BENEFITS OF WILDCARD SSL CERTIFICATE

The merits of switching from HTTP (or Hyper Text Transfer Protocol) to HTTPS (or HTTP Secure) are limitless however this can be a daunting task for new company that decides to have multiple subdomains of a single domain. Wildcard SSL Certificate are proving to be a boon for such websites saving them time and costs.

Typically, organizations resort to getting the Secure Sockets Layer (SSL) certification for their domains to ensure data protection and to restore faith in consumers’ mind. SSL is a standard security technology that enables organizations to establish an encrypted link between a web server and a client. This makes it impossible for attackers to intercept the data flow (between a web server and a client) and use the information. SSL is an absolute necessity for e-commerce or for organizations that collect sensitive data.

A Website is an organization’s face with the consumers—a very commonly accessed touch-point. The design, page layout, security features such as the SSL certification of the websites is a reflection of the company’s persona. Most organizations know this and dedicate a lot of efforts on the upkeep, it is therefore important that companies have a website that assures the customers security. A growing trend in the recent past has been getting the SSL certification. According to published reports, the number of organizations migrating from an HTTP website to a HTTPS website has doubled in just two years. This single touch-point often has several sub-layers that demand equal security.

A single Wildcard SSL Certificate can secure all related (unlimited number of) first-level subdomains of the principal domain, thus eliminating the need of buying an SSL certification for each of them. It lets you specify additional host names such as email addresses, IP addresses, URLs, DNS names etc. to be protected by a single certificate. In a nutshell, using a Wildcard SSL Certificate you can secure unlimited sub domains on a single domain name and the base domain for as little as 100 USD a year.

There is a borderline difference between SAN certificates and Wildcard SSL certificates. According to the OpenSRS blog, a wildcard certificate allows for unlimited subdomains to be protected with a single certificate. For example, you could use a wildcard certificate for the domain name opensrs.com and that cert would also work for mail.opensrs.com, ftp.opensrs.com and any other subdomain. The wildcard refers to the fact that the cert is provisioned for *.opensrs.com. A SAN certificate allows for multiple domain names to be protected with a single certificate. For example, you could get a certificate for opensrs.com, and then add more SAN values to have the same certificate protect opensrs.org, opensrs.net and even tucows.com.

Wildcard SSL Certificates not only save you costs while securing unlimited sub-domains, they also make the things easier to manage. If you have say 15 different SSL certificates, deploying them will be a hassle even with a managed interface. Further you will have to repeat the exercise at every renewal, thus blocking a lot of your resources.

The only drawback of Wildcard SSL Certificates is that since it has one common private key across all servers, one server being compromised can make others vulnerable to the threat. However this is very unlikely to happen given the complexity of the encryption. You can visit Here if you would like to know more about Wildcard SSL Certificate.