Seminarort

CCG-Zentrum, Technologiepark
Argelsrieder Feld 22, Geb. TE 03, D-82234 Weßling-Oberpfaffenhofen

Eine Lageskizze sowie Hinweise für die Anreise und Übernachtung schicken wir Ihnen mit der Bestätigung der Anmeldung zu.

Gebühr

EUR 1490,--
Die CCG ist ein gemeinnütziger Verein und in Deutschland von der Umsatzsteuer befreit. Für Veranstaltungen an ausländischen Standorten gelten die dortigen Steuerregelungen.

Mitglieder der CCG erhalten 10% Rabatt. Studentenrabatte sind auf Nachfrage verfügbar. Die Rabatte sind nicht miteinander kombinierbar.

Bitte zahlen Sie bargeldlos nach Erhalt der Rechnung.

Anmeldungen

Bitte melden Sie sich möglichst bis 14 Tage vor Seminarbeginn an:

Carl-Cranz-Gesellschaft e.V., Argelsrieder Feld 22, D-82234 Weßling
Tel. +49 (0) 8153 / 88 11 98 -12
E-Mail: anmelden@ccg-ev.de
Internet: www.ccg-ev.de

Die Anmeldungen werden schriftlich bestätigt.

Weitere Informationen zum Inhalt

Kurt Klein,
Dozent für Informationstechnologie
an der ARD.ZDF medienakademie, Nürnberg
Tel. +49 (171) 75 11 980, mail@kurtklein.de

Stornierung

Bei Stornierungen, die später als 14 Tage vor Seminarbeginn eingehen, werden 25% der Gebühr, bei Nichterscheinen die volle Gebühr in Rechnung gestellt. Die Vertretung eines angemeldeten Teilnehmers ist selbstverständlich möglich.

Ausfall von Seminaren oder Dozenten

Die CCG behält sich vor, bei zu geringer Teilnehmerzahl oder aus anderen triftigen Gründen ein Seminar bis 14 Tage vor Beginn abzusagen. Sie behält sich weiter vor, entgegen der Ankündigung im Programm auch kurzfristig einen Dozenten und evtl. auch dessen Thema zu ersetzen. Ein Schadensersatzanspruch bleibt ausgeschlossen.

Verschlüsselung mit Zertifikaten

Teilnehmer

Entscheider und Führungskräfte aus dem Bereich IT, z.B. CIO, CFO, CISO, Leiter Rechenzentrum, Informatiker, Ingenieure, Naturwissenschaftler und Spezialisten aus verschiedenen Bereichen.

Seminarinhalte

Während noch vor einigen Jahren ein Server viele unterschiedliche Websites auslieferte und sich die Entwickler um die Verschlüsselung keine Gedanken machen mussten – die Verschlüsselung mit Zertifikaten wurde von den Administratoren zentral für den Server erledigt – ist jetzt durch die Container-Virtualisierung jede einzelne Webanwendung eine eigene Instanz (ein Container bei Docker, ein Pod bei Kubernetes). Jeder Softwareentwickler und jeder Entscheider hat auf einmal mit dem Thema Verschlüsselung zu tun. So ist Datensicherheit durch verschlüsselte Kommunikation auf Basis der Protokolle SSL/TLS heute fast eine Selbstverständlichkeit – zumindest sollten sie es sein. Sie haben aber nur Erfolg, wenn sie bequem genutzt werden können und funktionieren. Was ist ein Zertifikat, ein Certificate Signing Request, eine Certificate Authority? Wie wird ein Schlüsselpaar erstellt und was kann man damit anfangen? Was ist eine Zertifikatskette, was ist RSA, DSA, Diffie-Hellman? Was muss man einer Zertifizierungsstelle geben, damit sie ein Zertifikat ausstellen kann? Was erhält man von der Zertifizierungsstelle zurück? Welches Material ist geheim und welches ist öffentlich? Was muss wohin, damit Authentifikation, Schlüsselaustausch und letztendlich verschlüsselte Kommunikation wie selbstverständlich im Hintergrund stattfinden können? Diese und viele weitere Fragen werden in diesem Kurs anschaulich beantwortet. Darüber hinaus stellen wir exemplarisch Tools zur Analyse und Erstellung von Zertifikats- und Schlüssel-Formaten vor. Auf eine leicht verständliche Art und Weise erhalten Sie somit das technische Hintergrundwissen zu Sicherheitsaspekten Ihrer Webanwendung.

Vortragende

Kurt Klein	Dozent für Informationstechnologie an der ARD.ZDF medienakademie, Nürnberg

Unterlagen

Jeder Teilnehmer erhält die Vortragsunterlagen.
Die Kosten dafür sind in der Gebühr enthalten.

Carl-Cranz-Gesellschaft e.V. | Weßling
Gesellschaft für technisch-wissenschaftliche Weiterbildung

Seminar IN 4.02

Verschlüsselung mit Zertifikaten und TLS/SSL verstehen

01. - 02. Dezember 2025
Oberpfaffenhofen bei München

Informatik

Wissenschaftliche Leitung
Kurt Klein
ARD.ZDF medienakademie, Nürnberg

Verschlüsselung mit Zertifikaten
Verschlüsselung mit Zertifikaten

Seminarprogramm

Montag, 01.12.2025
08:30 – 16:45 Uhr

08:30 – 08:45	**Begrüßung, Organisation**
08:45 – 10:15	**Kryptografische Grundlagen** **Hash, Message Authentication Code, SHA-256**
	Pause 30 Min.
10:45 – 12:15	**Symmetrische Verfahren, AES** **Asymmetrische Verfahren, RSA** **Schlüsselpaare, Private Key, Public Key**
	Mittagspause
13:15 – 14:45	**Eigenschaften und Funktionalitäten von Schlüsselpaaren** **Schlüsselaustausch, RDA, Diffie-Hellman**
	Pause 30 Min.
15:15 – 16:45	**Digitale Signatur** **Authentifikation mit Schlüsseln** **Demo/Praxis: Anwendungsbeispiel OpenSSH**

Dienstag, 02.12.2025
08:30 – 16:30 Uhr

08:30 – 10:00	**Standards: X.500 und X509** **PKI, Certificate Authority, Subscriber, Relying Party**
	Pause 30 Min.
10:30 – 12:00	**Certificate Signing Request** **Zertifikat, Zertifikatskette** **Zertifikatsformate (PEM, DER, PKCS#7, PKCS#12))**
	Mittagspause
13:00 – 14:30	**Demo/Praxis: Konfiguration TLS, Webserver und Browser**
	Pause 30 Min.
15:00 – 16:30	**Ausblick, Diskussion, Fragerunde, Verabschiedung**