

Fraunhofer SmartCard-Preis 2008 für



Wolfgang Effing



Wolfgang Rankl

Autoren des Buches „**Handbuch der Chipkarten**“

Liebe Freunde des SmartCard Workshops, verehrte Gäste,

was ich hier in meiner Hand halte, hat Gewicht im doppelten Sinne des Wortes. Es ist das Handbuch der Chipkarten, geschrieben von Wolfgang Rankl und Wolfgang Effing. Es enthält 353.781 Worte, wie im Vorwort vermerkt ist. Da das Buch 2.100 g wiegt, entfällt auf jedes Wort ein Gewicht von 0,0059 g. Es ist die 4. überarbeitete und aktualisierte Ausgabe, herausgegeben von dem renommierten Hanser-Verlag in München. Die 1. Auflage erschien bereits 1995, also vor 13 Jahren.

Wirft man einen Blick in das Handbuch, so findet man als Untertitel „Aufbau – Funktionsweise – Einsatz von Smart Cards“. Gegenstand des 1.057 Seiten umfassenden Handbuches ist also ein Stück Plastik mit integriertem Chip, dessen Form von der legendären Diner's Club-Karte herrührt, die 1950 auf den Markt kam. In das Jahr 1968 fällt das Urpatent der Chipkarte, das Jürgen Dethloff und Helmut Gröttrup als Erfinder nennt, und seit 1984 wird auf ISO-Ebene die Normung der SmartCard betrieben.

Herzstück einer jeden SmartCard oder SmartTokens ist der Chip. Er besteht aus einem hauchdünnen Silizium-Plättchen von meist weniger als 20 qmm Fläche und bietet in seiner SubMicron-Technologie Millionen von Transistoren Platz.

Getrieben von 1,8 V Spannung flitzen Milliarden von Elektronen in verschiedenen Ebenen auf Wegen, die durch unzählige Gatter aktionsbedingt vorgegeben sind, werden durch die Charge Pump mit erhöhter Spannung versorgt, um

in EEPROM-Zellen Zustände zu verändern, sprich Bits von 0 auf 1 oder umgekehrt zu setzen, laden Register, führen Aktionen in Akkumulatoren durch, rufen Informationen aus Zellen ab, deren Lage über Adressleitungen signalisiert wird, peitscht der Befehls-Lademechanismus mit einer vielfachen der von außen angelegten Taktfrequenz abertausende von Befehlen eines inzwischen mehrere hunderttausend Statements umfassenden Betriebssystems in Bruchteilen einer Sekunde durch die 32 Bit breite CPU, verwirbeln Scrambler die Bits auf dem Datenbus, um Reverse-Engineering-Angreifer in die Irre zu führen, messen Temperaturfühler, ob die Temperatur im zulässigen Bereich liegt, prüfen Taktfilter die Außenfrequenz auf Nicht-Über- oder Unterschreitung vorgegebener Werte, kontrollieren Spezial-Detektoren die Einhaltung definierter Arbeitsbedingungen oder Toleranzen, manipulieren Sonderschaltungen die Leistungsaufnahme, um Rückschlüsse auf Rechenoperationen via Differential Power Analysis verhindern zu helfen, lösen Acceleratoren schier unglaubliche kryptografische Aufgaben mit einem Wimpernschlag, um elektronische Signaturen zu berechnen oder Daten zu chiffrieren oder dechiffrieren - und so werden von außen gesandte ISO-Kommandos auf ihre syntaktische und semantische Korrektheit geprüft, die Erfüllung der Zugriffsbedingungen auf Schlüssel und Daten überwacht, die entsprechenden Aktionen ausgeführt und anfallende Daten als Ergebnis ggf. mit Secure Messaging zurücktransportiert.

Welche Befehle was machen, welche Sicherheitsbedingungen formuliert werden können, welche I/O-Transport-Protokolle zur Verfügung stehen und Beispiele für das, was eine SmartCard zu leisten vermag, all das und vieles mehr findet man in dem Buch von Rankl und Effing.

Die beiden Autoren sind keine Unbekannten.

