Encrypted NFC emergency tags based on the German Telematics Infrastructure

Sebastian Dünnebeil, Felix Köbler, Philip Koene, Helmut Krcmar
Chair for Information Systems
Technische Universität München
Garching bei München, Germany
{sebastian.duennebeil | felix.koebler | philip.koene | krcmar}@in.tum.de

Jan Marco Leimeister
Chair for Information Systems
Universität Kassel
Kassel, Germany
leimeister@wi-kassel.de

Abstract— **Patient data, particularly emergency data, must be available to medical personnel within a short time frame and independent of potential interruption of (mobile) network connections. Additionally, medical data is confidential information that must not openly be available to anyone with physical access to the storage media. The planned German electronic Health Card (eHC) is supposed to hold emergency data. However, the eHC smart card will not always be available to caregivers in emergency situations, e.g., unconscious patient, since it cannot be duplicated, customized or read without physical contact. We therefore propose the SemTag prototype which utilizes Near Field Communication (NFC) technology to provide secure and quick access to medical information. Caregivers have the opportunity to store encrypted medical data on tags for a particular group of addressees, e.g., for emergency cases in home care environments. The tags can be placed on highly visible locations, e.g., entrance areas of homes and carried by the user in form of a token. Neither ubiquitous network access nor the unique eHC is necessary, to view emergency medical data within home care environments. Hence NFC tags can be regarded as a tool for information and identification alternative to distributed information systems for the collaboration of caregivers. This manuscript shows the technical storage and encryption process of emergency data on NFC tags. The technical feasibility, benefits, limitations and future research prospects of the prototype system are discussed.**

I. INTRODUCTION

In Germany, over 70% of health-related emergencies happen at home and more than half of these emergencies occur in an age group older than 65 years. Additionally, approximately 23% of the population keep a single household and therefore live alone [1]. In the case of an emergency happening in a single household, caregivers and emergency personnel currently face the problem of acquiring timely and critical medical data within a short time frame, since the single source of information is the patient.

Therefore, documented historical and medical patient data by patients' care givers and general practitioners is in such case not available to emergency personnel on site. The possible information asymmetry causes serious threats to the patients' health. Integrated health information systems have the potential to resolve the described information asymmetry, improve healthcare quality [2] and increase the effectiveness of health-related emergency services.

Accordingly, German health authorities are currently building a nationwide telematics infrastructure (TI) to connect care providers' information systems via a common network [3]. On the basis of the proposed TI, telemedicine services will offer communication, cooperation, and documentation features implemented as Web services to ensure pervasive availability and integrity of medical data among the German public health system. In the case of the proposed infrastructure, medical patient data is either stored on central servers, portable carriers (i.e., smart phones and tablet devices) or electronic Health cards (eHC).

A major goal of the introduction of eHC is the enforcement of patient centered medicine [4], standardization and transparency of medical treatment processes. A commission composed by an equal representation of health insurance providers, medical associations, and governmental institutions worked out a specification [5] to guarantee universal accessibility of standardized data beyond institutional boundaries. The efforts aim to ensure reduction of healthcare costs by, e.g., avoiding redundant examination and administration of patients, and improve patient safety [6].

According to calculations, telemedicine services provide added value of between 7.5 and 29.5 billion Euros until 2020. [7]. Major advantages of electronic medical services are (i) pharmaceutical drug safety, (ii) insurance data maintenance, (iii) electronic healthcare records (EHR) and (iv) emergency records.

Nevertheless previously conducted surveys have shown that a vast majority of physicians displayed a tendency to reject telemedicine services, planned to be introduced by the implementation of the TI [8, 9]. Numerous campaigns have been started by medical associations and politicians, calling for a moratorium on national TI initiatives with a central storage [10]. The main reasons for a rejection of the TI initiative are safety concerns regarding centrally stored patients' medical data. This reaction can be regarded as a common pattern towards telemedicine initiatives, which negatively affect the acceptance of telemedicine services by health care personnel

978-0-7695-4327-7/11 $26.00 © 2011 IEEE
DOI 10.1109/NFC.2011.18

IEEE computer society

[11]. As of today, all planned German TI services except the emergency record are postponed due to privacy concerns.

