Die approbierte Originalversion dieser Diplom-/Masterarbeit ist in der Hauptbibliothek der Technischen Universität Wien aufgestellt und zugänglich.

http://www.ub.tuwien.ac.at

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology.

http://www.ub.tuwien.ac.at/eng

FAKULTÄT FÜR !NFORMATIK

Faculty of Informatics

Maintaining privacy of medical data

Analysis of existing approaches with special focus on ePrescription

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur/in

im Rahmen des Studiums

Information and Knowledge Management

eingereicht von

Manuela Sellner, Bakk.techn.
Matrikelnummer 0026108

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer/in: O.Univ.Prof. Dipl.-Ing. Dr. A Min Tjoa
Mitwirkung: Dipl.-Ing. Mag. Dr. Thomas Neubauer

Wien, 22. April 2014

(Unterschrift Verfasser/in)

(Unterschrift Betreuer/in)

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.ac.at

Declaration of independence

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit - einschließlich Tabellen, Karten und Abbildungen -, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 22. April 2014 Manuela Sellner

Contents

Chapter 1

Introduction

Today the public health system in most of the industrial nations provides a solid medical health care for the citizens. Mainly due to the advancing age of the working population it is on the one hand necessary to reduce the costs but on the other hand the quality of medical treatment should be kept up. Consequentially public health care is a big problem welfare states have (cf. [88], [57]).

The financing of a high-quality medical care gets more and more difficult and so the pressure on the compulsory health insurance fund grows. A possible way to reduce costs is improving the communication between people who provide medical services for a patient. A central repository where all medical data of a patient can be stored would make it easier for medical services to enter the whole anamnesis of a person. So it is guaranteed that all necessary medical information about a patient is available not only concerning the personal medical history but also possible allergies or other relevant data (cf. [87]).

Moreover an electronic health record (EHR) is not only a summarization of a patient's medical history, it also provides a faster and targeted access to the data. Additionally a faster assessment to new medical treatments is possible which is a benefit for the patients and for the research (cf. [3]).

To complete the information of an electronic health record it is also necessary that prescriptions are documented electronically too. Consequentially in the anamnesis a doctor can find an exact documentation of every prescribed medicament and also over-the-counter drugs the patient has received which can provide useful information for her further medical treatment. Particularly in a case of emergency a hospital needs to know immediately which drugs a person is consuming or which allergic reactions a certain medicament could possibly cause. Furthermore it would be easier for the patient to change the doctor or the pharmacy because her whole medical data is available to the successor. In general ePrescription is a good possibility to investigate and document interactions between different drugs, allergies and food intolerances and makes medication more efficient (cf. [52]).

However it has to be ensured that the privacy of this sensitive data is guaranteed because in Austria privacy is declared as a basic right by law and the patient has to agree explicitly on the usage of her medical data ([15]). For the regularization of the electronic data transfer between governmental offices and citizens the e-government law was passed in 2004 ([23]).

So the protection of the patient's privacy has to be guaranteed because a possible abuse of this sensitive data could affect the patient's life in a serious way. For example the publishing of a person's HIV-infection could lead to social exclusion. Another realistic setting is that an employer or an insurance company would have great interest in such information to use it for their own purpose. In addition it has to be kept in mind that also the doctor's privacy has to be protected because health insurance companies would be interested in the aggregate prescription patterns to do research in cost control matters (cf. [3]).

1.1 Objectives

The base of this thesis is provided by the evaluation results of the existing approaches. This thesis is going to evaluate how far existing approaches are able to meet the requirements concerning privacy of ePrescription. Some examples of abuse of sensitive data are described in chapter 4. To avoid such scenarios it is important to provide a security mechanism to assure that nobody unauthorized has access to this kind of data. In chapter 3 the technique of pseudonymization is analyzed which means that the identification of a user is avoided by replacing its identification data with a pseudonym. For the allocation to the origin identifier the secret encrypted key is needed, which has to be kept safe.

There are different existing approaches how pseudonymization can be used for securing sensitive medical information and they all have their strengths and weaknesses. So it is necessary to identify these weaknesses and to develop some methods of resolution (cf. [88]).

On grounds of these results it is possible to define on the one hand the weaknesses of the evaluated systems and on the other hand as an outcome of this the requirements for an appropriate solution. Consequentially this is the necessary input for finding a solution in adapting an existing concept in a way that these shortcomings will be corrected. This in turn will show a possibility how to implement a secure way for the process of ePrescription - avoiding the shortcomings of other implementations - which could serve as input for other research establishments.

1.2 Research Questions

The following research questions were specified for this thesis:

- What is the current state of the art of the utilization and development of systems and concepts that provide ePrescription services in Austria and in international comparison?
- Which requirements and needs should a solution fulfill, which uses the concept of pseudonymization to assure privacy in this context?

- How could a method of resolution look like and which difficulties have to be overcome?

To answer the above defined research questions a comprehensive literature research will be done to describe and evaluate the existing systems and concepts and to find and analyze their strengths and shortcomings. The choice which of these approaches will be selected for evaluation depends on some predefined selection criteria. So it is necessary that the investigated system/concept has a focus on providing security for the privacy of the medical data and that the process of ePrescription is covered.

The process of evaluation is based on some comparison criteria:

- Architecture of the System (data storage, technical requirements)
- Workflow of ePrescription process (different work steps and use cases)
- Security techniques and – measures for providing privacy (incl. recovery procedures of lost/stolen keys or access authority, possible offense scenarios)
- Actual status (prototype, productive operation, test run)

On the basis of this evaluation it shall be possible to identify the different shortcomings of the analyzed approaches.

1.3 Outline

This thesis can be divided into two parts. The first part will provide general knowledge about different terms and concepts. The chapter 2 describes the definition of privacy and which requirements have to be achieved to maintain it. Furthermore the (inter)national regularization of privacy by law is analyzed and possible legal loopholes or missing legal regularization and the resultant impact of privacy is uncovered. In the following chapter 3 the definition of pseudonymization is given and moreover it is described which different implementation versions in consideration of security measures can be found. Additionally the possibilities of using pseudonymization in the eHealth sector is discussed. In addition in chapter 4 there is the concept of ePrescription explained and for what reason ePrescription is used. Furthermore the process sequence is described.

The second part evaluates the existing concepts and systems according to the evaluation criteria which are defined in chapter 5. Based on the evaluation result the found shortcomings are identified and summarized in chapter 6. In the end the requirements and needs that should be covered by an appropriate solution are discussed.

Chapter 2

Privacy fundamentals

To guarantee privacy of medical data it is a prerequisite to know what privacy is about and how it can be secured. This chapter should provide this kind of information and furthermore it describes the regulatory framework especially in Austria to give an overview about the legal regulation that has to be respected.

2.1 Definition of Privacy

Over the intervening years there were many people who tried to put the definition of privacy into words. Some of the resulting definitions are listed here:

- "the right to be let alone" [7]
- "the extent to which we are known to others, the extent to which others have physical access to us, and the extent to which we are the subject of others' attention" [34]
- the right of people "to determine for themselves when, how, and to what extent information about them is communicated to others" [113]
- the right of "giving people property rights in information about themselves and letting them sell those rights freely" [83]

2.2 Securing of Privacy

Spiekermann describes an experiment which was carried out at Humboldt University in Berlin with the ambition to investigate the privacy preferences of the participants and their behavior during online shopping. The surprising result showed that the majority of the participants, who had declared their privacy attitude as higher–than–average, readily hand over a lot of personal data during the shopping activity. So they act against their self–reported privacy attitude. Thus this experiment shows the importance of privacy protection because of the monitored mismatch of what people said and their related behavior (cf. [96]).

There are three existing approaches to maintain and protect privacy:

- Technology
  There are some published technical standards which are mainly popular in the United States where many companies are using them (2.3). The underlying assumption is that people, who are privacy conscious, trust in these standards and so the companies have an advantage in competition (cf. [96]). So technical standards are closely associated with the principle of self–regulation, because the former is used to achieve the latter. In the following section 2.3 the most popular standards are introduced in detail. Furthermore there are some other technological approaches of privacy protection which are described in chapter 3.

- Self–regulation
  This approach is used in the United States, which contrary to the European Union only prohibit explicitly some data processing, whereas in the other cases the self–regulation is committed to the market economy. These settlements make it difficult to transfer data between the United States and European countries. According to a growing attitude of privacy among their customers many companies take part on privacy seal programs e.g. TRUSTe or BBBOnline (cf. [96]), which are introduced in the following section of this thesis.
  Altogether it has to be said, that self–regulation is not really effective for protecting privacy, because collected user data in general is seen as a profitable resource by the business world, which should be used for new business purposes. Self–regulation would only be useful if the whole industry would participate and this an unrealistic scenario. Another heavy problem of self–regulation is the difficulty to prove that a company has hurt the privacy of a customer, because the customer often has no clue who misused his personal data and in which way this had happened (cf. [8]).

- Regulation by law
  In particular European countries predominantly rely on regulation of privacy by law. But a huge disadvantage of this approach is that passing a law needs a lot of time, meanwhile the technology which should be regulated is long existing. So regulation often lags behind technological progress (cf. [96]).
  A further disadvantage of legal regulation is that it's only valid inside the borders of the law–giving country. Although this restrictive approach on the other side of the coin demands effective sanctions if law is violated. Unfortunately they are often missing, because of lacking qualification of the data protection officials or a lack of capacities (cf. [27]).
  The legal situation according to privacy in the case of Austria is explained more precisely in section 2.4. Naturally it is a fact that existing laws don't prevent criminals from committing crimes. Privacy is not only threatened by companies that are using personal data for their own purposes, also criminal subjects have interest in misuse of personal user data, if they are able to realize profit with it (cf. [8]).

The following figure 2.1 gives an overview about the different methods currently used to protect privacy. The main branches are presented by the three approaches mentioned above. The node which shows the regulation of privacy by law contains several samples of laws which are trying to control privacy protection all over the world. As mentioned above self–regulation and regulation by law are not able to assure privacy, at the best they are basic conditions for privacy protection.

Only technology provides ways to protect privacy effective and to give potential wrongdoers a hard time. In the next section 2.3 some of the technical standards shown in this figure are described more closely. The main focus of attention lies on the technique of pseudonymization, which will be analyzed more precisely at chapter 3. Also the listed pseudonymization approaches are described in detail and they partly combine some of the illustrated technology categories in their functionality e.g. blind signatures.

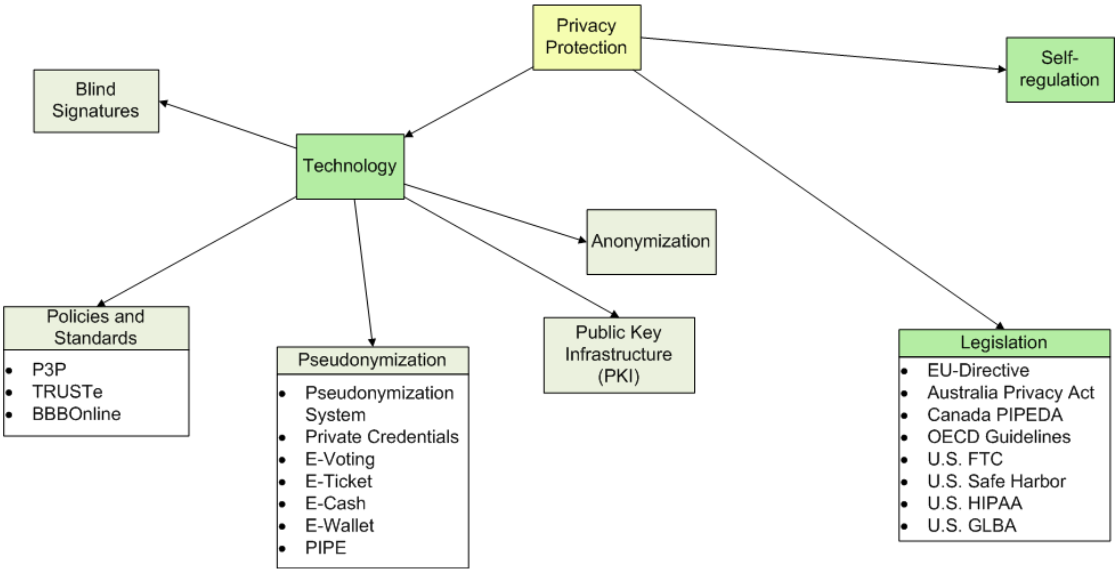


Figure 2.1: Means for Privacy Protection

2.3 Technical standards to obtain privacy

Because of the increasing consciousness of privacy in the mind of people different surveys confirmed the assumption that companies, which are using privacy standards and privacy seals, seems to be more trustable for customers. Though it has to be added that these surveys only asked for the attitude of the customer and not for their actual behavior (cf. [96]).

Technical solutions are able to make privacy policies of companies more transparent to the customers, but it is necessary that they are used by a critical mass of companies to become widely accepted (cf. [27]).

Nevertheless there are some representative privacy standards, though at this point only P3P and TRUSTe are introduced briefly. Of course there are several other technical solutions (e.g. BBBOnline), but in this chapter only an overview is given of how privacy can be protected.

Platform for Privacy Preferences (P3P)

The P3P–Project is a privacy standard supported by the World Wide Web Consortium (W3C) which should enable users to get information about the privacy policies used by websites. So it is apparent for the user which kind of data is captured, for which purpose and how long it is stored. This is automatically done on behalf of the user with an interoperable client program (integrated in the user's web browser) that communicates with a server program which represents the privacy policy on the website (cf. [2]).

