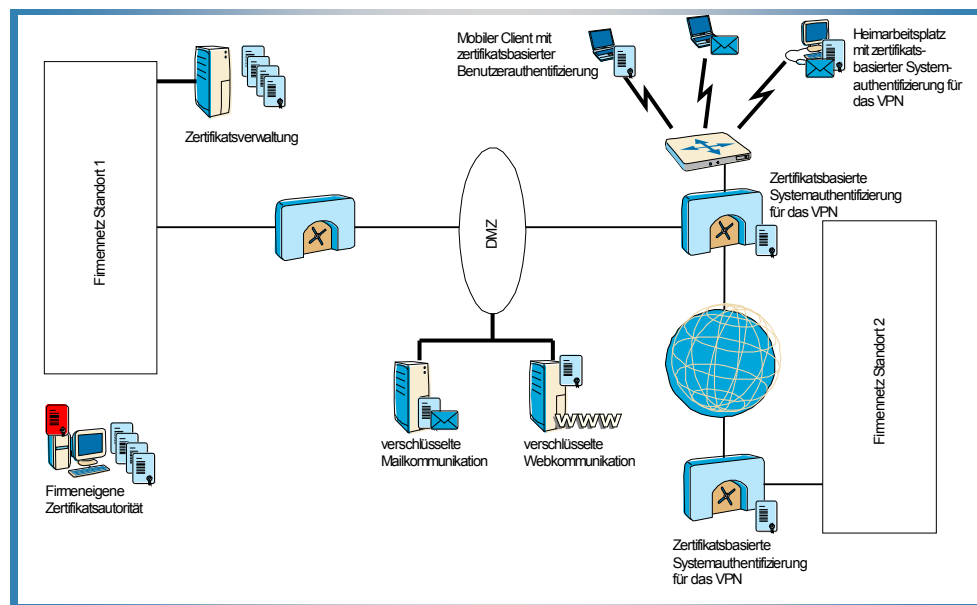


Public Key Infrastruktur

Verschlüsselung, Authentifizierung, Signatur

Eine Public Key Infrastruktur bietet eine unternehmensweite einheitliche Lösung für die Verschlüsselung von Daten und Kommunikation, die Authentifizierung von Benutzern und Systemen, sowie die Signatur von Dateien und Geschäftsprozessen. Die Integrität, der Ursprung und die Vertraulichkeit von E-Mails werden über den Einsatz von Zertifikaten sichergestellt.

Für eine verschlüsselte Webkommunikation authentifizieren sich Server und Client über das SSL/TLS Protokoll und gewährleisten so eine sichere Verbindung. Die Speicherung von Zertifikaten und den dazugehörigen privaten Schlüsseln auf Smartcards ermöglichen Zweifaktor-Methoden und die interaktionsfreie Verwendung von Einmalpasswörtern für die Benutzerauthentifizierung.



Eine Public-Key-Infrastruktur erreicht eine zuverlässige Zertifikatsverwaltung

Eine Public-Key-Infrastruktur gewährleistet eine sichere und effiziente Verwaltung der Zertifikate. So können die Teilnehmer jederzeit das Zertifikat des Kommunikationspartners auf Echtheit und Gültigkeit verifizieren, ohne selbst in den Verwaltungsprozess involviert zu sein.

Die Public-Key-Infrastruktur umfasst sowohl den topologischen Aufbau der beteiligten Komponenten, als auch die Definition der politischen Struktur für diese Komponenten. Beispielsweise legt die Zertifikatsrichtlinie fest, welche Informationen in das Zertifikat aufgenommen werden.

Sorgfältig geplante Gesamtkonzepte tragen zur Umsetzung der Sicherheitspolitik bei

Jede PKI muss sinnvoll in bestehende Sicherheits- und Betriebsabläufe integriert werden, damit sie ihren vollen Nutzen entfaltet. Die Bereitstellung der Funktionalitäten entsprechend Ihren Anforderungen setzt einen sorgfältigen Entwurf des Gesamtsystems voraus.

So erweist sich für Unternehmen mit mehreren Niederlassungen der Aufbau einer hie-

rarchischen Public-Key-Infrastruktur als sinnvoll. Dazu werden mehrere von einer Root-Beglaubigungsinstanz zertifizierte Beglaubigungsinstanzen in den Niederlassungen eingerichtet. Der unternehmensweit zugängliche Verzeichnisdienst für die Zertifikatsverwaltung basiert zumeist auf LDAP, unter Windows 2000 kann die Zertifikatsverwaltung direkt ins Active Directory integriert werden.

Mit ITPro sind sie in allen Fragen der Sicherheit bestens beraten

Der Aufbau einer funktionierenden PKI ist eine komplexe Aufgabe, die viel Erfahrung erfordert. Wir beraten Sie bei allen wichtigen Entscheidungen und begleiten Sie herstellerunabhängig von der Planung bis zur Umsetzung.

ITPro Informationstechnologie Beratung GmbH
Kaiserdamm 31
14057 Berlin

Tel.: +49 30 428 45 17-0
Fax.: +49 30-428 45 17-22

Mail: info@itpro.de

Ihr Ansprechpartner:
Public Key Infrastructure
Burkhard Klaus

Tel.: +49 30 428 45 17-3
Fax.: +49 30 428 45 17-29

Mail: bklaus@itpro.de