Model-based Security Analysis of the German Health Card Architecture

J. Jürjens
Computing Department, The Open University, UK

R. Rumm
Munich, Germany

Summary

Objectives: Health-care information systems are particularly security-critical. In order to make these applications secure, the security analysis has to be an integral part of the system design and IT management process for such systems.

Methods: This work presents the experiences and results from the security analysis of the system architecture of the German Health Card, by making use of an approach to Model-based Security Engineering that is based on the UML extension UMLsec. The focus lies on the security mechanisms and security policies of the smart-card based architecture which were analyzed using the UMLsec method and tools.

Results: Main results of the paper include a report on the employment of the UMLsec method in an industrial health information systems context as well as indications of its benefits and limitations. In particular, two potential security weaknesses were detected and counter measures discussed.

Conclusions: The results indicate that it can be feasible to apply a model-based security analysis using UMLsec to an industrial health information system like the German Health Card architecture, and that doing so can have concrete benefits (such as discovering potential weaknesses, and an increased confidence that no further vulnerabilities of the kind that were considered are present).

Keywords: model-based development, UMLsec, health information systems, security, German Health Card.

1 Introduction

The use of health-care information systems has experienced an explosive growth. However, this usage carries critical risks concerning information security that are particularly significant for health-care systems, due both to the inherent vulnerability of the devices and the significant complexity of the architectures. In order to address these risks and enable secure health-care information systems, the security analysis has to be embedded in the development and management of the systems.

This work presents the results of the model-based security analysis of parts of the security architecture and security policies for the German Health Card. The security critical parts of the system were analyzed using UMLsec [1], a UML extension which allows the user to embed security related information into the system design, as well as to conduct automated security analyses on the model layer (see Fig. 1). The goal of this work was to gain experiences in the use of the UMLsec method in a health-care information systems context and to explore its benefits and limitations.

Model-based security design approaches such as UMLsec generally aim to be applicable in various kinds of application domains, relying on the fact that one can define the main security requirements such as secrecy, integrity, authenticity etc. independently of the application at hand. However, when applying UMLsec to a new application domain, a common experience is that usability can be increased by further extending or adapting the UMLsec notation, tools, or processes to the application domain. UMLsec and its tool-support and processes have been designed to facilitate such extensions. Thus, innovations from the current application include:

- an adapted application of UMLsec to health information systems, at the hand of a concrete application to the German Health Card architecture
- evidence that UMLsec is indeed suitable for application within this domain, and
- concrete results from the application to the German Health Card architecture, including two potential security weaknesses and a discussion of counter measures.

Detailed technical results omitted due to lack of space can be found at [2].

2 Related Work

UMLsec applications: Previous applications of UMLsec in industrial application projects already demonstrated the usefulness of tailoring the UMLsec notation or tools to an application domain. An application of UMLsec to information systems in an intranet at BMW is reported in [3]. There the use of single-sign-on mechanisms was central, so the application of UMLsec was targeted to demonstrating that it was used correctly within the system context. An application of UMLsec to mobile communication systems at O2 (Germany) is reported in [4]. Here, a new verification routine for UMLsec was developed to analyze data flows through such a communication architecture. Overviews on other applications of model-based security engineering in practice include [5, 6]. No previous application concerned health information systems, so the application presented here is novel.

More generally, there have been only few experience reports on applications of model-based development to health-care information systems focusing on security requirements, as discussed below. These approaches differ from UMLsec (and could thus not be used in our application here) in so far as they do not aim to formally and automatically verify UML models of architectures, business processes, and detailed protocol specifications against security requirements.

ISHTAR: An approach where based on UML models, security services can be integrated into advanced systems architectures is presented in [7]. Ongoing work for the German health telematics platform using a model-driven architectural framework and a security infrastructure based on Electronic Health Records and multifunctional Electronic Health Cards is presented in [8].

SECTET: Usage scenarios for access control in contemporary health-care scenarios are presented in [9] and it is shown how to unify them in a single security policy model. Based on this model, the SECTET framework for Model Driven Security [11] is specialized for health-care scenarios, including access control policies, their target architecture, and model-to-code transformations. It is extended to the operating system-level and application-level security mechanisms in [12].

Business processes: An e-health case-study on analyzing secure business process specifications with respect to goals capturing the functional, security and trust requirements of IT systems and their operational environments is presented in [13]. The CORAS approach for model-based risk assessment [14] has, in particular, been applied to telemedicine systems.

Deployment: A framework to rapidly develop, simulate, and deploy clinical information system (CIS) prototypes based on model-based design techniques and high-level modeling abstractions is presented in [15].

3 Security Challenges in Health Information Systems

We discuss the particular characteristics of health information systems regarding security requirements, and how software engineering and software management processes have to be adapted to the application domain of health information systems in order to deal with the resulting challenges.

