



## Höchste Sicherheit für sensible Zahlungskarten-Daten

### Profil

#### Die DSV-Gruppe

Die DSV-Gruppe, die sich aus dem Deutschen Sparkassenverlag sowie seinen Tochter- und Beteiligungsunternehmen zusammensetzt, zählt mit einem Jahresumsatz von rund 713 Millionen Euro zu den zehn umsatzstärksten Medienhäusern Deutschlands. Als spezialisierter Lösungsanbieter für die Verbände und Unternehmen der Sparkassen-Finanzgruppe bietet die DSV-Gruppe klassische Verlagsmedien wie Bücher, Ratgeberreihen, Fach- und Kundenzeitschriften sowie organisatorische Medien wie Vordrucke, technische Geräte und Bankkarten. Ergänzt wird das Leistungsportfolio durch informatikgestützte Dienstleistungen, Internet-Angebote, elektronische Beratungssysteme sowie Full-Service-Agenturleistungen inklusive Kommunikationskonzepte und PR-Events. Das 1935 gegründete Unternehmen beschäftigt 1.660 Mitarbeiterinnen und Mitarbeiter. Hauptsitz der DSV-Gruppe ist Stuttgart-Vaihingen, darüber hinaus ist das Unternehmen bundesweit an zahlreichen Standorten vertreten.

Weitere Informationen unter [www.dsv-gruppe.de](http://www.dsv-gruppe.de)

### Anforderung

**Die Produktion, Personalisierung und Distribution von Zahlungsverkehrs-Karten muss ähnlich abgesichert werden wie der Druck und Transport von Banknoten. Die DSV-Gruppe (Deutscher Sparkassenverlag) – Marktführer unter den Kartemittentem und Vorreiter bei der Einführung der elektronischen Signatur in Deutschland – setzt bei der Kartenpersonalisierung und der Datenaufbereitung (PIN-/TAN-Generierung) bereits seit zehn Jahren das Hardware-Sicherheitsmodul (HSM) CryptoServer des IT-Sicherheits-spezialisten Utimaco ein.**

Die DSV-Gruppe (Deutscher Sparkassenverlag) gehört zu den zehn größten Medienhäusern in Deutschland. Der spezialisierte Lösungsanbieter für die Institute der Sparkassen-Finanzgruppe gilt als führender deutscher Anbieter von Bank- und Zahlungsverkehrskarten mit einem Marktanteil von 65 Prozent und einer jährlichen Produktionskapazität von 25 Millionen Karten.

Im Mittelpunkt des vielfältigen Angebotes der DSV-Gruppe rund um den kartengesteuerten Zahlungsverkehr steht die Herstellung von Kartenkörpern mit Microprozessorchips sowie die Initialisierung und Personalisierung von Bankanwendungen jeglicher Art. Neben der Kartenproduktion entwickelt die DSV-Gruppe auch zu-

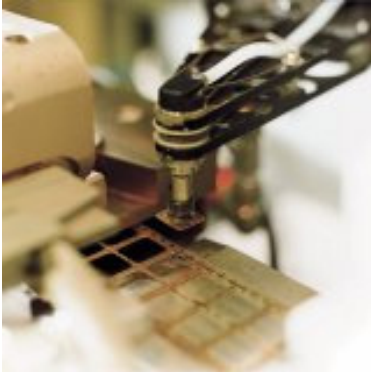
kunftsweisende Anwendungen rund um die GeldKarte, mit denen Sparkassenkunden beispielsweise Fahrkarten für Busse und Bahnen sowie Parktickets elektronisch bezahlen können.



Die neueste Karteninnovation des Deutschen Sparkassenverlags (DSV) ist seit kurzem auf dem Markt: Als erste Kreditinstitute in Deutschland bieten die Sparkassen ihren Kunden Bank- und Signaturfunktionen auf einer Karte an. Mit dieser SparkassenCard (ec-Karte) oder einer kontounabhängigen GeldKarte mit qualifiziertem Zertifikat können Sparkassenkunden nicht nur wie gewohnt bezahlen und Geld abheben, sondern von nun an alle Geschäfte, die die gesetzliche Schriftform erfordern, prinzipiell auch elektronisch erledigen.

*„Diese neuen SparkassenCards – mit kartenbasierten Zertifikaten – machen die elektronische Signatur jedem Bürger einfach zugänglich und erweitern damit deren*

*Einsatzmöglichkeiten*“, erläutert Dr. Rüdiger Mock-Hecker, Leiter der Geschäftssparte Kartensysteme beim DSV.



