SOFTCON

Single Sign-On mit Kerberos V5

Froscon 2006

Michael Wiesner
SOFTCON IT Service GmbH

SOFTCON

Über mich

- **Softwareentwickler und Sicherheitsexperte bei der Firma SOFTCON**
- **Projekte: Enterprise Software, Webportale, Sicherheitslösungen, ...**
- **Trainings und Vorträge über Security**

SOFTCON

Agenda

1. Identitätsmanagement
2. Single Sign-On
3. Kerberos Grundlagen
4. Implementierungen
5. Installation & Konfiguration Linux
6. Integrationsmöglichkeiten Linux/Windows
7. Ausblick

SOFTCON

Agenda

1. Identitätsmanagement
   - Begriffe
   - Identitätsnachweis
   - Kryptographische Grundlagen
2. Single Sign-On
3. Kerberos Grundlagen
4. Implementierungen
5. Installation & Konfiguration Linux
6. Integrationsmöglichkeiten Linux/Windows
7. Ausblick

SOFTCON

Identitätsmanagement Begriffe

- **Authentifizierung (Authentication)**
  - **Identitätsfeststellung**
  - **z.B. Personalausweis, Pass, ...**

- **Autorisierung (Authorization)**
  - **Zuweisung von Rechten**
  - **z.B. Mitgliedsausweis, Access Control Lists**

- **Überwachung (Auditing)**
  - **Aufzeichnen von Authentifizierungen und Autorisierungen**
  - **z.B. Auth-Log bei Linux**

SOFTCON

Identitätsnachweis

- **Benutzername/Kennwort**

- **Key bzw. Zertifikat**

- **Smart Card**

- **Foto**

- **Fingerabdruck**

- **Iris**

SOFTCON

Kryptographische Grundlagen

- symmetrische Verschlüsselung
  - Ein Key zum Ver- und Entschlüsseln
  - schwierige Verwaltung, dafür sehr schnell
  - z.B. DES, 3DES, AES, RC5
  - Verwendung: Kerberos, SSL

- asymmetrische Verschlüsselung
  - Zwei Keys jeweils zum Ver- und Entschlüsseln
  - einfachere Verwaltung aber dafür langsam
  - z.B. RSA, DSA, ElGamal
  - Verwendung: PGP, Signaturen, SSL

SOFTCON

Agenda

SOFTCON

Was bedeutet Single Sign-On?

- Benutzerauthentifizierung nur einmal
- Anschließend Zugriff auf (alle) Systeme
- Führt i.d.R. keine Autorisierung durch
- Eine Stufe darunter: Single Credential
  - Ein Benutzername/Kennwort für alle Systeme

SOFTCON

Wieso brauchen wir das?

- Produktivitätssteigerung
  - Arbeitsfluss wird nicht gestört
  - Einfachere Administration
- Erhöhte Sicherheit, denn ohne SSO...
  - wird oft das gleiche Kennwort benutzt
  - wird das Kennwort auf mehreren Systemen gespeichert
  - geht das Kennwort mehrmals über das Netzwerk
- Nachteil: Bei einer Kompromittierung erhält der Angreifer Vollzugriff.

SOFTCON

Lösungsansätze

- „Lokale Lösungen“
  - Benutzername/Kennwort wird lokal gespeichert (z.B. durch Browser, Outlook, ...)

- Portale
  - Einloggen bei einem zentralen Portal
  - Portal steuert weitere Zugriffe

- Ticket Systeme
  - Ticket mit Identitätsnachweis wird bei der ersten Anmeldung erstellt
  - Authentifizierung anschließend über dieses Ticket

SOFTCON

Agenda

SOFTCON

Was ist Kerberos?

- **Kerberos...**
  - **... ist ein verteilter Authentifizierungsdienst.**
  - **... ist konzipiert für offene und unsichere Netze.**
  - **... ermöglicht Single Sign-On.**
  - **... ist Plattform- und Systemunabhängig.**
  - **... verwendet symmetrische Verschlüsselung.**
  - **... ist in RFC 1510 beschrieben.**

