

## PKI – Die Technik im Detail

### Theoretische und praktische Funktionsweise einer PKI

Im Zeichen der Globalisierung der Märkte hat das Bedürfnis, sensible Informationen über elektronische Medien zu übertragen, sprunghaft zugenommen. Daher ist auch der Bereich der elektronischen Medien mehr und mehr im Zentrum des Interesses bei Institutionen, die – mehr oder weniger legitimiert – diese Information mitnutzen wollen.

Schon die römischen Feldherren bekamen ihre Befehle verschlüsselt gemeldet, warum daher nicht auch Ihre Mitarbeiter, Kollegen und Vorgesetzten? Und genau wie die alten Römer müssen wir uns auch heute noch sorgen, dass der Bote mit der Nachricht auch der richtige ist! Unverschlüsselte E-Mails beispielsweise sind genauso offen zugänglich wie Postkarten. Würden Sie vertrauliche Informationen als Postkarte versenden?

Der Begriff PKI ist zwar inzwischen schon eine Art Allgemeingut geworden, dennoch verbleiben meist noch eine Reihe ungeklärter Fragen. Gerade das Zusammenspiel der verschiedenen Technologien und Standards macht eine gute PKI Lösung aus. Insofern ist es für jeden wichtig, die Hintergründe einer PKI zu verstehen.

In diesem Seminar erfahren Sie alle nötigen Details der verschiedenen Algorithmen, Protokolle und Standards. Dabei wird nicht nur die Theorie dargestellt, sondern auch deren Einsatz an vielen Beispielen erläutert.

Dieses Seminar vermittelt unter anderem:

- ✓ Überblick über gängige Algorithmen zur Verschlüsselung, Integritätssicherung und Signierung
- ✓ Gebrauch von Kryptographie innerhalb verschiedener Betriebssysteme und Produkte
- ✓ Notwendigkeit einer PKI
- ✓ Aufbau einer Beispiel-CA
- ✓ Bedeutung von Chip- und Smartcards

### Themenauswahl

#### ▲ Grundlagen

- Asymmetrische und symmetrische Verschlüsselung
- Verschlüsselungsalgorithmen
- Stärken und Schwächen der Algorithmen

#### ▲ Algorithmen im Detail

- DES • AES • IDEA • Blowfish
- Diffie-Hellman • RC2/4/5 • RSA
- ElGamal

#### ▲ Verschlüsselung in der Praxis

- TLS (SSL) • Kerberos • PEM
- PGP • PKCS • Public Key Infrastructure • S/MIME

#### ▲ Zertifikate

- X.509 • Inhalt • Erstellung und Verwaltung • Einsatzmöglichkeiten
- Erweiterungen zum Standard

#### ▲ Betrieb einer einfachen CA

- Einsatz von OpenSSL • Erzeugen von Zertifikaten • Erstellen einer CRL • Konfigurieren der technischen Parameter

#### ▲ Chip- und Smartcards

- Unterschiede Chip-/Smartcard
- Smartcardleser • Betrieb von Karten und Lesern

#### Zielgruppe

- IT-Mitarbeiter
- Administratoren
- Datenschutzbeauftragte

#### Voraussetzung

- Kenntnisse im Umgang mit Windows/Linux

#### Dauer

3 Tage

#### Maximalzahl Teilnehmer

8

#### Preis

EUR 1.290,00 zzgl. MwSt.

#### Termine

23.02. – 25.02.2011

29.06. – 01.07.2011

21.11. – 23.11.2011

#### Ort

München

Auch jederzeit Inhouse möglich



### ▲ Teilnahme

Die Auswahl der gewünschten Veranstaltung liegt beim Teilnehmer, der die notwendigen Voraussetzungen mit seiner Anmeldung anerkennt.

Die jeweilige Veranstaltung wird nach heutigem Stand der Technik sorgfältig vorbereitet und durchgeführt. Beratungen zur Teilnahme und den Teilnahmevoraussetzungen seitens des Teilnehmers sind unverbindlich.

### ▲ Anmeldung

Die Anzahl der Teilnehmer an den Trainings und Workshops der GENIA-SEC GmbH sind begrenzt. Anmeldungen können nur 14 Tage vor dem geplanten Termin entgegengenommen werden, wobei die Reihenfolge des Eingangs der Anmeldung berücksichtigt wird.

Ein Vertrag kommt erst durch die Auftragsbestätigung der GENIA-SEC GmbH zustande.

### ▲ Teilnahmegebühr

Sämtliche Preise verstehen sich pro Teilnehmer, sind in Euro angegeben und verstehen sich zzgl. der gesetzlichen Mehrwertsteuer. Die Teilnahmegebühr ist vor dem Beginn der Veranstaltung auf das auf der Rechnung angegebene Konto zu zahlen. In der Teilnahmegebühr sind sämtliche Unterlagen sowie die Pausenverpflegung enthalten.

### ▲ Stornierung

Bei der Absage einer verbindlich bestätigten Teilnahme fällt bis zwei Wochen vor Beginn der Veranstaltung eine Bearbeitungsgebühr von € 50,- an. Erfolgt die Stornierung bis eine Woche vor Beginn der Veranstaltung, ist die halbe Seminargebühr fällig. Erfolgt die Stornierung noch später oder erscheint der Teilnehmer nicht, wird die volle Gebühr berechnet. Ersatzpersonen werden von GENIA-SEC GmbH selbstverständlich akzeptiert.

### ▲ Vorbehalte

GENIA-SEC GmbH behält sich vor, Veranstaltungen aus organisatorischen oder anderen Gründen abzusagen. In diesem Fall werden angemeldete Teilnehmer umgehend benachrichtigt und bereits gezahlte Gebühren erstattet. Weitere Ansprüche bestehen ausdrücklich nicht.

### ▲ Weiteres

Die im Rahmen der Veranstaltung überreichten Unterlagen obliegen dem Copyright, so dass hiervon keine Kopien angefertigt oder sie Dritten überlassen werden dürfen.

Mit der Anmeldung werden die oben genannten Bedingungen akzeptiert.

Für Rückfragen steht Ihnen das Team von GENIA-SEC GmbH gerne zur Verfügung:

GENIA-SEC IT-Sicherheitsmanagement GmbH  
Lerchenstr. 40  
D-86830 Schwabmünchen  
Telefon: +49 (8232) 730 221  
Telefax: +49 (8232) 730 227  
E-Mail: [info@genia-sec.de](mailto:info@genia-sec.de)

## Anmeldung



▲ Per Fax an +49 (8232) 730 227

Hiermit melde ich mich verbindlich für folgende(s) Training(s) an:

Titel des Trainings	Termin/Ort	Code	Kursgebühr

Meine persönlichen Daten:

Name, Vorname	
Funktion/Abteilung	
Firma	
PLZ, Ort	
Straße	
Telefon	
Telefax	
E-Mail	

Geben Sie hier bitte eine ggf. abweichende Rechnungsanschrift an:

Ort, Datum

Unterschrift

Tagungsunterlagen, Pausengetränke und Mittagessen sind in den Kursgebühren (zzgl. MwSt.) enthalten. Den Teilnahmebedingungen stimme ich durch meine Unterschrift zu.