



Workshop
PKI - Grundlagen und praktische Anwendung

Workshop
PKI
Grundlagen und praktische
Anwendung

Die aktuellen Termine, Referenten und Programme finden Sie im Internet unter
<http://seminare.tele-consulting.com>

Tele-Consulting GmbH
security | networking | training
Seminarinstitut
Siedlerstraße 22 - 24
71126 Gäufelden

fon (0 70 32) 97 58 20
fax (0 70 32) 74 75 0
eMail seminare@tele-consulting.com
web <http://seminare.tele-consulting.com>

Gliederung

1	Kurzbeschreibung	1-1
2	Zielgruppen	2-2
2.1	Workshopziel	2-2
2.2	Zielgruppe	2-2
2.3	Vorraussetzungen	2-2
3	Seminarbeschreibung	3-3
3.1	1. Tag: 09.30 - 17.00 Uhr	3-3
3.2	2. Tag: 09.00 - 17.00 Uhr	3-4
4	Referenten	4-5
5	Termine, Orte, Preise	5-6

1 Kurzbeschreibung

Einführung in die theoretischen und technischen Hintergründe

- **Architektur einer Public Key Infrastructure (PKI)**
- **Kryptologische Hintergründe**
- **Zertifikate**
- **Betrieb einer Certification Authority**
- **Standards im Bereich PKI**
- **Problemstellungen aus der Praxis**
- **Rechtliche Hintergründe**
- **Aktuelle Entwicklungen**
- **1,5 Tage Vermittlung der Hintergründe mit Beispielen und Demonstrationen**
- **ca. ½ Tag praktische und betreute Anwendung am Beispiel von 2 PKI-Lösungen (kommerziell und Open Source) durch die Teilnehmer**

2 Zielgruppen

2.1 Workshopziel

Ziel des Workshops ist die Vermittlung der Hintergründe und Zusammenhänge im Rahmen einer Public Key Infrastructure (PKI). Dabei werden die theoretischen Hintergründe beleuchtet, die sich durch die angewendeten kryptographischen Methoden und durch die geltenden Standards ergeben. Ebenso werden die technischen Zusammenhänge zwischen den Elementen einer PKI umfassend erklärt.

Weiterhin werden notwendige Rahmenbedingungen für die Umsetzung von PKI-Projekten erläutert. Hierzu gehört auch die Betrachtung der geltenden rechtlichen Rahmenbedingungen sowie die Diskussion von aktuellen Entwicklungen.

Für die Vermittlung der Hintergründe und Zusammenhänge werden die theoretischen Grundlagen durch Beispiele und Demonstrationen ergänzt.

Die theoretischen Grundlagen werden schließlich anhand von 2 unterschiedlichen PKI-Lösungen in der Praxis gezeigt. Hierzu werden Strukturen einer PKI in einem Testnetzwerk aufgebaut. Die Teilnehmer haben dann selbst die Möglichkeit, unterschiedliche Rollen einzunehmen und die PKI durch praktische Übungen zu testen. Die praktischen Anwendungen der Teilnehmer werden stets durch die Referenten betreut.

Die für die praktische Anwendung genutzten PKI-Lösungen kommen sowohl aus dem kommerziellen Bereich als auch aus dem Open-Source-Umfeld. Um eine geeignete Durchführung der praktischen Übungen zu gewährleisten, ist die Teilnehmerzahl auf eine kleine Gruppe beschränkt.

Die Teilnehmer können mit den Kenntnissen des Workshops eigene PKI-Projekte konzipieren oder direkt die praktische Umsetzung planen.

2.2 Zielgruppe

Zielgruppe sind all diejenigen, die an den Grundlagen von PKI interessiert sind, die ggf. eigene Berührungspunkte damit haben oder bereits planen, ein eigenes PKI-Projekt in ihrer Organisation durchzuführen. Der angesprochene Personenkreis hat beispielsweise folgende Funktionen:

- Sicherheitsbeauftragte
- Projektleiter, IT-Leiter
- Administratoren

2.3 Voraussetzungen

Grundkenntnisse über Netzwerke und Betriebssysteme sind vorteilhaft.