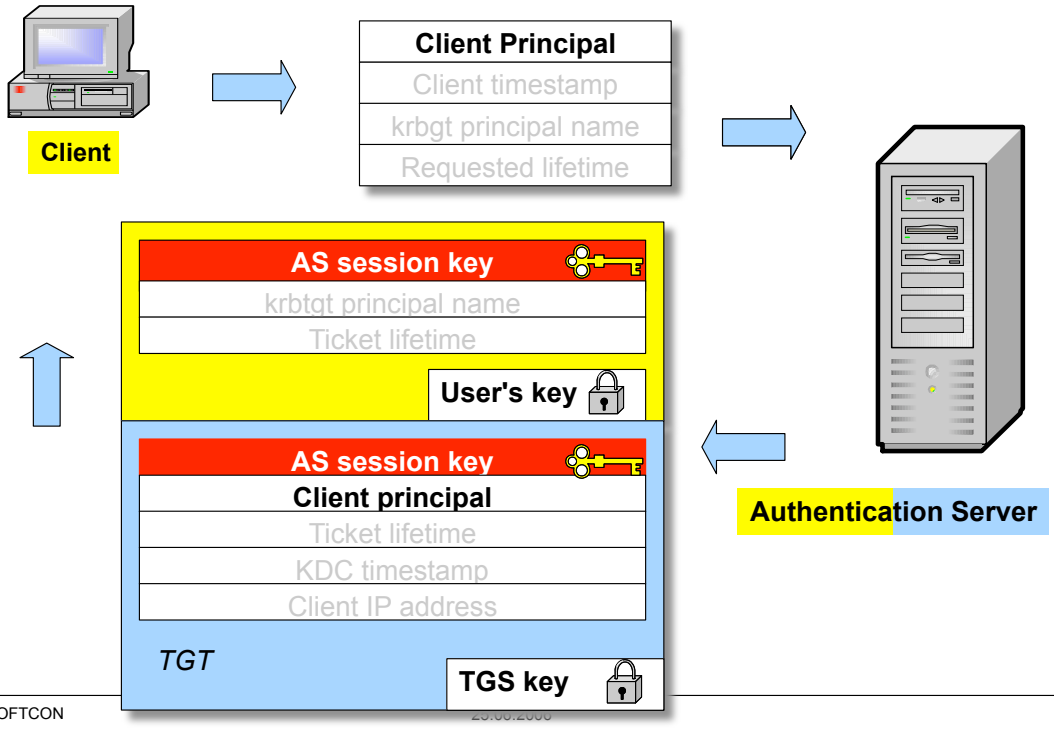
SOFTCON

Principals & Realms

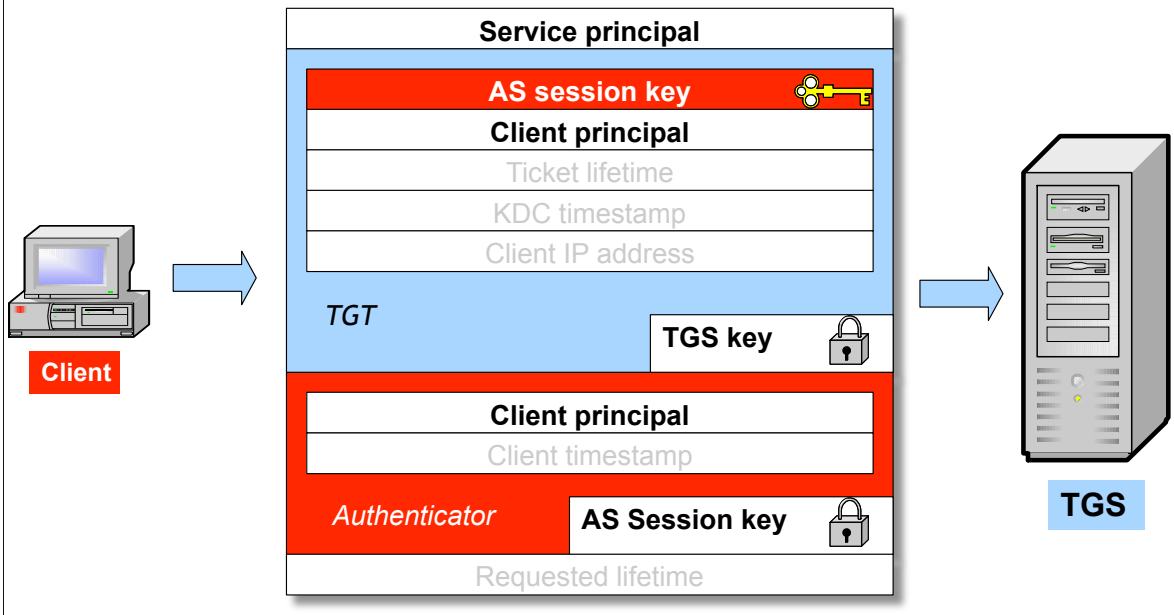
- **Kerberos Principals bestehen aus:**
  - `component[/component]...@REALM`
  - **z.B.:** `mike/admin@SECPOD.DE`
- **Die erste component gibt den Benutzernamen an.**
- **Die zweite (optionale) component die „Rolle“.**
- **Der Realm gibt die Authentifizierungs-Domäne an.**