How does an interaction between client and service program look like? In the first step a service sends a machine–readable proposal in which the organization identity and the privacy policy is declared. The user agent (e.g. a web browser or a browser plug–in) can automatically parse this proposal and compares it with the user's privacy preferences. If the proposal matches the user's preferences the user agent sends a PropID back, which acts like a fingerprint, otherwise the proposal is rejected. If an agreement is reached the user agent can store this information, so it is possible to refer to past agreements, which helps to accelerate this process at the next time (cf. [84])

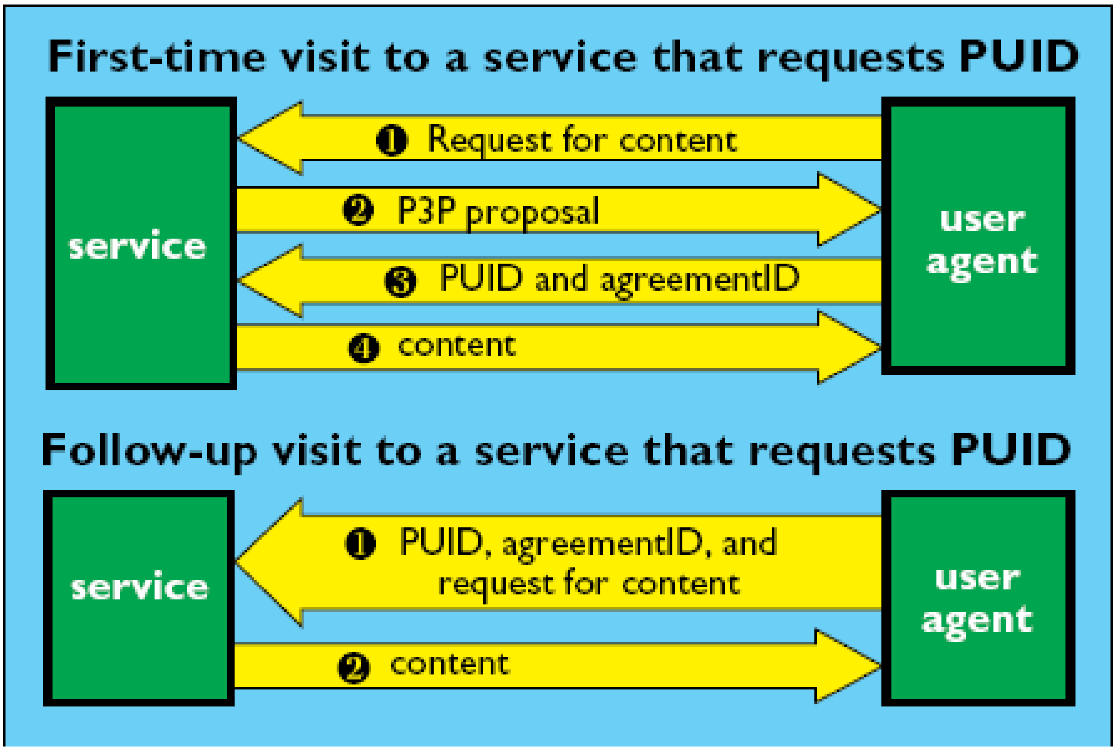

First-time visit to a service that requests PUID
service
user agent
❶ Request for content
❷ P3P proposal
❸ PUID and agreementID
❹ content
Follow-up visit to a service that requests PUID
service
user agent
❶ PUID, agreementID, and request for content
❷ content

Figure 2.2: Interaction between service and client [84]

TRUSTe

TRUSTe is a non–profit, privacy seal program for websites. The websites which use TRUSTe are showing a special trust–mark to signalize users that they agreed in disclosing their information gathering and further potential dissemination of the collected data which is ensured by a trustful third–party instance.

The following core requirements have to be met to get a TRUSTe license:

- Notice
  On the website there has to be a privacy statement in evidence which includes information about the site's information gathering and dissemination practices.
- Choice
  There should be a possibility for the user to negate the use of their personal information by third–parties.
- Security
  The personal data of the user has to be protected against loss, misuse and unauthorized alteration.
- Data quality and access
  The user needs to be able to correct her personal information.
- Verification
  All personal information has to be treated in accordance with the privacy policy.

(cf. [5])

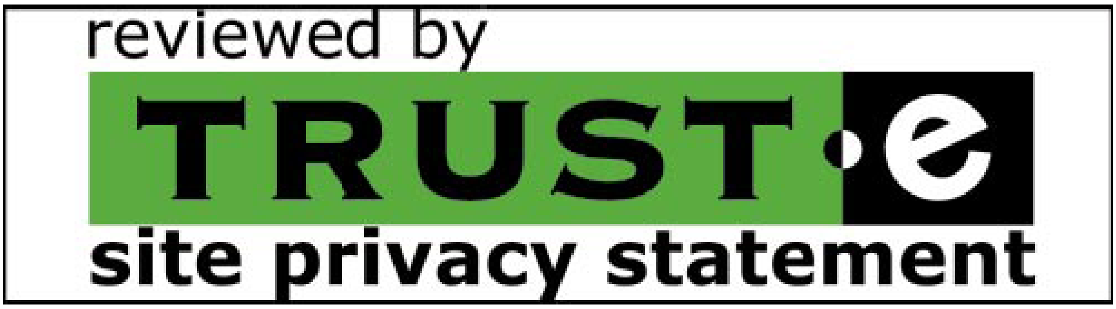


Figure 2.3: TRUSTe Privacy Seal [5]

2.4 Legal regulation of privacy in Austria

In Austria privacy is regulated by different laws and these laws in turn are strongly influenced by basic conditions and directives of the European Union. Today much information about people is collected and recorded electronically. So for protecting privacy of a person it is necessary to define rules which kind of data and how long it is allowed to be stored and in particular which part of the data may be seen by a third party. Also it has to be secured that only authorized people have access to personal data and that these people are identified correctly. In this chapter the most important legal regulations concerning privacy are introduced.

One of the earliest formulations of a person's right of privacy is found at article 12 in the Universal Declaration of Human Rights [110]:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."

The following sections shall give an overview about the legal regulation of privacy in Austrian and European law.

Datenschutzgesetz (DSG 2000)

The Austrian Data Protection Act was coming into effect on 01.01.2000 and is the most important regulation in this area in Austria. It is based on the European Community Directive 95/46/EG and its goal is the harmonization of the protection of personal data within European Community (cf. [15], [22]).

Already in §1 I 1 DSG [15] the fact that a person's privacy has to be protected is defined as

> "Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such protection."

Furthermore in §1 III DSG it is written that everybody has the right to know which personal information is processed, where it originates from and to whom it may be transferred. For illegally processed data the erasure can be demanded (cf. [15]).

Simplified it can be said that the kind of data, which can give conclusion about a person's identity can threaten privacy and has to be protected more intense. In §4 I 1 DSG the term of "personal Data" is defined as information which can be related to an identified or an identifiable person. Moreover the §4 II DSG classifies 'sensitive data', which covers information about political, religious or philosophical beliefs, health or sexual orientation as data deserving special protection.

The special protection of sensitive data is described in §9 I–XIII DSG where in general the usage of this kind of data is only allowed under certain conditions e.g. when a person has given her consent explicitly (§9 IV) or if the data is required for medical purposes and it is only used by persons who have a duty of secrecy (§9 XII) (cf. [15]).

An important information about the responsibility for the used data gives §14 I DSG, which indicates the need and legal obligation to protect this data from loss, malicious mischief and unauthorized access. On the other side is has to be assured that data is only used in a proper way. To guarantee this the adopted measures has to be lean on the current state of the technology and thus resulting costs has to be adequate to the kind of data and the related risks of their use (§14 II 9 DSG) (cf. [15]).

The confidentiality of data — in particular the principle of holding confidential data secret — is regulated in §15 I 1 DSG. Employees who have access to confidential data due to their workaday life have to keep their knowledge about it secret. Data may be only transmitted due to an explicit directive of the employer (§15 II 1 DSG).

According to §26 I 1,3 DSG every concerned person has the right to get information about data which is related to her. This information includes the data itself, the origin, potential recipients of data transmission and the purpose of the data usage. Furthermore the person has the possibility to refuse the usage of her personal data if no legal prescription exists (§28 I 1 DSG) or to demand erasure of unlawfully used data (§27 I 1,2 DSG) (cf. [15]).

In 2010 an amendment for the DSG was passed which assigns the responsibility of implementing privacy protection to the Federal Government — to disburden the states (cf. [15]).

Gesundheitstelematikgesetz (GTelG)

The Austrian law of Electronic Health Data Transmission is part of the Austrian law of Health Care Reform and went into effect on 01.01.2005. This law defines additional rules for health data protection and its electronic transmission. The current legal regulation of data protection is not compromised but supplemented (§1 I–III GTelG) (cf. [41]).

At first the term of health data should be announced. In §2 I GTelG it is defined as personal data according to the Austrian Federal Act which is reviewed in section 2.4. Furthermore this term includes data of physical and psychical constitution, prescribed drugs, former diagnoses and therapies and all kind of health care utilization (cf. [41].

If health service provider want to access or hand over personal health data this is only allowed if the concerning health service provider and the potential recipient are able to prove their identities (using an electronic certificate) (§4 I 1 GTelG) and their roles (classification of the health service provider) (§2 IV 1 GTelG) (cf. [41]).

In addition the concept of an eHealth index is described, which facilitates the identification of the registered health service providers due to their identities and roles (cf. §§9,10 GTelG). The registration for this index is voluntary and for free (§11 I GTelG). Alternatively identification is also possible without the registration in the eHealth index but with a corresponding electronic certificate as above–mentioned (§5 III GTelG) (cf. [41]).

Naturally the health service provider is obligated to ensure the confidentiality and integrity of the health data. Confidentiality according to §6 I GTelG means that the health service provider has to encrypt the data to avoid that a third party is able to access it. In §7 I GTelG it is appointed that the integrity of health data has to be provided by electronic signatures (cf. [41]).

In 2012 a further regulation was passed — the Gesundheitstelematikverordnung (GTelV) — which became effective in January 2013. This regulation defines the minimum requirements for encryption techniques and electronic signatures, furthermore it lists the possible classifications for health service providers (cf. [42]).

eGovernment–Gesetz (E–GovG)

The Austrian Federal Act on Provisions Facilitating Electronic Communications with Public Bodies entered into force on 01.03.2004 and is the legal foundation for electronic data exchange with public bodies. Mainly this law should improve the legal protection according to automated data processing (§1 II E–GovG) (cf. [23].

The interaction of the citizens with public bodies requires the correct authentication and identification via the citizen card, which is containing an electronic signature related to an unique identification with a natural person (cf. §§2,4 E–GovG) (cf. [23]).

In §3 I 1 E–GovG it is clearly said, that the access to sensitive data, which is described at section 2.4 as data deserving special protection, is only provided if the unique identity and authenticity of the person is clearly detected. The term unique identity designates a person as unmistakably distinguished from all other persons (§2 II E–GovG) and authenticity means the purported author of a declaration of intent is also the actual author (§2 V E–GovG). Both can be proved by means of the electronic signature of the citizen card (§4 II,IV E–GovG) (cf. [23]).

Additionally it is possible for the card owner to authorize a representative for specified actions. A reference for this authorization has to be noted at the representative's citizen card (§5 I E–GovG) (cf. [23]).

ELGA–Gesetz (ELGA–G)

The necessity for a law, that adapts the legitimate situation in Austria so that an electronic health record would become realizable, was already acknowledged in a feasibility study for the implementation of an electronic health record in Austria. This study also listed the key points this law would have to resolve e.g. the formal definition and purposes of this electronic health record (ELGA), patient rights, storage and documentation responsibility and so on (cf. [52]).

The ELGA Act was passed in December 2012 and became operative in January 2013. It regulates the data privacy measures when using electronic health data (cf. [25]) such as:

- Definition of opt–out possibility
  Patients can refuse to participate in ELGA and are able to make all or parts of their medical data inaccessible, this opt–out can be revoked at any time (cf. §15, ELGA–G).

- Unambiguous identification of patients and health service providers (cf.§§18,19, ELGA–G)

- Responsibility and methods for health data storage, data access rights, data usage rights and documentation required (cf. §20-22,24, ELGA–G)

- Penalty for abuse or careless handling of health data (cf. §25, ELGA–G)

Chapter 3

Pseudonymization

Pseudonymization is a technique to uncouple sensitive data with the related person by assigning an unique label to this person without uncovering her identity (cf. [81]). Vice versa it is possible to reverse this operation. It can be used for securing privacy in the process of ePrescription and due to the fact that one of the research questions of this thesis gives attention to this technique this chapter provides an overview what the meaning of pseudonymization is and how it is used and implemented in practice.

3.1 Meaning of pseudonymization

To understand what pseudonymization means it is necessary to explain the meaning of anonymization first, because they are depending on each other. With anonymization it is possible to change personal data in a way that this data cannot be used anymore to identify the person in the background. In this process all personal properties, which could reveal the identity of a person are deleted or changed. The process of anonymization is irreversible, that means it is impossible to re–identify the concerned person again (cf. [46]).