Hence we subsequently propose the SemTag prototype, which might contribute to the acceptance of the eHC system by implementing smart cards and Near Field Communication (NFC) technology, to enhance the security of technical utilities during medical emergencies. Dependency on centrally stored data is avoided by employing NFC as decentralized storage media. This manuscript shows a proposed prototype for the interaction of NFC tags and eHC, using signature, encryption and authentication features of the TI to improve and ensure a secure accessibility of patients' emergency data.

II. Related Work on Security in NFC Applications

NFC is a comparatively novel wireless communication technology that is primarily used for mobile payment and ticketing applications [12, 13], involving smart cards or mobile devices. It is a short range high frequency wireless communication technology that allows data exchange between devices that are about four inches apart [14, 15]. It is an extension of the ISO/IEC 14443 [16] proximity-card standard (such as contactless card, RFID, etc.) that combines the smart card and the reader into the same device. Due to the majority of NFC applications using sensitive data, e.g., bank account details, a comparatively large body of scientific literature deals with security aspects in NFC applications [12, 14-20].

NFC applications generally implement one of three distinct operation modes, defined by the NFC forum [21]:

- The *peer-to-peer mode* is used for a bidirectional communication between two NFC enabled devices. This mode enables the transfer of small amounts of information between mobile phones, e.g., contact and social networking information [22] or Bluetooth pairing information.
- In the *card emulation mode*, an NFC device acts as a smart card. In this mode, an external NFC reader cannot distinguish between an actual smart card and the NFC device. This mode is primarily used for payment and ticketing applications [13].
- The *reader/writer mode* enables the NFC device to "read and alter data stored in NFC compliant passive (without battery) transponders" [14]. These transponders or NFC tags are attached to *SmartPosters* and store additional information, e.g., a URL or location information for a location-based application [23-25].

There are multiple security issues, involved in all three operation modes, e.g., eavesdropping in peer-to-peer and card emulation mode [18], or denial of service (DoS) attacks with wrong NFC tags [12]. The relevant security issues for the proposed prototype however, involve the reader/writer operation mode in which sensitive, encrypted patient data is stored and read from a NFC tag. This entails that used NFC devices have a secure means to store a decryption key and decrypt sensitive data.

The storage of personal and sensitive data, e.g., a decryption key, necessitates the use of a tamper-prove secure element (SE) that provides a secure area for the execution of the NFC application (in case of the proposed prototype, the decryption) and protection for the data assets (in case of the proposed prototype, the decryption key) [20]. There are a few alternatives for these secure elements that can be divided into removable and non-removable variants. Non-removable secure elements are either integrated into the *baseband processor* of the mobile device or implemented as a piece of *embedded hardware*. However, since non-removable secure elements are soldered into the device, they have "to be replaced and personalized every time the user changes his/her handset" [20]. Removable variants of secure elements are, e.g., *secure memory cards* consisting of a memory card and a smart card or a *SIM* (Subscriber Identity Module) card. The use of SIM cards as secure elements for NFC applications can be argued, since SIM cards have a widespread dispersion in almost any mobile device. They provide a network connection, computing power for decryption algorithms and an integrated secure storage that makes it "possible to store keys, which aren´t accessible from the outside" [26]. Nokia introduced a novel NFC enabled mobile device, the Nokia 6216, which is suspended by today, to be the first to use SIM cards as a secure element for NFC applications.

III. Technical and Legal Framework of the German Telematics Infrastructure

In Germany the TI is used as the backbone for the mandatory eHC system. The infrastructure connects existing information systems of care providers via a common network [3]. Within the service-oriented architecture of the TI, centralized servers or decentralized components provide services, e.g., the encryption, digital signature and authorization of emergency data. The primary systems of the TI, i.e., information systems of medical institutions can utilize these services to communicate or collaborate with other care providers to maintain, review or share medical data objects. A local *Connector* component encapsulates all local services as encryption or card access and establishes a secure virtual private network (VPN) connection to the central servers if needed [5]. The *Connector* is connected to smart card readers, which allow access to the eHC. All individual related medical and administrative data uploaded to the central servers have to be encrypted, using a hybrid encryption method [5]. The private keys are located on the smart card chip of the eHC and cannot be extracted from there. Hence, they can be used for digital signatures and the encryption of medical data. Decryption of the access key happens within the microchip of the smart card after authorization with a Personal Identity Number (PIN). Patients can use public keys of health care institutions to encrypt the data for the receiver in order to grant them access to their personal medical data. Given, that the receiver of the medical data is a specific physician, the patient needs to access the physician's certificate, either located on the so-called health professional card (HPC), or available via a public key infrastructure. To encrypt the medical data for larger groups of caregivers, e.g., emergency physicians, institutional smart cards, called Smart Media Card (SMC) hold private keys of institutions [27].