3 Seminarbeschreibung

Die Themen der ersten 1 ½ Tage werden mit Beispielen bzw. Demonstrationen veranschaulicht.

3.1 1. Tag: 09.30 - 17.00 Uhr

Architektur einer PKI

- Einführung: Wozu braucht man eine PKI?
- Elemente und Aufgaben einer PKI
 - CA (Zertifizierung), RA (Identifizierung, Registrierung)
 - Verzeichnisdienste (Veröffentlichung)

Kryptographie und PKI

- Symmetrische Kryptographie (DES, AES, IDEA)
- Asymmetrische Kryptographie (RSA, Diffie-Hellman)
- Hashing
- Digitale/elektronische Signatur

Zertifikate und Standards

- Aufbau und Inhalte: Zertifikatsprofile
- Erstellung von Zertifikaten und deren Einsatzmöglichkeiten
- X.509, PKIX, PKCS, ISIS-MTT, Vergleich mit PGP

PKI in der Praxis: grundsätzliche Problemstellungen

- Gültigkeit der Zertifikate
- Zertifikatssperrungen
- Verteilung von Zertifikaten, Key-Recovery
- Zertifikatsverlängerung bzw. -erneuerung
- Prüfung einer Signatur oder eines Zertifikats(-Pfades)
- Schnittstellen zum Verzeichnisdienst (LDAP, OCSP)

3.2 2. Tag: 09.00 - 17.00 Uhr

Chip- und SmartCards

- Vor- und Nachteile des Einsatzes
- Arten und Aufbau von SmartCards
- Zertifikate und SmartCards

Betrieb einer CA

- Zertifizierungs-Richtlinien, Rollen einer CA
- Prozesse und Randbedingungen

Rechtliche Hintergründe

- Signaturgesetz und Signaturverordnung
- weitere gesetzliche Regelungen
- aktuelle Entwicklungen

Die folgenden Punkte der Agenda bestehen im wesentlichen aus Demonstrationen und praktischen Übungen. Die Teilnehmer können an verschiedenen Systemen Anwendungen einer PKI testen.

Der praktische Teil ist zur besseren Übersicht **rot** gekennzeichnet.

PKI in der Praxis

- Aufbau einer CA und Teilen einer RA anhand von 2 PKI-Lösungen bzw. -Produkten (kommerziell bzw. Open-Source).
- Lösungen für einen Verzeichnisdienst
- Active Directory als Alternative für einen Verzeichnisdienst
- Was bringen die Zertifikatsdienste von Microsoft
- Ausstellung und Verteilung von Zertifikaten

Anwendungen für Zertifikate einer PKI

- Einbindung von Zertifikaten
- eMail-Verschlüsselung (S/MIME) anhand von 2 Beispiel-Anwendungen
- Zertifikate für gesicherten Web-Zugriff (TLS/SSL)
- Signatur von Dateien

Anwendungen für Zertifikate unter Microsoft Windows

- Nutzung des Encrypting File System (EFS)
- Authentisierung am System am Beispiel von Logon an einem Microsoft-Domänen-Controller (SmartCard-basiert)
- Nutzung von Zertifikaten für IPsec-Verschlüsselung

4 Referenten

Reto Lorenz **Evaluator**

Reto Lorenz ist bei der Tele-Consulting GmbH als Evaluator im Bereich IT-Sicherheit tätig. Hierzu gehört die Mitwirkung bei der Durchführung von Risikoanalysen und der Erstellung von IT-Sicherheitskonzepten. Als wichtiger Baustein gehört dazu auch die Unterstützung für die Umsetzung von Maßnahmenkatalogen aus IT-Sicherheitskonzepten. Herr Lorenz ist ein vom BSI lizenzierter IT-Grundschutzauditor (Registrierungsnummer: BSI-GSL-0033-2002). Als Netzplaner arbeitet er bei der Erstellung von Studien verantwortlich mit. Als weiterer Schwerpunkt plant, entwirft und realisiert er Internet- und Intranet-Lösungen. Reto Lorenz verfügt über mehrjährige Erfahrung mit IT-Security-Komponenten (Firewalls, Scanning-Tools, etc.). In jüngerer Zeit hat Herr Lorenz in mehreren Fällen die Umsetzung von zertifikatsbasierten Lösungen auf Basis einer PKI maßgeblich mitgestaltet.