3.1 Characteristics of Security for Health Information Systems

As part of the German health-care reform, the current health insurance card is being upgraded to an electronic health card. On it, data on patient investigations, drug regulations, vaccinations and emergency data are stored. The aim is among other things to improve medical care and the prevention of drug incompatibilities and duplication of investigations. The goal is to maintain the security of this very highly sensitive data. It is expected that by 2009 all people insured through the state health insurance will receive an electronic health card. It replaces the existing (non-smartcard based) health insurance card. The health card will be further developed so that it is capable of including health data, in addition to its administrative functions. Therefore, it is necessary to develop the health card as a smart-card that is capable of authentication (electronic identity verification), encryption and electronic signature. This is designed to ensure maximum security of the data.

The architecture of the German Health Card was designed and implemented by an industrial consortium called "bIT4health" (short for "better IT for better health"), which consists of the companies IBM Germany, SAP, the smart card vendor ORGA, the patient file specialist InterComponentWare, and the Fraunhofer-Institute for Process Organisation.

The bIT4health architecture (cf. Fig. 2) consists of the following system nodes: Primary Systems node, Multi-functional Card Terminal, bIT4Health Platform, bIT4Health Applications node, and bIT4Health Integrator Backend. The client applications on each Primary Systems node are connected to the bIT4Health Platform through the bIT4Health Connector subsystem and over an Internet connection which is protected by a VPN channel and a firewall. Each Primary Systems node is connected to one or more multi-functional Card Terminals, each of which has one or more card slots that support any of the cards involved in the bIT4Health transactions: the Electronic Health Card itself (abbreviated EHC, or eGK for the German "elektronische Gesundheitskarte"), the Security Module Card (SMC), and the Health Professional Card (HPC, or HBA for the German "Heilberufsausweis"). The bIT4Health Platform contains the following subsystems: Security Services, Generic Common Services, and bIT4Health Common Services.

In this application, we investigated the security aspects of this architecture using model-based security analysis with UMLsec, in particular regarding attacks on:

- Data integrity: protection against unauthorized manipulation.
- Confidentiality: protection against unauthorized knowledge.
- Authenticity and non-repudiation protection.

3.2 Selection of security mechanisms

The freedom of choice in the selection of security mechanisms for the applications of telematics systems and infrastructure for the bIT4Health consortium is rather restricted.

3.2.1 Availability requirements on central IT systems

The Health Modernization Act [16] describes no alternatives or emergency substitutes to the services of the telematics infrastructure. The use of these services is mandatory in all use cases for the management of contract data, prescription, and treatment. Accordingly, the provision of personal data is absolutely critical for a successful fulfillment of orders, and treatment requires constant availability over 24 hours every day of the year. The availability requirement on the data implies of course the availability necessary for the proper processing hardware and software components of the IT system.

3.2.2 Availability requirements on decentralized IT systems

The influence of the bIT4Health consortium on the security of the decentralized IT systems of service providers is relatively low. A certain role is played by the bIT4Health connector, which is the interface between bIT4health client applications and the telematics infrastructure. It provides the runtime-environment for business components, which implement generic and reusable business logic, and offers interfaces for the use of central services of the telematics infrastructure and of local services and devices (such as the card terminal). The connector in particular provides many local services for data security for the primary systems of doctors and pharmacists. The availability of local systems is, however, not guaranteed: The IT systems found in German doctors‘ offices, hospitals and pharmacies are based on a large variety of hard- and software with hardly any overarching commonalities. The responsibility for the existing hardware, operating systems, primary system, applications and networks, as well as its security standards and administration, rests with the health practitioners themselves. With the introduction of the Electronic Health Card, however, the availability of the decentralized IT systems receives a much greater importance: Doctors are no longer in a position to treat patients without the support of the electronic contract data, treatment and prescription management, and pharmacists require their local IT infrastructure for the redemption of electronic prescriptions. Although the success of the health reform based on the Electronic Health Card depends on the security systems of the service providers, this topic has been insufficiently considered in the professional circles of doctors and pharmacists.

3.2.3 Other security requirements

Also in the selection of security mechanisms for authentication, data integrity and confidentiality of information, the bIT4Health consortium only had limited freedom of choice. Numerous laws, e.g. the German Data Protection Act [17] or the Health-care Modernisation Act [16], together with compulsory security standards (such as standards and architectures for e-government applications [18], or IT security on the basis of the Common Criteria [19]), contain very specific requirements on the implementation. Although these standards describe the use of digital signatures and public key infrastructures in detail, there is a definition gap e.g. regarding the question of which advanced transactions or qualified signatures should be used.