KDC

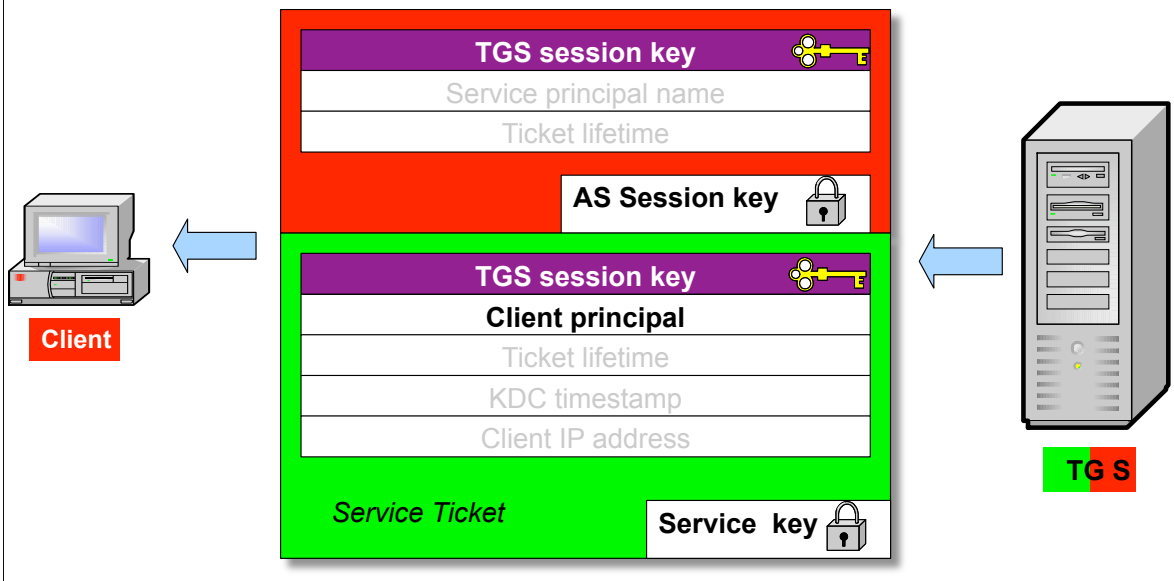
- **KDC = Key Distribution Center**
- **Besteht aus:**
  - **Principal Database**
    - **Speichert Principals und Keys**
  - **Authentication Server (AS)**
    - **Erstellt das Ticket Granting Ticket (TGT)**
  - **Ticket Granting Server (TGS)**
    - **Erstellt Service Tickets für ein TGT**