The patient related requirements for the development of the TI are derived from legal conditions, given in the German code of social law [28]. Following the political goals of achieving high patient involvement into medical processes, patients are required to be in full control of their data. They have to agree on collection, usage and processing of their medical data for each service and care provider ex ante. In order to warrant this requirement, the medical data needs to be encrypted with the public key of the source patient and is therefore solely accessible with the private key stored on the patient's smart card [27]. It is furthermore a mandatory requirement for the TI that patients can view all their data and a record of its usage. These requirements apply in the same way to the proposed SemTag prototype system. To ensure that patients can exercise these legally granted rights, three types of patient interfaces were suggested for the TI:

1. All primary systems using the TI (stationed at medical sites, e.g., practices or hospitals) will have dedicated patient front-ends, comprising a separate trusted viewer (patient monitor) and a card reader [3].
2. Shared patient interfaces are provided as Point of Information (POI) terminals, set up in, e.g., hospitals, surgeries or common locations [3].
3. The initial architecture also suggested an Internet-based front end for home usage, i.e., Patient@Home [3].

However, the cost analysis for the TI indicates that the Patient@Home access will not be supported [7] in the medium term. Therefore the mandatory patient transactions cannot be supported via this interface. Thus, emergency data will only be processed within the practices of caregivers. Therefore it is necessary by law that the emergency tag is authorized by the patient at the caregivers' facilities. Additionally, the patient has to accept the authorization of the addresses personally.

IV. Use Case Scenario

In the following a use case scenario for a possible employment of the SemTag prototype is outlined. In the course of the use case scenario description we focus on an application within the home environment as described previously. We believe that the proposed scenario could be formulated in various versions by simply expanding the field and environment of application, e.g., public and hospital environments:

The sirens' sound of the ambulance vehicle yell through the streets of a Southern German suburb, while the ambulance crew is getting ready and prepared for an emergency which was registered and answered by the control room just some minutes ago. The ambulance crew received basic information on the circumstances at site and general status of the patient. The patient seems to live in a single household and fell unconscious while communicating with the control room's personnel. On site, the ambulance crew enters the patient's home with the help of the police which arrived slightly earlier. In addition to the medical (emergency) equipment, the ambulance crew is equipped with the SemTag prototype. The patient is found unconscious in the living room. While the first care is provided by a rescuer, the second rescuer uses the mobile device to "scan" the patient's wallet for her personal NFC equipped eHC or health information token. The application reads out the data in real time and provides the ambulance crew with health-related information of the patient who is still unconscious. Therefore the ambulance crew is aware that the patient is suffering from life threatening allergic reactions on certain medicines and adjusts their counter measures in helping the patient accordingly. The data stored on the NFC equipped eHC or health-information token was recently updated by the patient's general practitioner (with approval by the patient) and resembles the basic medical data set as implemented in the German TI. The data was decrypted in real time through the use of the NFC SE implemented in the mobile device by the ambulance personnel.

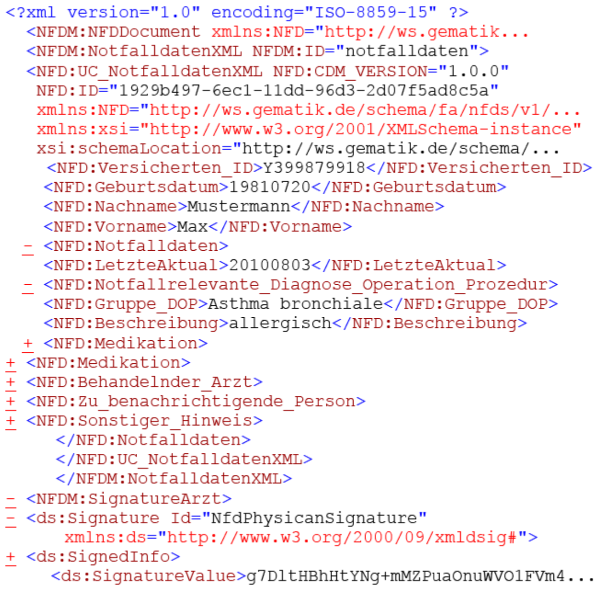
Requirements for the SemTag prototype system, as well as a technical description and potential process routine that supports the use case scenario are described in the following chapters.

