UnderstandingMultiUseSSLCertificates

Understanding Multi-Use Digital Certificates

Abstract

With the proliferation of internal Web-based services that must be exposed to the Internet, organizations are turning more and more to the use of SSL certificates. However, using traditional SSL certificates can become cumbersome and quite expensive, especially when organizations offer several Internet-facing services. This is where multi-use certificates – certificates that can be reused for different purposes – can help. Using a single multi-use certificate, organizations can reduce costs and simplify certificate management.

Introduction

The best way to prove who you are on the Internet is to use a digital certificate. That's because a digital certificate relies on a trusted, third-party authority to verify your identity. In fact, it uses a chain of trust that begins with you and works its way up to the trusted authority that validates who you are. This chain of trust provides verifiable Internet security.

Take Internet user Bill for example. Bill uses a digital certificate to sign all of his emails. This example demonstrates the concept of authenticity. The certificate authenticates Bill as the author of the email. The digital certificate also verifies that Bill is the actual author and sender of the email. This is the concept of non-repudiation – by using a certificate, you can certify with reasonable certainty that the signed document is trusted to be from Bill or at least someone who possesses the private key corresponding to the signing certificate.

In addition, because Bill signs his emails with a digital certificate, the email cannot be tampered with without invalidating the signature. This is the concept of integrity. Because the email includes a digital signature, it cannot be modified while in transit without the tampering being obvious to the recipient.

Two more security concepts are supported by digital certificates. Availability is critical to the third-party organization that certifies that Bill is who he claims to be. The verification service must be available when you need to verify Bill's certificate. Finally, confidentiality is provided by the ability to encrypt data both in the content itself and in the transport mechanism that is used to send the data to a destination on the Internet.

Similarly, organizations that process transactions on the Internet or that offer Internet-based services need to rely on digital certificates to validate that they are who they claim to be; otherwise, no one will trust their services. Most organizations do this by adding certificates to their Internet-facing servers. When users access a web page hosted on one of these servers, their Web browser will automatically detect the certificate and modify the session, from an open session using the HyperText Transfer Protocol (HTTP) to secure HTTP (HTTPS). This will allow for the encryption of all the data sent between the user's workstation and the server. HTTPS data encryption is provided by the Secure Sockets Layer (SSL). Basically, SSL creates an encryption tunnel between the client and the server protecting the transfer of data from one point to the other during the communication exchange. You know you are using SSL when your browser displays a closed padlock in its status bar.

Working with SSL Certificates

In order to enable SSL on their external-facing servers, organizations must purchase a certificate from a trusted certification authority for each protected service they provide. Today, organizations can offer several services to their end users – email, instant messaging, mobile device management, Web-based interactions and more – and each one of the servers providing these services requires its own certificate.

SSL certificates are tied to the unique domain name on which a service is hosted. Embedding the domain name into the certificate is important since this makes it possible to ensure the identity of the remote computer providing the service by comparing the domain name being accessed to the domain name included in the certificate itself. Certificates are issued for a finite period, usually in 12-month increments. Because of this, you should aim to obtain certificates that are valid for extended periods of time. You should also aim to select static service names because each time a service name changes, the certificate must be changed on each server that provides the service. These strategies will reduce the workload associated with periodic renewal and installation of certificates on your servers.

These problems are compounded when organizations must use different domain names for each secure service they make available on the Internet. In fact, organizations often find themselves in a situation where they need to use sub-domain names – names that use the same root name, but require a different prefix name – to secure each of the services they offer. Because prefix names are embedded into SSL certificates, organizations usually buy one certificate per service. As you can imagine, this can become expensive and time-consuming to manage, especially in organizations that run a multitude of Internet-facing services.

Enter the multi-use SSL certificate. There are two types of multi-use certificates:

Wildcard certificates can secure multiple sub-domains on a single unique Fully Qualified Domain Name using a single certificate. Multi-domain certificates can secure multiple Fully Qualified Domain Names using a single certificate. Each certificate can simplify management and reduce costs given the right situation.

Wildcard Certificates

The first type of multi-use certificate is the wildcard certificate. The name you embed in a certificate must always follow the fully-qualified domain name (FQDN) format. If you want a certificate for the Session Initiation Protocol (SIP) used by instant communication servers in the VirtualSpaceShip.com domain, the name embedded into the certificate will be SIP.VirtualSpaceShip.com. If you want a certificate for the email service, then you would normally have to buy a second certificate with the second service name – mail.VirtualSpaceShip.com – embedded into it.

In addition, some secure service implementations require internal as well as external validation and you use a different name for each; for example, Internal Sip.VirtualSpaceShip.com and ExternalSIP.VirtualSpaceShip.com. In this case, you must have a certificate on each server in the internal and external service to allow users to work unimpeded whether they are in the office or on the road. This is the case for instant messaging infrastructures where you want to ensure messages are encrypted whether they are internal or external. Note that servers cannot include two certificates for the same purpose.

Wildcard certificates do not include service names. Instead, they are standard certificates that support the use of a wildcard character to replace the prefix name in the subject name field, for example, *.VirtualSpaceShip.com. Using a wildcard certificate is much more practical and versatile than using multiple single purpose certificate since the wildcard certificate can be applied to a number of different services without requiring any updates. In addition, you can add, change or replace services without needing to update the certificate.