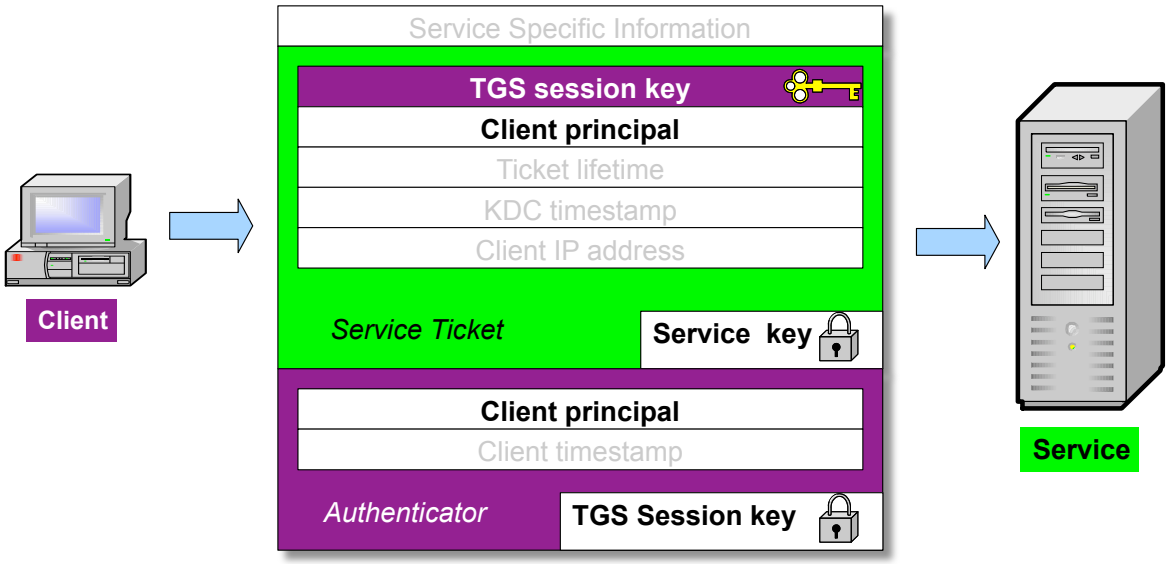


SOFTCON



SOFTCON





Vorteile von Kerberos

- **Sichere, gegenseitige Authentifizierung aller Beteiligten**
- **Keine Verbindung zwischen KDC und Services nötig**
- **Geringe Belastung des KDCs**
- **Autorisierung wird dem Service überlassen**
- **Plattform- und Systemunabhängig**

SOFTCON

Nachteile von Kerberos

- Keys müssen zu den Services verteilt werden
- Uhrzeiten müssen synchronisiert sein (ntpdate, rdate)
- nicht ohne weiteres mit Firewalls einsetzbar (NAT)
- mangelnde Unterstützung bei den Clients (derzeit)

SOFTCON

weitere Protokolle

- Generic Security Services API (GSSAPI):
  - generisches Interface zur Unterstützung von „strong Authentication“, wie z.B. Kerberos
  - wird oft von Services verwendet um Kerberos zu unterstützen
- Security Support Provider Interface (SSPI):
  - Microsoft Pendant zu GSSAPI
- Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO):
  - Übermittlung eines Kerberos-Tickets per HTTP

SOFTCON

Agenda

SOFTCON

MIT

- **Referenzimplementierung**
- **für Linux und Windows erhältlich**
- **weit verbreitet**
- **wird in den USA entwickelt**
- **Unterstützt seit 1.3 unter anderem RC4 und AES zur Verschlüsselung**
- **wird von vielen Anwendungen unterstützt**

SOFTCON

Heimdal

- neuere Implementierung
- nur für Linux erhältlich
- wird außerhalb der USA entwickelt
- bessere Master/Slave Synchronisierung
- Unterstützung von (3)DES, AES und RC4
- Kerberos API und GSSAPI unterscheiden sich jedoch von den MIT APIs

SOFTCON

Microsoft

- neueste Implementierung (seit Windows 2000)
- unterstützt nur Kerberos 5
- unterstützt nur RC4 und DES, kein 3DES
- Unix Clients mit Windows KDC ist möglich
- Windows Clients mit Unix KDC ist nicht ohne weiteres möglich.
- kein GSSAPI (dafür SSPI)

SOFTCON

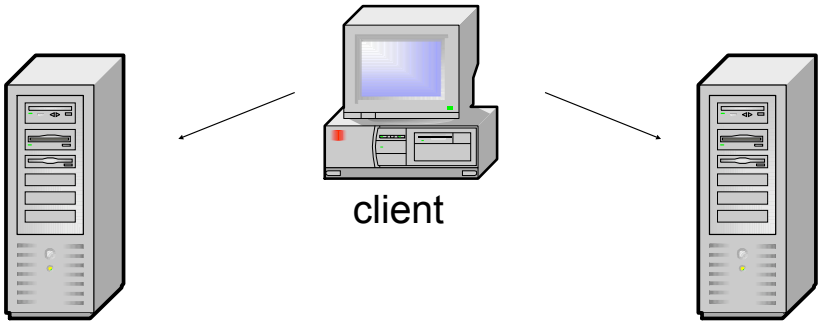
Agenda

1. Identitätsmanagement
2. Single Sign-On
3. Kerberos Grundlagen
4. Implementierungen
5. Installation & Konfiguration Linux
   - KDC einrichten
   - Client einrichten
   - Kerberized Service einrichten
6. Integrationsmöglichkeiten Linux/Windows
7. Ausblick

