

MICHAEL STRÖDER

Klauprechtstr. 11, D-76137 Karlsruhe
Telefon +49 721 8304316
michael@stroeder.com
<http://www.stroeder.com/>

ART DER TÄTIGKEIT

Freiberuflich als Berater für Systemintegration und IT-Sicherheit, insbesondere Verzeichnisdienste, Identity Management, Single Sign-On, Public-Key-Infrastrukturen (PKI) und verwandte Anwendungen.

KOMPETENZFELDER

- Planung und Implementierung von Architekturen zur sicheren Nutzung von IT-Diensten (PKI, SSL, S/MIME, VPNs, LDAP, Identity Management, Single Sign-On, Firewalls)
- Entwurf und Implementierung sicherer Software (z.B. Web-Applikationen), objektorientierte Programmierung (z.B. Python)
- Systemintegration und Benutzerverwaltung in komplexen und heterogenen Umgebungen (Datenmigration und -synchronisation)
- Schulungen und Workshops

PROJEKTE

Bank in Frankfurt (06/2011..08/2011)

- Konzeption und Installation OpenLDAP-Server als Basis für LDAP-basierte Anmeldung via CAS
- Implementierung eines Delta-Synchronisationsprozesses von einer Oracle DB zu OpenLDAP in Python

Bundesbehörde in Deutschland (12/2010 bis 07/2011)

- Konzeption und Installation für eine Migration eines bestehenden Systems von Novell eDirectory und DirXML hin zu einer Open-Source-Lösung
- Implementierung eines Delta-Synchronisationsprozesses von eDirectory zu OpenLDAP in Python

Internationaler Konzern (10/2009 bis 06/2011)

- Sicherheitsberatung hinsichtlich Design, Entwicklung und Betrieb eines proprietären Messaging-System mit Nachrichtenverschlüsselung und digitaler Signatur
- Coaching von Entwicklern, Software-Reviews
- Konfiguration nCipher HSMs
- Konzeption/Konfiguration eines OpenLDAP-basierten Verzeichnisdienstes für die projektinterne Mitarbeiter- und Benutzerverwaltung

Bundesbehörde in Deutschland (06/2009 bis 10/2009)

- Konzeption für eine Migration eines bestehenden Systems von Novell eDirectory und DirXML hin zu einer Open-Source-Lösung
- Pilotimplementierung der Synchronisation von MS AD zu OpenLDAP in Python

Mittelständische Bank in Stuttgart (10/2007 bis 03/2009)

- Konzeption für ein Single Sign-On für Web-Applikationen
- Pilotinstallation von Central Authentication Service (CAS) mit wahlweiser Authentifizierung gegen MS AD mit SPNEGO/Kerberos oder LDAP
- Implementierung einer Benutzerdatensynchronisation zwischen einer PostgreSQL-Datenbank, MS Active Directory und Lotus Domino

Landesbehörde in Baden-Württemberg (12/2005 bis heute)

- Konzeption, Pilotinstallation und Dokumentation eines OpenLDAP-basierten Verzeichnisdienstes zur zentralen Speicherung von abstrakten Rollen und anwendungsspezifischen Autorisierungsmerkmalen
- Beschreibung/Entwurf von Prozessen, Schnittstellen und Use-Cases für eine delegierte Benutzerverwaltung

Internationaler Pharmakonzern (02/2006 bis 11/2007)

- Konzeption einer stark mit Lotus Notes integrierten PKI zur Nutzung verschlüsselter E-Mail gemäß S/MIME-Standard
- Vorstudie für eine konzernweite PKI als Basis für Windows Smartcard Logon und Dateiverschlüsselung. Arbeitsergebnis umfasste Kostenschätzung, Meilensteine für Projektplanung etc.
- Konzeption und Installation einer konzernweiten PKI (s.o.), Integration mit Konzernverzeichnisdienst
- Erstellung eines Certification Practice Statements (CPS) gemäß RFC 3647 für öffentlichen Teil der PKI

Luftfrachtunternehmen (02/2007 bis 04/2007)

- Vorstudie inkl. Konzeption und Kostenschätzung einer Lösung für Single Sign-On an web-basierten B2B-Applikationen
- Dokumentation von bestehenden Anwendungen

Internationaler Telekommunikationskonzern (09/2005 bis 04/2006)