For example, single wildcard certificate could easily support the following names and more: www.VirtualSpaceShip.com, shop.VirtualSpaceShip.com, mail. VirtualSpaceShip.com, SIP.VirtualSpaceShip.com, register.VirtualSpaceShip.com, and so on. In actual fact, the wildcard certificate supports the use of multiple sub-domain or prefix names within the same certificate. Using a wildcard character as a placeholder in the domain name embedded into the certificate makes the certificate much more versatile. In addition, it can be applied to any number of uses since the wildcard character can represent any sub-domain name. Because of this, wildcard certificates provide very good value for the cost.

Multi-Domain Certificates

The second type of multi-use certificate is the multi-domain certificate. While the wildcard certificate will include a special character for the prefix name, the multi-domain name provides the ability to include multiple Fully Qualified Domain Names within the same certificate. However, unlike wildcard certificates which can support an unlimited number of prefix names so long as the root domain name remains the same, multi-domain certificates will only support the specific Fully Qualified Domain Names entered into the certificate. In most cases, multi-domain certificates will support up to 25 or more different Fully Qualified Domain Names in one certificate.

Multi-domain certificates include the standard Subject Name field which supports a single primary service name, as well as an additional entry called the Subject Alternative Name field which supports the additional service names. The SAN certificate can therefore be installed on several servers and function properly to support internal/external service delivery.

SAN certificates have the same issues as single-purpose certificates however. Because the actual service names are embedded into the certificate, you must make sure your services always use the same name otherwise you must change the certificate and since the certificate is a multi-use certificate, you must change it on each of the computers that host the service which the certificate supports. Additionally, when you want to add services to provide further functionality to your users, you must update the SAN certificate with the new service names.

Multi-domain, SAN, or UCC certificates are useful when organizations require different root domain names to run Internet-facing services. Subject alternate name certificates are also called Unified Communications Certificates (UCC) since they were primarily designed to support real-time communications infrastructures. For example, an organization providing both internal and external unified communications services with two different domain names – for example, SIP.VirtualSpaceShip.com the external domain and SIP.VirtualSpaceShip.com for the internal name – would benefit from a multi-domain certificate because in this case, the wildcard certificate would not work. In fact, if the organization was using wildcard certificates, two wildcard certificates would be required because the root domain name is different in each case.

A single multi-domain certificate could easily support the following names and more: www.VirtualSpaceShip.com, www.VirtualSpaceShip.ws, www. VirtualCDVD.com, www.VirtualWorkersInSpace.com

Multi-domain certificates are also useful for application service providers (ASP) who host applications for multiple clients with each client using their own domain name. By using a multi-domain certificate, ASPs can use a single certificate to support multiple clients. Note that the site seal and certificate "Issued To" will only be for the primary domain name entered in the certificate and will not include any of the other domain names. However, the certificate itself will include all of the domain names that have been entered when the certificate was purchased.

While multi-domain certificates are also useful when used to support unified communications deployments, there are some caveats for their use:

- Multi-domain certificates do not support use of wildcard characters. For this reason, sub-domain names must be added as a unique domain name entries in the certificate. Each time a new domain name is added or an old one is removed the certificate must be updated and re-deployed to each host server.
- When hosting Web sites for multiple clients, ASPs should be aware that all domain names appear in a multi-domain certificate. If the ASP does not want one site to seem as if it is connected to another, then a different certificate type should be used.

Keep these caveats in mind when choosing a multi-domain certificate.

Wildcard vs. Multi-Domain Certificates

Organizations wanting to move to subject alternate name or unified communication certificates should choose between the wildcard and the multi-domain certificate types. Table 1 outlines the similarities and differences between the two certificate formats.

Both certificate types offer several benefits and include several features. In addition, both are available in full authentication format only. Domain-only authentication certificates only require the validation of the domain before they are issued, and because of this, cannot be used with multi-use certificates. Full authentication certificates require both the validation of the domain itself and the validation of the business running the domain. Because of this, full certificates are more trustworthy than domain-only certificates. This is another reason the full authentication model is used for multi-use certificates. Keep this in mind as you make your choice.

Making the Selection

Multi-use certificates were developed to provide multiple secure services originating from a single IP address. To accomplish this, these certificates either add a subject alternate name (SAN) field to the common single-use certificate or use a wildcard to replace the service name in the certificate. Microsoft Exchange Server 2007 is an excellent example of this type of requirement. The same external Exchange server can publish several different types of services: Outlook Web Access, Outlook Anywhere Access, AutoDiscovery configuration information, and more. Each of these services requires the publishing of its own name – for example, OWA.VirtualSpaceShip.com, Mail.VirtualSpaceShip.com, Autodiscover.VirtualSpaceShip.com – ideally within a single certificate.

Multi-use certificates reduce cost and simplify management by supporting the inclusion of multiple names within the same certificate or the replacement of service names with a wildcard. However, each multi-use certificate type should only be used in specific situations:

- Wildcard certificates should be used when a single root name is used for all services or where there is a single domain and only multiple sub-domains that cover all services.
- Multi-domain certificates should be used when multiple root names are required for each service.

Both certificate types offer reduced total cost of ownership (TCO) when they are deployed. But obviously, both certificates only fit specific situations.

Ideally, organizations would only use a single root name for all functions, but in most environments, this is not possible. Many organizations use a least one public root name and one private root name to segregate the internal from the external namespaces they work with. In this case, only multi-domain certificates will work. But, if you only need a certificate for external purposes and you only use one single public root name, then the wildcard certificate is the certificate of choice.

In summary, multi-use certificates make it much easier to deploy multiple secure services both internally and externally. This is particularly useful in environments that include several services like mail, instant messaging, Web, mobile device management, and File Transfer Protocol (FTP). If this is the case for your organization, then your best choice is to acquire the multi-use certificate that is tailored to fit your needs.