SSL Certificates

Duration: 1 day **Price: € 699**

Open Schedule

Audience Course SSL Certificates

The course SSL Certificates is intended for system administrators, security professionals, developers and others who want to learn how obtain, configure and maintain SSL Certificates.

Prerequisites Course SSL Certificates

General knowledge of information technology is required to participate in this course. Experience with security concepts and web applications is beneficial for understanding but not required.

Realization Training SSL Certificates

The course SSL Certificates has a hands-on character. The theory is treated on the basis of presentation slides and is interchanged with practical exercises. The course material is in English. Course times are from 9.30 up and to 16.30.

Certification Course SSL Certificates

After successful completion of the training the participants receive an official certificate SSL Certificates.

Content Course SSL Certificates

The course SSL Certificates covers the theory and practice of SSL certificates that are essential in setting up secure and encrypted Internet connections. The original SSL 2 and SSL 3 protocols have since been replaced by the TLS protocol, but the name SSL is still used. With SSL, one side of the connection has a private key, while a public key is made available to others who want to connect.

SSL Intro

The course starts with a discussion of how an SSL connection is established. Attention is paid to how the SSL connection starts with a handshake between client and server. In the first step in the connection, the client uses the server's public key to encrypt a message. The server has the corresponding private key and can read the message with it. Then a secret key is generated. That key is only known to both the client and the server and is used in the mutual message traffic.

Encryption Algorithms

Next attention is paid to the various forms of encryption that play a role in SSL. With asymmetric encryption, both sides of the connection have different keys that fit together and that can decipher each other's messages. With symmetric encryption, both sides have the same key, which must then be hidden from the outside world. And with hash encryption there is one-way encryption. A message cannot be deciphered then, but it is possible to check whether the message has been changed.

SSL Certificates

The course also covers what SSL certificates are and how they are used to identify a server or a client. It is explained which types of certificates there are. Client, server and self-signed certificates are discussed and root certificates and wild card certificates are also treated. Attention is also paid to how certificates can be created or requested and how to install them in known servers.

Public Key Infrastructure

Recognized certificates are issued by certificate authorities such as Thawte, Verisign, Let's Encrypt and other organizations. They check whether the applicant for a certificate is really who he claims to be and use various verification methods for this. The certificate authorities are part of the Public Key Infrastructure. Protocols such as DANE and DNSSEC are also discussed.

Modules Course SSL Certificates

Module 1 : SSL Intro	**Module 2 : SSL Encryption**	**Module 3 : Certificates**
SSL Overview	Encryption Algorithms	SSL Certificates
Secure Sockets Layer (SSL)	RSA algoritme	Creating Certificates
SSL en TLS	ECC algoritme	CSR's
SSL Characteristics	SSL Encryption Types	Server Certificates
SSL Handshakes	Asymmetric Encryption	Client Certificates
SSL Connectors	Symmetric Encryption	Common Name
Configuring SSL	Hash Encryption	Root Certificates
Server Name Indication	HTTPS Connections	Wild Card Certificates
SNI Protocol	HTTP Strict Transport Security	Subdomains
Key Files	Secure Mime	Certificate Revocation List
Private and Public Key	Digital Signing	Black and White Listing
OpenSSL Library	Salt Function	OCSP and Stapling
Module 4 : PKI Infrastructure		
Chain of Trust		
Certificate Authorities		
Domain Validation		
Organization Validation		
Cipher Suites		
Handshake		
CAA Record		
Configuring CAA		
DANE Protocol		
Trust Anchor		
File Approver		
DNSSEC Protocol		