By contrast pseudonymization connects personal data with an unique person, but nothing is published about the identity of this person. It is necessary that a third party holds the secret to reallocate a person to the appropriate data, but for other people, who have no access to the secret, it is not possible to find out which identity lies behind the pseudonym. Attention should be paid to the fact, that because of the retraceability of the pseudonym to the physical person it is often necessary that the person has to sign a letter of agreement before the personal data can be used for pseudonymization (cf. [81]).

Pseudonyms can be classified according to the degree of anonymity they offer. There are three criteria of how to determine the strength of anonymity (cf. [79]):

- The attacker model which describes opposite to whom anonymity should be kept up, how much the anonymity is affected when several parties are working together and sharing their information and if there are instances who are allowed to uncover one's identity in exceptional cases.

- With a special kind of aggressor in mind how big is the estimated number of actual attackers under a certain number of potential attackers. So for example among 10 people is especially one person, who is a customer in a publishing house for anti–constitutional literature. So a possible way might be to question the loyalty to the constitution of all these persons.
- The possibility to gain information about someone by observing the chaining of activities performed by this person, which is summarized under the term of linkability. So linkability should be hold as low as possible for protecting privacy but for some reasons it can be necessary to a certain extent e.g. multiple communication with the same partner.

According to the classification above pseudonyms can be divided into different groups. A person pseudonym is a long–term used pseudonym which was applied for many activities. Due to the linkability between the pseudonym and the person it can be categorized into 3 subgroups (cf. [79]):

- Public person pseudonym
  The relation to the identity of the person is known (e.g. telephone number).
- Non–public person pseudonym
  The relation to the identity of the person is only known by some people (e.g. account number).
- Anonymous person pseudonym
  Nobody except the owner knows the relation to the identity of the person.

The disadvantage of non–public and anonymous person pseudonyms is that after using the pseudonym for a while person–related information is collected and eventually it is possible to link the pseudonym with a concrete person. With a role pseudonym this scenario can be avoided because it is not connected with the person but with the executed role. Role pseudonyms differentiates between role–relationship pseudonyms, which are used for numerous transactions, and transaction pseudonyms, which are just used for a single transaction. Role pseudonyms reduce the linkability to a minimum but increment the degree of anonymity (cf. [79], [78]).

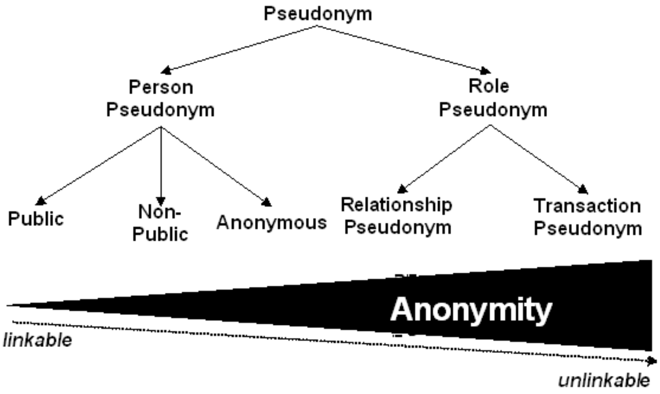


Figure 3.1: Classification of pseudonyms [79]

3.2 Architecture of pseudonymization

There are different existing approaches of how pseudonymization can be implemented. They differ in the way the pseudonyms are created and shared, which security measures are taken to protect the pseudonyms and who is the owner of the secret (cf. [88]).

There are different possibilities for creating pseudonyms (cf. [80]):

- Deterministically
  Creation of the pseudonym with means of one way functions or hash functions from invariant data by a centralized party.
- Arbitrarily
  The user creates the pseudonym from her secret with a fixed one way algorithm.
- Randomly
  The pseudonym is chosen for free or created at random. This kind of pseudonym has to be saved at a reference list to be considered as reusable.

Furthermore an approach can vary in its secret owner. Who is authorized to be owner of the secret and in which cases is she allowed to uncover the person's identity behind the pseudonym? Ideally the owner of the secret is similar to the user but this is not reasonable in every case. So there has to be a confidential third party who acts as the secret carrier. (cf. [80])

This third party is responsible for creating pseudonyms in a deterministic way or for storing the pseudonyms in a code book. A code book has the advantage that it is easier to handle but on the other side it can become really large and also the code book has to be kept safe from attackers. By using deterministic methods only the key has to be protected but also in this case it has to be ensured that the key cannot be spied out (cf. [80]).

Different pseudonymization models

There are many possibilities to categorize the variable approaches of pseudonymization. The society of insurance science and design (GVG) has published an overview of the different pseudonymization models in its management paper (cf. [46]) which should be analyzed closer at this point.

Basically the models differ among each other in the data management and the number of stages:

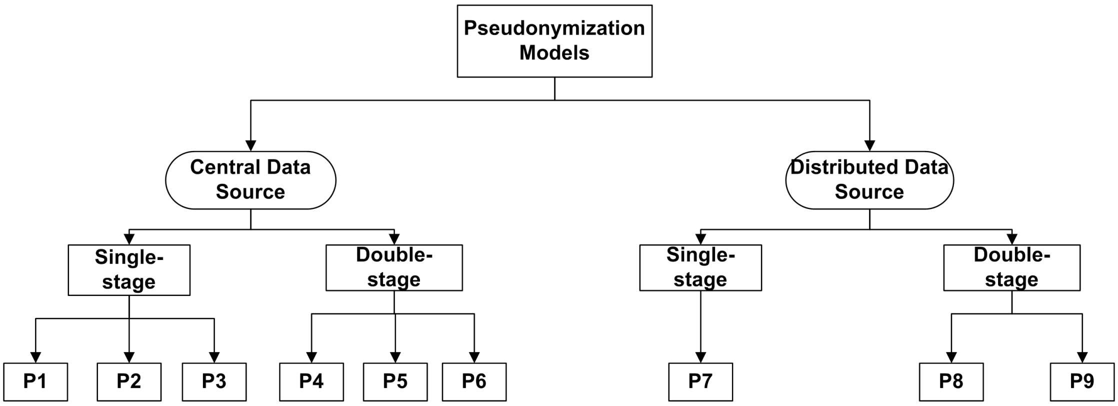


Figure 3.2: Pseudonymization Models [46]

The central data management does not mean that data is also physically kept at a central location but that it is under control of a single institution. In distributed data management the data is managed by different parties nevertheless it is possible to recall the data by the means of strict access rights. The number of stages of a pseudonymization model means how many times the pseudonymization process is executed by different institutions while data is transported from the data source to the place where the data is collected for further use. Indeed if pseudonymization is executed several times by the same institution it is only counted as one stage, because such a procedure would not provide more security (cf. [46]).

- Model P1
  For each data source the same pseudonymization procedure with the same key is used before all the data is merged together at the institution for data collection. This means that every single data source knows the pseudonymization procedure and the key which increments the risk of publishing this information. Furthermore the model provides a really high degree of linkability because the data sources could conclude from the user data to the personal data. Thus this model is too unsafe to be used in practice.

- Model P2
  The model P2 schedules that only the institution, which is responsible for the data collection executes the pseudonymization process and therefore has full control over the data. The resulting disadvantage of the model is obvious: the data collection institution could retrieve every information from the merged data as it has access to the plain text user data.

- Model P3
  The encrypted user data and the unencrypted personal criteria are sent to a trusted third party (TTP), which executes the pseudonymization without knowledge about the user data. The data collection institution is able to decrypt the user data and reallocate it to the pseudonyms, but it has no access to the identification data. The only party which can execute de–pseudonymization is the data collection institution, so the key is only known at this place. Unfortunately for this model it is necessary to share the personal data with an external institution.

- Model P4
  Like at the model P1 every data source executes the same pseudonymization procedure with the same key, which leads to a higher risk of getting known outside these institutions. The unencrypted user data and the pseudonyms are sent to the data collection institution, which executes a second pseudonymization. So none of these two institutions is able to re–identify the pseudonyms at its own. Indeed the data collection institution might be able to draw a conclusion from the unencrypted user data to personal data because it knows the data sources.

- Model P5
  Every data source executes the pseudonymization using the same key. The pseudonyms and the encrypted user data are transferred to the TTP, which executes a second pseudonymization. The data collection institution decrypts the received user data and reallocate it with the pseudonyms. This model provides a higher security but at the expense of higher administrative costs.

  Another variant of this model can reduce the administrative effort while providing a good security level. Thereby the data sources are transferring the encrypted user data and the plain text personal criteria to the TTP, which executes pseudonymization. The data collection institution executes a second pseudonymization, decrypt the user data and reallocates it to the new pseudonyms. This variant model has the disadvantage that the personal data is known to an external institution, otherwise the administrative effort that every data source has to deal with when executing the process of pseudonymization can be avoided.

- Model P6
  The data sources transfer the encrypted user data and the plain text personal data to a TTP, which executes the first pseudonymization procedure. Afterwards the data is send to a second institution, which executes a second pseudonymization and only now the data is sent to the data collection institution, that decrypts the user data and reallocates it to the

pseudonyms. This model provides a good security because of the two instances that are necessary to re–identify the personal data, but it also causes a higher effort. Furthermore the personal data again has to be passed to an external institution.

- Model P7
  This model is quite similar to the model P1 with the only difference that the data management is not centralized. This means that several institutions provide the data. If one of these institutions is demanding for some kind of data the request is sent to all other data providing institutions. The demanding institution is responsible for merging the received data. Like model P1 also P7 is too insecure for an application in practice.

- Model P8
  The demanding institution sends its request to a TTP, which forwards it to the other data providing parties. They all execute the pseudonymization with the same key and send their results back to the TTP, which starts a second different pseudonymization procedure before transferring the result to the demanding institution. This model assures that none of the data sources is able to re–identify the personal data although they all know the key for the first pseudonymization procedure. A big disadvantage is again the high administrative effort.

- Model P9
  This model is very similar to model P6 with the difference that, concerning all decentralized models, the data collection institution is replaced by the data demanding institution. Also the high security level has to be paid by high administrative costs.

Model	Security	Effort/Costs
P1	very bad	very good
P2	very bad	excellent
P3	ok	good
P4	ok	very good
P5a	good	ok
P5b	good	good
P6	good	ok
P7	very bad	ok
P8	good	very bad
P9	good	very bad

Table 3.1: Overview of pseudonymization models [46]

Pseudonymization requirements

Pseudonymization has to meet certain requirements for being able to protect privacy. On the one hand there are some basic requirements which have to be achieved by all means otherwise the whole system of pseudonymization won't work. This set of requirements can be divided furthermore in privacy–related and security–related requirements (cf. [94]).

Privacy–related requirements:

- Pseudonymity
  Basically pseudonymity is the possibility for a person to choose a pseudonym like an alias to mask the own identity. Despite this alias cannot be linked to the physical identity of the person it is possible to use it for authentication.

- Unlinkability
  The meaning of unlinkability was already mentioned in section 3.1, in summary it can be described as the potentiality to reveal a person's pseudonym by gaining information about the different actions this person is executing with the pseudonym. In the ideal case the linkability should not be better than random guessing of the pseudonym (cf. [61], [94]).

- Property sharing resistance
  In the case of a user, who shares her pseudonym with other users, it has to be avoided that these users are able to use the shared pseudonym and acquire privileges which they should not have. Especially for multi–use credentials it is very difficult to achieve this objective.

Security–related requirements:

- Authentication
  This is a fundamental security requirement for all kind of eServices, not restricted to eHealth area. It has to be possible to clearly authenticate valid users and reject hackers and other harmful people.

- Unforgeability
  Another fundamental requirement, which demands that a user cannot create a pseudonym on her own but in cooperation with the organization.

- Security of the user's secret key
  It has to be guaranteed that a user's secret key cannot be published during the singular steps of the computer processing. Also it is necessary to choose a key generation technology, which can provide best possible security.

- Security of the protocols
  Not only the user's key but also the used protocols have to be considered as secure as possible due to the state–of–the–art of cryptanalysis technologies.

Additionally there are some more requirements, which don't have the priority of the basic requirements mentioned above, because they are only describing supplemental properties that are not included in every pseudonymization application. Nevertheless these properties can be very useful for special pseudonymization technologies (cf. [94]).

Advanced requirements (cf. [94]):

- Selective disclosure
  This property is very useful for multi–use credentials. It means that the user is able to select which attributes of her credential are revealed to an organization and which continue to stay hidden.

- Reissuance
  Reissuance means that an existing credential can be refreshed by the organization without revealing its related attributes. Furthermore it is possible for an organization to certify different attributes than another organization, that is also using the same credential (cf. [94], [8]).

- Dossier resistance
  This property should prevent a certification authority from gaining information from a multi–use credential during recurrent validation process.

- Non–repudiation
  Using this property makes it impossible for the user to deny former actions, which she has executed with her credential. In most cases different signature technologies are used to ensure non–repudiation but they don't gain any personal information from the credential itself.

- Confidentiality
  For this requirement it is necessary to use encryption/decryption within the pseudonymization technique to ensure that neither the communication messages of the user, nor the credential attributes could be read by unauthorized persons.

3.3 Different approaches of using pseudonymization

There exist a lot of different pseudonymization schemes and –technologies which were developed during the last years. This section will introduce a small selection of them to show how pseudonymization could be used in practice with special focus on eServices, which set a high value on privacy protection.

The following table gives a short overview about the introduced examples and how they meet the requirements in section 3.2.