SOFTCON

Fallbeispiel Linux

- **Betriebssystem: Debian GNU/Linux 3.1 (sarge)**
- **Domain: secpod.de, Realm: SECPOD.DE**
- **Benutzer: root, mike**



SOFTCON

KDC einrichten (1)

✓ KDC installieren

```
kdc# apt-get install krb5-kdc krb5-admin-server
```

✓ Realm erzeugen

```
kdc# kdb5_util create -s
```

✓ Admin Benutzer anlegen und testen

```
kdc# kadmin.local
kadmin.local: addprinc mike/admin
kadmin.local: listprincs
kadmin.local: exit
kdc# /etc/init.d/krb5-kdc restart
kdc# /etc/init.d/krb5-kdc restart
kdc# kinit mike/admin
kdc# klist
```


SOFTCON

KDC einrichten (2)

✓ Admin Benutzer Rechte zuweisen

```
kdc# vi /etc/krb5kdc/kadm5.acl
mike/admin@SECPOD.DE  *
```

✓ Keytab mit Kadmin Principals erzeugen

```
kdc# kadmin.local
kadmin.local: ktadd -k /etc/krb5kdc/kadm5.keytab kadmin/admin kadmin/changepw
kadmin.local: exit
kdc# /etc/init.d/krb5-adminserver restart
```

✓ Benutzer anlegen und testen

```
kdc# kadmin
kadmin: addprinc mike
kadmin: addprinc root
kadmin: exit
kdc# kdestroy
kdc# kinit mike
kdc# klist
```

SOFTCON

KDC einrichten (3)

1. DNS Serviceeinträge vornehmen (optional)

```
_kerberos._udp.SECPOD.DE.       IN SRV 1 0 88  kdc.secpod.de.
_kerberos._tcp.SECPOD.DE.       IN SRV 1 0 88  kdc.secpod.de.
_kerberos-adm._tcp.SECPOD.DE.   IN SRV 1 0 749 kdc.secpod.de.
_kpasswd._udp.SECPOD.DE.        IN SRV 1 0 464 kdc.secpod.de.
```


SOFTCON

Client einrichten

✓ Kerberos Client-Pakete installieren

```
client# apt-get install krb5-user krb5-clients ssh-krb5
```

✓ Testen

```
client# kinit mike/admin
client# kadmin
```

SOFTCON

Kerberos Login anlegen (1)

✓ Host-Principal anlegen und Key exportieren

```
client# kadmin
kadmin: addprinc host/client.secpod.de
kadmin: ktadd host/client.secpod.de
kadmin: exit
```

✓ lokalen Benutzer anlegen

```
client# adduser --disabled-password mike
```

✓ PAM Modul installieren

```
client# apt-get install libpam-krb5
```


SOFTCON

Kerberos Login anlegen (2)

✓ PAM einrichten

```
client# vi /etc/pam.d/common-auth
auth    sufficient    pam_krb5.so forwardable
auth    required      pam_unix.so nullok_secure
client# vi /etc/pam.d/common-password
password    sufficient    pam_krb5.so use_authtok
password    sufficient    pam_unix.so ...
client# vi /etc/login.defs
CLOSE_SESSIONS yes
```

✓ testen

```
login mike
klist
```

SOFTCON

Kerberized SSH

✓ **Kerberized SSH installieren**

```
server# apt-get install ssh-krb5 krb5-user
```

✓ **Principal anlegen und Key exportieren**

```
server# kinit mike/admin
server# kadmin
kadmin: addprinc host/server.secpod.de
kadmin: ktadd host/server.secpod.de
kadmin: exit
```

✓ **Benutzer anlegen**

```
server# adduser --disabled-password mike
```

✓ **testen**

```
client# login mike
mike@client$ ssh server
mike@server$ klist
mike@server$ exit
mike@client$ klist
```


SOFTCON

weitere Services

- **Cyrus IMAP**
- **OpenLDAP**
- **Putty**
- **Reflection X**
- **Eudora**
- **Apple Mail.app**
- **Telnet**
- **...**

