the option of ordering, authorizing, monitoring, and reporting on certificates from inside the ITSM platform. Additional workflow options such as a REST API or optional agent-based management increase flexibility for subscribers.

ADMINISTRATION

IT teams should be able to delegate web server management to different individuals as roles within the organization evolve. A certificate should no longer be associated with someone who left the company months earlier.

INSTALLATION

Misconfigurations are often the bane of certification existence. The installation process needs to be automated to eliminate downtime by reducing the opportunity for human error. However, while serving to reduce costs by eliminating manual processes, that installation process should not lock a customer into a specific certificate authority platform.

STANDARDS

The certificate authority platform needs to comply with all aspects of the Automatic Certificate Management Environment (ACME) communications protocol for automating interactions between certificate authorities and web servers. ACME is based on JSON-formatted messages and was designed by the Internet Security Research Group (ISRG). Organizations should make certain it is securely implemented on all elements of their website, including load balancers.

Other important communications protocols available you may want include SCEP (Secure Certificate Enrollment Protocol) and EST (Enrollment over Secure Transport). As all of these protocols are employed in different use cases, a CA should support all three to provide the most flexibility now and in the future.

SECURITY

IT teams should be wary of platforms requiring the provisioning of administration passwords into automation tools. When passwords are changed the installation will fail, which results in automatic expiration of certificates. IT teams should also be able to integrate certificate management with platforms such as Azure Key Vault running on a public cloud.

SINGLE-PLATFORM SUPPORT FOR ALL CERTIFICATE TYPES

IT teams should be able to manage all certificates regardless of application from within a single pane of glass, including web servers, load balancers, networking equipment, cloud services, mobile applications, and Internet of Things (IoT) environments. Anything less will drive up the total cost of certification management. As a general rule, it's always a good idea to be able to apply the same management platform used to manage SSL certificates to manage any other type of certificate.

FLEXIBLE PRICING

There should be no surprises when it comes to pricing. IT teams should expect predictable fees for the duration of the agreement. For example, adding permanent or temporary web servers or load balancers should not result in higher fees or the need to create additional purchase orders. Similarly, changes in the number of domains should not result in higher costs.

Organizations should also expect to be able to decide how long a certificate will be in effect without having to commit to a contract that might last a year or more. They should also have the flexibility to alter the type of certificates issued as requirements change once the initial contract is signed.

Summary

Any investment in an SSL certificate pays for itself almost immediately. Google, for example, improves rankings for websites with SSL certificates. Picking the right CA provider is nothing less than making a choice between managing certificates proactively and waiting for some suboptimal event related to certificates to occur.

When all the other benefits of certificates are added along with the services provided by a CA, the return on that investment compounds. The simple truth is the right CA partner offloads a range of routine tasks critical to the business that most IT teams simply don't have the time, resources, or expertise to perform.

SECURITY
BOULEVARD

securityboulevard.com
twitter.com/securityblvd
facebook.com/secboulevard/

THANKS TO

SECTIGO