

Schulung *Kryptografie/Zertifikate*

Factsheet

THEMA Grundlagen Kryptografie und Zertifikate

KURZBESCHREIBUNG Viele Sicherheitstechnologien in der IT basieren auf kryptografischen Verfahren. Dieses Modul startet mit einer Einführung der wichtigsten Verfahren und vertieft dann mit konkreten Anwendungen wie Verschlüsselung, digitale Signatur, Zertifikate und sichere Transportprotokolle.

ZIELGRUPPE IT Spezialisten, Softwareentwickler

VORAUSSETZUNG Grundkenntnissen in Softwareentwicklung, Mathematik Sekundarstufe II

AUFBAUENDE MODULE -

DAUER 1 Halbtage, inkl. Fragen und Diskussion

KURSART Frontalschulung, Praxisbeispiele, Demos, Diskussion

Inhalt

- Symmetrische, asymmetrische und hybride Verschlüsselung
- Hash Funktionen und deren Anwendungen
- digitale Signatur
- asymmetrische Verschlüsselung am Beispiel RSA
- sichere Transportprotokolle (SSL/TLS)
- Identifikation, *Trust Chain*
- Zertifikate (Sinn und Zweck, Typen, Templates, CSR, Revozierung, ...)
- Smartcard, TPM und HSM, PKI
- Praktische Anwendung kryptografischer Verfahren

Ziele

Nach der Absolvierung des Moduls wissen die Teilnehmenden, was eine Hash Funktion ist und wie eine digitale Signatur funktioniert. Sie kennen den Unterschied zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren und verstehen, warum diese in der Praxis meist kombiniert werden. Sie wissen, wozu Zertifikate dienen, welche Arten es gibt und welche Rolle dabei Smartcard, TPM und HSM spielen. Behandelt werden auch PKI, CA und *Trust Center*. Weiter wissen sie, worauf bei der Anwendung kryptografischer Verfahren zu achten ist und welche Anforderungen an den Umgang und die Speicherung von Schlüsselmaterial zu stellen sind.