3.2.4 Requirements on Digital Signatures

According to the German Signature Act [20], so-called "Qualified Signatures" must have a valid signature created using a secure signature-creation device. In principle, the two basic requirements of qualified digital signatures must be satisfied by the German Health Card architecture: All digital signatures are generated directly on the signature cards (either the Health Professional Card e.g. of the doctor or pharmacist, or the Electronic Health Card owned by the patient, or the Security Card modules part of the application systems), which according to the German Signature Act are considered secure signaturecreation devices. All signature cards are issued with individual certificates. These certificates must be issued by a trusted authority. For use in the health sector, this means that the root certificate was issued by the German Regulatory Authority for Telecommunications and Post. From this, further subordinate certificates can be certified within the telematics infrastructure.

The application use cases of the digital signatures, however, further require the ability to provide a proof of the time of creation of a signature (e.g. for the proof of a diagnosis or the date of an electronic prescription). To this end, time-stamps are used. Again, a distinction is made between normal and qualified time-stamps. The latter must meet the requirements of the Signature Act and the Signature Regulation [21], and also be certified by the Regulatory Authority for Telecommunications and Post. For the practical implementation, this means that qualified time-stamps have to be issued by a central time-stamp service within the telematics infrastructure. "Normal" time-stamps do not have to meet the requirements of the Signature Act and the Signature Regulation. The bIT4Health consortium made the assumptions for the solution architecture [22, 23] that altogether, annual processing of 3.173 billion documents is expected, which results in a significant challenge for the signature creation. The lower security of normal time-stamps could however lead to a lack of legal certainty for medical transactions particularly in the case of legal disputes.

3.2.5 Conflicting requirements: usability and application security

As explained in the previous section, the use of qualified time-stamps offers a much greater application security than the use of normal time-stamps. However, it requires an Internet connection at the time of signature creation. There are use case scenarios in which according to the current wide-spread state of technology in practice, an online connection is not possible, such as the creation of an electronic prescription at a home visit of a practitioner. Except for the qualified time-stamp on the digitally signed prescription, this can be carried out offline on a notebook with a card terminal, the application software and the bIT4Health connectors. Although in the longterm we can expect a wide availability of mobile Internet connections, in the short-term we still have to permit an offline scenario.

4 Model-based Security Analysis of the German Health Card Architecture

We now explain how model-based security analysis was used at the German Health Card architecture. We illustrate this with a few representative examples.

Starting from a given set of security requirements (i.e. the relevant security policy), which focuses on health information system security, we conducted an analysis to identify the parts of the UMLsec framework which are most suitable to model these requirements and allow for a subsequent security analysis.

4.1 Security Analysis using UMLsec

Model-based Security Engineering (MBSE, [1, 24, 25]) provides a formally based approach for developing security-critical software where recurring security requirements (such as secrecy, integrity, authenticity and others) and security assumptions on the system environment can be specified either within a UML specification, or within the source code as annotations (cf. Fig. 1). The goal is for example to be able to perform an analysis of a newly defined security design pattern, but also to be able to analyze whether an established security design pattern has been concretely instantiated in a given design.

Various analysis plugins in the associated UMLsec tool framework [26] (Fig. 3) generate logical formulas for the execution semantics and the annotated security requirements. Automated theorem provers for first-order logic (FOL) automatically establish whether the security requirements hold. One can also use this framework to implement verification routines for the constraints of self-defined stereotypes. The semantics for the fragment of UML used for UMLsec is defined in [1] using so-called UML Machines, which is a kind of state machine with input/output interfaces and UML-type communication mechanisms. On this basis, important security requirements such as secrecy, integrity, authenticity, and secure information flow are defined.

4.2 Security analysis of the public key signature procedures

The UML models of the German Health Card architecture have been formally verified against the security requirements using the UMLsec analysis tools presented in earlier sections. We present some representative findings.

4.2.1 Mutual authentication

The automated analysis of the modeled application scenario of the mutual authentication smart card did not detect any vulnerabilities. The documentation of the security architecture does, however, permit technical variants of the use case. The used multifunctional card terminals need not necessarily have two smart card slots (i.e. places where smart-cards can be inserted into the terminal). Since an exchange of cards during the authentication process would find little acceptance in practice, it must also be possible to have two card terminals. Furthermore, in many doctors' offices several PC workstations are used in the primary system where applications are installed, but which do not have separate card terminals. In this case, it has to be assumed that the card terminals are connected via a computer or a network (cf. Fig. 4). However, the primary systems and networks of practitioners' offices are not standardized and are not sub ject to any security regulations or certifications. Under these circumstances, it is significantly easier for an attacker to manipulate the communication between the Health Professional Card and the Electronic Health Card using a man-in-the-middle attack [27]. This threat could be countered by sub jecting the practitioners' systems to security regulations (although enforcing this would of course be a significant effort).

