

Michael P. Kuehle - Career History

CURRICULUM VITAE

Education: Master Degree in Computer Science, University of Bonn, Germany
Army: 1977 – 1979, Electronic Combat (West Germany)
Preferred Location: Germany, Europe or USA
Last Employment: Independent Freelance Consultant

Skills & Knowledge: Design and Specification of E/M-Commerce Architectures, Project Management, Security, SmartCard & Cryptography Consulting, Editing of Specifications and Concepts, Smart Card Application (Design, Programming, Development)

Keywords: PKI, RSA, ECC, ECDSA, PKCS, SPA, EMV, M/Chip, MCI Banknet, GSM, WAP, WIM, SIM, OSS, TLS, SSL, X.509, OpenSSL, LINUX, Apache, ModSSL

Since January 1999: Consultant for ORGA Card Systems (Germany / USA). Major projects: Specification and Development of SmartCard Based Authentication System. Specification of Public Key Infrastructure for SmartCard based Internet Transaction Authorization System (AUTELO). Specification of various documents (Security Concept, API Specification, PKI Specification, Message- & Command Handler Specification) for European VHE (Virtual Home Environment) Project. Specification of GSM Sim Toolkit Application for transaction authorization with symmetric- and- asymmetric key infrastructures (GSM SIM and JavaSIM). Specification and development of PKI Trust Center (RA, CA, CRL) and implementation of HTTPS demo application for TLS Server- and Client Authentication (under employment LINUX, Apache, ModSSL).

Since November 2001: Consultant for EDS Germany: Specification of SmartCard Based Cryptographic Use Cases, concepts and applications.

Sep 2000 – November 2001: Consultant for MasterCard Inc. Purchase, NY. Major projects: Evaluating of planed and existing worldwide payment schemes. Specification of MCI's new GMCIG standard for GSM STK based Authentication System (White Paper, System Concept EMV, System Concept SPA, STK Application Specification, Authentication Server API Specification).

Aug 1997 – Oct 1998: Technical Project Manager and Smart Card Consultant for Brazilian's Social Security Smart Card Project in behalf of ORGA Card Systems. Specification of Smart Card Concepts for combined Automated Fingerprint ID System and Multiple Application Solutions (including Banking Application). Editor of various documents, such as Smart Card Security, Third Party Application Integration, Terminal Security Modules and Key Management. Consulting in Smart Card Security and Key Management for ORGA Consult, Brazilian Banks and GE Capital ITS.

Jan 1997 – July 1997: Conceptual Design, Specification, Project Management and Development of ORGA's first "Over The Air" Gateway, the OTA Express. The OTA Express is an automated server (linked to various clients) to transfer data via a Mobile Communications Network's Short Message Service Center (SMSC) into a GSM Smart Card. The system is running on a IBM Server platform (OS Windows NT), programmed in Visual Basic (GUI), C++ (OTA Software Library and Encryption Software) and Oracle (internal Database). Interfaces to various SMSCs (or 3rd party applications) using TCP/IP socket communication had to be designed and implemented. The concept can easily be adapted for Internet based services with secure data transfer.

Feb 1996 – Dec 1996: Implementation of ORGA USA's Telecom Technical Support Group and Customization of ORGA USA's Personalization System for Smart Cards. Training and consulting on all Smart Card related issues for internal staff and ORGA's customers. Business development and system integration. Member of the North American GSM Group (NAIG) and the SIM Vendor Group (within the NAIG). Specification of the (US) standard for "Over The Air" SIM Vendor Libraries (within NAIG). Technical Manager for all major ORGA USA customers, especially for Omnipoint Inc. and Sprint Spectrum/APC.

Jun 1995 - Jan 1996: Consultant for Master Card International, NY within the Canberra IC Card Pilot. Editor of MasterCard's Certification Authority Documentation (Operating Requirements and Technical Specifications). The CA supports the secure generation, distribution and management of cryptographic keys.

Aug 1994 – Apr 1995: Commercial Operation of the GSM Operations Support System (OSS) for the Turkish GSM Network TELSİM. Full responsibility for all technical and security aspects. Consulting in general aspects of GSM, GSM Customer Billing and Accounting, Smart Card Technology & Security, SIM Personalization and security aspects in a GSM environment. Training on the job of TELSİM's staff in VAX System Management, Database Management and Smart Card Personalization. The core system (Customer Care and Billing System) was implemented on a DEC VAX platform (OS VMS) and VAX RDB (internal Database). Interfaces to various Network Components via TCP/IP socket communication had to be implemented.

Oct 1993 - Jul 1994: Project Management, Implementation and Customization of TELSİM's Billing and Customer Care System and the Personalization Center for SIMs (PCS). Smart Card Testing and Quality Assurance, Acceptance testing of PCS components (on behalf of TELSİM). Specification and implementation of TELSİM's SIM Activation System for fast customer activation. Implementation of all interfaces between the OSS components (Customer Care & Billing System and PCS) and to the HLR (GSM home location register). The PCS was implemented on a SUN Workstation (OS UNIX).

Mar 1992 – Sep 1993: International Consultant in Smart Card Technology, Smart Card Security and Cryptography, Project Management, Billing & Accounting Systems and System Implementation. Consulting on marketing, operation and support of a GSM network for the Australian PTT (AOTC). Training on the job in Smart-Card Technology and Cryptography at ORGA Card Systems (U.K.) LTD. Product design of ORGA's PCS 1000 Personalization System.

Mar 1991 – Feb 1992: Manager for Quality Assurance OSS - DPPS (GSM Billing System). Chairman of Implementation Group I-1, responsible for Implementation of the Billing and Administration System (included overall co-ordination of all installation activities). Head of the German Telekom's GSM Network Data Processing Center and responsible for initial operation until hand over of fully functional system to Telecom in July 1991. Manager for acceptance tests for various milestones for GSM Operations Support System, responsible for developing test procedures and documentation. With a \$100 Mio system price tag the DPPS was on one of the largest DEC VAX VMS/RDB Clusters in Europe

Sep 1987 – Feb 1991: Head of the PDM Data Processing Center (PDM - Project Digital Mobile Communications - GSM Network implementation for German Telekom). Project Management and operation of the PDM Data Processing Center for 500 engineers. Specification, selection and installation of one of the largest Digital Equipment VAX/VMS Clusters in Germany (a \$10 Mio investment, including several large VAX9000/600 Mainframes, UNIX /VMS Workstations, PCs and fiber optic based data network). Staff training on the job in VAX System Management, Network Management and Database Management.

1979 – August 1987 (summary): Studies of Computer Science at University of Bonn, Germany. System Management at the University's DEC VAX Systems (OS VMS, UNIX). For two years General Manager and Co-Owner of ATON GmbH Software Development Company. Software development on IBM PC (OS DOS) platform in Cobol, Pascal and C.