V. Requirements for the SemTag Prototype

Requirements for the SemTag prototype were collected in the Bavarian testbed region for the eHC. A network of physicians comprising 500 ambulatory care physicians and an emergency facility were interviewed to elicit and verify the requirements [29]. The requirements entail that the emergency data for the SemTag prototype would be compiled by the patients' general practitioner from an extensive documentation of patient's historical medical data, stored within the practitioner's local information system. The patient would have to agree on the usage of emergency data and additional data that might be included by the patient's general practitioner. The signature of the document will guarantee that the content is reviewed and agreed on by both physician and patient. Within the network of physicians, it was recommended to agree upon a common location for the NFC tag to be stored in, e.g., the patient's wallet, or attached near the patient's entrance door. The authorization should include regional ambulance institutions that can equip their personnel with medical tablet devices running the SemTag prototype. The requirements elicitation shows that NFC tags should be updated, whenever the patient's general practitioner considers it necessary, e.g., change in medication treatment or new relevant diagnosis or possible allergies. After the general practitioner has updated a patient's emergency record, the patient can grant access to several individuals or groups.

VI. SemTag Prototype Technical Description

The SemTag prototype consists of a web application that can use the *Connector* and a smart card reader to access the private and public keys of care providers and patients. The application is suitable to create an Extensible Markup Language (XML) file compliant to TI emergency data specifications [30]. The application receives the XML schema from a server to validate whether the file is well formatted.



```
<?xml version="1.0" encoding="ISO-8859-15" ?>
  <NFDM:NFDDocument xmlns:NFD="http://ws.gematik...
  <NFDM:NotfalldatenXML NFDM:ID="notfalldaten">
  <NFD:UC_NotfalldatenXML NFD:CDM_VERSION="1.0.0"
   NFD:ID="1929b497-6ec1-11dd-96d3-2d07f5ad8c5a"
   xmlns:NFD="http://ws.gematik.de/schema/fa/nfds/v1/...
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://ws.gematik.de/schema/...
    <NFD:Versicherten_ID>Y399879918</NFD:Versicherten_ID>
    <NFD:Geburtsdatum>19810720</NFD:Geburtsdatum>
    <NFD:Nachname>Mustermann</NFD:Nachname>
    <NFD:Vorname>Max</NFD:Vorname>
  - <NFD:Notfalldaten>
    <NFD:LetzteAktual>20100803</NFD:LetzteAktual>
  - <NFD:Notfallrelevante_Diagnose_Operation_Prozedur>
    <NFD:Gruppe_DOP>Asthma bronchiale</NFD:Gruppe_DOP>
    <NFD:Beschreibung>allergisch</NFD:Beschreibung>
  + <NFD:Medikation>
+ <NFD:Medikation>
+ <NFD:Behandelnder_Arzt>
+ <NFD:Zu_benachrichtigende_Person>
+ <NFD:Sonstiger_Hinweis>
     </NFD:Notfalldaten>
     </NFD:UC_NotfalldatenXML>
     </NFDM:NotfalldatenXML>
- <NFDM:SignatureArzt>
- <ds:Signature Id="NfdPhysicanSignature"
      xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
+ <ds:SignedInfo>
     <ds:SignatureValue>g7DltHBhHtYNg+mMZPuaOnuWVO1FVm4...
```

Fig. 1. XML Emergency Data set including signature (own illustration)

All medical institutions apply the same schema for emergency data; therefore the syntactic and semantic interoperability can be guaranteed. The file contains XML tags for the patient's personal data, the insurance status and various medical parameters. Caregivers who created the document sign the content with their private keys (Figure 1).