Requirements	Pseudonym System	Private Credentials	eVoting	eTicket	eCash	eWallet
Pseudonymity	x	x	x	x	x	x
Authentication	x	x	x	x		x
Unlinkability	x	x	x	x	x	x
Unforgeability	x	x	x	x	x	x
Security of the secret key	x	x	x	x	x	x
Security of the protocols	x	x	x	x	x	x
Property sharing resistance	x	x	x	x	x	x
Selective disclosure		x				
Reissuance		x		x		
Dossier resistance	x	x	x	x	x	x
Non–repudiation	x	x		x		
Confidentiality	x	x	x	x		

Table 3.2: Overview of different pseudonymization approaches [94]

Pseudonym System

The Pseudonym System of Lysyanskaya (cf. [61]) is based on using the intractability of the discrete logarithm problem and the Diffie–Hellman problem, which is closely connected to the former. The Diffie–Hellman problem is the security–related foundation of many cryptographic schemes, also for the ElGamal public–key encryption, which is as well a cornerstone of Pseudonym System (cf. [63], [94]).

Particularly Pseudonym System is created to that effect of avoiding two main forms of attacks. At first nobody, which includes also the certification authority, should be able to forge a credential in a user's name. Secondly it should not be possible to gain any information about the user not even with pseudonym linking (cf. [61]).

In Pseudonym System the concept of creating master key pairs for users and organizations, consisting of a master public key and a master secret key, is used. The user has to register with a certification authority with her master public key. The certification authority has to check if the user is in possession of a corresponding master public/secret key pair. If the validation is successful the certification authority gives the user a credential that marks her as a valid user (cf. [61]).

After this validation procedure the user is able to register with different organizations creating different pseudonyms with them. Although these pseudonyms are not linkable there is still existing a relation between them and that is the master secret key. So it is possible to compute a user's master key pair with an identity extractor which was given to a rewindable user who is able to authenticate herself as the owner of the pseudonym. With the validation credential given by the certification authority she could prove her legality. So Pseudonym System meets most of the requirements described in 3.2 except for selective disclosure and re–issuance (cf. [61], [94]).

There are some determined presumptions that are important to made this approach work properly. Mainly it is supposed that the user possesses a master public key with an corresponding master secret key, which she is keeping secret as good as possible. This should dissuade the user of propagating her pseudonyms to other people. In this scenario sharing the pseudonym would also mean sharing the secret key. So this leads to the next presumption that a pseudonym only belongs to a unique user (cf. [61]).

The underlying model of Pseudonym System is restricted to single–use credentials although it could be adapted with slight modification to the support of multi–use credentials (cf. [61]).

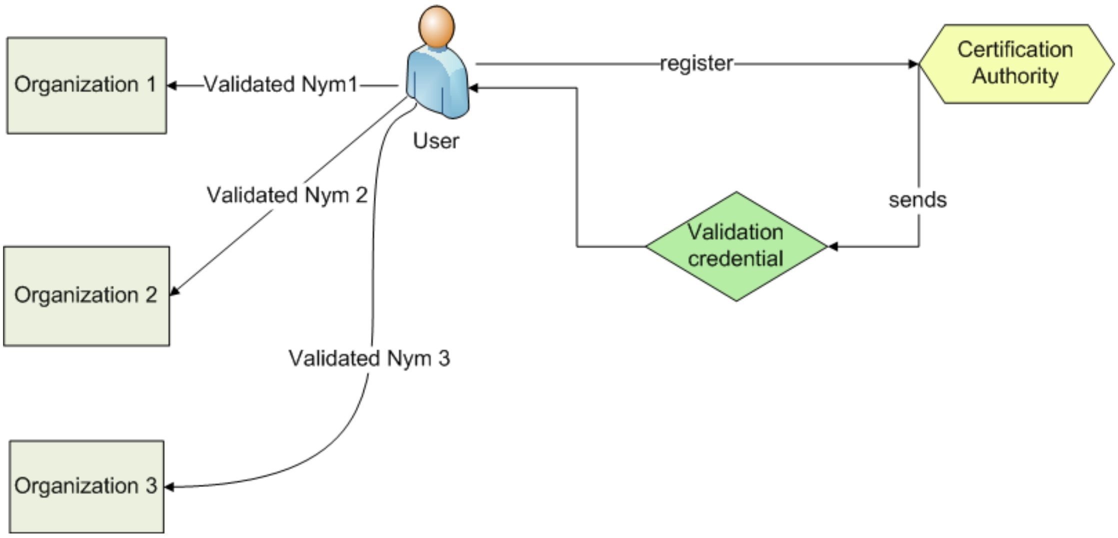


Figure 3.3: Pseudonym System system components

Private Credentials

Private Credentials was developed by order of Zero–Knowledge Systems, which today is known under the name Radialpoint. The idea behind it was that users should be able to decide themselves which information they want to publish to the organizations they communicate with. In general identity certificates retrieve much more information about the user than necessary for the current purpose. So the user doesn't have control over the collection or furthermore the prospective utilization of her personal data. In principle the functionality of Private Credentials is very similar to the one of blind signatures, which by contrast have a few drawbacks (cf. [8]).

The process of blind signatures is executed as follows: the inquiring partner wants to have a signed message from a certification authority. The certification authority gives the enquirer a blank signature, it has no idea which kind of message it is signing. Unfortunately the certification authority is not able to encode attributes into the certificate, respectively if every combination of attributes is signed with an own key, the number of attributes is highly restricted. Also blind signatures are very inflexible in hiding some attributes or identifiers when requested. Furthermore there are some serious security risks like unauthorized lending of certificates cannot be detected by blind signatures or stolen credentials can be used at any time without being retraced (cf. [8]).

During the life cycle of a Private Credential it passes through two stages: an issuing protocol and a showing protocol (cf. [8], [61]).

- Issuing protocol
  The user wants to have a public key (to which she has the corresponding private key) and a signature from the certification authority. This public key is bound to one or more attributes by the certification authority's signature. An example for an attribute is i.e. the age or family status of the user. This package, consisting of the pseudonym and the secret part for later authentication, presents the Private Credential. Together the created public key and signature for each Private Credential are unique, so the certification authority has no possibility to link different requests of a certain user.
- Showing protocol
  With the Private Credential the user is able to send the public key and the signature of the certification authority to the organization and to authenticate a message with her private key. Additionally this message has to contain a randomly chosen number to assure that the message is unique and is not replayed by a malicious user.

If the same Private Credential is used for several actions it makes these actions linkable but not traceable to the user. To put things right it is recommendable to request multiple Private Credentials with the same attributes from the certification authority, which should not harm effectiveness too hard with today's technical facilities (cf. [8]).

So Private Credentials are able to meet all requirements specified in section 3.2, also the both which are not fulfilled with Pseudonym System in section 3.3. Selective disclosure is met because of the non–restrictive decision of the user which information she wants to publish to her communication partner. So it is comparable with a paper–based document where some lines are blackened with a marker to hide information. Furthermore re–issuance is also supported because it is possible for the certification authority to refresh a previously given Private Credential without knowing the containing attributes (cf. [8]).

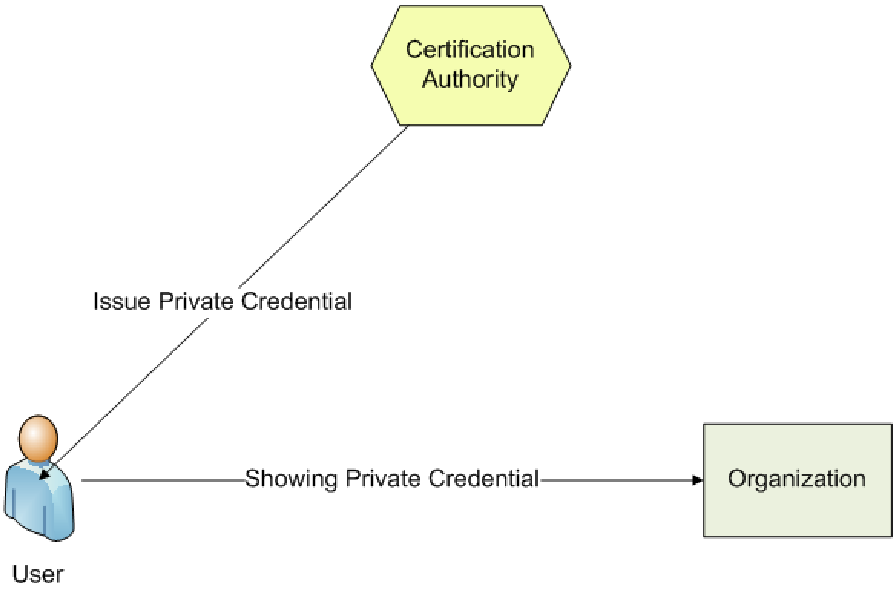


Figure 3.4: Private Credentials system components [94]

eVoting

eVoting is an electronic voting system, which allows citizens to deliver their voting ballots in a secret and secure way. Like in Private Credentials it is technically based on the blind signature technology. It should offer a solution for different problems an electronic voting scheme has to deal with, like completeness, non–cheating, effectiveness and robustness (cf. [60], [94]).

In this system five roles are involved: the certification authority, the voters, the publisher, the signer and the decrypter. The voting ballot presents a single–use credential, the protocol itself has four different stages (cf. [60], [94]):

1. System preparation period
   The voters, the signer and the publisher are generating their master key pair by means of the certification authority, which had also authorized the smart–cards in advance for each voter. Every smart–card has a unique number and contains the public keys of the signer and publisher to allow messaging. In the voting center an untraceable decrypter is available to validate the incoming voting ballots. Also the decrypter gives some encryption information to the certification authority where the other parties could request it on demand.

2. Voting period
   After filling in the voting ballot each voter has to encrypt and blind the content with her smart–card using the public keys of the signer and the publisher and additionally a randomly chosen number. The signer receives this blinded message and after successful validation which shows that the message was sent by an eligible voter she signs it and sends it back to the voter. Afterwards the smart–card generates a copy of the voting ballot and sends the message back to the signer.

3. Scrutiny period
   After a new validation of the blinded message and the related signature by the signer the voting ballot is forwarded to the decrypter.

4. Publishing period
   The decrypter decrypts the incoming message and forwards the output to the publisher who publish the vote. Due to the voting receipt the voter has got before she is able to control if her vote has been counted correctly. If this was not the case she has the possibility to send an untraceable email to the voting center with the request to recount her vote.

The eVoting system cannot meet all the requirements defined in section 3.2 like non–repudiation, selective disclosure and re–issuance. Indeed this is also up to the different requirements an eVoting system has in contrast to the other approaches described above. Instead it fulfills a lot of other requirements which are special for a voting system like completeness, mobility and non–cheating (cf. [60], [94]).

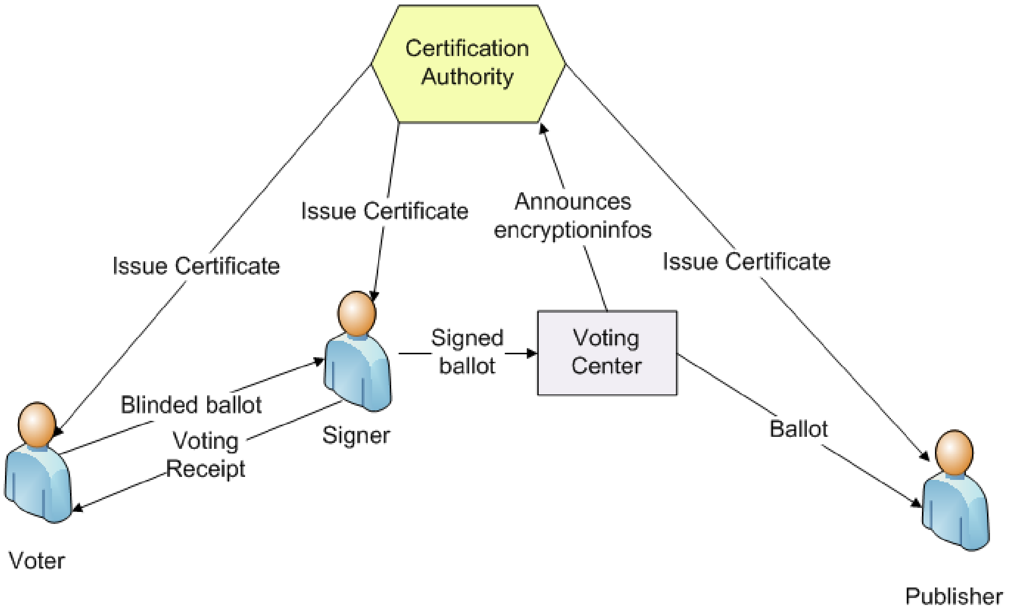


Figure 3.5: eVoting system components [94]

eCash

The first version of eCash was developed by David Chaum in 1982, her main focus was set on the protection of the anonymity of the person who did a payment with digital money and the possibility of this person to prove this payment. The basic technology for realizing this system are blind signatures (cf. [12]). Naturally until this day the original system was improved by different enhanced eCash schemes like the one of Abe and Fujisaki ([1]) which is also the one used in the eTicket system described in the next section (cf. [94]).

The eCash system still is based on the technology of blind signatures which on its part is based on the RSA public key cryptosystem. In the scheme of Abe and Fujisaki the blind signature protocol consists of four phases (cf. [95], [94]).

1. Initializing phase
   The bank is creating a pair of public and private keys, the public key is published together with other predefined parameters e.g. the expiration date. Every eCash document has a preassigned value of X dollars.

