

# **Zertifikatsverzeichnis zur Unterstützung von Digitaler Signatur und Verschlüsselung**



---

## **Was ist PKI?**

Um Daten und Email-Kommunikation im Internet zu schützen und zu authentifizieren, setzt sich die sogenannte asymmetrische Verschlüsselungstechnologie immer mehr durch. Hierdurch ist es möglich, ein Dokument so zu verschlüsseln, dass es nur vom Adressaten wieder entschlüsselt werden kann, ohne dass vor der Übertragung ein Austausch von geheimen Schlüsseln stattfinden muss. Hierzu wird ein öffentlicher Schlüssel benutzt, der in einem mathematischen Zusammenhang mit einem privaten, geheimen Schlüssel (der zum Entschlüsseln verwendet wird) steht.

Ein Zertifikat ist ein solcher öffentlicher Schlüssel dessen Zugehörigkeit zu einer bestimmten Person von einer vertrauenswürdigen Stelle (Certification Authority, CA genannt) zertifiziert worden ist. Die gleiche Technologie ermöglicht außer Verschlüsselung auch das digitale Signieren von Dokumenten, sowie die Überprüfung ihrer Authentizität. Entsprechende Technologien sind Public Key Infrastructure (PKI), X.509, S/MIME, SSL und PGP.

## **Unsere Lösung**

Wir bieten DFN-CA's an, ihre Zertifikate (X.509 oder PGP) in einem von uns betriebenen Verzeichnisdienst zentral zu veröffentlichen. Wir können Sie aber auch dabei unterstützen, einen eigenen Verzeichnisdienst so aufzubauen, dass die Daten in einen deutschlandweiten Index integriert werden können.

Neben dem gängigen Standard zur Ablage von Zertifikaten in Verzeichnisdiensten [1], unterstützen wir für einen solchen Index zusätzlich eine neues, im Rahmen eines DFN-Forschungsprojektes von uns konzipiertes Datenmodell, das wir in die IETF (Internet Engineering Task Force) zur Standardisierung eingebracht haben [2]. Mit diesem Ansatz wird zusätzlich das Problem multipler Zertifikate eines Benutzers gelöst.

- [1] "Internet X.509 Public Key Infrastructure - LDAP Schema and Syntaxes for PKIs", Chadwick, D. and S. Legg, Internet Draft (a work in progress), June 2002, <draft-ietf-pkix-ldap-pki-schema-00.txt>.
- [2] "An LDAPv3 Schema for X.509 Certificates", Gietz, P. and N. Klasen, Internet Draft (a work in progress), November 2002, <draft-klasen-ldap-x509certificate-schema-01.txt>

Für weitere Informationen zum zentralen Authentifizierungsdienst und unseren anderen Dienstleistungen, wenden Sie sich bitte an:

DAASI International GmbH  
Wilhelmstrasse 106  
D-72074 Tübingen  
www.daasi.de

Tel. 07071 2970336  
Fax 07071 295114  
info@daasi.de