VII. SemTag Prototpye Process Routine

Figure 2 illustrates the process routine of the proposed SemTag prototype which enables the secure exchange of emergency data between general practitioners, emergency personnel and patients. The *Connector* service provides a symmetric key which encrypts the emergency data record (1). Since decryption of the data set should be restricted to a specific group of caregivers, the key for decryption of medical data must be only available to them. Therefore the symmetric key is encrypted with public keys of the receivers by the patient (2). Afterwards the encrypted data and the encrypted keys are stored on one or multiple SemTag NFC tags (3). These tags can be placed in a highly visible location in the home environment and carried by the patient in order to enable a quick discovery by emergency personnel (4). A medical tablet device, equipped with a RFID and smart card reader, is used to read and decrypt the data stored on the NFC tag (5). The symmetric key is decrypted within the smart card of the physician (6) using the physician's private key (6). The decryption of the data with the symmetric key is facilitated by the SemTag software component in combination with the *Connector* (7). The emergency data is then displayed by the (mobile) device (8). The application uses the Extensible Stylesheet Language (XSL) to transform and render the XML documents to ensure uniform illustration for all physicians. The XSL files are provided by the German health authorities to all caregivers over the internet.

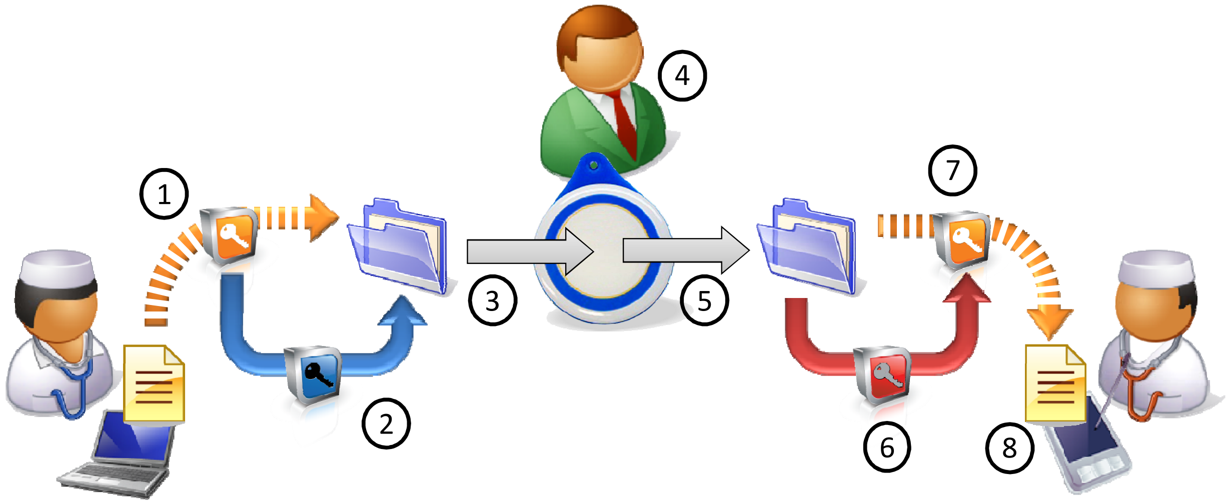


Fig. 2. SemTag Process Routine (own illustration)

To encrypt the data for a specific group of users, e.g. emergency personnel, the data can be secured with a Secure Module Card (SMC-B), which allows access to the data for the members of a specific institution. The size of the emergency data set is currently up to 7 kilobyte, which exceeds the storage capacity of most passive NFC tags, currently available on the market. However tags with up to 32 kilobyte have recently been introduced [31]. A large number of keys for different groups of receivers might require additional storage capacity on the NFC tag. Thus far, the proposed SemTag prototype is conceptualized for only one public key from a HPC. The HPC is used to encrypt and decrypt the data. Currently there is no public key infrastructure available to implement the authorization process within the prototype. Therefore all public keys of the physicians to be authorized must be read directly from the corresponding HPC. Currently the prototype implements all services provided by the TI. The prototype allows the dynamic inclusion of potential further services given that the service description is provided by authorities in the Web Service Description Language (WSDL).