2. Withdrawing phase
   If the customer wants to withdraw eCash from the bank she creates a message with a randomly chosen number as pseudonym and blinds the message with a special one–way hash function. The message also contains the identity of the customer and her account number, so the bank is able to authenticate her. Afterwards the bank signs the blinded message and debits the customer's account, the signed message is sent back to the customer.

3. Unblinding phase
   In this phase the customer reads out the bank's signature from the returned message using another one–way hash function.

4. Depositing phase
   When the customer spends her eCash the payee verifies it by means of the bank's signature and after a positive validation she sends a request to the bank for a double–spending check. If the eCash was not spent yet the payee accepts the payment and transfers it to her account. In the meantime the bank stores the eCash document in the double–spending check database and credits the payee's account in the amount of the eCash value of X dollars.

An important purpose of this scheme is to stop the bank's databases of growing by leaps and bounds, because they usually had to store all the spend eCash for the provided double–spending check. Hence the idea was to extend the eCash documents with an expiration date, so that the expired eCash can be removed from the database (cf. [95]).

eCash is not using a public key as pseudonym but a randomly chosen number, so there is also no private key available for user authentication, which has to be done alternatively e.g. by SSL. In other aspects eCash meets most of the requirements defined in section 3.2 except authentication, selective disclosure, re–issuance, non–repudiation and confidentiality. Although authentication, which is a basic security requirement, could be provided by SSL technology, this would reveal the user's identity and so unlinkability is not supported anymore. This could be solved with the solution to replace the random number for the pseudonym by a public key (cf. [94]).

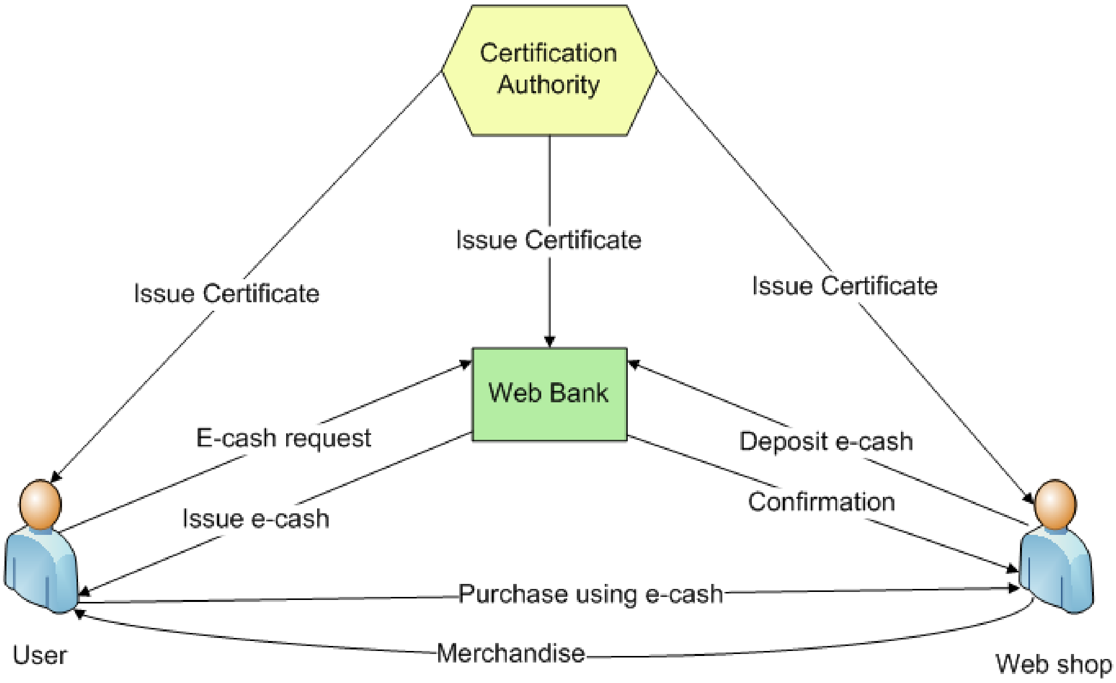


Figure 3.6: eCash system components [94]

eTicket

eTicket is a conditional access system mechanism (CAS) for Pay–TV systems which protects the privacy of the customers against attacks from outsiders on the one hand and misuse by the provider on the other hand. The reason for developing such a CAS was the fact that most customers not only fear attacks from outsiders but also feel inconvenient because the providers gain a lot of information about them e.g. their TV–watching habits (cf. [95]).

This approach is based on a protocol which uses a modification of the partial blind signature scheme by Abe (cf. [1]) that is also used in the eCash technology described in the former section 3.3. In this protocol customers directly buy their eTickets from the TV channel provider. Later when they want to subscribe to further TV channels they have only to show their eTickets. In the modified partial blind signature scheme an anonymous public key is inserted into the blinded message, which means that this key does not contain any information about the customer who is sending it. Nevertheless the customer, who is the owner of the key and the eTicket, is the only one who possesses the corresponding private key. So it is possible for the Pay–TV system to provide a non–repudiation service using the anonymous signature (of the owner) of the eTicket. Additionally the customer can be sure that nobody can send an eTicket in her name even if somebody has a copy of such an eTicket. So with this approach nobody can reassign the customer with the channels she has subscribed, not even the provider who has only the information how much money every customer is spending on eTickets (cf. [95]).

The protocol itself includes four phases (cf. [95]):

1. eTicket issue phase
   The customer inserts a public key into the blinded message to which she is holding the corresponding private key. This eTicket also contains an expiration date and the costs predefined by the provider, it is signed by the customer and additionally encrypted with the provider's public key. Afterwards it is sent to the provider. After the receipt of the eTicket the provider decrypts it with her private key and verifies the provided attributes. If they are correct she signs the message, encrypts it with the customer's public key and sends it back to the customer.

2. TV channel subscription phase
   If the customer wants to subscribe to some TV channels she selects the favored channels and signs the eTicket with her private key. After an encryption, as done in the first phase, the eTicket is sent to the provider. After decryption and positive validation of the provided attributes the provider calculates the costs for the selected channels. If the price is lower than the value of the eTicket the provider has to compute the balance and a new signature and sends the message back to the customer. This message also contains the authorization keys for the requested channels which are encrypted with the eTicket's public key. If the price equals the eTicket no balance and no new signature has to be included in the message. If the price is higher than the eTicket the provider is waiting for further eTickets of this customer. When a subscription message is sent to the customer a copy is stored for the non–repudiation service and double–spending check. When the customer is receiving the eTicket she can decrypt it with her private key and gets the authorization keys for the favored channels.

3. TV channel adaption and suspension phase
   If the customer wants to change or stop her TV channel selection she has to encrypt her latest modified eTicket which contains the changed channel information. After sending the eTicket to the provider she will decrypt and validate it. If the validation was correct the provider has to compute the balance fee for the changing of the TV channels. Furthermore she has to renew the old authorization keys and send the eTicket back to the customer as in phase two.

4. eTicket renew phase
   The customer has the possibility to renew her eTicket when it is close to the expiration date. For this purpose she fills the renewal form which contains the new expiration date and the latest balance fee. After signing the message and the encryption with the provider's public key the eTicket is sent to the provider. The provider decrypts and veri-

fies the message, afterwards she computes a new signature and encrypts the message with the eTicket's public key. Finally the customer receives her renewal ticket.

As shown in table 3.2 this approach meets nearly all pseudonymization requirements defined in section 3.2 except selective disclosure, which is not too bad because selective disclosure is not a requirement of Pay–TV systems. As mentioned in phase two of the protocol sharing resistance is satisfied by a double–spending check (cf. [94]).

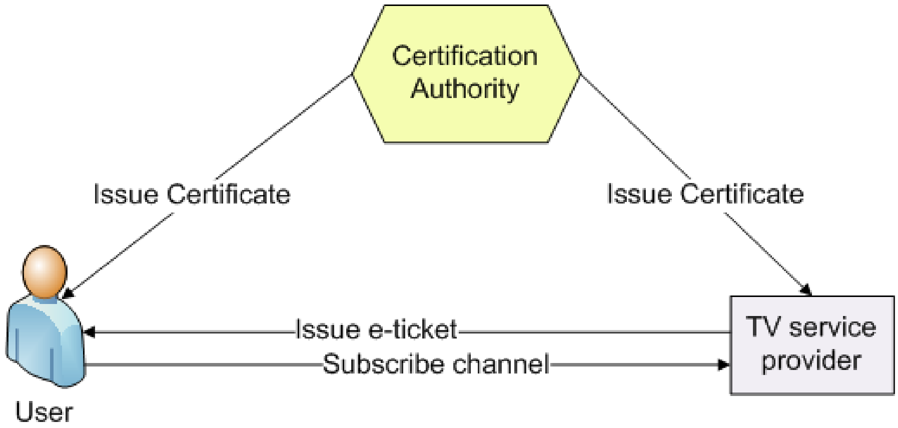


Figure 3.7: eTicket system components

eWallet

eWallet provides a possibility for users to spend digital money and receive services from service providers and at the same time keeping up their pseudonyms so that organizations are not able to trace back their identities. Though eWallet is similar to eCash it presents more features e.g. using it also in the offline way and having better protection for users and service providers (cf. [94]).

The first concept of eWallet was proposed by Chaum and Pedersen, who defined correctness and anonymity as their main requirements. They want to assure that only correct information was stored in the databases and this data should only be read or written by people with the according permissions. While organizations assume correctness as their most important requirement, for individuals this seems to be their privacy. So protection of privacy presents the second focal point (cf. [13]).

eWallet consists of two fundamental components(cf. [13], [94]):

- A purse, which is a small hand–held device, trusted by the user. With the purse the user is able to connect to the service device and spend her eCoins. She can keep a check on the communication between service provider and observer, the latter is not able to send any extra information to the issuer and vice versa. Otherwise the purse has no possibility to modify the messages observer and issuer are exchanging or has access to the stored data in the observer. The purse itself is able to communicate with the outside world at will without the knowledge of the observer but organizations are supposed to only accept messages previously approved by the observer.

- An observer, which is a tamper–proof device (e.g. a smart–card), trusted by the issuer who could be represented by a bank for example. The observer is only able to communicate through the purse and not directly with the outside world, which is an essential prerequisite for a correct working of the system. Ideally the observer is embedded inside the purse she acts as a container for the electronic coins.

For a correct and secure process flow Chaum and Pedersen developed the eCoin Issuing Protocol. This protocol assures that the user's privacy is protected and no misuse of the system is possible. So only messages which were approved and validated by the observer before they were sent — after further blinding — to the organization for signing. In return the organization cannot retrieve any extra information from the messages, although the observer knows the original messages, but the purse would prevent such an action (cf. [94]).

Summing up the process could be executed as follows: The purse (user) requests an eCoin from the organization(bank), which is deposited at the observer. At a later time the user wants to spend some eCoins and shows them to other organizations. The observer deducts these eCoins from the smart–card and gets an approved payment confirmation from the organization. In return the organization gets also an approved message from the observer (over the purse) and can use the received eCoins to recover the money from the bank (cf. [94]).

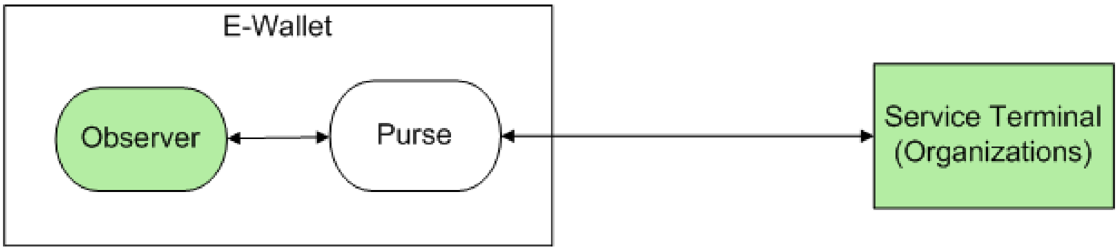


Figure 3.8: eWallet system components [94]

PIPE

PIPE (Pseudonymization of Information for Privacy in eHealth) is a centralized pseudonymization service specifically developed for securing sensitive medical data in EHR architectures. PIPE is storing medical data and patient master data separately, so that those two types of data are only related via pseudonyms. The calculation of the pseudonyms is done by using encryption which is executed via a central server–side hardware security module. This module serves as a secure environment for storing the inner symmetric key and it processes the heavy cryptographic operations. The user authentication is done via a security–token on the client–side, that is stored on a smart–card. This security–token is responsible for the cryptographic operations on the client–side and contains the outer private key, which can be accessed by input of a PIN (cf. [50]).

The figure 3.9 shows the architecture of PIPE which consists of at least 3 nested hulls, each of them has to be passed successfully to get to next one and eventually to the medical data in the center, which is connected with clear text pseudonyms. The relationship between pseudonym and user ID is encrypted with the inner symmetric key. The outer hull represents the authentication layer which can be passed with the outer asymmetric key pair, that is stored in the security–token of the user. The inner hull is the user permission layer for which the inner asymmetric key pair and the inner symmetric key are necessary. The inner private key is encrypted with the outer public key and the inner symmetric key is encrypted with the inner public key (cf. [50], [86]).

