Pressemitteilung

PLUSCARD bietet mehr Sicherheit mit EMV-Chip für MasterCard und Visa

Sparkasse Leipzig setzt auf Sicherheit als Verkaufsargument

Saarbrücken, den 22. Februar 2006

„Die Pilotierungsphase ist erfolgreich verlaufen, der EMV-Chip ist live und nichts steht einer flächendeckenden Einführung bei allen PLUSCARD-Kunden im Wege“, zeigt sich Geschäftsführer Thomas Maas zufrieden. „Wir wissen, wie sensibel das Thema Sicherheit gerade im Umgang mit Karten von der Öffentlichkeit beobachtet wird. Deshalb haben wir auch mit Hochdruck an der Realisierung zur Einführung des EMV-Chips – den gemeinsam von Europay, MasterCard und Visa festgelegten, zertifizierten Standard für Chipkarten – gearbeitet.“

Die EMV-Technologie dient zur sicheren Abwicklung von Zahlungen am Point of Sale (POS), Verfügungen am Geldausgabeautomaten (GAA) oder Zahlungen im Internet und schützt vor missbräuchlichem Einsatz von Totalfälschungen und Kartenduplikaten. Seit Anfang vergangenen Jahres gilt die Haftungsumkehr (Liability Shift) für Visa Karten und MasterCards. Das bedeutet: Wenn es bei Totalfälschungen zu einer missbräuchlichen Transaktion kommt, so muss die Partei, die EMV nicht unterstützt, für den Schaden haften.

Mehr Sicherheit ist auch das Hauptargument für den Verkauf einer EMV-Kreditkarte. Jürgen Geller, stellvertretendes Vorstandsmitglied der Sparkasse Leipzig, stellt die Gründe für die Teilnahme seines Institutes an der Pilotierung dar: „Im Umgang mit Kreditkarten legen unsere Kunden besonderen Wert auf Sicherheit – sie vertrauen darauf, dass wir stets den modernsten Stand der Technik anbieten. Diesem Vertrauen werden wir gerecht: Für uns wird künftig das schlagkräftigste Argument im Verkauf EMV sein. Hierin sehen wir auch die Chance Kunden anderer Institute, die EMV noch nicht anbieten, für unsere sichere Lösung zu gewinnen.“

PLUSCARD setzt im Kampf gegen Kartenmissbrauch auf die Implementierung des SECCOS-Chips mit dynamischer Kartenechtheitsprüfung (Dynamic Data Authentication = DDA). Hierbei werden im Gegensatz zur statischen Prüfung nicht vom Kartenterminal lediglich die auf der Karte hinterlegten Zertifikate abgefragt, sondern bei jeder Transaktion wird ein neues Kryptogramm generiert und Kartenduplikate werden am Terminal erkannt und abgewiesen.