

MICHAEL STRÖDER

Klauprechtstr. 11, D-76137 Karlsruhe, Germany

Phone +49 721 8304316

michael@stroeder.com

<http://www.stroeder.com/>

OBJECTIVE

A contractor position as a consultant for planning and implementing identity management, security infrastructures (PKI, directory services) and related applications.

CAPABILITIES

- Planning / designing architectures and implementing mechanisms for secure usage of IT services (PKI, SSL, S/MIME, VPNs, LDAP, Identity Management, Single Sign-On, Firewalls)
- Designing and implementing secure software (e.g. web applications), object-oriented software design and programming (e.g. Python)
- System integration and user management in large and complex environments
- Training and workshops

EXPERIENCE

International Group (10/2009 ongoing)

- Security consulting and software reviews for proprietary messaging system with encryption and digital signature

National Government Agency in Germany (06/2009..10/2009)

- Design and pilot installation for a migration from Novell eDirectory and DirXML to a solution based on OpenLDAP
- Implemented pilot for user data synchronisation from MS AD to OpenLDAP in Python

Financial Institute in Stuttgart (10/2007 bis 03/2009)

- Designed Single Sign-On for web applications
- Implemented pilot installation of Central Authentication Service (CAS) with authentication based on MS Active Directory via SPNEGO/Kerberos or LDAP
- Implemented user account synchronization between PostgreSQL database, MS Active Directory and Lotus Domino

Federal Government Agency in Baden-Württemberg (12/2005..today)

- Design, pilot installation and documentation of OpenLDAP-based directory service as central repository for abstract roles and application-specific authorization data
- Described processes, interfaces and use-cases for delegated user management

International Pharmaceutical and Chemical Group (02/2006..11/2007)

- Designed and installed a PKI tightly integrated with Lotus Notes for securing e-mails with S/MIME
- Pre-study for group-wide PKI for Windows Smartcard Logon and file encryption including cost estimation, milestone planning etc.

- Designed and installed concern-wide PKI
- Wrote a certification practice statement (CPS) compliant with RFC 3647 for public part of the PKI

Air Cargo company (02/2007..04/2007)

- Pre-study including conception and cost estimation for a single sign-on to web-based B2B-applications
- documentation of existent applications

International Telecommunications Group (09/2005..04/2006)

- Re-design and pilot implementation of data synchronization processes for group-wide directory service.
- Evaluation and performance testing of LDAP server products (interoperability and performance tests)

International Logistics Group (09/2003..06/2005)

- Designed X.509-based PKI infrastructure enabling retail systems to use digital signature for secure archival of posting data
- Designed architecture for secure authentication and single sign-on at sales point systems using smartcards
- Designed concept for managing users of retail systems even when systems are offline most of the time including syncing with HR systems
- Resolved security-relevant topics related to accountancy with auditors

International Telecommunications Group (11/2002..09/2003)

- Designed registration, self-administration and recovery procedures for Entrust-based PKI architecture
- Documented experiences of integrating web and desktop applications with Entrust security architectures in a best-practice guide („cookbook“) for other projects following
- Integrated X.509-based single sign-on solution (Entrust TruePass) and the LDAP-based user management into a web application
- Coaching of Java developers
- Workshops for administrators

International Pharmaceutical and Chemical Group (09/2001..05/2003)

- Designed specific public-key infrastructure for issuing certificates used e.g. for SSL servers and machine entities. This work included defining the certificate profile, writing the PKIX compliant certificate policy (according to RFC 2527) and certification practice statement and designing the software.
- Evaluated PKI products (Entrust und RSA Keon) in pilot project for VPN, single sign-on, S/MIME e-mail.
- Designed, implemented and tested a corporate-wide LDAP directory (iPlanet Directory Server) for single-password user authentication. This system was designed as a central user store for internal and external users of web-based e-commerce applications and various other systems.
- Designed and implemented process for synchronizing user data stored on a mainframe with LDAP directory (DB2 on S/390, based DB2 Connect on Linux)
- Setup LDAP-backend for profile store of Tibco Portalbuilder 4.5, implemented synchronization process for user data stored in Domino/LDAP

- Conducted in-depth analysis of the security mechanisms of Netegrity Siteminder and integrated it with LDAP directory service of user management

Various activities since 04/2001

- Consulting for unified user management process and centralized user LDAP directory for internal and external users at an international textile group.
- Designed and implemented centralized, LDAP-based address book for the municipal administration of Karlsruhe. Integrated web content management system (ZOPE) with user management of Lotus Domino via LDAP.
- Held various LDAP workshops (basics, application-programming coaching).

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

- Designed PKI-related software providing value added service to financial B2B applications (e.g. Identrus compliant applications).
- Designed concept for more general certificate workflow handling with arbitrary certification authorities for a *Registration Authority* server.

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

- Introduced, planned, installed and maintained various Internet services for internal and external communication needs which highly improved the productivity by providing an integrated concept based on open protocol standards in a heterogeneous computing environment.
- Designed and set up a firewall which fulfilled the company's need for a highly secure internet connectivity.
- Established a public key infrastructure with an own certificate authority for securing the usage of Internet/Intranet services with encryption techniques (X.509, S/MIME, SSL, VPN).
- Installed a IPSec-based virtual private network (VPN) for reducing the communication costs by transferring the corporate IP-traffic securely via the Internet.
- Introduced and deployed a directory service (LDAP) providing relevant corporate information (e.g. phone book, mail addresses, certificate data) and serving as a base for a single sign-on user authentication system.
- Implemented several LDAP clients for using the LDAP directory in various services.

Open Source Projects

- Designed and implemented a web-based LDAPv3 client for comfortable and secure access to LDAP servers with full support for sub schema, DNS SRV records, efficient group administration, etc. (see <http://www.web2ldap.de>).
- Developing of module package for LDAP programming with Python (see <http://python-ldap.sf.net>). This module is sometimes also used in my customers' projects.
- Implemented a PKI software accessible from web browsers (see <http://www.pyca.de>).

Various projects as software engineer for industrial automation and quality control (1992-1994)

EDUCATION

Dipl.-Inform. (comparable to M.S. in Computer Science) at the [University of Karlsruhe](#), Germany (Degree January 1999)

- [Diploma thesis](#):
"Introduction and Deployment of cryptographic Technologies for secure Usage of Internet

Services at Propack Data GmbH"

- Relevant Courses:
Telematics (Computer Networks, Distributed Systems), Interactive Systems, Performance Analysis, Automation Systems

TECHNICAL SKILLS

Data encryption and PKI standards

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

Authentication techniques

- Passwords including syncing passwords, Kerberos, SPNEGO, SASL, X.509 client certificates, PAM for Linux/Solaris

Security products

- Entrust Authority, Cybertrust UNICERT (formerly Baltimore UNICERT), Windows Certificate Services, Lotus Domino CA, RSA Keon CA, Netegrity SiteMinder, OpenSSL, Central Authentication Service (CAS)

Network services

- Directory services:
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, Fedora Directory Server
- E-mail services:
postfix, sendmail, qmail, fetchmail, dovecot
- WWW:
Apache, Tomcat, Squid, FastCGI, SCGI
- File server: Samba (SMB/CIFS), NFS
- DNS: bind9, PowerDNS

Operating Systems:

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

Software development skills and tools

- Python, Pascal, Modula-2, Shell-scripting, HTML/CSS, CVS, Subversion

Computer hardware / virtual machines:

- Knowledge of PC hardware and basic knowledge of embedded systems
- VMWare workstation

REFERENCES

Available upon request.