

## Ein Stück Darmstädter Know-how in jedem neuen Reisepass

### FlexSecure-Software schützt digitale Signaturen im Pässeinband

Darmstadt/Worms, 23. Juni 2005. Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat die Darmstädter FlexSecure GmbH beauftragt, eine für die neuen Reisepässe nötige Sicherheitstechnologie zu entwickeln: Die so genannte Country Signing Certification Authority (CSCA) soll die Gültigkeit von digitalen Signaturen garantieren, um ein per Chip im Einband gespeichertes digitales Bild des Passinhabers vor Veränderungen zu schützen.

Die Sicherheit von digitalen Identitäten ist das gemeinsame Ziel, das die Partner Kobil Systems aus Worms und FlexSecure aus Darmstadt bei der Entwicklung ihrer Lösungen verfolgen. Beide Unternehmen sind seit vielen Jahren eng miteinander verbunden durch gemeinsame Projekte und insbesondere durch die Forschungsarbeit von Prof. Buchmann und seiner weltweit anerkannten Arbeitsgruppe an der Technischen Universität Darmstadt (TUD). Darin eingebunden sind auch die Mitarbeiter von Kobil, die disziplinübergreifend und im ständigen Austausch mit Wissenschaftlern der Kryptographie für Forschung und Entwicklung arbeiten. Aus dieser Arbeitsgruppe der TUD ist FlexSecure als Spin-off-Firma hervorgegangen.

Die von FlexSecure entwickelte hoch sichere Software FlexiTrust kommt nun auf den neuen Reisepässen zum Einsatz, die ab November in Deutschland eingeführt werden. Auf einem Chip im Einband der Pässe wird künftig ein digitales Bild des Inhabers gespeichert. Das Bild wird durch eine elektronische Unterschrift, einer digitalen Signatur vor Veränderungen geschützt. Um die Gültigkeit dieser Signatur zu garantieren, ist eine Zertifizierungsinstanz nötig. Das BSI hat nun FlexSecure mit der Entwicklung dieser Zertifizierungsinstanz, der so genannten Country Signing Certification Authority (CSCA) beauftragt. Für dieses Projekt setzen die Darmstädter Experten die Software FlexTrust ein, die auch schon bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) verwendet wird und dort alle qualifizierten digitalen Signaturen in Deutschland absichert. In diesem Projekt wird zum ersten Mal eine neue Generation maschinenlesbarer Reisedokumente (MRTD = machine readable travel documents) der International Civil Aviation Organization (ICAO) in Betrieb genommen. Dabei kommt modernste Kryptographie in Form von 256-Bit-elliptischen Kurven zum Einsatz.

#### Über FlexSecure

Im Sommer 2000 wurde die FlexSecure GmbH als Spin-off-Firma der weltweit anerkannten Arbeitsgruppe von Herrn Prof. Dr. Johannes Buchmann der Technischen Universität (TU) Darmstadt gegründet. Die durch die TU Darmstadt entwickelte Trustcenter-Software FlexiTrust wird allein durch die Firma FlexSecure GmbH vermarktet. Die Firma beschäftigt derzeit acht Mitarbeiter hauptberuflich und vergibt entsprechende projektbezogene Aufträge an die TU Darmstadt. Hier stehen in der Arbeitsgruppe etwa 20 Mitarbeiter zur Verfügung.

#### Referenzen für FlexiTrust

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) betreibt die Wurzel-CA (Certificate Authority) gemäß dem deutschen Signaturgesetz (SigG) und setzt als Software FlexiTrust ein. Hier wurde die Evaluierung des Produktes nach SigG durchgeführt und bestätigt. Der Standard ISSIS-MTT wurde implementiert.

Das Trustcenter der DGN Service GmbH hat am 1.1.2003 den Betrieb aufgenommen und personalisiert Smart Cards. Die jeweils drei anwendungsspezifischen Zertifikate sorgen für eine transparente Nutzung in unterschiedlichen Szenarien auch im medizinischen Bereich. Die verwendeten Kryptomodule kombiniert mit einem gut durchdachten und von FlexiTrust voll unterstützten Rollenkonzept bilden die Basis für eine hochsichere, mandantenfähige Trustcenterlösung.

An der Universität Gießen werden circa 20.000 Smart Cards für Studierende mit FlexiTrust erzeugt und verwaltet. Der Prozess ist vollständig in die bestehenden Verwaltungsprozesse integriert. Die bereitgestellten Dienste umfassen unter anderem Anmeldung zur Prüfung und Lehrveranstaltungen, Semester-Rückmeldung, Drucken von Bescheinigungen und sicheres Login. Durch die Verwendung eines zusätzlichen Mifare-Chips auf den Karten ist eine anonyme Bezahlungsfunktion in Zusammenarbeit mit dem Studentenwerk realisiert.

Das IT-Systemhaus u.s.d. AG nutzt FlexiTrust zur Absicherung des Zugangs von Mitarbeitern und zur Absicherung des Entwicklungsprozesses. Dazu wird ein Software-PSE mit getrennter Key-Usage (Sign/Encrypt) verwendet.

Bei der Deutschen Bausparkasse Badenia AG ermöglicht FlexiTrust den Außendienstmitarbeitern einen zertifikatsbasierten Zugang zu Geschäftsdaten und zu Diensten der Zentrale. (z. B. Kundennamen ändern). Die Authentifizierung gegenüber der Unternehmens-Firewall und der Aufbau einer sicheren Verbindung (VPN) ist dabei granular steuerbar.

#### Über Kobil Systems:

Die 1986 gegründete Kobil Systems GmbH agiert als Hersteller hochsicherer Basistechnologie im Umfeld von Smart Cards, Einmalpasswörtern (OTP) und Zertifikaten. Sicherheit ohne Einschränkungen, einfach, überall und jederzeit, zu ermöglichen, dieses Ziel hat Kobil durch langjährige Forschungs- und Entwicklungsarbeiten verwirklicht. Das Unternehmen bietet seinen Kunden heute nicht nur patentierte Basistechnologie, sondern vor allem die wichtige und umfassende Lösungskompetenz, um gemeinsam mit namhaften Technologiepartnern für jedermann die Verwendung seiner digitalen Identität bequem und gleichzeitig absolut sicher zu ermöglichen.

---

Weitere Informationen: KOBIL Systems GmbH, Marius Schmidtke, Pfortenring 11, D - 67547 Worms

Tel.: (06241) 3004-31, Fax: (06241) 3004-80, E-Mail: marius.schmidtke@kobil.com, Internet: <http://www.kobil.com>

FlexSecure GmbH, Erwin Stallenberger, Industriestr. 12, 64297 Darmstadt

Tel.: 06151-50123-0, E-Mail: [info@flexsecure.de](mailto:info@flexsecure.de), Internet: <http://www.flexsecure.de>

Pressekontakt: Konzept PR GmbH, Andrea Finkel, Karolinenstr. 21, D-86150 Augsburg

Tel.: (0821) 34300-15, Fax: (0821) 34300-77, E-Mail: [a.finkel@konzept-pr.de](mailto:a.finkel@konzept-pr.de), Internet: <http://www.konzept-pr.de>