Attacks on the PIN authorization procedure were not investigated. According to the bIT4Health specifications, only secure card terminals may be used. Since the PIN does not leave the multifunctional card terminal at any point in time, this requirement should cover the risks.

4.2.2 Confidentiality and integrity of the communication channel

The UMLsec tool based security analysis showed that the method chosen to protect the confidentiality and integrity of the communication channel presented no security gaps. Even if the smart cards inserted in separate card terminals communicate over insecure channels, the encryption in conjunction with the cryptographic checksums should provide adequate security.

The security of the procedure does, however, depend on the secure exchange of the pre-master secrets k1 and k2, from which the actual session key is calculated. Should an attack on the mutual authentication procedure succeed, this would also put the security of the communication channel at risk. The cryptographic protocol that secures this exchange was therefore specified and analyzed using the UMLsec tools.

The results from the UMLsec analysis tools showed that this exchange is in fact secure as used within the architecture.

4.2.3 Non-repudiation of medical transactions

For the communication between the Health Professional Cards of the doctor and the pharmacist and the Electronic Health Card of the patient it is assumed that, prior to the exchange of data, all communication partners are identified using a PIN-based procedure and mutually authenticated, as specified in the previous section. The encryption of the communication channel and verification of the data integrity is made in accordance with the procedures described in previous sections.

The exchange of digital signatures for an electronic prescription is specified as a sequence diagram in Fig. 5. The variables used in the model are explained as follows:

Data of the Health Professional Card (HPC):

- inv(k hp c) private signature key

Symmetric session keys:

- hash(k1::k2) Shared between HPC of practitioner and Electronic Health Card (EHC), constructed from pre-master secrets k1 and k2.
- hash(k3::k4) Shared between HPC of pharmacist and Electronic Health Card (EHC), constructed from pre-master secrets k3 and k4.

Key targets for the attacker:

- prescri Prescription data

We shortly explain a walk-throw of this sequence diagram, and the UMLsec specific notation. The transaction is started with the primary system application displaying the prescription data (at the practitioner's office). It then sends a hash of the data to the practitioner. The practitioner views the prescription data and signs this hash using his Health Professional Card (HPC), and performs a symmetric encryption of this signature using a key shared between HPC of practitioner and the Electronic Health Card (EHC) (which is constructed as the hash of the concatenation of two pre-master secrets k1 and k2, although this detail is not important here). Also, the primary system application sends the prescription data to the EHC card. The card decrypts the message from the practitioner and verifies the integrity of the signature using the public key of the practitioner. It then computes the hash of the prescription data received from the primary system application and compares it with the one received from the practitioner. If all these checks are satisfied, the card submits the prescription and the practitioner's signature of it to the pharmacist, signed with a symmetric key shared between HPC of pharmacist and the EHC (constructed similarly to the earlier symmetric key, although again the details are not important here). The pharmacist then decrypts the message from the card and verifies the integrity of the practitioner's signature using the public key of the practitioner. If it is valid, the medication is dispatched to the patient, and the pharmacist sends a message to the card confirming this.

The automated security analysis of this model using UMLsec uncovered a possible attack on the confidentiality of the prescription data that is sent out. The bIT4Health specifications do not require any encryption for the transmission of electronic document prescription onto the Electronic Health Card (as can be seen in the fourth message in Fig. 5). Only the transmission of electronic signatures between the Health Professional Card and the Electronic Health Card is protected. In most cases, the multifunctional card terminal will be directly connected to PCs with the primary system application (e.g. via USB or RS232). An attack on that connection seems relatively unlikely. However, it is perfectly permissible to connect the card terminal through a network and possibly other computers. Since these heterogeneous network and system environments cannot be assumed to be completely secure, an attacker could thus intercept the unencrypted prescription data. Such an attack on the prescription data is very worrying indeed in particular from data protection legal aspects. If the attacker manages to get repeated access to the system of the health practitioner, there is the possibility of a comprehensive data collection, which can be abused for economic benefits (e.g. by insurance companies). This threat could be significantly reduced by defining an operational constraint which prevents the card terminal from being connected through a network or other computers. The manipulation of the prescription itself, on the other hand, seems to be successfully prevented. A manipulation of the data would not only be recognized by the auditing service, but also by comparing the different hash values of the document and of the transmitted signature.

5 Discussion and Conclusions

The use of UMLsec was generally appropriate and reasonably practical for this application. The method showed that, apart from two issues that could be resolved by operational constraints, the system under consideration is indeed secure with respect to the security requirements and adversary model that were considered: An adversary who uses modest means to eavesdrop on and manipulate communication over communication networks that may themselves be insufficiently secured (such as plain Internet connections, or local area networks in practitioners' offices). This result is non-trivial, given the high number of insecure or untested systems. We are not aware of any issues that the approach did not notify but which were nevertheless present.