VIII. Potential and Limitations

The eHC is not yet available to all health care institutions in Germany. The content of the emergency data is currently revised; therefore it is not yet possible to include the final emergency data set in the underlying manuscript. Currently passive NFC tags do not yet provide enough storage capacity to store comprehensive sets of emergency data and several encrypted keys at the same time. Despite these limiting factors, the system shows several advantages, compared to other options of patient data storage. Medical data stored on the eHC cannot be encrypted and read without physical contact. NFC tags could hold further data, which might improve the data logistics in care facilities or during home care of elderly people. Centralized electronic health records are not a feasible method for cooperation of caregivers in case of emergencies. Resistance among German medical personnel against centralized records led to the removal of this service from the eHC. Ubiquitously available (mobile) network access is not a likely option either, especially since latency time is a critical issue during emergencies [32]. Placing NFC tags in ideal locations for the processing of treatment or care, e.g., beside the entry door, can accelerate daily routines of caregivers.

IX. Future Research Prospects

So far, the status of the SemTag prototype is implemented as a proof of technology. The SemTag prototype demonstrates how NFC technology improves medical data accessibility, while utilizing the security features of the eHC. Further research could provide more use cases and is needed to evaluate the proposed infrastructure in a real world setting. Therefore we plan an evaluation of the SemTag prototype to gain insights into the potentials and pitfalls of the proposed system. The potential to securely exchange data via NFC tags can be utilized and embedded into various processes linked to healthcare [33]. In combination with the TI encryption and decryption services, the NFC peer-to-peer communication mode could provide a secure method of data exchange between medical devices.

X. Acknowledgment

The SemTag prototype was developed in the context of the research projects Mobile HybriCare and NuSiB. Mobile HybriCare is funded by the German Federal Ministry of Education and Research (BMBF - FKZ: 01FG08001). It is a joint project of the Technische Universität München and various partners. For further information, see www.mobilehybricare.de. NuSiB is funded by the Bavarian Ministry of Environment and Health.

References

[1] S. Prückner, M. Becker, H. Storf, and C. Madle, "Notfallmedizin - Medizin für eine alternde Gesellschaft. Epidemiologische Studie zum Kontext von Notarzteinsätzen bei alten Menschen " in *Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie*, Essen, 2009.

[2] P. Shekelle, S. C. Morton, and E. B. Keeler, "Costs and Benefits of Health Information Technology," 2006.

[3] Fraunhofer Institut, "Spezifikation der Lösungsarchitektur zur Umsetzung der Awendungen der elektronischen Gesundheitskarte," Fraunhofer, Projektgruppe FuE-Projekt, 2005.

[4] M. Marschollek and E. Demirbilek, "Providing longitudinal health care information with the new German Health Card - a pilot system to track patient pathways," *Computer Methods and Programs in Biomedicine,* vol. 81, pp. 266-271, 2006.

[5] gematik, "Einführung der Gesundheitskarte - Gesamtarchitektur." vol. 1.5.0: gematik GmbH, 2008.

[6] Bundesministerium für Gesundheit, "The German eHealth Strategy (Target and strategy, concept, legal framework, activities/roll-out plan, costs and return of investment, European perspective)," Berlin/Bonn, 2005.

[7] R. Bernnat, "Kosten-Nutzen-Analyse der Einrichtung einer Telematik-Infrastruktur im deutschen Gesundheitswesen," Booz Allen Hamilton GmbH, 2006.

[8] Techniker Krankenkasse, "Branchenbarometer E-Health," *F.A.Z. - Institut fuer Management-, Markt- und Medieninformation,* vol. 1, 2009.

[9] O. Kalthoff, N. Marsden, S. Kalthoff, and F. Drescher, "Abschlussbericht Evaluation der Einführung der elektronischen Gesundheitskarte in der Testregion Heilbronn," 2008.

[10] A. Tuffs, "Germany plans to introduce electronic health card " *BMJ.com Medical publication of the year,* 2008.

[11] C. M. Angst and R. Agarwal, "Adoption of Electronic Health Records in the Presence of Privacy Concerns: The Elaboration Likelihood Model and Individual Persuasion " *MIS Quarterly,* vol. 33, pp. 339-370, 2008.

[12] C. Mulliner, "Vulnerability Analysis and Attacks on NFC-Enabled Mobile Phones," in *Availability, Reliability and Security, International Conference on*, Los Alamitos, CA, USA, 2009, pp. 695-700.

[13] J. Ondrus and Y. Pigneur, "An Assessment of NFC for Future Mobile Payment Systems," in *Mobile Business, International Conference on*, Los Alamitos, CA, USA, 2007, pp. 43-43.