- Neukonzeption und Pilotimplementierung der Datensynchronisation für den konzernweiten Verzeichnisdienst
- Evaluierung verschiedener LDAP-Server-Produkte (Interoperabilitäts- und Performance-Tests)

Internationaler Logistikkonzern (09/2003 bis 06/2005)

- Konzeption zur Nutzung archivfester digitaler Signatur mit einer X.509-basierten PKI in Filialkassensystemen und den beteiligten Backend-Systemen
- Konzeption für persönliche, offline-fähige Anmeldung und Single Sign-On an Filialkassensystemen basierend auf Smartcards
- Konzeption zur Verwaltung der Benutzer der Filialkassensysteme mit automatischem Abgleich der Benutzerstammdaten mit Personaldatenbank
- Abstimmung und Koordination mit Wirtschaftsprüfern hinsichtlich GOB/GOBS-relevanter Sicherheitsthemen bei Filialkassensystemen und den beteiligten Backend-Systemen

Internationaler Telekommunikationskonzern (11/2002 bis 09/2003)

- Konzeptionelle Arbeiten für Entrust-basierte PKI-Architektur (Registrierungsprozeduren, Selbst-Administrierung, etc.)
- Dokumentation für Integration der Entrust-basierten PKI-Architektur in Web- und Desktop-Anwendungen
- Konzeption für die Integration einer X.509-basierten Single Sign-On-Lösung (Entrust TruePass) und eines LDAP-Verzeichnis (Siemens Dir/X) in eine web-basierte Anwendung
- Coaching der Java-Entwickler
- Workshops für Administratoren

Internationaler Pharmakonzern (09/2001 bis 05/2003)

- Entwurf, Implementierung und Pilottests eines konzernweiten, LDAP-basierten Verzeichnisdienstes (iPlanet Directory Server) zur Benutzerauthentifizierung als Single-Password-Lösung. Das System wurde konzeptioniert als zentrale Benutzerdatenbank für interne und externe Nutzer von Web-basierten Anwendungen und anderen Systemen.
- Konzeption und Implementierung der Synchronisation der LDAP-Benutzerdaten mit einer Datenbank auf Host-Systemen (DB2 auf S/390, Einsatz von DB2 Connect unter Linux)

- Entwurf einer Public-Key-Infrastruktur (PKI) zur Ausgabe von X.509-Zertifikaten für Computersysteme (z.B. SSL-Server, IPSec-Router). Diese Arbeit umfaßte die Definition des Zertifikatprofils, Schreiben einer PKIX-konformen Zertifizierungsrichtlinie (CP und CPS gemäß RFC 2527) und Unterstützung beim Entwurf der Java-basierten Software.
- Evaluierung von PKI-Produkten (Entrust und RSA Keon) in einer Pilotumgebung für VPN, Single Sign-on, S/MIME-basierte E-mail.
- LDAP-Integration/-Konfiguration für das Profil-Verzeichnis des Tibco Portalbuilder 4.5, Implementierung eines Prozesses für die Synchronisation der Benutzerdaten gegen Domino/LDAP
- Tiefgehende Analyse der Sicherheitsmechanismen von Netegrity Siteminder und Integration mit LDAP-Verzeichnisdienst der Benutzerverwaltung gemäß fachlicher Vorgaben

Verschiedene Aktivitäten (von 04/2001 bis heute)

- Einführungsschulung, Workshops und Beratung bzgl. einheitlicher Benutzeradministration und zentralem LDAP-Verzeichnis für interne und externe Benutzer bei einem internationalen Textilunternehmen
- Entwurf und Realisierung eines zentralen, LDAP-basierten Adressbuchs für die Stadtverwaltung Karlsruhe, Anbindung des Web-Content-Management-Systems (ZOPE) an Domino/LDAP
- Diverse Schulungen und Workshops zum Thema LDAP-basierte Verzeichnisdienste

[emagine GmbH](#), Eschborn (10/2000 bis 04/2001)

- Entwurf von PKI-bezogener Software zur Bereitstellung von Mehrwertdiensten im Bankenbereich (basierend auf Identrus)
- Erstellung eines Konzepts für einen generalisierten Zertifizierungsablauf zur Integration mehrerer Zertifizierungsdienstleister in den *Registration Authority* Server

[Propack Data GmbH](#), Karlsruhe (05/1996 bis 09/2000)