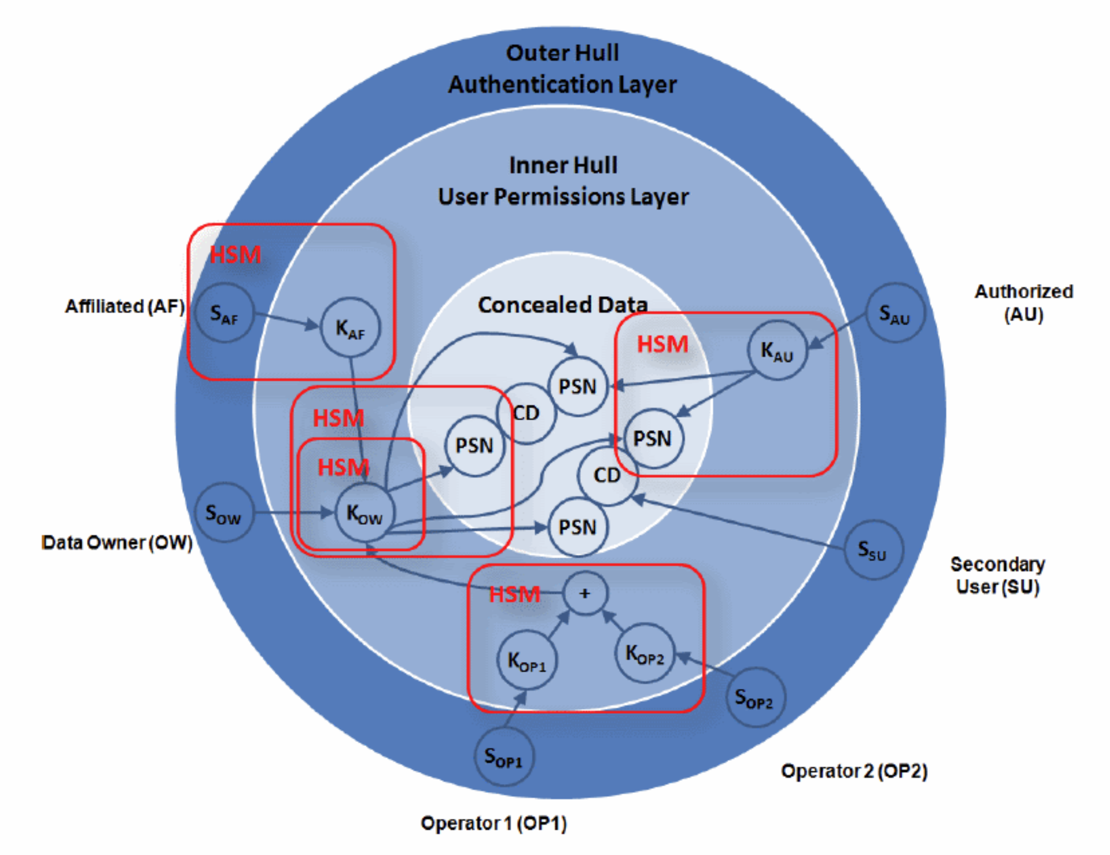


Figure 3.9: PIPE Architecture [50]

To find out which user is connected to a pseudonym the user has to authenticate herself by entering the PIN on her security–token to gain her outer private key. If this action is successful the user's identifier is signed with the certificate on the security–token and sent to the PIPE server, which verifies the signed identifier. If the verification is successful the PIPE server sends back the user's encrypted inner private key, which can be decrypted by the user's outer private key. To increase security a session key is used during the communication process with the server, where the generated session key encrypts the data symmetrically. The session key is encrypted with the public key of the PIPE server, which in turn can decrypt it with its private key and use the decrypted session key for decrypting the sent data (cf. [50], [86]).

After the successful authentication the user sends her decrypted inner private key to the PIPE server, where the security module uses it for decryption of the inner symmetric key. The inner symmetric key is necessary to find out which pseudonym is connected to the user and so the required medical data can be queried. An intruder who gains access to the user's key store on the client–side and therefore the encrypted inner private key is not able to use it because that would require the user's outer private key (cf. [50], [86]).

Because of the separate storage of the user's health and master data and the role–based access different types of pseudonyms are used. Master data is connected to Identification–Pseudonyms and health data to Health–Pseudonyms, the relationship between the data and the pseudonyms is encrypted with the inner symmetric key. Both types of pseudonyms can exist as Root– or Shared–Pseudonyms. Root–Pseudonyms are used exclusively by the patient (the data owner) and her relatives, only the patient is authorized to delete those pseudonyms and therefore has full control over her data. The relative is able to use the inner private key of the data owner — which is encrypted with the inner symmetric key of the relative — and therefore has access to the same data. The connection between data owner and relative is only known between those two and can be revoked by the data owner (cf. [50], [86]).

Further roles are the administrator, who has no access to the de–pseudonymized medical data but is responsible for administrative tasks e.g. user management. Secondary users have direct access to the pseudonymized medical data for research purposes but the data owner is notified that her data has been queried. Shared–Pseudonyms are used for persons who are authorized to access certain data records. Those pseudonyms are generated for each authorization and are known to the data owner and the authorized person, they are connected with the authorized data records and are deleted when the authorization is revoked (cf. [50]).

In the case of losing the security token the inner private key cannot be decrypted anymore, so a backup strategy is necessary. The user's inner private key is divided into several parts, the parts are randomly assigned to operators, each operator is restricted to one part. The user identifier is encrypted with the secret key of the hardware security module and the inner public key of the operator, so even the operator doesn't know for which user she is storing the part which increases security even more. The operator encrypts the part with her inner symmetric key and stores it together with the encrypted user identifier in her own key store. For recovering the user's inner private key a minimum number of shares is necessary, in case a new security token has to be issued the operators decrypt their shares with their symmetric keys and send them to the hardware security module which decrypt the shares with its secret key and combines them. After the necessary number of shares is reached the user's inner private key is reconstructed. Afterwards a new outer key pair has to be created and the inner private key is encrypted with the new outer public key. Then the new security token is issued, the operators delete their shares and new operators are selected for holding the new shares of the user's inner private key. So it is ensured that the old security token cannot be used anymore (cf. [50], [86]).

Chapter 4

ePrescription

ePrescription is one of the principal points in this thesis due to its privacy protection needs in conjunction with the electronic health record. The technique of pseudonymization should be applied to ePrescription systems for preserving a patient's confidential data. The following chapter should give a view about the concept of ePrescription, the advantages of its use on the contrary to the conventional solutions and which forms of realization are possible.

4.1 Electronic prescription versus conventional prescription

The conventional prescription is made out by a doctor using a default form, which is filled out by hand or with the practice computer system. Afterwards the patient is able to go to any pharmacy to fill the prescription.
Every prescription has a period of validity and is restricted in terms of reuse (cf. [85]).

A proper prescription has to include the following elements (§3 I Rezeptpflichtgesetz) (cf. [85]):

- The doctor's name and place of work
- The patient's name
- The name of the prescription medicine
- Dosage form of the prescription medicine
- Directions for use
- The year of birth if the medicine was prescribed for a child
- Issue date
- The doctor's (electronic) signature

There exist a lot of additional rules for special prescriptions like those for narcotic substances, which are regulated by the order of addictive drugs. For example this regulation dictates the maximum amount of the medicament which the doctor is allowed to prescribe for the patient per prescription as well as for the whole doctor's surgery per day (§15 Suchtgiftverordnung). These prescriptions are also obliged to have an accurately specified appearance (§§19, 22 Suchtgiftverordnung)(cf. [100]).

ePrescription is the electronic representation of the conventional prescription document including the data transmission between doctor, pharmacy, patient and health insurance. It also contains the computer based evaluation, completion and verification of the prescription data (cf. [45]).

On the one hand ePrescription can be used as a stand–alone solution with focus on electronic prescribing or on the other hand it could be a part of a more comprehensive solution like the electronic health record (cf. [24]). The Centers for Medicare & Medicaid Services developed a definition of the term ePrescribing:

> "ePrescribing means the transmission, using electronic media, of prescription or prescription–related information between a prescriber, dispenser, pharmacy benefit manager, or health plan, either directly or through an intermediary, including an ePrescribing network. ePrescribing includes, but is not limited to, two–way transmissions between the point of care and the dispenser" ([24]).

The concept of ePrescription is including

- undirected communication (e.g. between doctor and pharmacy)
- directed communication (e.g. between pharmacy and health insurance)
- dedicated reports
- management information (cf. [45]).

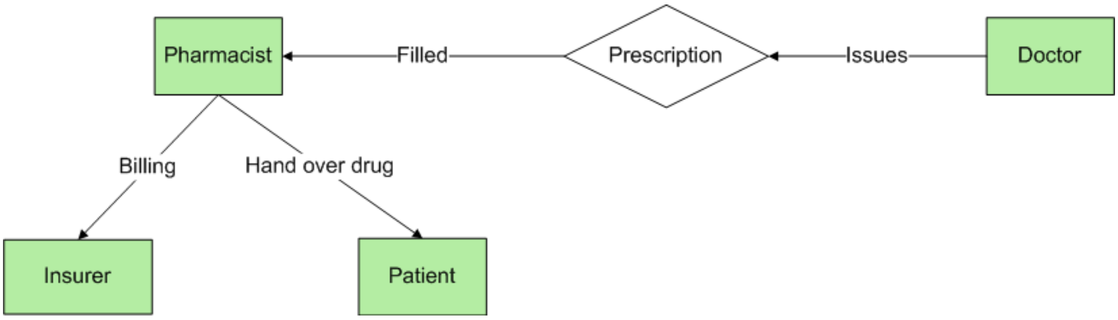


Figure 4.1: ePrescription components and their interaction

4.2 Positive and negative effects of using ePrescription

The traditional paper–based prescription entailed a lot of problems. One of them — which sounds pretty simple — is the misinterpreted handwriting of the doctor. The illegibility rate of prescriptions may be 1 to 2 %. In general medication errors are representing a big part of the total quantity of medical errors, they are responsible for approximately 20 % of all adverse drug events. Especially in the case of pediatric patients a lot of dosing errors are happening. The prescription of wrong drugs or the wrong dosage is still going strong, also newly developed drugs, which were recently put on the market could cause unknown allergies or negative interactions with other drugs. A further negative influence is given by incomplete or missing patient information. Gerstle et. al. refers to a study which has shown that nearly half of the cases of adverse drug events could have been avoided (cf. [39]).

So ePrescription tools could help to reduce such errors by providing knowledge, information and data for optimization in selecting and specifying medication. Also in the prescription of gender–specific drugs ePrescription has helped to avoid assignments of these drugs to patients of the opposite gender (cf. [39]).

Accordingly ePrescription provides considerable advantages for different groups of people. The patients benefit from the reduced medication errors and as a outcome of this the patient satisfaction is rising. Another consequence of the reduction of medical errors is a decrease of health care costs, which is welcomed by public health and health insurances. Moreover the use of ePrescription tools helps to save money by increasing the efficiency of the prescribing process and in general the optimization of workflows. Therefore also pharmacists can take advantage from ePrescription, because the improved compliance of prescription and the consequential reduction of drug costs are also in their interest. Last but not least also physicians can profit by ePrescription due to better record keeping and documentation methods and more efficient medication renewals (cf. [39]).

Unfortunately there is also another side of the coin because of the problem of maintaining confidentiality of medical prescriptions. In general today medical data is not only available at the patient's family doctor, it is necessary that this information has to be also on–hand for the referral specialists, the hospital surgical team, the nursing staff and the laboratory personnel and everybody else who is involved in the health practice workflow. So it was necessary to convert the patient's data into an electronic format to make it accessible for a range of authorized people, who need this information to provide an appropriate medical care for the patient (cf. [3]).

With creating a basic regulatory framework for privacy protection in many countries an important precondition for electronic health records was established. But for all that in some cases — like in the United States of America — this legislation covers only the least common denominator of the privacy requirements as per description in chapter 2.2. So there is enough room for possible misuse of confidential data (cf. [3]).

For example in the United States pharmacists are not bound to the same legal privacy principles as physicians. There exists no cross–boarder law for privacy protection concerning records kept of the pharmacies. Different surveys allocate cases of companies, which were using medical records as a base of personnel decisions e.g. hiring or promotions. An extraordinarily case was the banker who gathered records of cancer patients and used them to call in their loans. Furthermore there is a documented case of a HIV positive man who has to take the accordant drugs. His employer got the information about the disease via the company's health benefit insurance the man used to pay his prescription (cf. [3]).

But not only the patients are threatened by misuse of their confidential data, also doctors have to deal with that. The health insurance companies can collect a doctor's prescription data and compare it with prescription patterns of other doctors for reasons of cost control research. They prepared guidelines to regularize the prescription of certain drugs and are giving bonuses to the doctors who follow them. In case of non–compliance the doctors could be dropped from the plans. On the other side there is also a counter movement from the pharmaceutical companies that are trying to dispose the doctors to prescribe large amounts of their drugs (cf. [3]).

As discussed in chapter 2.4 the legal regulation concerning privacy in Austria is much stronger than in the United States. Although legal loopholes and vaguely phrasing must not lead to privacy injuries.

4.3 Concept of ePrescription process

There are several stakeholders who are involved in the concept of ePrescription. On the one hand there are the obviously necessary parties like a patient, a doctor, a pharmacist and a insurer, who are presenting the central point in the ePrescription process. But there are also a lot of people participating in ePrescription that are not visible of the first sight. For understanding the ePrescription process it is necessary to identify all possible participants and their duties (cf. [3]).

- Patient
  The patient is the recipient of the prescription and her confidential data and privacy has to be protected. She has to prove her enrollment status in a health insurance at the doctor (e.g. by presenting a smart–card). Additionally it may be necessary that the patient has to prove her agreement for the release of medical information and methods of treatment (cf. [3]). It is important to inform the patient (and her family caregivers) about the ePrescription process, so that they understand how it works. In general patients tend to appreciate when their providers are using the best available technology (cf. [24]).

