Cheatography

Websites SSL Certificates Cheat Sheet

by [deleted] via cheatography.com/2754/cs/13653/

Introduction

This cheatsheet will explain the different kinds of certificates available for website encryption. It's important to note that certificates just encrypt the transmission of data and they do not make your website secure against hackers.

Credit: https://www.webstix.com/the-differences-between-ssl-ev-and-ucc-certificates

SSL Certificates

SSL stands for Secure Sockets Layer. It establishes an encrypted link/connection between the web server and the browser. SSL ensures all the data passed between the web server and the website visitors' computers remains private and secure.

An SSL certificate is standard certificate that has been used by websites to protect the online transaction. It's unique for every website and consists of a private key, public key and sometimes a CA (Certificate Authority) key as well.

Websites are secured with SSL certificates. When a website is secure, you will see a padlock in the browser's address bar and sometimes a green address bar if it is secured by an EV certificate.

EV Certificates

EV stands for Extended Validation Certificate. This is the highest class of SSL available. It provides the strongest security encryption level available. It enables both the padlock and green address bar.

Websites of bigger brands are often targeted for phishing attacks and they go for this higher level of encryption.

Any website collecting confidential data like a login, credit card information or online payments can also benefit using this kind of certificate. This gains level of trust for the users and to compete with the familiar brands.

How SSL and EV Certificates Work

An SSL or EV certificate is pointed to a single domain name and unique/dedicated IP address. An SSL certificate is set to a unique domain name, company name, address, city, state, country and has an expiration date.

This is great but what happens if you have two or three websites using a CMS/ecommerce on a single IP address and each website needs to have its data secured? You don't need to buy SSL certificate for each domain if it's going to be multi website setup. Then what would you do? What is the best solution? The answer is UCC.

Certificates

Unified Communications Certificate (UCC)

UCC stands for Unified Communications Certificate. A Unified Communications Certificate is an SSL certificate which secures multiple domain names and host names. In a UCC certificate, you can secure one primary domain and up to 99 Subject Alternative Names (SANs). A UCC can also be used in a shared web hosting. UCC lets you to use a single SSL certificate and secure multiple domains and multiple hostnames within a domain.

In a shared hosting environment, the UC Certificate "Issued To" will only list the primary domain (but the site seal can list the remaining domains in the SAN). Please be aware that any other or secondary domains will be listed in the UCC SSL certificate as well.

When you would like to have a multi website set up and each website has a shopping cart, you should use a UCC certificate. This works well for storeowners who run multiple websites using a single instance of software – like Magento.

Choose UCC over SSL in these situations:

- You need a single certificate to secure different/multiple domains – both internal and external
- For reducing server security administration complexity
- To reduce cost – they provide huge savings to the organizations that need to secure multiple domains
- UCC certificates are fully trusted as SSL by over 99.9% of current browsers