

PKI und ePA: Konkurrenz oder sinnvolle Ergänzung? **Whitepaper zum Thema „Neue Techniken für elektronische Identitäten“**

Eine elektronische Identität soll Mensch oder Maschine, Organisationseinheit oder Kommunikationskomponente sicher und zuverlässig in der digitalen Welt abbilden. Um sichere elektronische Geschäftsprozesse zu gestalten, muss eine Vielfalt organisatorischer Rollen (z.B. Mitarbeiter, Kunde, Lieferant) oder aber technischer Komponenten (z.B. LKW Onboard Unit, elektronischer Fahrausweis oder IP Router) abgebildet werden.

Die PKI (Public Key Infrastructure) Technologie bietet die Möglichkeit, alle denkbaren Entitäten exakt nach Bedarf und Anwendungsfeld zu modellieren und in digitalen Zertifikaten abzubilden. Die Bandbreite der Zertifikatsinhalte reicht dabei vom personenbezogenen elektronischen Mitarbeiterausweis bis hin zur vollständig anonymisierten Identifikationsnummer. Je nach Gefährdungslage und Sicherheitsanforderung kann das Zertifikat auf einer SmartCard, auf einem Hardware Token oder auch als Softwaretoken ausgegeben werden. Dasselbe Zertifikat kann parallel in verschiedenen Anwendungen genutzt werden und bietet den Mehrwert, neben der Authentifizierung der Kommunikationspartner auch die Vertraulichkeit und Authentizität ausgetauschter Informationen durch Verschlüsselung und Signatur sicherstellen zu können. Moderne PKI Plattformen sind flexibel und schnell einsetzbar und lassen sich einfach in beliebige Arten von Anwendungen integrieren.

Ab November 2010 wird in Deutschland ein weiteres vielversprechendes Medium zum Identitätsnachweis in Gestalt des elektronischen Personalausweises (ePA) vorhanden sein. Dieser Ausweis im Scheckkartenformat enthält einen kontaktlosen Chip, der vom Gesetzgeber definierte Zusatzfunktionalitäten erbringt. Sind die notwendige Clientsoftware sowie ein Kartenleser beim Bürger vorhanden, können persönliche Daten wie Name oder Adresse im Rahmen von Online Anwendungen vom Ausweis gelesen werden. Ebenso ist eine Altersverifikation sowie eine Nutzung als sicherer Login/Passwort Ersatz möglich. All diese Funktionalitäten benötigen die explizite Zustimmung des Bürgers durch Eingabe einer PIN. Diensteanbieter, die diese neuen Möglichkeiten in ihren Onlineprozessen nutzen möchten, benötigen einen eID-Server, der Anwendungen entlastet, indem er die erforderlichen komplexen Kommunikationsabläufe und Anbindungen sicherheitstechnischer Funktionen übernimmt.

Als Fazit bleibt festzuhalten, dass neben dem elektronischen Personalausweis (ePA) mit nur nationaler Anwendbarkeit und fest vorgegebenen Nutzungsszenarien die bewährte PKI Technologie mit ihren deutlich flexibleren Möglichkeiten auch weiterhin eine wesentliche Rolle bei der elektronischer Identitätsbildung behalten wird.