



COMPARISON WILDCARD, MULTIDOMAIN AND MULTI-DOMAIN SSL CERTIFICATES

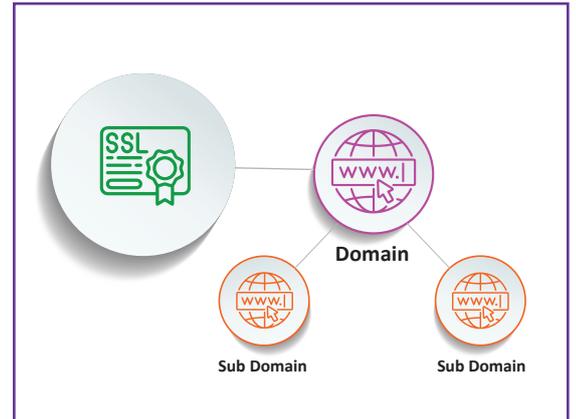


Wildcard, Multi-domain and Multi-domain SSL Comparison

Wildcard SSL certificate, multi-domain and multi-domain wildcard SSL certificates are three different types of SSL certificates. These are categorized based on the number of domains and sub-domains they can secure. These offer flexibility for securing multiple domains or sub-domains.

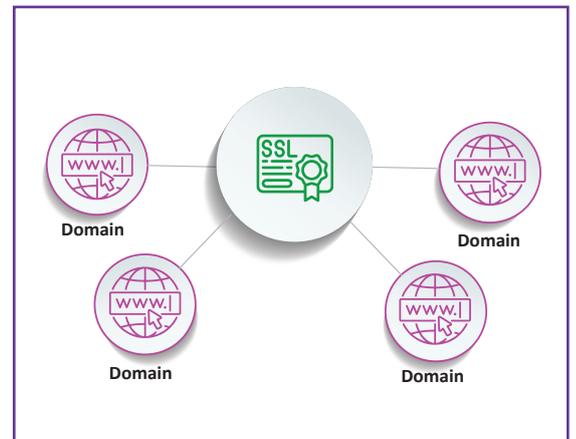
Wildcard SSL Certificate

A wildcard SSL certificate secures one base domain along with all sub-domains associated with the main domain. Wildcard certificates eliminates the need to buy a separate SSL product for each subdomain you create. It saves you time and money. You can secure unlimited subdomains with a single wildcard installation. It is recommended for websites wherein the content is organized using subdomains. It allows the management of all subdomains under a single interface, enabling ease of administration and cost savings.



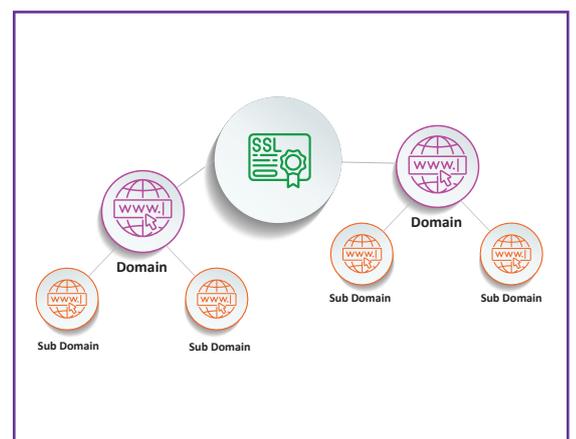
Multi-domain SSL Certificate

A multi-domain SSL certificates secure multiple base domains. These are the most versatile and cost-efficient SSL certificates. They can secure multiple domains under a single SSL installation saving you time and money in the process. They are also called Subject Alternative Name Certificates (SAN SSL) or Unified Communication Certificates (UCC SSL). If you need to secure several domains, the multi-domain certificates are the only viable option. It can secure up to a hundred domains. It is recommended for large businesses with multiple domains to secure. It is available for all OV, DV and EV SSL certificates.



Multi-domain Wildcard SSL Certificate

Multi-Domain Wildcard certificates allow you to secure multiple domain names like 'Multi-Domain SSL Certificates', and also allow to use Wildcard domain combinations within them. All of them protected under a single SSL installation. There's no need to spend a fortune on multiple wildcard certs for each of your main domains and subdomains when you can protect your entire network of sites with just one Multi-Domain Wildcard certificate.



Following are some of the differences between wildcard, multi-domain and multi-domain wildcard SSL certificates:

FEATURES	Wildcard SSL Certificate	Multidomain SSL Certificate	Multi-domain Wildcard SSL Certificate
Scope	Secures one base domain and all subdomains under it.	Secures multiple base domains.	Secures multiple wildcard domains as well as its associated subdomains.
Ideal for	Ideal for websites with a number of subdomains.	Ideal for large businesses with a number of domains.	Ideal for large businesses with a number of domains including wildcard and subdomains.
No. of domains secured	Secures a single domain and all subdomains associated with it.	Secures up to 250 domains.	Secures up to 250 domains and all subdomains under the base domains including wildcard.
Cost	It is less expensive than wildcard & multi-domain SSL certificate	It is more expensive than a wildcard SSL certificate	It is more expensive
Scalability	Limited scalability as it can secure only one domain and its associated subdomains.	Highly scalable as it can secure up to 250 domains.	Highly scalable.

eMudhra offers both wildcard and multi-domain SSL certificates with a validity of 1 year at cost-effective prices.

About eMudhra

eMudhra, a global provider of digital identity and cybersecurity solutions, specializes in digital signature certificates, Public Key Infrastructure (PKI) services, and robust authentication protocols. Our impactful presence in India and international presence have allowed us to support governments and enterprises in safeguarding their digital transactions and vital information.

eMudhra offers digital certificates, PKI-based solutions, authentication and identity governance services. With a strong presence in India and a global footprint, eMudhra helps organizations securely manage their digital transactions and protect sensitive information. Being a leading digital identity and cybersecurity solutions provider, eMudhra is now focused on futureproofing cybersecurity using Post Quantum Ready Cryptography and Zero-Trust Identity Governance model.