To our knowledge, this was the first application of UMLsec to health-care information systems. It differs from previous applications in so far as the healthcare specific properties of the application had to be taken into account. These include security properties derived from data protection on the patient data (in particular confidentiality). They also include integrity requirements on the prescription data which must withstand scrutiny in court, should it come to a trial about medical misconduct (for example, by making use of digital signatures that comply with the relevant standards). These specific properties in particular required a particular emphasis in the way UMLsec was applied, and on the system parts which had to be focused on.

Note that UMLsec, much as UML itself, is in a first instance mainly a notation with associated tool-support, and does not prescribe, for example, a particular development process to be used. The advantage of this is that it is applicable in varying contexts and application domains. Since different application domains may pose specific challenges which can be addressed particularly well by using a certain development process, it also means that if one wants to profit from such a tailored development process, a certain tailoring in the way UMLsec is used may be beneficial. The work reported in this paper provides experiences from an application of UMLsec in the health information system domain, which will be useful for defining a UMLsec development process targeted to this application domain.

Note that this paper does not aim to be a large-scale controlled empirical study; instead its aim is to present a particular application, and the experiences learnt from it, in some technical depth, rather than providing a quantitative overview. New scientific insights gained from this application include the following conclusions, which are significant also because our work seems to be the first application of UMLsec of health information systems, and the first application of a formal model-based security analysis to the German Health Card architecture.

- The results indicate that it can be feasible to apply a model-based security analysis using UMLsec to an industrial health information system like the German Health Card architecture.
- They further indicate that doing so can have concrete benefits (such as discovering potential weaknesses, and an increased confidence that no further vulnerabilities of the kind that were considered are present).

6 Conclusions

This paper presented a report on the deployment of the UMLsec method in an health information system context. A model-based security analysis was conducted on the German Health Card architecture currently in development. The focus was on the application's security mechanisms and policies. Using the UMLsec notation, the security analyst was able to annotate his models with information regarding the security critical aspects of the system in a concise and clear way.

The model-based security analysis revealed (at two concrete examples for weaknesses) that there is a certain security risk arising from the heterogeneous hardware and software systems of doctors, pharmacists, and hospitals which could not completely be secured by the local bIT4Health software components. Many practitioners' offices are either too small or they lack the awareness of the secure use of IT systems. Whether this vulnerability will be exploited in practice remains to be seen when the system is put to wide-spread use (currently expected for 2009, after a number of delays).

The application also demonstrated that developers familiar with the UML notation should have no problem to learn and use UMLsec quickly. Furthermore, by embedding the security analysis directly into the IT development and management process, and by providing automated security analysis tools, a better understanding and clearer communication of these issues is made possible.

Acknowledgements: Part of this work was performed while the authors were at TU Munich. The first author is supported by the Royal Society through the Joint International Project with TU Munich on „Modelbased Formal Security Analysis of Crypto-Protocol Implementations“. Comments from the reviewers which helped to significantly improve the presentation of the paper are gratefully acknowledged.

References

[1] Jürjens J. Secure Systems Development with UML. Heidelberg: Springer; 2004.

[2] Jürjens J, Rumm R. Security analysis of complex telematics systems at the hand of the electronic health card: Experimental results. 2007. http://mcs.open.ac.uk/jj2924/umlsectool/Applications/Healthcard.

[3] Best B, Jürjens J, Nuseibeh B. Model-based security engineering of distributed information systems using UMLsec. 29th International Conference on Software Engineering (ICSE 2007), Minneapolis. IEEE Computer Society, 2007; 581-590.

[4] Jürjens J, Schreck J, Bartmann P. Model-based security analysis for mobile communications. 30th Intern. Conference on Software Engineering (ICSE 2008), Leipzig. ACM, 2008; 683-692.

[5] Apvrille A, Pourzandi M. Secure software development by example. IEEE Security & Privacy 2005; 3,4: 10-17.

[6] Jürjens J, Model-based security engineering for real. 14th Intern. Symposium on Formal Methods (FM 2006). LNCS 2006; 4085: 600-606.

[7] Blobel B, Nordberg R, Davis J, Pharow P, Modelling privilege management and access control. International Journal of Medical Informatics 2006; 75,8: 597-623.

[8] Blobel B, Pharow P. A model-driven approach for the German health telematics architectural framework and security infrastructure. International Journal of Medical Informatics 2007; 76, 2-3: 169-175.

[9] Alam M, Hafner M, Memon M, Hung P, Modeling and enforcing advanced access control policies in healthcare systems with SECTET. In Sztipanovits et al. [10].

[10] Sztipanovits J, Breu R, Ammenwerth E, Bajcsy R, Mitchell J, Pretschner A (eds.). Workshop on Model-based Trustworthy Health Information Systems (MOTHIS@Models), 2007. Contributions available at http://mothis.isis.vanderbilt.edu .