- Einführung, Planung, Installation und Administration verschiedenster Internet- und Intranet-Dienste basierend auf offenen Standards.
- Entwurf und Realisierung Firewall zur Gewährleistung einer sicheren Internet-Anbindung basierend auf Linux mit diversen Proxy-Diensten (Squid, postfix, dnscache).
- Entwurf, Implementierung und Einführung einer Public-Key-Infrastruktur (PKI) zur Ausgabe von X.509-Zertifikaten an alle Mitarbeiter. Die X.509-Zertifikate wurden hauptsächlich für S/MIME-basierte E-Mail (Verschlüsselung und digitale Signatur) und zur Benutzerauthentifizierung mobiler Benutzer eingesetzt (VPN, IMAP via SSL, SMTP mit StartTLS und X.509-Client-Zertifikaten für die Relaying-Regeln).
- Installation IPSec-basierter VPN-Verbindungen zur kostengünstigen Anbindung international verteilter Geschäftsstellen basierend auf Linux und FreeS/WAN.
- Einführung und Einsatz eines LDAP-Verzeichnisdienstes (OpenLDAP) als zentrales Adreßbuch und PKI-Repository.
- Integration von Domino/LDAP und die PKI.
- Implementierung verschiedenster LDAP-Clients zur Integration bestehender Anwendungen mit dem LDAP-Verzeichnis (z.B. Kennwortprüfung am Web-Proxy Squid).

Open Source

- Entwurf und Implementierung eines komfortablen, web-basierten LDAPv3-Clients mit Unterstützung für LDAPv3-Schema, StartTLS/LDAPS, Referrals, Root Naming Context, DNS SRV Records, Gruppenadministration, Manage DSA IT, etc. (siehe <http://www.web2ldap.de>).
- Intensive Weiterentwicklung eines Modulpaketes zur objektorientierten Programmierung von LDAP-Applikationen mithilfe der Programmiersprache Python (siehe <http://python-ldap.sf.net>). Dieses Modulpaket wird ggf. in eigenen Projekten bei Kunden eingesetzt.
- Implementierung einer web-basierten PKI-Software basierend auf OpenSSL (siehe <http://www.pyca.de>).

AUSBILDUNG

Abschluß als Dipl.-Inform. an der [Universität Karlsruhe](#) (Januar 1999)

- Diplomarbeit:
"Einführung kryptographischer Techniken zur gesicherten Nutzung des Internet bei der Propack Data GmbH"
- Vertiefende Ausrichtung: Telematik (Computer-Netzwerke, Verteilte Systeme), Interaktive Systeme, Leistungsanalyse von Rechensystemen, Automatisierungstechnik

FACHKENNTNISSE

Verschlüsselungs- und PKI-Standards:

- SSL, S/MIME, X.509, PKIX, IPSec

Authentifizierungsmechanismen:

- Passwortmechanismen/-synchronisation, Kerberos, SPNEGO, SASL, X.509-Client-Zertifikate, PAM unter Linux

Sicherheitsprodukte:

- Entrust Authority, Cybertrust UNICERT (früher Baltimore UNICERT), Windows Certificate Services, Lotus Domino CA, RSA Keon CA, Netegrity Siteminder, OpenSSL, Central Authentication Service (CAS der JA-SIG), Thales nCipher nShield/netHSM

Netzwerkdienste:

- Verzeichnisdienste:
OpenLDAP, iPlanet/Netscape/SunONE Directory Server, Novell eDirectory, MS Active Directory, MS ADAM, IBM/Tivoli Directory Server, CA eTrust Directory, Critical Path, Siemens DirX, Lotus Domino/LDAP, OpenDS/OpenDJ, Fedora Directory Server
- E-Mail-Dienste:
postfix, sendmail, qmail, fetchmail, dovecot
- WWW:
Apache, Tomcat, Squid, FastCGI, SCGI
- Datei-Server : Samba (SMB/CIFS), NFS
- DNS: bind9, PowerDNS

Betriebssysteme:

- Linux (openSUSE, SLES, Debian etc.), Windows NT/2000/XP, Solaris, OS/2, MS-DOS

Softwareentwicklung:

- Python, Pascal, Modula-2, Shell-Scripting, HTML/CSS, Versionskontrolle mit CVS und Subversion

Computer Hardware / virtuelle Maschinen:

- PC-Hardware und Grundlagen von Embedded-Systemen
- VMWare workstation

REFERENZEN

Details zu den oben genannten Kunden auf Anfrage.