emSign
powered by emudhra

emudhra
Trust Delivered

Domain Validation SSL Certificates

Boost Your Credibility and Confirm Your Business Authenticity

Domain Validated (DV) SSL certificates are a type of SSL/TLS certificate used to secure websites and online transactions. Unlike other types of SSL certificates, such as Organization Validated (OV) and Extended Validation (EV), DV certificates do not require extensive verification of the organization or business behind the website. Instead, they only require verification that the certificate requester owns or controls the domain(s) listed in the certificate.

It is a no-frills, encryption-only certificate that doesn't necessitate extensive vetting and can be issued almost instantaneously by using email-based, DNS-based, or file-based validation methods, which ascertains that you own the domain you wish to protect. It is an encryption-only SSL certificate primarily used for small websites such as blogging or online information websites.

There are four types of DV certificates available:

emSign
powered by emudhra

emudhra
Trust Delivered

Domain Validated (DV) SSL Certificate

The Single Domain DV SSL certificates are the most popular and affordable type of SSL products as they secure one primary domain (Fully Qualified Domain Name) or one subdomain under a single SSL installation.

The certificate authority (CA) issuing the certificate will verify that the requester has control over the domain by sending an email to an email address associated with the domain or by having the requester place a file on the website's server.

emSign single domain DV SSL secures only a single domain with a validity of 1 year starting at $32. Businesses or individuals can obtain single Domain DV SSL almost instantaneously by a single factor validation.

Domain Validated Wildcard (DV WC) SSL Certificate

Wildcard certificates eliminate the need to buy a separate SSL product for each subdomain. It saves you time and money. This type of DV secures unlimited subdomains with a single wildcard installation.

For example, a DV WC certificate for example.com would also secure subdomains such as blog.example.com, shop.example.com, and so on. The verification process for a DV WC certificate is the same as for a regular DV certificate.

emSign wildcard domain DV SSL secures unlimited subdomains with a validity of 1 year starting at $213. Businesses or individuals can obtain wildcard domain DV SSL almost instantaneously by a single factor validation.

Domain Validated Multi-Domain (DV Multi-Domain) SSL Certificate

This type of DV certificate secures multiple domains or subdomains within a single certificate. Multi-Domain SSL Certificates are the most versatile and cost-efficient SSL certificates. For example, a DV Multi-Domain certificate could secure example.com, blog.example.com, and shop.example.com all within a single certificate. The verification process for a DV Multi-Domain certificate is the same as for a regular DV certificate, but the requester will need to provide proof of control over each domain listed in the certificate.

Multi-Domain SSL certificates can secure multiple domains under a single SSL installation saving time and money in the process. They are also called Subject Alternative Name Certificates (SAN SSL) or Unified Communication Certificates (UCC SSL). You can get multi-domain SSL with a validity of 1 year starting at $94. If you need to secure several domains, multi-domain certificates remain the only viable option.

Features of Domain Validated SSL

- Secures Single & Multiple Domains
- Validity Period of 1 year
- Domain Validation
- The average Issuance Timeframe will be minutes
- Unlimited Server Licenses
- Strongest SHA2 & ECC Encryption
- Major Browser & Mobile Device Compatibility
- Free Expert Support
- Priority Support is not provided
- $500,000 Warranty

emSign
powered by emudhra

emudhra
Trust Delivered

Domain Validated Multi-Domain with Wildcard (DV Multi-Domain with Wildcard) SSL Certificate

Multi-Domain Wildcard certificates allow you to secure multiple domain names like Multi-Domain SSL Certificates and allow you to use Wildcard domain combinations within them. All of them are 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. You can opt for multi-domain wildcard SSL with a validity of 1 year starting at $638.

While DV certificates are the least expensive and easiest to obtain, they also provide the least amount of trust and security compared to OV and EV certificates. Because the verification process for DV certificates is minimal, it is may be possible for attackers to obtain them fraudulently and use them for phishing attacks or other malicious purposes. Therefore, it is important to carefully consider the level of security needed for your website and choose a certificate accordingly.

Why should the users opt for emSign's DV Certificates?

- **Cost-effective:** Unlimited server licenses; unlimited free re-issues and replacements for the lifetime of the certificates.
- **Convenient:** DV SSL certificates issued almost immediately.
- **Universality:** emSign's SSL DV Certificates are trusted by every popular browser, device and application.
- **Encryption:** Symmetric 256-bit encryption, 2048-bit RSA keys/256-bit ECC keys.

Best Suitable for:

- Static Websites/Blogs
- Personal websites
- Non-business websites

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 global reach have allowed us to support governments and enterprises in safeguarding their digital transactions and vital information.

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.