[11] M. Alam, M. Hafner, and R. Breu, Model-driven security engineering for trust management in SECTET. Journal of Software 2007; 2,1: 47-59.

[12] Agreiter B, Alam M, Hafner M, Seifert J.-P., Zhang X. Model driven configuration of secure operating systems for mobile applications in healthcare. In Sztipanovits et al. [10].

[13] Lopez H, Massacci F, Zannone N. Goal-equivalent secure business process re-engineering for e-health. In Sztipanovits et al. [10].

[14] Fredriksen R, Kristiansen M, Gran B, Stølen K, Opperud T, Dimitrakos T. The CORAS framework for a model-based risk management process. SAFECOMP. LNCS 2002; 2434: 94-105.

[15] Mathe J, Duncavage S, Werner J, Malin B, Ledeczi A, and Sztipanovits J. Implementing a model-based design environment for clinical information systems. In Sztipanovits et al. [10].

[16] Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz / GMG). Germany, Bundesgesetzblatt 2003; I: 2190.

[17] Bundesdatenschutzgesetz (BDSG). Germany, Bundesgesetzblatt 2007; I: 201 and 1977; I: 66.

[18] Bundesministerium des Innern. Standards und Architekturen fur E-Government-Anwendungen (SAGA Version 4.0). Germany, Mar. 2008.

[19] Bundesamt für Sicherheit in der Informationstechnik, IT Sicherheit auf Basis der Common Criteria - ein Leitfaden. Germany, 2005. Available at http://www.bsi.bund.de/cc/cc_leitf.pdf .

[20] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz / SigG). Germany, Bundesgesetzblatt 2001; I: 876 and 2007; I: 179, 185.

[21] Verordnung zur elektronischen Signatur (Signaturverordnung / SigV). Germany, Bundesgesetzblatt 2001; I: 3074 and 2007; I: 2631, 2671.

[22] eHealth card - bIT4Health architecture. http://www.dimdi.de/static/en/ehealth. 2007.

[23] German health professional card & security module card specification v2.1.0. 2006. http://www.dimdi.de/dynamic/de/ehealth/karte/downloadcenter/technik/kartenspezifikation/spez_testphase_archiv/spez_testphase_archiv_1_egk/hpc_p3_smc_v2-10.pdf .

[24] Jürjens J, Sound methods and effective tools for model-based security engineering with UML. 27th Int. Conf. on Softw. Engineering (ICSE 2005), St. Louis. ACM 2005: 322-331.

[25] Jürjens J, Shabalin P. Tools for secure systems development with UML. Intern. Journal on Software Tools for Technology Transfer 2007; 9: 527-544. Invited submission to the special issue for FASE 2004/05.
[26] UMLsec tool. 2001-08. http://mcs.open.ac.uk/jj2924/umlsectool.
[27] Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons, 2001.

