

Wolfgang Stecher

Die Sicherheit digitaler Daten am Beispiel
der elektronischen Gesundheitskarte (eGK)

Diplomarbeit

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



Diplomarbeit
zur Erlangung des akademischen Grades
Diplom Betriebswirt (FH)
an der
Fachhochschule Nordhessen
Studienzentrum Bonn

DIE SICHERHEIT DIGITALER DATEN
AM BEISPIEL DER
ELEKTRONISCHEN GESUNDHEITSKARTE (eGK)

eingereicht von
 cand. Diplom Betriebswirt (FH)
 Wolfgang Stecher

Düren, den 14.10.2008

„Die elektronische Gesundheitskarte wird die Qualität, die Sicherheit und die Transparenz der medizinischen Versorgung verbessern.“

[Ulla Schmidt,
Bundesministerin für Gesundheit]

INHALTSVERZEICHNIS

Abbildungsverzeichnis	V
Tabellenverzeichnis	VI
Abkürzungsverzeichnis	VII
1. Einleitung	1
2. Die Smart Card als Basis	2
2.1 Die elektronische Gesundheitskarte	3
2.2 Der Heilberufsausweis.....	5
2.3 Security Module Cards	7
2.3.1 Security Module Card Typ A	7
2.3.2 Security Module Card Typ B.....	8
3. Die elektronische Gesundheitskarte in der Praxis	10
3.1 Der Arztbesuch	10
3.1.1 Anmeldung des Patienten an der Rezeption	10
3.1.2 Behandlung durch den Arzt.....	13
3.2 Einlösen eines elektronischen Rezeptes	16
3.2.1 Einlösen eines elektronischen Rezeptes durch den Patienten selber.....	16
3.2.2 Einlösen eines elektronischen Rezeptes durch einen Dritten	17
3.3 Der Notfall	18
3.4 Änderung von Vertragsdaten.....	19
3.5 Zusammenfassung	20

4	Sicherheitsaspekte der elektronischen Gesundheitskarte	21
4.1	Das Lichtbild	21
4.2	Authentifizierung.....	23
4.2.1	Public Key Infrastructure.....	24
4.2.2	digitale Zertifikate	25
4.2.2.1	CV-Zertifikate (CVC)	25
4.2.2.2	X.509-Zertifikate	26
4.2.3	Zertifizierungsstelle	30
4.2.4	Secure Socket Layer / Transport Layer Security.....	31
4.2.5	Hashwert-Funktion	34
4.3	Kryptologie	36
4.3.1	symmetrische Verschlüsselung.....	37
4.3.1.1	(Triple-) Data Encryption Standard.....	39
4.3.1.2	Advanced Encryption Standard.....	39
4.3.2	asymmetrische Verschlüsselung.....	40
4.3.2.1	RSA-Verschlüsselung.....	41
4.3.2.1.1	Berechnung eines öffentlichen Schlüssels.....	42
4.3.2.1.2	Berechnung des privaten Schlüssels.....	43
4.3.2.1.3	Verschlüsseln einer Nachricht	44
4.3.2.1.4	Entschlüsseln einer Nachricht	45
4.3.2.2	ECC-Verschlüsselung.....	47
4.3.3	Hybride Verschlüsselung.....	49
4.3.4	Die Verschlüsselungsalgorithmen der eGK	51
4.4	Die Signatur.....	52
4.4.1	Arten von Signaturen.....	53
4.4.2	Funktionsweise einer qualifizierten elektronisch Signatur.....	54
4.5	PIN und PUK.....	55
4.6	Datenschutz bei der elektronischen Gesundheitskarte	56
5	Datensicherheit bei der elektronischen Gesundheitskarte	58
6	Abschließende Gesamtbetrachtung	64
	Literaturverzeichnis	X

Abbildungsverzeichnis

Abbildung 1:	Die aktuelle Krankenversichertenkarte	3
Abbildung 2:	Die elektronische Gesundheitskarte	3
Abbildung 3:	Heilberufsausweis	5
Abbildung 4:	Konnektor der Firma Siemens	8
Abbildung 5:	Kartenterminal mit HPC/HBA und eGK	14
Abbildung 6:	Die neue Krankenversicherungsnummer der eGK	29
Abbildung 7:	Symmetrische Verschlüsselung	33
Abbildung 8:	Asymmetrische Verschlüsselung	36
Abbildung 9:	Hybide Verschlüsselung	45

Tabellenverzeichnis

Tabelle 1:	Dateistruktur der elektronischen Gesundheitskarte	4
Tabelle 2:	Dateistruktur des Heilberufsausweises	6
Tabelle 3:	Dateistruktur einer Security Module Card Typ A	8
Tabelle 4:	Dateistruktur einer Security Module Card Typ B	9
Tabelle 5:	Übersicht: Anmeldung des Patienten an der Rezeption	12
Tabelle 6:	Übersicht: Behandlung durch den Arzt	15
Tabelle 7:	Übersicht: Einlösen eines elektronischen Rezeptes.....	17
Tabelle 8:	Übersicht: Der Notfall	19
Tabelle 9:	Übersicht: Änderung von Vertragsdaten	20
Tabelle 10:	Verschlüsseln einer Nachricht	44
Tabelle 11:	Entschlüsseln einer Nachricht	46
Tabelle 12:	Vergleich RSA – ECC	47

Abkürzungsverzeichnis

3DES:	Triple Data Encryption Standard, auch „Triple-DES“
AES:	Advanced Encryption Standard
AMTS:	Arzneimitteltherapiesicherheit
BE:	Behandlungsmanagement
BGBI:	Bundesgesetzblatt
BSI:	Bundesamt für Sicherheit in der Informationstechnik
CA:	Certification Authority
C2C:	Card to Card
CPU:	Central Processing Unit
CA:	Certification Authority
CRL:	Certificate Revocation List
CVC:	Card Verifiable Certificate
DES:	Data Encryption Standard
DN:	Distinguished Name
dt.:	deutsch (deutsche Übersetzung)
ECC:	Elliptic Curve Cryptography
eGK:	elektronische Gesundheitskarte
gematik:	Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH
EHIC:	European Health Insurance Card
engl.:	englisch (englische Übersetzung)
eRezept:	elektronisches Rezept
eVerordnung:	elektronische Verordnung
HBA:	Heilberufsausweis
HIDS:	hostbasierter Intrusion-Detection-Service
HPC:	Health Professional Card
IEC:	International Electrotechnical Commission
IP:	Internet Protocol
ISO:	International Organisation for Standardization
IT:	Informationstechnologie
LAN:	Local Area Network