rung bietet zudem den Vorteil, soweit erforderlich schnell und flexibel auf Änderungen reagieren zu können – dies ist gerade im Onlinebereich von entscheidender Wichtigkeit. Ein einerseits nachhaltiger und rechtssicherer, andererseits aber auch innovationsfreundlicher Handlungsrahmen liegt darüber hinaus auch im Interesse der Nutzer.

Die beteiligten Unternehmen und die FSM werden die Verhandlungen unter Beteiligung des Bundesministerium des Innern und der anderen betroffenen Ressorts der Bundesregierung zügig fortsetzen, um zeitnah einen erfolgreichen Abschluss zu erzielen. Der bereits bestehende Kontakt zum Düsseldorfer Kreis, in dem die Datenschutzaufsichtsbehörden von Bund und Ländern zusammenarbeiten, ist weiterhin vorgesehen.

Bundesdruckerei erhält Berechtigungszertifikat für Login-Lösung mit dem neuen Personalausweis

Bundesverwaltungsamt lobt neues kundenfreundliches Geschäftsmodell

Am 08.03.2012 überreichte Klaus Wolter, Leiter der Vergabestelle für Berechtigungszertifikate im Bundesverwaltungsamt, der Bundesdruckerei GmbH auf der CeBIT ein Berechtigungszertifikat für das Login mit der Online-Ausweisfunktion. Dr. Matthias Merx, Leiter Trusted Solutions der Bundesdruckerei und Geschäftsführer der D-TRUST GmbH, nahm das Zertifikat entgegen. Der Bescheid für das Berechtigungszertifikat wurde bereits in der Vorwoche erteilt.

Bisher war die Nutzung der Online-Funktion des neuen Personalausweises oder des elektronischen Aufenthaltstitels für das Login in einen geschützten Bereich eines Online-Shops oder Web-Portals technisch und organisatorisch aufwändig, mit dem Zukauf unterschiedlicher Dienstleistungen verbunden und ein komplexes und eher teures Vorhaben.

Von jetzt an bietet die Bundesdruckerei mit ihrem Kooperationspartner AGETO alles aus einer Hand: Will ein Online-Shop seinen Kunden das Login mit dem Personalausweis anbieten, braucht er nur den ‚Digital Handshake' auf seiner Web-Plattform integrieren und muss nicht zusätzlich ein eigenes Berechtigungszertifikat beantragen. „Unser neues Geschäftsmodell für Unternehmen und Behörden ist so einfach wie ein Handschlag", beschreibt Merx den entscheidenden Vorteil der Lösung. Der ‚Digital Handshake' richtet sich an alle Internet-Portale und -Shops, die einen abgesicherten Benutzerbereich haben. Die Lösung ermöglicht das Login mit der Online-Ausweisfunktion ab 9,90 Euro pro Monat. Erstmals sind damit die Kosten überschaubar, die technische Integration wird wesentlich vereinfacht und auch eine webasierte AusweisApp ist Teil des ‚Digital Handshake'.

Klaus Wolter lobt bei der Übergabe des Berechtigungszertifikats insbesondere den kundenfreundlichen Ansatz: „Unternehmen und Behörden brauchen sich jetzt nicht mehr um technische Schnittstellen, System-Fragen, Richtlinien oder eine installierte AusweisApp kümmern. Das macht das Angebot hochinteressant und wird dazu beitragen, dass künftig mehr Anbieter den Ausweis in ihre Geschäftsprozesse einbinden werden. Der Prozess stellt sicher, dass keine personenbezogenen Daten ausgelesen oder an Dritte weitergeleitet werden," so Wolter.

Weitere Informationen unter *www.bundesverwaltungsamt.de*

G&D wird Trusted Service Manager für Intel-Mobilgeräteplattformen

Giesecke & Devrient (G&D) wurde von Intel für das Lebenszyklusmanagement der eingebetteten Secure Elements des Intel Smartphone-Referenzgeräts ausgewählt. G&D wird die Partitionierung und Schlüsselverwaltung der eingebetteten Secure Elements Over-the-Air, also über das Mobilfunknetz, übernehmen. Durch eingebettete Secure Elements wird ein zusätzlicher geschützter Bereich für sicherheitssensible Anwendungen wie Zahlung oder Ticketing mittels NFC-Technik (Near Field Communication) bereitgestellt.

Intel hat sein erst vor kurzem angekündigtes Smartphone-Referenzgerät zusätzlich zum herkömmlichen SIM-Kartensteckplatz mit einem eingebetteten Secure Element ausgestattet. Dieser geschützte Bereich bietet Sicherheit auf einem Niveau, das mit dem von Chipkarten wie EMV-Kreditkarten und SIM-Karten vergleichbar ist. Dies bringt für die Nutzer von Mobilgeräten noch größeren Schutz und noch höheren Komfort bei neuen Anwendungen wie dem kontaktlosen Bezahlen in Geschäften.

G&D wird als Trusted Service Manager für den Secure Element Issuer (SEI-TSM) das Lebenszyklusmanagement der eingebetteten Secure Elements übernehmen. Das SEI-TSM-System von G&D wird mit Service-Provider-TSMs (SP-TSM) verbunden – Systemen, über die Anwendungen im Auftrag von Anbietern wie Banken, Mobilfunkbetreibern oder Verkehrsbetrieben in vertrauenswürdiger Weise auf das eingebettete Secure Element übertragen werden. TSM-Lösungen (Trusted Service Management) von G&D unterstützen bereits zahlreiche sichere Dienstleistungen u. a. für Kunden aus den genannten Branchen.

Intels Strategie zielt auf ein offenes NFC- und Wallet-Ökosystem ab, das die Interoperabilität zwischen Finanzinstituten, Mobilgeräteherstellern, Mobilfunkbetreibern und Zahlungsabwicklern sicherstellen soll. Unsere strategische Beziehung mit Giesecke & Devrient ermöglicht dieses neue Ökosystem. Wir verfolgen das gemeinsame Ziel, NFC-Dienste allgegenwärtig, sicher und für alle beteiligten Seiten erfolgreich zu machen."

G&D verbindet das Secure Element als einen integralen Bestandteil des Smartphone-Referenzgeräts von Intel mit sicheren TSM-Diensten. Dabei spielen die langjährigen vertrauensvollen Partnerschaften mit Banken, Mobilfunkbetreibern und Verkehrsbetrieben auf der ganzen Welt eine wichtige Rolle.

Certgate Lösungen: NFC-Funktionen für viele Anwendungen

Aktuelle Smartphones dienen als Werkzeug für viele Aspekte im geschäftlichen und privaten Alltag. Eine wachsende Zahl von Anwendern und Sicherheitsverantwortlichen in den Unternehmen akzeptiert auf diesen Plattformen aber nur noch Werkzeuge und Anwendungen, die mit allen heute technisch machbaren und wirtschaftlich vertretbaren Schutzmechanismen gegen bösartige Angriffe und mögliche Schäden ausgerüstet sind.

Mit der Möglichkeit starke kryptographische Funktionen über ein mobiles Gerät mit NFC-Antenne zu verwenden, ermöglicht certgate es jetzt, eine wesentlich umfangreichere Reihe von zeit- und kostensparenden Anwendungen auf Smartphones oder Tablets einzusetzen. Der Schutz mobiler Smartcard-Payment-Lösungen, hardwarebasierte Sprachverschlüsselung und physische Zugangs-