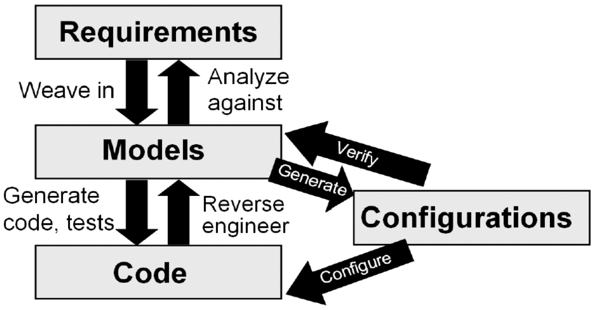

Figure 1: Model-based Security Engineering

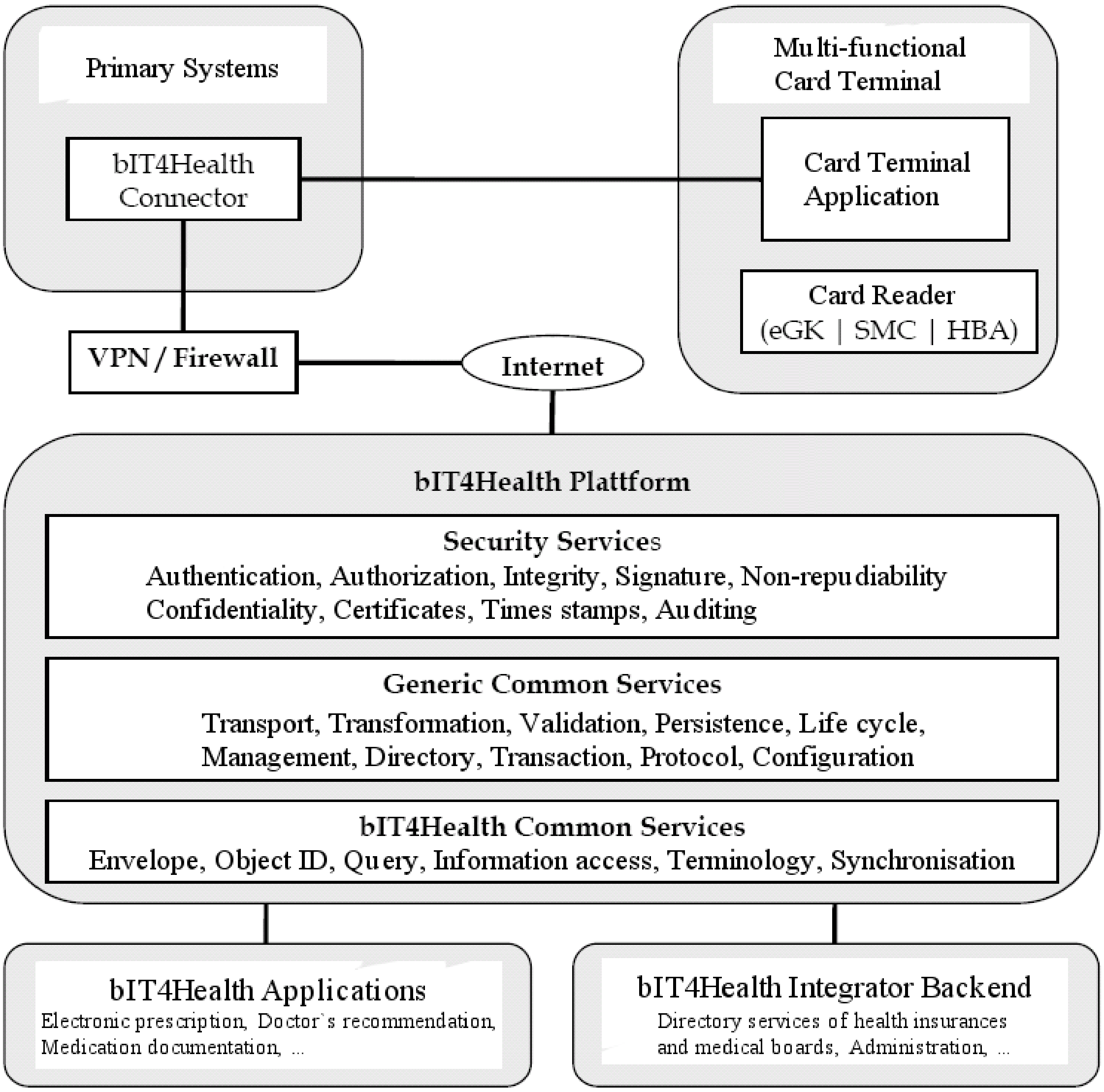
Primary Systems
bIT4Health Connector
Multi-functional Card Terminal
Card Terminal Application
Card Reader (eGK | SMC | HBA)
VPN / Firewall
Internet
bIT4Health Plattform
Security Services
Authentication, Authorization, Integrity, Signature, Non-repudiability
Confidentiality, Certificates, Times stamps, Auditing
Generic Common Services
Transport, Transformation, Validation, Persistence, Life cycle,
Management, Directory, Transaction, Protocol, Configuration
bIT4Health Common Services
Envelope, Object ID, Query, Information access, Terminology, Synchronisation
bIT4Health Applications
Electronic prescription, Doctor`s recommendation,
Medication documentation, ...
bIT4Health Integrator Backend
Directory services of health insurances
and medical boards, Administration, ...