[14] G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger, "NFC Devices: Security and Privacy," in *Availability, Reliability and Security, International Conference on*, Los Alamitos, CA, USA, 2008, pp. 642-647.

[15] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "A Security Framework Model with Communication Protocol Translator Interface for Enhancing NFC Transactions," in *Advanced International Conference on Telecommunications*, Los Alamitos, CA, USA, 2010, pp. 452-461.

[16] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for*, 2010, pp. 1–8-1–8.

[17] Y. C. Chen, W. L. Wang, and M. S. Hwang, "RFID authentication protocol for anti-counterfeiting and privacy protection," in *Advanced Communication Technology, The 9th International Conference on*, 2007, pp. 255–259-255–259.

[18] A. J. Jara, M. A. Zamora, and A. F. G. Skarmeta, "An architecture based on internet of things to support mobility and security in medical environments," in *Proceedings of the 7th IEEE conference on Consumer communications and networking conference*, Las Vegas, Nevada, USA, 2010, pp. 1060-1064.

[19] G. Madlmayr, J. Langer, C. Kantner, J. Scharinger, and I. Schaumüller-Bichl, "Risk Analysis of Over-the-Air Transactions in an NFC Ecosystem," in *Near Field Communication, International Workshop on*, Los Alamitos, CA, USA, 2009, pp. 87-92.

[20] M. Reveilhac and M. Pasquet, "Promising Secure Element Alternatives for NFC Technology," in *Near Field Communication, International Workshop on*, Los Alamitos, CA, USA, 2009, pp. 75-80.

[21] N. Forum, "NFC Forum: Home." vol. 2010, 2010.

[22] F. Köbler, P. Koene, S. Goswami, J. M. Leimeister, and H. Krcmar, "NFriendConnector - Verbindung zwischen virtueller und realer sozialer Interaktion," in *5. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2010)*, Göttingen, Germany, 2010, pp. 139-153.

[23] F. Ko□bler, P. Koene, H. Krcmar, M. Altmann, and J. M. Leimeister, "LocaTag - An NFC-Based System Enhancing Instant Messaging Tools with Real-Time User Location," in *Near Field Communication (NFC), 2010 Second International Workshop on*, 2010, pp. 57-61.

[24] P. Koene, F. Köbler, P. Burgner, F. Resatsch, U. Sandner, J. M. Leimeister, and H. Krcmar, "RFID-based Media Usage Panels in Supportive Environments," in *Proceedings of the 18th European Conference on Information Systems*, Praetoria, South Africa, 2010.

[25] F. Resatsch, U. Sandner, J. M. Leimeister, and H. Krcmar, "Do Point of Sale RFID-Based Information Services Make a Difference? Analyzing Consumer Perceptions for Designing Smart Product Information Services in Retail Business," *Electronic Markets,* vol. 18, pp. 216-231, 2008.

[26] G. Kalman and J. Noll, "SIM as Secure Key Storage in Communication Networks," in *2007 Third International Conference on Wireless and Mobile Communications (ICWMC'07)*, Guadeloupe, French Caribbean, 2007, pp. 55-55.

[27] gematik, "Einführung der Gesundheitskarte - Gesamtarchitektur," gematik GmbH, 2008.

[28] Bundesrepublik Deutschland, "Sozialgesetzbuch (SGB) Fünftes Buch, Gesetzliche Krankenversicherung," 1988.

[29] ZTG Zentrum für Telematik im Gesundheitswesen GmbH, "Testregionen in Deutschland," 2009.

[30] gematik, "Facharchitektur Daten für die Notfallversorgung (NFDM)." vol. 1.7.0: gematik GmbH, 2008.

[31] Dressen, "Consideration for RFID technology," *ATMEL Application Journal,* p. 46, 2006.

[32] J. Leimeister, H. Krcmar, A. Horsch, and K. A. Kuhn, "Mobile IT-Systeme im Gesundheitswesen, mobile Systeme für Patienten," *HMD-Praxis der Wirtschaftsinformatik,* 2005.

[33] A. Schweiger, A. Sunyaev, J. M. Leimeister, and H. Krcmar, "Information Systems and Healthcare XX: Toward Seamless Healthcare with Software Agents," *Communications of the Association for Information Systems,* vol. 19, pp. 692-709, 2007.