

Eine Public Key-Infrastruktur (PKI) stellt ein skalierbares System dar, das digitale Zertifikate für sichere und interoperable Kommunikation zwischen verschiedenen Organisationen unterstützt.

Eine PKI erreicht dies durch die Bereitstellung öffentlicher Schlüssel zur Unterstützung von Sicherheitsaspekten wie z.B. Vertraulichkeit, Integrität, Authentifizierung und Nachweisbarkeit.

Aufgrund vielfältiger Anforderungen an eine PKI, werden Unternehmen nicht umhinkommen ein maßgeschneidertes System zu implementieren. Hierbei gilt es ebenso die rechtlichen, wie die wirtschaftlichen und die technologischen Aspekte zu berücksichtigen, die im Einzelfall genau untersucht werden müssen.

Ein detailliert schlüssiges Konzept beinhaltet unter anderem folgende Aspekte:

- Evaluierung der Voraussetzungen
- Entwurf der Zertifizierungsstellenhierarchie
- Organisation der ausstellenden Zertifizierungsstellen
- Auswahl einer Architektur
- Sammlung der erforderlichen Informationen
- Identifikation PKI-fähiger Anwendungen
- Bestimmung der Sicherheitsanforderungen
- Bestimmung der technischen Anforderungen
- Ermittlung der betrieblichen Anforderungen
- Ermittlung externer Anforderungen
- Ermittlung interner Anforderungen

Sollten Sie den Einsatz von Zertifikaten zur Bereitstellung von *Smart Cards*, *Code-Signing*, *Sicherer E-Mail (S/MIME)*, *SSL-Verschlüsselung*, *Network Device Enrollment Service (NDES)*, *VPN*, *EAP-TLS* etc. planen, stelle ich Ihnen gerne mein professionelles Know-How und meine langjährigen Erfahrungen zum Thema PKI zur Verfügung.