Wolfgang Rankl, der die Idee zu diesem Handbuch hatte und auch den größeren Teil geschrieben hat, hat an der FH München Feimechanik und Wirtschaftsingenieurwesen studiert, war ab 1990 Entwicklungsingenieur und Projektleiter im F&E-Bereich bei der GAO, der damaligen Entwicklungsgesellschaft von G&D, dann ab 1995 Abteilungsleiter Systementwicklung im F&E-Bereich bei G&D und ist dort seit 1999 Leiter Entwicklung Telekommunikation. In dieser Funktion ist er im Rahmen des G&D-Konzerns weltweit verantwortlich für Produktentwicklung, Applikationsentwicklung, Toolentwicklung und Testentwicklung für Karten im Telekommunikationsbereich, der 2007 bei G&D ein Volumen von 350 Mio. Karten erreichte.

Herr Rankl hat auch in einigen ETSI-Normungsgremien mitgearbeitet, u.a. bei der Entwicklung des DECT-Standards für Digital Enhanced Cordless Telecommunications.

Wolfgang Effing, der Co-Autor des Handbuches für Chipkarten, gehört zum Ur-Gestein im Chipkartensektor. Er hat an der TU Karlsruhe Nachrichtentech-

nik studiert, war von 1976 bis 1979 Entwicklungsingenieur bei AEG-TELE-FUNKEN in Backnang und beteiligt an der Entwicklung von Sende- und Empfangseinheiten für die erste optische Übertragungsstrecke der Bundespost in Berlin. Von 1980 bis 1984 war er Leiter der Elektronikentwicklung beim Apparatebau Gauting, wo es um die Entwicklung von Bordelektronik für Luftfahrzeuge ging. Ab 1984 ist sein Arbeitsgebiet die Chipkarte. Von diesem Jahr an bis 1993 war er Leiter der Elektronikentwicklung für Chipkarten bei der GAO. Entwickelt wurden damals die ersten Telefonkarten für die Feldversuche der Deutschen Bundespost, die C-Netz-Karten mit dem nationalen Übertragungsprotokoll T=14, die Karten für den Feldversuch des ZKA in Regensburg und – last, but not least – die erste Version des STARCOS-Betriebssystems. 1993 wechselte die Chipkartenentwicklung von der GAO zu G&D. Seitdem ist er dort Bereichsleiter für Forschung und Entwicklung von Chipkarten, Terminals und Personalisierungsanlagen. Natürlich war und ist Wolfgang Effing auch in der Normung aktiv: 1984 wurde er Mitglied im DIN NI17.4 und war DIN-Deligierte bei der ISO-WG4. In dieser frühen Phase ging es um Themen wie Lage der Kontakte und Übertragungsprotokolle, Themen, die insbesondere zwischen den Franzosen und den Deutschen heiß umkämpft waren. Nach Übergabe der NI17.4-Aktivitäten an Franz Weikmann, der sie seinerseits wieder weitergab an Gisela Meister, wandte er sich anderen Normungsthemen zu. Heute ist er noch Mitglied im DIN NI17.

Seine vielfältigen Erfahrungen sind natürlich auch in das Handbuch für Chipkarten eingeflossen. Für die mühsame, zeitintensive und umfangreiche Arbeit an diesem Handbuch, das praktisch zu einem unverzichtbaren Standardwerk geworden ist und auch in englischer und chinesischer Sprache vorliegt, hat die Jury den beiden Autoren Rankl und Effing einen Teil des in diesem Jahr gesplitteten Fraunhofer-Preises zuerkannt. Wie wir alle wissen, ist das Schreiben von solchen Büchern eine Frage des Idealismus, keine des kommerziellen Nutzens, wovon nahezu jeder Autor technischer Literatur ein Lied singen kann. Das Aufrechterhalten der Informationen in solchen Werken ist darüber hinaus eine Fleißarbeit, die spätestens nach der 2. Auflage nicht mehr mit dem Gefühl belohnt wird, "ein Buch geschrieben zu haben". Es braucht Enthusiasmus und oft ziemliche Überwindung, die neuen Informationen, die von einer zur nächsten Auflage entstehen, zu sichten, zu sortieren, zu selektieren und letztlich leserfreundlich darzustellen.

Ich darf daher Ihnen, Herr Rankl und Dir, Wolfgang, für dieses ausgezeichnete Werk danken und Ihnen Urkunde und Preis überreichen – verbunden mit der Hoffnung, dass das Werk noch möglichst lange immer wieder aktualisiert wird und es noch manche Auflage erfährt.

Laudatio von Bruno Struif, 5.2.2008