SOFTCON

Agenda

SOFTCON

Windows Clients mit Linux KDC

- **mit Hilfe eines Windows Domain Controllers via Cross-Realm Trust**
  - **Authentifizierung über den Linux KDC**
  - **Autorisierung über Windows Domain Controller**
- **mit Windows Standalone PCs über das Tool ksetup**
  - **Authentifizierung über den Linux KDC**
  - **Autorisierung über lokale Benutzerrechte**
- **Achtung: Einige Windows Programme haben Probleme mit einem Linux-KDC!**

SOFTCON

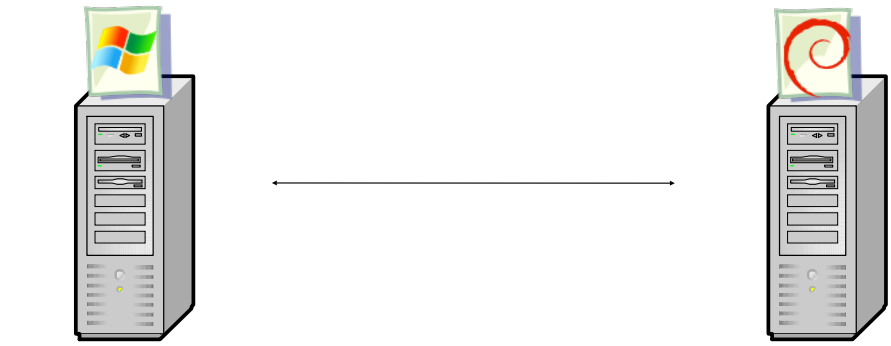
Linux Clients mit Windows KDC

- **Windows Domain Controller in der /etc/krb5.conf als kdc eintragen**
- **Kerberos Client muss RC4 Verschlüsselung unterstützen**
- **Kennwortänderung und Administration nur mit Hilfe von Samba möglich**

SOFTCON

Fallbeispiel Linux/Windows

- **Betriebssystem: MS Windows 2003 Server Standard**
- **Domain: winsecpod.de, Realm: WINSECPOD.DE**



winkdc
(MS Kerberos)

server
(http)

SOFTCON

HTTP einrichten

✓ Apache Kerberos Modul installieren (Linux)

```
server# apt-get install libapache2-mod-auth-kerb
```

✓ Service Key erzeugen (Windows)

Benutzer http_server im Active Directory anlegen

```
winkdc C:\> ktpass -out http.keytab -princ HTTP/server.winsecpod.de@WINSECPOD.DE
-pass * -mapuser http_server
```

✓ Apache Kerberos Modul konfigurieren (Linux)

```
server# vi /var/www/test/.htaccess
AuthType Kerberos
AuthName „Kerberos Test Login“
KrbAuthRealms WINSECPOD.DE
Krb5Keytab /http.keytab
KrbServiceName HTTP
require valid-user
```


SOFTCON

Agenda

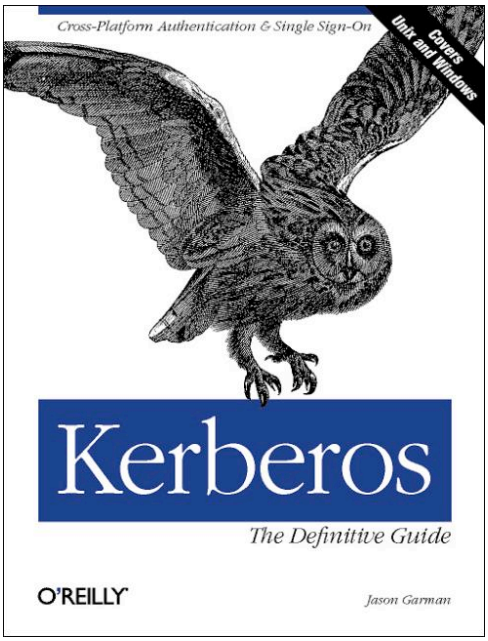
SOFTCON

Ausblick

- **Public-Key**
  - **Initial Authentication (PKINIT)**
  - **Cross-Realm (PKCROSS)**
- **Smart Cards**
- **Bessere Verschlüsselung**
  - **RC4**
  - **AES**
- **Webservices**
  - **WS-Security**

SOFTCON

Buchempfehlung



Kerberos
The Definitive Guide

Jason Garmen

ISBN: 0596004036

SOFTCON

Fragen?

- Michael.Wiesner@acm.org
- http://www.mwiesner.com
- http://www.softcon.de