Kurzbeschreibung coolPACS

Die zunehmende Vernetzung von IT-Systemen im Firmenumfeld und insbesondere die Verlagerung von Diensten in die Cloud erfordern neue Wege bei der Identifizierung und Authentifizierung berechtigter Mitarbeiter. Weil Benutzerkennung und Passwort keinen adäquaten Schutz bieten, setzen viele Unternehmen hierfür PKI Systeme und Hardware Token für die sichere Speicherung von Zugriffsschlüsseln und Zertifikaten ein. Als Hardware Token kommen heute überwiegend Chipkarten und USB-Token zum Einsatz, in manchen Fällen auch Kombinationen aus RFID Mitarbeiterausweis und kontaktbehaftetem Chip.

Das coolPACS Konzept führt die beiden Welten Logische Zugangskontrolle (Login, VPN-Zugang, eSignatur und Verschlüsselung) mit der Physischen Zugangskontrolle (Gebäude, Zonen, Zeiterfassung, Kantinenabrechnung) in einem sicheren Chip zusammen. Der sichere Chip kann dabei wahlweise ein Smart Card Controller im Mitarbeiterausweis oder ein Secure Element im Mobiltelefon sein. Dies wird möglich durch die Realisierung der coolPACS Anwendung als JavaCard Applet, das nach dem Prinzip Write-Once-Run-Everywhere sowohl auf einer entsprechenden Smart Card, einem USB-Stick, einer uSD Karte, einer USIM oder einem Embedded Secure Element lauffähig ist. Unabhängig von der Ausprägung der Hardware ist eine zentrale Funktion, nämlich die entfernte Verwaltung von Schlüsseln und Zertifikaten gleich.

Die Kommunikation mit der coolPACS Anwendung erfolgt dabei über die kontaktlose RFID Schnittstelle des Mitarbeiterausweises oder über die NFC Schnittstelle des Mobilgerätes. Mobile Anwendungen können den Schlüsselspeicher wahlweise per Secure Element Schnittstelle oder – wenn als Teil des Mitarbeiterausweises realisiert – über die NFC Schnittstelle im Reader-Mode ansprechen.

Das coolPACS Design trägt auch der Anforderung Rechnung, dass sensitive Daten an der kontaktlosen Schnittstelle durch Verschlüsselung gegen Abhören gesichert werden müssen. Hierzu wird zwischen Lesegerät und coolPACS Anwendung ein Secure Messaging Kanal nach dem Funktionsprinzip des Neuen Personalausweises aufgebaut. Die hierbei verwendeten asymmetrischen kryptographischen Verfahren erfordern keine weiteren Schlüssel im Lesegerät, ihre Funktionsweise ist mit der im Internet gebräuchlichen SSL/TLS Verschlüsselung vergleichbar.

Die coolPACS Anwendung und die benötigte Middleware ist derzeit für JavaCard Smart Cards und USB-Sticks verfügbar. Eine Portierung für ein Secure Element ist derzeit in Planung.

Als Systemarchitekt berät CardContact Kunden bei der Konzeption, Umsetzung und Einführung von großen SmartCard und PKI Systemen. In dieser Rolle war CardContact maßgeblich an der Umsetzung des Neuen Personalausweises, der e-card in Österreich oder der e-Health Karte in Slowenien beteiligt. Mit dem OpenSCDP Projekt (www.openscdp.org) stellt CardContact eine leistungsfähige Plattform für die Entwicklung und den Test von Systemen in den Anwendungsfeldern SmartCards, RFID, NFC und PKI bereit. Das SmartCard-HSM als sicherer Schlüsselspeicher für die M2M Kommunikation ist das Kernprodukt für die Realisierung vertrauenswürdiger Kommunikationssysteme. Es findet seinen Einsatz überall dort, wo abgesetzte Systeme Schlüssel sicher erzeugen und speichern müssen und die Schlüsselverwaltung durch zentrale Systeme über offene Kommunikationswege erfolgen muss.

Für weitere Informationen wenden Sie sich bitte an

Andreas Schwier
andreas.schwier@cardcontact.de
Telefon: +49 571 56149
CardContact Software & System Consulting, Schülerweg 38, 32429 Minden