- Doctor
  The doctor is the issuer of the prescription and of course also her privacy has to be guaranteed. She has to prove her legitimate capacity for prescribing (cf. [3]). The doctor is supported by the clinical decision support information which provides information about the patient's medication history, formula, drug–allergy interaction alerts etc (cf. [24]).

- Pharmacist
  The Pharmacist is responsible for filling the prescription. She could also get involved in measures of fraud–prevention by means of profiling techniques and statistical analysis. Definitely she has the duty to handle possible prescription claims in consideration of the current legislation (cf. [3]). ePrescription will help the pharmacist to save time because of less medication errors due to the ePrescription system (cf. [24]).

- Insurer
  This entity has the responsibility to accept the costs of certain prescribed drugs for the patient. Also the insurer is the prime suspect for the misuse of patient data because she is trying to evaluate the collected prescription data and to create profiles of doctors and patients for cost and risk estimates (cf. [3]).

- Privacy officer
  She is responsible for the database which contains the mapping of patient names with their pseudonyms. The privacy officer has the duty to pay attention to the correct abidance of the law concerning privacy protection (cf. [3]).

- Enforcement agent
  She is an employee of a governmental institution and has to supervise the medicine prescription and the use of certain controlled substances for medical care. For her work it is necessary that prescriptions can be clearly connected to the patients and doctors (cf. [3]).

- Judge
  A judge is a legislative authority who has the entitlement to influence the legal situation of privacy protection. So she could participate in defining parameters under which revocations of pseudonyms can be clearly classified as legitimate or abusive. Also she has the authorization to annihilate the patient's or doctor's confidentiality in the ePrescription process (cf. [3]).

- Certification boards and certification authorities
  These entities are controlling the capacities of issuing prescriptions and the digital certificates within an ePrescription system (cf. [3]).

The prescribing process is more than creating a prescription for a patient, which is dispensed in a pharmacy. A lot of different technologies and hardware systems are involved in this process that entails a crossfire of needs and challenges (cf. [24]).

The process of ePrescription can be divided into five phases which are covering different key functions (cf. [24]):

1. Prescribe
   At the beginning of the prescribing process the patient's identity has to be confirmed. So it is possible to get access to the linked patient data like demographic information, insurance and contact data. For gathering this kind of data it is necessary that the ePrescription system is connected with external databases. The coordination between these different

information systems is important for the data management and administration. Also it has to be ensured that only persons, who are authorized to inspect the patient's data, have access to it.
It is necessary to have insight into the patient's current medication list and the medication history information, which could be corrected, updated or merged with other historical information at any time. For prescribing it is possible to select medication from favorite lists and to look up standard or recommended dosing. Safety alerts will warn the clinician about known contraindications with other drugs or are pointing to possible complications concerning allergies or former laboratory test results of the patient. Also the clinician is warned when drugs are selected which don't met the formula requirements.

2. Transmit
   Medication information will be shared between prescribers, payers and dispensers, this will include medication history, renewal authorizations, change requests etc.

3. Dispense
   Assessment tools can analyze which patients are likely to become non–adherent and so encourage pharmacist's counseling which will make personal medication profiles available to the patient.

4. Administer
   It's necessary to provide information material for the patient concerning therapies and possible side–effects. Also it is important to develop the collaboration for the management of medication therapy between the involved persons (e.g. clinicians, pharmacists, health plan care coordinators, etc.). Comprehensive administration aids like visual medication administration support for complex dosing schedules will be provided.

5. Monitor
   This process phase is responsible for supplying the patients, prescribers and pharmacists with additional information about new laboratory test results or the therapy progress of the patient. Also different reminders are provided e.g. the caregiver is alerted that the patient has missed a medication dose or for refilling the patient's medication.

The following table shows an overview about the different phases of the prescribing process and their key functions (cf. [24]):

Process Phase	Key Functions of Innovations
Prescribe	1 Patient identification
	2 Current medication list
	3 Medication selection
	4 Safety alerts, clinical decision support
	5 Formula alerts
	6 Renewal authorizations
Transmit	7 Bidirectional electronic data interchange
Dispense	8 Pharmacist assessment and counseling
Administer	9 Patient education materials
	10 Administration aids
	11 Collaborative medication management
Monitor	12 Linkages to lab testing
	13 Adherence alerts
	14 Patient outreach
	15 Refill reminders
	16 Remote compliance monitoring

Table 4.1: Functions of ePrescription process

4.4 ePrescription models

On the basis of the investigations of the society for insurance research (cf. [45]) there are two different basic techniques of how ePrescription can be realized:

1. Prescription data transport over the server network
   At this case primarily the doctor has to confirm the patient's identity by means of the patient's insurance card and a direct connection to the insurance server for the latest information. Afterwards the doctor creates an ePrescription with an unique number for identification (e.g. a prescription key), all insurance information about the patient, the doctor's data and the prescription details have to be transferred to the responsible server. The prescription key is stored at the patient's smart–card or at paper voucher or similar.

   The patient goes to a pharmacy of her choice and grants it an one–time access to her prescription key, so the pharmacy is able to get the ePrescription from the server. Eventually the pharmacy rounds off the prescription with dispense data and sends it to an accounting server, that forwards the prescription to the concerning health insurance company. Additionally there are different servers for statistical analysis of the filled prescriptions to which authorized users have access.

This technique assumes that a nation–wide electronic networking of doctors, pharmacies and health insurance companies with the server network is available.

2. Prescription data transport over a data medium (e.g. smart–card)
The second technique is reducing the requirements of networking because an electronic supporting medium (e.g. a smart–card) is used. Like in the first variant the doctor checks the patient's identity before she creates the prescription. Instead of sending the ePrescription to the server network she stores it at the supporting medium. The patient again goes to a pharmacy where the prescription is transferred to the pharmacy's computer and deleted from the supporting medium. The other actions are similar to the first technique.

For the supporting medium there are concretized two possibilities: On the one hand an empty memory card for the transport of the prescription data and on the other hand a new form of the insurance card with the patient identification data where additional data can be stored e.g. the current prescription.

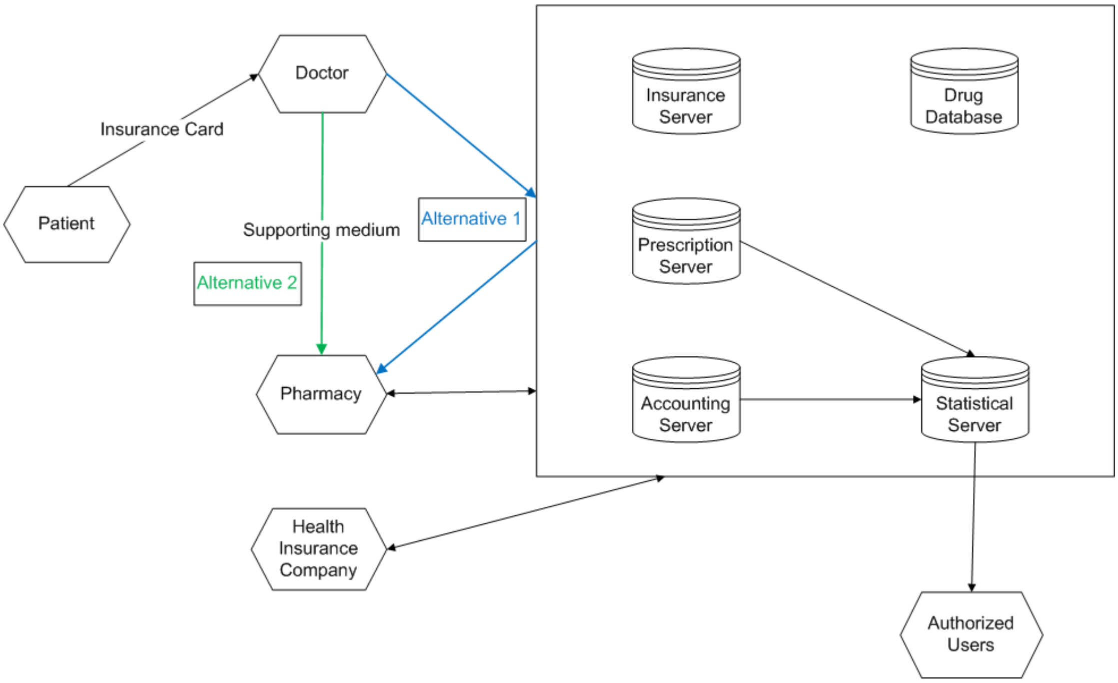


Figure 4.2: Data–flow of ePrescription data [45]

The master thesis of Schubert (cf. [90]) describes four different ePrescription models, which are overlapping to some extent with the models of the society for insurance research (cf. [45]).

The following criteria are the decisive factor for choosing these models, because they were covered by all four models (cf. [90]):

- Free choice of the pharmacy by the patient
- Identification and authentication of the doctor with her signing or her digital signature
- Identification and authentication of the pharmacist with her signing or her digital signature
- A high degree of transparency of the prescription for the patient (paper based)

The models of Schubert (cf. [90] are:

1. Model Server
   This model is almost equivalent to the model of the society for insurance research "Prescription data transport over the server network" described at the previous page. Additionally it is pointed out that the patient is only identified by her smart–card, there is no explicit authentication carried out. A weak point of this model is the fact that a non–compliance of a prescription by the patient is not possible without the knowledge of the doctor or the pharmacist, because deleting of the prescription data is only provided for these two instances.

2. Model Smart–card
   Equivalent to the model "Prescription data transport over a data medium" of the society for insurance research more detailed information about this model is provided at the previous page. A disadvantage compared to the model Server is the missing control about the prescriptions concerning narcotic substances. These prescriptions could be created in unlimited number — e.g. by misuse of the doctor's computer — without discovery of the dispensing pharmacists.

3. Model Voucher
   The prescription is created by the doctor and transmitted to a central server for storing, where it will get a unique transaction number. This transaction number is encoded into a bar–code at the voucher which is handed over to the patient. The patient goes to a pharmacy and the transaction number is read out from the voucher over the bar–code by the pharmacist who is now able to get access to the concerning prescription at the server.

   The prescription at the server is now marked as dispensed, the transaction number in the bar–code cannot be used anymore. The identification of the patient in the pharmacy is based on the voucher, there is no further authentication provided. Also the full security functionality of the prescription of narcotic substances is covered by this model. For the prevention of misuse there is the possibility that the server could reject a huge number of prescriptions at unusual times.

4. Model Bar–code
   The doctor creates a prescription with a bar–code, all the prescription information is available in clear text and additionally encoded into this bar–code. The prescription is signed by the doctor's own hand. In the pharmacy the prescription data is read out from the bar–code, all necessary dispense and prescription data has to be transmitted to a central server in regular intervals. The basic advantage of this model compared to the conventional prescription is the faster and less error–prone readability. The protection against forgery is warranted by the use of specialty paper. In the case of prescription for narcotic substances further security measures would be necessary.

Chapter 5

Evaluation of existing approaches

There is a number of existing ePrescription systems, some of them are already in use, others are just concepts. In this chapter a selection of them will be evaluated in consideration of the following criteria:

- Description of the system architecture and features of the approach. This includes facts about how data is stored and which technical requirements are fulfilled by the system.
- Which security techniques and –measures are provided to protect privacy? This includes also provided recovering procedures of lost or stolen keys and how access authority is handled.
- How does the workflow of the ePrescription process look like and which use–cases are covered?
- How is the current status of the system (prototype, productive use, test run...)?

The investigated systems have to achieve some preconditions: They have to provide an ePrescription component, which needs not to be the main part of the system, but has to provide security for privacy matters.

Based on these evaluation criteria the positive and negative aspects of each approach were derived and analyzed. The defined evaluation criteria were derived from those used in [44] and are representing a subsumption of them.

5.1 ELGA — Electronic Health Record (Austria)

ELGA is the German abbreviation for "Electronic Health Record" and is based on a performed feasibility study in order of the Federal Ministry of Health, which is the foundation for the further planning and implementation by an especially created working group for this purpose (cf. [40]).

Medical data of patients is already stored by many medical service providers in Austria, but a huge problem was the lack of uniform technical standards for the structure of documents and the form of saving them, so that these isolated applications were not able to work together. With ELGA it should be possible to standardize these applications and connect them among themselves (cf. [40]).

A main goal of ELGA is providing a lifelong health record for patients, which means no additional documentation of medical information but a substitution of the paper–based documentation. It includes storage, communication and processing of medical data and offers the patient an active role in her medicare (cf. [52]).

ELGA will provide a range of functions for supporting different medical services (cf. [52]):

- Basis
  The primary task of ELGA lies mainly in the unambiguous identification of patients and healthcare providers, providing a nationwide patient index and management of treatment processes.

- Storage and safe–keeping
  The storage of all lifelong medical data of a patient in electronic form and the possibility of access to these documents for authorized people at the location of medical care.

- Documentation and recording
  The possibility for the patient and the medical service providers to record multimedia–based data from different sources e.g. diagnostic findings, test results and diagnoses.

- Reproduction and communication
  Preparation, reporting and management of medical data based on consistent technical standards.

- Support of administrative processes
  Simplification and facilitation of processes e.g. management of appointments, waiting periods or medication.

- Support of patient's medicare
  All sanitary activities of the patient should be supported e.g. reminders, patient diaries and access to medical knowledge for laymen.

