C. & E. Becker

EDV-DIENSTLEISTUNGEN

SEMINAR

APPLIED CRYPTOGRAPHY IN THE ATM BUSINESS

This one day compact seminar is aimed at consultants, software architects and developers who wish to aquire knowledge about cryptographic and security issues of the ATM business.

Participants should have some computer science background. The focus of the seminar is however on the application of cryptography rather than the underlying mathematical theory or implementation details

The goal of the seminar is to get an understanding about the fundamentals of symmetric and asymmetric cryptography, to know the cryptographic protocols used in the ATM business and to learn about possible cryptographic attacks and how to thwart these.

AGENDA

Introduction
- History, purpose and limitations of cryptography
- The advent of DES

DES and the ATM Business
- Offline PIN Verification
- PIN Blocks
- Message Authentication with MACs
- Cryptographic Attacks and Countermeasures
- How secure is DES ?
- Session keys
- Triple DES, Retail-MAC
- The problem of key exchange

Smart Cards
- Offline PIN Verification, again ?
- Card Authentication
- Electronic Purses

Asymmetric Cryptography
- What is asymmetric cryptography ?
- Public / Private Key Pairs
- RSA
- Signatures and Certificates
- Public Key Infrastructures

RSA and the ATM Business
- EMV
- Remote Key Loading
- Attacks against RSA

C. & E. Becker

Terms & Conditions

Location	Frankfurt, Germany walking distance from Frankfurt Airport
Duration	1 day
Language	English
Fee	EUR 450,- / participant
Included	Seminar material (printed and online) A copy of "The Code Book" by Simon Singh Lunch and refreshments

You may cancel reservations free of charge until 30 days before the seminar.

The payment of the seminar fee is due 30 days before the seminar date. By this date we will charge your credit card.

If you cancel your reservation after this date, we refund 80 % of the payed fee.

If we cancel the seminar for whatever reason, we refund the full amount paid. Any further liability is excluded in this case.

For German customers only, the seminar fee is subject to German VAT (Umsatzsteuer).

In-House Seminar

The seminar may be held in-house at the client's premises in which case special rates apply while proven travel expenses are billed.

The agenda may be adjusted in consultation with clients in order to meet their needs and the participants' previous knowledge.

Please contact seminars@becker-wiesbaden.de to make arrangements.

The Instructor

Carl Becker is a freelance system programmer and consultant from Germany who has been working as a contractor for major ATM manufacturers since 1988.

Besides software development he has performed consulting in various ATM projects.

His professional focus in recent years has been on CEN/XFS, J/XFS and cryptography.

Contact

Mail	C. & E. Becker EDV-Dienstleistungen Aschenbrödelweg 5 D-65199 Wiesbaden
Phone	+49 611 29495
Fax	+49 611 29467
Mobile	+49 172 666 9716
E-mail	seminars@becker-wiesbaden.de
Web	www.becker-wiesbaden.de/seminars