### HSM sichern Daten und Schlüssel für die Karten-Initialisierung und -Personalisierung

Die DSV-Gruppe verfügt über jahrelange Erfahrung in der Initialisierung und Personalisierung von Bankkarten: Von der Herstellung (Druck) und der Prägung der Karten bis zu deren Ausstattung mit allen individuellen Merkmalen und Servicefunktionen, die ein Finanzinstitut seinen Karteninhabern zur Verfügung stellen möchte. Dazu gehört auch die Generierung, Verteilung sowie Verwaltung der Chipkarten- und Terminalschlüssel. Im DSV-Rechenzentrum werden alle für die Funktionsfähigkeit der Karte erforderlichen Sicherheitswerte berechnet und die Daten für die Produktion aufbereitet. Auch die Berechnung der Geheimzahlen (PIN) liegt beim DSV, der als TrustCenter für die Sparkassen Finanzgruppe fungiert.

Seit dem Start der Chipkarten-Produktion im Jahr 1996 setzt der DSV bereits das Hardware-Sicherheitsmodul (HSM) CryptoServer des IT-Sicherheitsspezialisten Utimaco ein, um damit die Personalisierungsdaten zu berechnen. Ab dem Jahre 2003 wurden auch Zertifikate für EMV und die Komponentenauthentikation mit dem CryptoServer berech-

net. Der CryptoServer ist ein Sicherheitsmodul, das kryptographische Funktionen und Schlüssel in einer gesicherten Hardware kapselt und verarbeitet. Es wird zur Absicherung von unterschiedlichsten geschäftskritischen IT-Prozessen eingesetzt. Im Unterschied zu reinen Software-Lösungen ermöglicht der CryptoServer zudem einen physikalischen Schutz bei der Durchführung von kryptographischen Operationen, wie zum Beispiel die Generierung und Speicherung von Schlüsseln sowie digitale Signaturen. Typische Einsatzbereiche sind besonders sicherheitskritische Anwendungen, wie im Bereich der Kartenproduktion (Visa, Mastercard, ecMaestro, ec-cash), oder in Trust Centern.

Dr. Mock-Hecker erläutert, warum sich der DSV für eine Systemarchitektur entschieden hat, bei der das Hardware-Sicherheitsmodul von Utimaco zum Einsatz kam: *„Wichtig war für uns ein jederzeit erweiterbares System, das unabhängig vom bzw. parallel zu unserem vorhandenen Host-Rechner läuft und zudem technisch nicht an Grenzen stößt – damit wir schnell auf neue Anforderungen reagieren können. Nachdem wir uns gründlich im Markt umgeschaut hatten, kam für uns nur der CryptoServer in Frage.“*

### Neues High-End-Modul verarbeitet bis zu 11.000 Rechenoperationen pro Sekunde

Auf Grund der dynamischen Entwicklung des Karten- und Zahlungsverkehrsmarktes in den letzten zehn Jahren hat Utimaco auch den CryptoServer kontinuierlich weiterentwickelt. Um neue Kartenanwendungen und längere kryptographische Schlüssel in der notwendigen Geschwindigkeit verar-

beiten zu können, setzt der DSV seit 2004 eine neuere, leistungsfähigere Version des CryptoServers ein. Mit dieser Gerätegeneration können die aufwändigen kryptographischen Operationen für 100.000 Karten pro Stunde berechnet und verarbeitet werden.

Seit Sommer 2006 ist ein ganz neues, noch schnelleres HSM lieferbar, das der IT-Sicherheitsspezialist für künftige, hochperformante Anforderungen entwickelt hat. Durch seine Prozessortechnologie im Gigahertz-Bereich kann diese neueste Version des CryptoServers bis zu 11.000 Verschlüsselungsoperationen pro Sekunde verarbeiten – die fünffache Leistung des Vorgängermodells. Das HSM ermöglicht die sichere Speicherung, Applikation und Distribution von kryptographischen Schlüsseln und Zertifikaten für die Verschlüsselung und für digitale Signatur-Prozesse. Der neue CryptoServer entspricht den EU-Bestimmungen der Umweltschutz-Verordnung RoHS (European Restriction of Hazardous Substances Directive) und ist gemäß dem internationalen Sicherheitsstandard für Kryptographiemodule – dem Federal Information Processing Standard (FIPS) 14-2 – zertifiziert.