Tobias Glemser **IT-Sicherheitsberater**

Tobias Glemser ist bei der Tele-Consulting GmbH als Mitarbeiter des Prüflabors für IT-Sicherheit vornehmlich in den Bereichen der toolgestützten Schwachstellenanalyse und Security Audits tätig. Zu seinen Tätigkeiten gehören neben den Aspekten der IT-Sicherheit auch die Konzeption und Realisierung von Intranet- bzw. Web-Services. Ebenfalls ist er mit Netzplanungsaufgaben im LAN/MAN/WAN-Bereich sowohl bei der Grob- als auch bei der Ausführungsplanung betraut. Tobias Glemser verfügt über Kenntnisse im Umgang mit vielen Systemplattformen und IT-Komponenten. Insbesondere im Bereich von Open-Source-Anwendungen konnte er ein fundiertes Know-How aufbauen.

5 Termine, Orte, Preise

Termine

22. – 23.10.2003

26. – 27.11.2003

weitere Termine auf Anfrage und nach Vereinbarung

Orte

Seminar-Institut, Siedlerstraße 22-24, 71126 Gäufelden

Preise

2 Tage € 1.200,00 zuzüglich. MwSt.

Weitere Hinweise

In der Gebühr sind die Seminar-Unterlagen, Pausengetränke und das Mittagessen enthalten. Die Rechnung wird 14 Tage vor Seminarbeginn zugestellt. Die Gebühr ist ab Rechnungsdatum innerhalb von 10 Tagen netto fällig.

Für Ihre Anmeldung benutzen Sie bitte das über uns beziehbare Anmeldeformular oder gehen direkt ins Internet: <http://seminare.tele-consulting.com>. Nach Eingang der Anmeldung erhalten Sie eine Anmeldebestätigung. Die Teilnehmerzahl ist auf einen kleinen Kreis begrenzt; melden Sie sich deshalb bitte rechtzeitig an.

Der Teilnehmer kann bis 14 Tage vor Beginn gebührenfrei absagen. Bei Absage durch den Teilnehmer innerhalb von 2 Wochen vor Beginn, wird eine Kostenpauschale in Höhe von € 150,00 zuzüglich ges. MwSt. berechnet. Bei Nichterscheinen oder Absage innerhalb von 5 Tagen vor Beginn wird die halbe Gebühr erhoben. In diesem Fall bekommt der Teilnehmer die kompletten Seminar-Unterlagen zur Verfügung gestellt. Der Teilnehmer kann jederzeit einen Ersatzteilnehmer benennen. Der Teilnehmer hat außerdem die Möglichkeit, dasselbe Seminar gebührenfrei auf einen anderen Termin umzubuchen.

Auf Wunsch des Teilnehmers bucht unser Sekretariat die Übernachtung im nahegelegenen Sporthotel ARAMIS zu folgenden derzeitigen Konditionen: € 64,00 für ÜF im Sporthotel ARAMIS und € 58,00 für ÜF im ARAMIS Gästehaus. Die Preise schließen Sauna-/Dampfbad-, Fitness und Gesundheitsstudio-Nutzung mit ein. Wir übernehmen auf ausdrücklichen Wunsch den kostenlosen Transfer von S-Bahnhof Herrenberg nach Gäufelden oder organisieren die Fahrt vom Flughafen Stuttgart zum Preis von € 46,00 pro Fahrt.