digicert®

SSL CHEAT SHEET

DigiCert Secures:

- 89% of Fortune 500 companies
- 97 of the 100 largest banks in the world
- 81% of encrypted global e-commerce transactions
- 54% of secure global e-commerce revenue
- 35% of encrypted worldwide traffic
- 18% more than the next competitor

The DigiCert Smart Seal:

- The most dynamic seal on the market, packed with unique features
- Display a brand's verified logo inside the seal
- Quickly show a company is using the highest level of identity protection for websites
- Improves user confidence, increases conversions and provides a symbol of trust
- Is included with all DigiCert Secure Site and Secure Site Pro products

Product Descriptions

SINGLE DOMAIN CERTIFICATES

Used to secure a single domain. Includes one SAN to cover www.example.com and example.com with the same certificate

Available for: all brands and authentication types

WILDCARD CERTIFICATES

Used to secure an unlimited number of subdomains within one common name. The subdomain will appear as a "*" field in the certificate information

Example: *.site.com used to secure subdomain1.site.com, subdomain2.site.com, etc.

Ideal for dynamic environments where subdomains are often or occasionally added to a common name as new subdomains can be easily added to the initial certificate

Saves money. Provides better economies of scale through one certificate securing an array of subdomains

MULTI-DOMAIN CERTIFICATES (SAN)

Also called SAN certificates, multi-domain certificates offer organizations the ability to secure multiple names across different domains and subdomains.

Example: One certificate to secure all of: www.example.com, www.example2.com, mail.example.com, mail.example.net

Ideal for more stable environments including multiple domain names owned by the same organization name

Saves money with less flexibility. Any lifecycle management (reissue, revoke and replace, etc.) to one of the SAN fields results in the need to reissue all associated certificates with this SAN certificate

Authentication Types

DV

- Verifies ownership and control of the domain name only
- Issued in minutes
- Maintains browser compliance

Ideal for: non-critical web pages, internal pages, server to server communications, blogs or informational pages

OV

- Enhanced validation including authenticating the identity of the applicant
- Issued within hours
- Maintains browser compliance

Ideal for: public-facing and more sensitive web pages that collect personal data from site users. Pages could include login pages, payment pages, new account signup pages, etc.

EV

- Standards-based approach to authentication, representing the highlest level of authentication for SSL certificates
- Additional visual cues to inspire user confidence
- Typically issued within one day
- Maintains browser compliance and other industry compliance

Ideal for: business critical webpages including any e commerce, online banking, account signups and any other pages where the goal is additional transactions of any type