Figure 2: bIT4Health Architecture

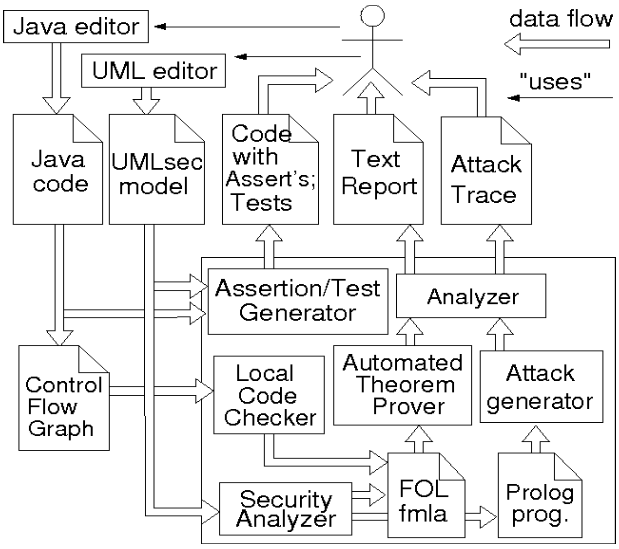

Figure 3: Model-based Security Tool Suite

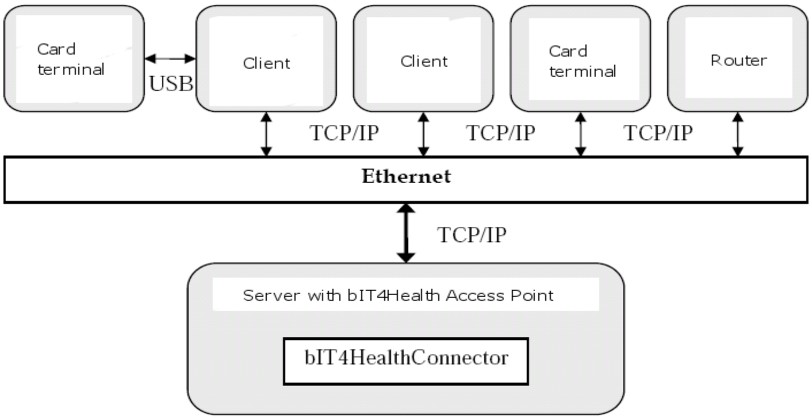

Figure 4: bIT4Health Connector in the Thick Client Environment

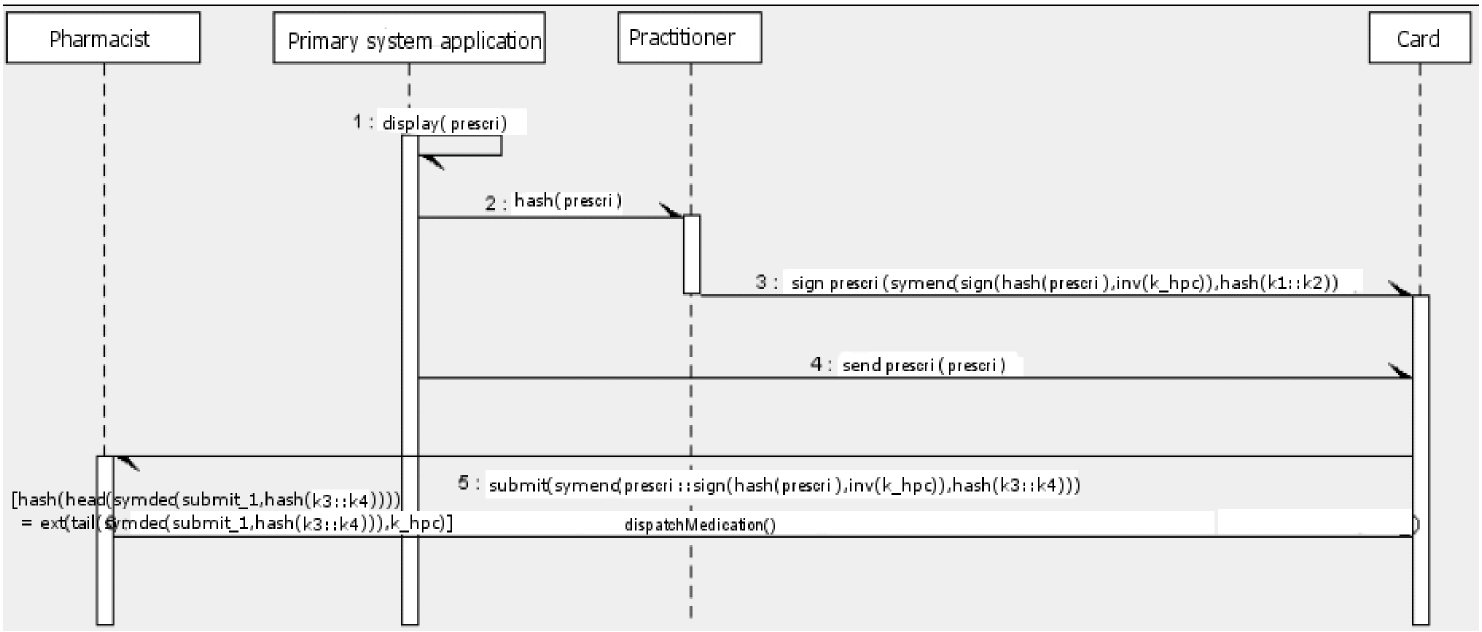
Pharmacist
Primary system application
Practitioner
Card
1 : display(prescri)
2 : hash(prescri)
3 : sign prescri (symenc(sign(hash(prescri),inv(k_hpc)),hash(k1::k2))
4 : send prescri (prescri)
5 : submit(symenc(prescri ::sign(hash(prescri),inv(k_hpc)),hash(k3::k4)))
[hash(head(symdec(submit_1,hash(k3::k4))))
= ext(tail(symdec(submit_1,hash(k3::k4))),k_hpc)]
dispatchMedication()

Figure 5: Electronic prescription transaction