



Maximum Security for Sensitive Payment Card data

Profile

The DSV group

The DSV group consists of the German company Deutscher Sparkassenverlag, along with its subsidiaries and companies in which it has an interest. Its annual revenues of around 713 million Euros make it one of the ten biggest grossing media houses in Germany. As a specialized solution provider for the associations and companies in the Sparkassen (German savings banks) financial group, the DSV group offers classic publishing media such as books, technical and customer periodicals, and also organizational media such as printed forms, technical devices and bank cards. Its portfolio of offerings is rounded off by IT-based services, Internet offerings, electronic consultation systems, and also full service agency offerings, including communications concepts and PR events. The business, which was founded in 1935, employs 1,660 staff. The headquarters of the DSV group are located in Stuttgart, but it is also represented across Germany at numerous locations .

For more information, go to:
www.dsv-gruppe.de

Requirement

The production, personalization and distribution of payment data cards must be made secure, in a similar way to the printing and transportation of bank notes. The DSV group (Deutscher Sparkassenverlag) is the German market leader among card issuers and is leading the way in introducing electronic signatures in Germany. It has been using the CryptoServer hardware security module (HSM), supplied by Utimaco, the IT security specialist, for card personalization and data provision (PIN and TAN generation) for over ten years.

The DSV group (Deutscher Sparkassenverlag) is one of the ten biggest grossing media houses in Germany. Specialized solution provider for the institutions of the Sparkassen (German savings banks) financial group, the DSV group is the leading German supplier of bank and payment data cards, with a market share of 65% and an annual production capacity of 25 million cards.

At the center of the DSV group's extensive offering, covering card-based payments, is the manufacture of card bodies with microprocessor chips, and also the initialization and personalization of banking applications of every kind. In addition to card production, the DSV group also develops innovative applications for the GeldKarte, a sort of electronic

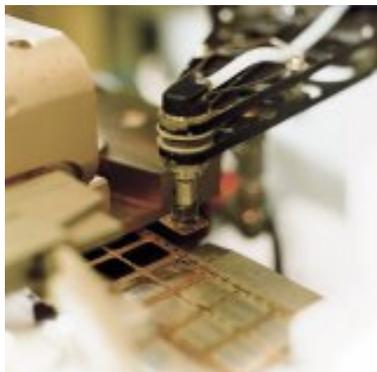
purse, used by Sparkassen customers in Germany to make electronic payments for bus and train tickets, or parking tickets, for example.



The DSV's latest card innovation has just been launched: the Sparkassen are the first credit institutions in Germany to offer their customers banking and electronic signature functions on one card. Not only can Sparkassen customers use this SparkassenCard (ec card) or a non-account-specific GeldKarte with a qualified certificate to make payments and withdraw money in the usual way, but, from now on, they can also use them to perform all business transactions, that legally require to be made in writing, electronically.

"These new SparkassenCards, with card-based certificates, give every each citizen easy access to electronic signatures, creating many more ways in which they can be used", explained Dr. Rüdiger

Mock-Hecker, head of the card systems division at DSV.



HSMs secure data and keys for card initialization and personalization

The DSV group has many years experience in initializing and personalizing bank cards, from the manufacture (printing) and embossing of the cards to giving each one the individual features and service functions that a financial institution would like to provide to its card holders. This also includes the generation, distribution and administration of the chip card and terminal keys. In the DSV computing centre, all security values necessary for the card's functionality to be available are calculated and the data is prepared for the production process. DSV, which functions as the trust center for the Sparkassen financial group, also calculates the security number (PIN).

Since it started producing chip cards in 1996, DSV has always used the CryptoServer hardware security module (HSM) supplied by Utimaco, the Data Security Company, for calculating the personalization data. From 2003 the CryptoServer was also used to calculate certificates for EMV and for component authentication. CryptoServer is a security module that encapsulates and processes cryptographic functions and keys in a secured hardware module. It is

used for securing the widest range of business-critical IT processes imaginable. In contrast to pure software solutions, the CryptoServer also enables cryptographic operations, such as the generation and storage of keys and digital signatures, to provide with physical protection when they are being performed. Typical areas of use are especially security-critical applications, such as those involved in card production (Visa, MasterCard, ecMaestro, ec-cash) or in trust centers.

Dr. Mock-Hecker explained why DSV chose a system architecture in which Utimaco's hardware security module was used: *"It was important for us to have a system that could be extended at any time, that ran independently of or parallel to our existing host computers, and that had no technical limitations, enabling us to react quickly to new requirements. We made analyzed the market in detail, and only CryptoServer was suitable."*

The new high-end module processes up to 11,000 computing operations per second

As a result of the dynamic development of the market for bank card and electronic payments in the last ten years, Utimaco has also continually developed the CryptoServer on an ongoing basis. Since 2004, DSV has been running a newer, more powerful version of the CryptoServer, to enable it to process new card applications and longer encryption keys at the necessary speed. With this generation of the device, the time-consuming cryptographic operations for 100,000 cards per hour can be calculated and processed.

Since summer 2006 it has been possible to obtain a completely new, even faster, HSM, which Utimaco, the IT security specialist, has developed to meet the high-performance requirements of the future. This latest version of the CryptoServer has processor technology running at gigahertz speeds, enabling it to process up to 11,000 encryption operations per second process – five times the performance of its predecessor. With the HSM, cryptographic keys and certificates for encryption and for digital signature processes can be stored, applied and distributed securely. The new CryptoServer complies with the RoHS (European Restriction of Hazardous Substances Directive) and has been awarded certification in accordance with the international security standard for cryptography modules – Federal Information Processing Standard (FIPS) 140-2.