



## Enterprise SSL

**Enterprise SSL server certificate confirms a remote computer (server) identity on the Internet or LAN, includes Internet address and the information about the owner. The certificate makes it possible to establish a secure (encrypted) connection between the server and customer's software. To do so the server imposes the strong 128-bit encryption effected by means of the Secure Sockets Layer (SSL) protocol. Enterprise SSL certificate provides a high level of security due to appropriate procedures for the identity validation and high liability of the certificate issuer.**

.....

### Application

Enterprise SSL server certificate is mainly used in case the server transmits personal data, passwords, identification numbers, credit card data or confidential information. The certificate can be used for the secure access to a server since it provides the encrypted connection between the customer's software and server. Moreover, the certificate is used for the authentication of the server on the net, validation of its reliability and protection against the replacement by a fake server.

## Enterprise SSL certificates are used for:

- server authentication
- protection of business and commercial transactions carried out by a server, such as placing orders, contracting and making offers
- protection of on-line store websites
- protection of communication with mailing servers
- protection of communication with database servers

### Benefits

- server authentication
- server reliability
- protection of basic security services (authentication, integrity and confidentiality on the basis of the SSL protocol)
- secure (encrypted) communication
- reliability and confidence from persons who use the certified server

### Features

- compliance with X.509 v.3 (RFC3280)
- protection by means of RSA-SHA1 encryption function



- issue by CERTUM certified for the compliance with WebTrust standards
- issue by CERTUM whose root certificate is automatically recognized as trusted on website browsers
- possibility of certificate status validation by CRL and OCSP services

### Financial warranty

- \$ 100,000.00

### Price

Enterprise SSL	USD	EUR	Validity	
Issue	\$ 199.00	€ 149.00	1 year	<a href="#">BUY</a>
Renewal	\$ 139.00	€ 99.00	1 year	<a href="#">BUY</a>

### Verification

- domain owner data verification in WHOIS base to check the conformity with data given in order form
- verification if person has access to the server with domain for requested certificate: CERTUM sends metatag to be placed on the server and verifies it's presence
- e-mail with link to get certificate will be sent to one of the following:
  - admin@yourdomain.com
  - administrator@yourdomain.com
  - webmaster@yourdomain.com
  - ssladmin@yourdomain.com
  - root@yourdomain.com
  - hostmaster@yourdomain.com
  - postmaster@yourdomain.com

where domain name is detailed in certificate request (CSR)

Only if one of mentioned requirements is not fulfilled additional documents must be supplied as follows:

- document to assure the person responsible for certification procedure is an employee or representative of company/institution
- document to verify company/institution authenticity, e.g.:
  - DUNS number (Dun and Bradstreet)
  - Articles of Incorporation
  - Business License
  - Doing Business As (DBA) registration
  - Partnership documentation
  - Sole Proprietorship documentation



- Factitious Name Statement
- Assumed Name Statement
- Seller's Permit
- Occupational License
- Sales Permit

All delivered documents must be signed by official representative. Delivered documents must be in English or must be translated into English by sworn translator or certified by a notary.

### **Submission of documents**

Documents can be delivered by:

- e-mail
- post
- fax
- in person

### **Go to**

- [Certificate Features](#)