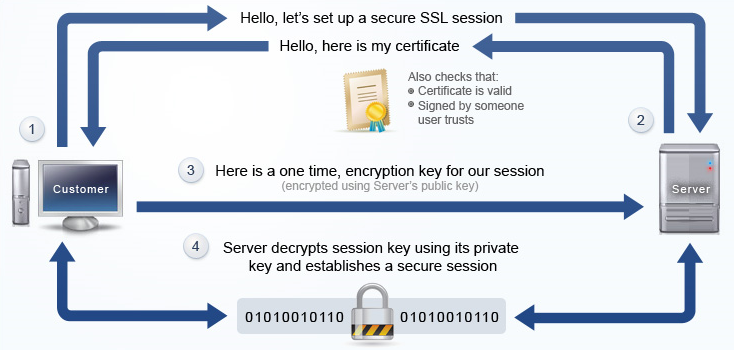
**SSL Certificates**

**What is SSL Certificate?**

SSL Certificate secures your website and promotes customer confidence with superior encryption  
and authentication. Its function is to establish a secure encrypted connection between a Client and a Server – typically a Web server and a Browser, and protects sensitive data, such as login credential, Identification number, credit card information, exchanged during each session



**Symantec**

Symantec uses industry-leading SSL encryption across all products, with various solutions for website and server security. Extended Validation (EV) SSL certificates will increase customers' confidence and help your website reach its full potential. Symantec 'Pro' SSL products offer ECC encryption, strong security on a short key length. Wildcard SSL certificate protects multiple subdomains under one SSL certificate.

The Core features of Symantec SSL Certificates:

|  |  |
| --- | --- |
| Daily Malware Scan | Discover any active threats so you can take remediation actions and secure your website |
| Management Tools | Tools to help you manage, find and install your SSL certificates easily |
| DSA Certificates | DSA Certificates meet compliance requirements with certain government agencies |
| Unified Communications (SAN) Support | Allows for multiple domain names to be protected with a single certificate. Unified Communications/ SAN certificates are required in applications like Microsoft Exchange. |
| Nearly 100% End-User Compatibility | Symantec SSL Certificates are nearly 100% compatible with browsers and systems |
| Installation Help | Server specific instructions include a set of articles with operating system-specific installation instructions. Downloadable tools are run on your server and guide you through a short wizard to install your certificate on Windows and Linux. |
| Expiration Protection  Norton Secured Seal | Reminder emails and calls from account manager protect against certificate expirations. You also have a 30 day grace period to renew your certificate.  #1 most recognizable trust mark on the Internet |

We offer 5 types of Symantec SSL Certificates:

***SecureSite***

* [Symantec DSA SSL Certificate and Symantec RSA Certificate](https://www.symantec.com/ssl-certificates/)
* $1,500,000 warranty

***SecureSite Pro***

* **S**[**ymantec ECDSA SSL Certificate**](https://www.symantec.com/ssl-certificates/), Symantec DSA SSL Certificate and Symantec RSA Certificate
* $1,500,000 Warranty

***SecureSite EV***

* [Symantec DSA SSL Certificate and Symantec RSA Certificate](https://www.symantec.com/ssl-certificates/)
* Displays the green address bar, promotes trust and boosts customer confidence
* Extended Validation with visual indicator to instill trust and differentiate your authentic site from a phishing (fake) site.
* $1,750,000 warranty for added assurance

***SecureSite Pro with EV***

* [**Symantec ECDSA SSL Certificate**](https://www.symantec.com/ssl-certificates/), Symantec DSA SSL Certificate and Symantec RSA Certificate
* Displays the green address bar, promotes trust and boosts customer confidence
* Extended Validation with visual indicator (green address bar) to instill trust and differentiate your authentic site from a phishing (fake) site.
* $1,750,000 warranty for added assurance

***SecureSite Wildcard***

* [Symantec DSA SSL Certificate and Symantec RSA Certificate](https://www.symantec.com/ssl-certificates/)
* One certificate extends Symantec's trusted and secure SSL to multiple subdomains under one domain on your server.
* **$1,500,000 warranty** for added assurance

**Managed PKI for SSL Certificates**

Managing SSL certificates for multiple Web servers across the enterprise can be a daunting task. You need a centralized and easy-to-use solution for issuing, renewing, revoking, and managing access privileges for all your company's certificates.

Managed PKI for SSL is designed for companies that need to have as little as 5 to thousands of SSL certificates in the organization. It is suitable for multiple servers, server farms, clustered server environments, server load balancers, SSL accelerators and SSL VPN appliances.

With one simple purchase, our Managed PKI for SSL service lets you issue all the Server Digital Certificates you need. This will allow you to secure all of the Web servers in your domain throughout even the largest enterprise.

* **Convenient one-step purchasing:** Take advantage of a single enrolment process, purchase order, and volume discounts
* **Easy to set up and configure**: Start issuing Server Certificates quickly via our intuitive Web-based process.
* **Efficient centralized Certificate management:** Secure and manage multiple servers throughout your domain, and easily renew Certificates or buy additional Certificates
* **Flexible Certificate bundles:** Certificates are available in bundles of 10, 25, 50, 100, or more.
* **Broad compatibility:** Global Server Certificates are compatible with major Web servers, including Microsoft IIS, Netscape, Apache, Lotus, Tandem, and Nanoteq

**SSL Verification Process**

1. Customer need to submit below documents in order to process SSL order:

* Complete enrolment form (Web Server Specification, Domain Name, Organization Contact, Technical Contact)
* CSR file – Customer need to generate the csr file at the server

**2. Domain Authentication Requirements**

MSC Trustgate first tries to authenticate the domain listed in your enrolment through publicly available domain name registration information. If we cannot automatically authenticate your domain name control, we require an authorization letter from that domain's owner. This step prevents applicants from fraudulently or accidentally obtaining SSL Certificates for domains that do not belong to them

1. Verification Call

* The organizational contact is an employee of the organization
* The organizational contact is aware and approves of the certificate request
* The technical contact is authorized to receive the certificate

1. Once validation and verification done, the SSL certificate will be issue to the technical contact by email.
2. Customer may proceed install the SSL certificate at their server