- Processing and data usage
  With means of decision–based systems the quality of health care can be improved by ELGA e.g. pro–active analysis concerning allergies or medical observation systems.

- Reporting and monitoring
  Brings the prevention into focus with different monitoring applications.

- Knowledge management
  Provides access to qualitative assured knowledge for the patients and the medical service providers.

Architecture and technical details

There are three fields of action, which are necessary for a successful use of ELGA. Primarily the prerequisites of ELGA, which comprehends necessary legal regulations in area of privacy, measures for augmenting the acceptance of the citizens and different organizational arrangements (cf. [40]).

The second field contains the basic components of ELGA, which provide the eHealth infrastructure and are the foundation for the ELGA core applications. Actually ELGA itself consists of these basic components. The other two fields of action are strongly connected to ELGA and are necessary for its formation, but they are not a physical part of it (cf. [52]).

An overview of the basic structure of ELGA is shown in the graphic below. The upper area shows the basic components, the lower area presents some possible core applications which are attached to ELGA via adapters (cf. [52]).

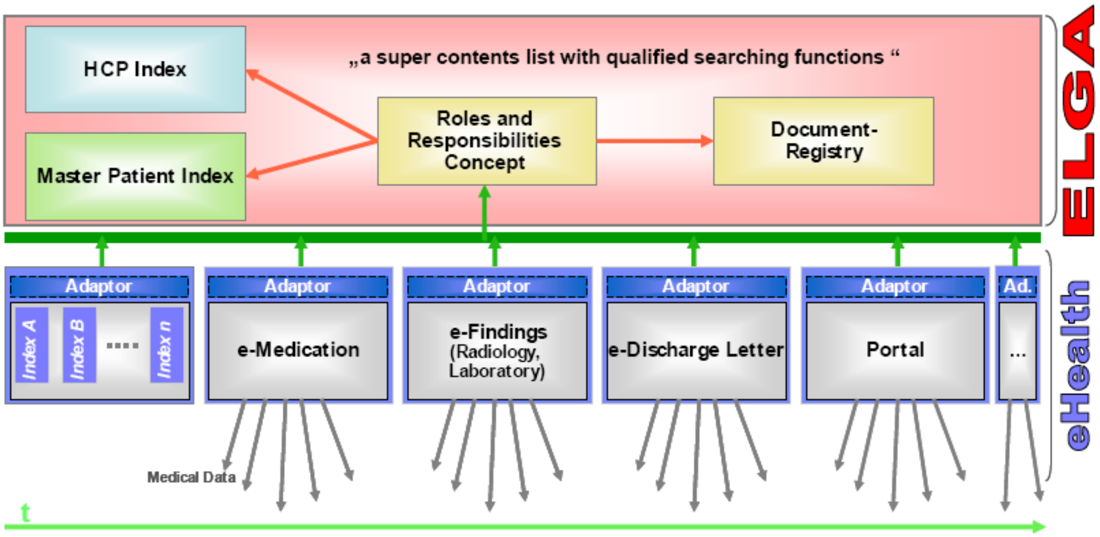


Figure 5.1: Basic structure of ELGA [52]

The main focus of this architecture is set to a central document registry, whereas the documents themselves are stored decentrally by the associated medical service providers. In the following the different basic components and their co–operation is specified (cf. [40]).

- Master patient index
  One important condition for ELGA is the unique identification of each citizen and its

registration in a centrally stored patient index, established throughout Austria and the European Union. This master patient index has the function to union the existing individual identifiers of a patient to one collective identification. These individual identifiers are used to connect the documents — stored in different IT–systems of medical service providers — with the patient. With the aid of the patient index it is possible to allocate the individual identifiers to an unambiguously identifiable person (cf. [40]).
For the implementation of the patient index the IHE–Profile XDS will be used, that stands for Cross–Enterprise Clinical Document Sharing. This profile is part of the IHE Technical Framework and supports the inter–divisional cross–referencing of patient identifiers, so it is possible to create any number of logical keys for a patient. Actually patient identification in Austria is already provided by the eCard (electronic health card) and there also exist some patient indexes, which are already in use. Unfortunately these patient indexes are restricted to Federal State level. There is no solution throughout Austria and the European Union yet (cf. [52]).

- Health care provider index
  For ELGA it is necessary to have a nationwide, complete and up–to–date index of health care providers with interfaces for data maintenance by the different associations. Additionally to the identity of the health care provider miscellaneous information like area of expertise, particular roles and access pattern has to be considered (cf. [40]).
  For big institutions like hospitals a more precisely gradation has to be made e.g. departments (cf. [53]). This index can also be used by the citizens as an electronic reference book (cf. [40]).The main function of this index is to assure that ELGA documents can only be accessed by authorized health care providers restricted to their roles and access rights (cf. [53]). This will be encouraged by the allocation of certificates for each provider (cf. [52]).
  Already existing projects which can be used for identification and authentication of health care providers are eHVD (eHealth directory service) and eVGA (electronic index of medical service providers) (cf. [52]).

- Document registry
  The document registry is responsible for the central storing of meta data of the patient's documents, which is necessary for searching them with good performance, independent from the location where the documents are physically stored. So a central point of the architecture is the fact that the registry entries are always referencing to external documents. A connection to the patient can only be made by the master patient index of ELGA. It also has to be assured that documents cannot be registered twice in the registry. For every document together with its meta data a link to its physical storage location is provided. Additionally registry entries can be summarized in virtual folders for a better general view, naturally it is also possible to allocate access rights to folders (cf. [52]).
  Before a request at the document registry is accepted a correct identification of the health care provider and the concerning patient had to be made. Furthermore the health care provider has to show the proper access rights and roles memberships and at last an agreement of the patient has to be on hand (cf. [53]).

Such registry components are already implemented in a couple of national systems but they were not realized as a whole according to the IHE Technical Framework. Some examples for it are the medical records index NÖGUS, ProDok (problem–oriented documentation) and OpenMEDOCS (hospital information system) (cf. [52]).

- Document repository
  The health care providers continue storing the medical data as hitherto and are responsible for a secure and permanent storage. They are also obliged to grant access to authorized persons for their documents provided by the document registry (cf. [40]).
  Already existing projects in this area are the patient index KAV and the medical records index NÖGUS (cf. [52]).

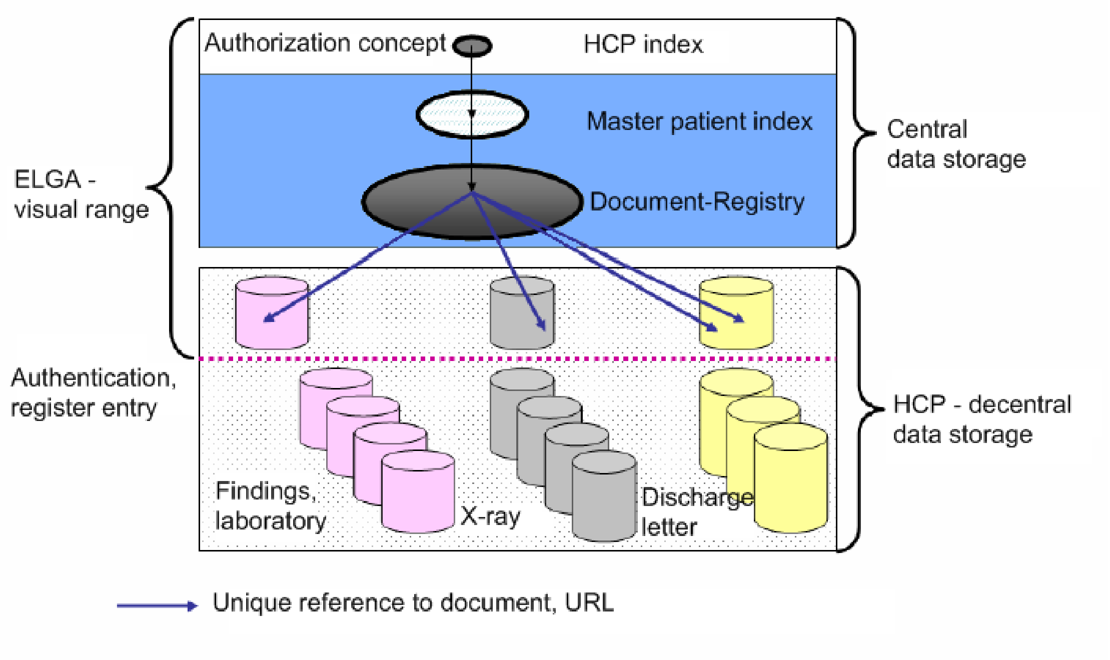


Figure 5.2: Hierarchical view of ELGA ([40])

The last field of action of ELGA includes a number of core applications for common used services that the medical service providers offer. These core applications facilitate the electronic data exchange of medical information and its traceability. They make use of the basic components and together with them they complement one another to an entire electronic health record (cf. [52]).

The first services whose adoption in ELGA is already planned are (cf. [40]):

- e–Discharge Letter
- eMedication

- e–Finding Radiology
- e–Finding Laboratory

Security and authorization details

For ELGA a nationwide authorization and role concept is obligatory necessary, which conforms with the legislative demands and the security measures for privacy. This will guarantee the predictability of legal decisions for the medical service providers and the citizens (cf. [40]).

Basically every patient has to give — according to the legal regulation 2.4 — her agreement to a participation to ELGA. Though this is not realizable for each data transaction it will be handled in such a way that every patient has the possibility to enter an objection, which is also registered in the master patient index. Then the decentrally stored documents and data of this patient could be connected via the central master patient index and the document registry. The read– and write access to this information is assigned separately and the patient can decide to which persons she want to grant data access (cf. [52]).

ELGA stores and uses medical data only for the purpose of diagnosis and medical treatment of patients and the management of health services, it doesn't provide this data for scientific research or medical reporting as is defined in the ELGA Act — in opposition to the original plan in the feasibility study of ELGA, where it was mentioned, that anonymized or pseudonymized health data would be provided for that matter (cf. §14 ELGA–G, [52], [99]).
In contrast to this the social insurance agencies are legally obliged to provide specified public authorities with pseudonymized diagnostic and medical performance data (cf. §84a Gesundheitsreformgesetz 2005).

The IHE Technical Framework — that is used in the authorization component — provides the profile "Basic patient privacy consents (BPPC)", which defines that the patient's agreement can be stored as a document and that registry entries have to be highlighted with a "confidentiality code" (cf. [52], [76]).

The GTelG (Gesundheitstelematikgesetz 2.4) issues the order that for medical data access an approved principle like RBAC (Role based access control) has to be used. The authorization system for ELGA was widened to fulfill some additional requirements e.g. the fact that medical documents always have two principals, the patient (subject) and the health care provider (creator). In many cases the recipient of created documents is unknown at the moment of creation and access rights are often temporally restricted (cf. [52]).

To meet privacy requirements the ELGA authorization system checks every external request and transfers only authorized requests to the appropriate core application. Therefore ELGA has to provide some standard interfaces for this filtering facade: the Cross–Domain Document Sharing Registry (XDR), the Patient Demographics Query (PDQ) and the Patient Identity Cross–Reference Manager (PIX). Furthermore the authorization system has to support the profile ATNA Secure Node, which demands a trusted connection to the partner systems via SSL v3 or TLS with alternating authentication. This profile has to be supported by all core applications too (cf. [53]).

The authorization system that was planned for ELGA is using profiles and tickets to comply with requirements. A ticket symbolizes a mutual trust between the patient and the health care provider. Profiles administer the access rights for a certain object which includes the allowed operations and the necessary roles for whose execution. Additionally there is the possibility to allocate access rights directly to a principal in exceptional cases (cf. [52]).

A ticket is addressed to a principal for documenting a doctor–patient–relationship and defining its validity according to the therapy period and the selected roles. It is also possible to define special arrangements like varying periods of validity for different operations (cf. [52]).

Additionally ELGA provides a log component which collects and archive the internal and external data access of all components with different report possibilities (cf. [53]).

Although privacy of medical data is an important topic in ELGA and its securing has a high priority and is supported by a system of rules, a lot of people — patients and healthcare professionals — are skeptical of ELGA and worry that their private medical data is going to be compromised. This system of rules declares that the patients have to be those who choose if they want to put their medical data into ELGA and to regulate who has access to this information. Furthermore it is stated that nobody is allowed to access ELGA without the patient's consent and the medical data in ELGA has to be admitted by a healthcare professional.

A possible weakness is the inappropriate use of the patient's access data, which mainly lies in the patient's own authority. Naturally there is always the possibility that somebody is able to break into the ELGA system and gains access to the document registry. To avoid this scenario a high value is set to using state–of–the–art technical security measures. The decentral storing of data helps on that front, because the document registry doesn't actually contain medical data, it is an index of contents of medical documents which references to their storage location. A further potential danger to patients' privacy is the possibility of data abuse by an employee of the healthcare system, this should be prohibited using a strict set of rules and protocols and the impending legal consequences due to the ELGA Act (cf. [99]).

ePrescription component details

The core application eMedication supports all process steps of the prescription process and tries to improve the quality of medical treatment. The attending doctor or pharmacy only know a small part of the medication history of a patient and often their only source of information is the patient herself. This could be a problem particularly in a hospital in cases of emergency, where the patient is not responsive. Furthermore if the patient is frequently changing her doctors or pharmacies her medication history will suffer as well (cf. [52]).

For eMedication all drugs, which are only available on prescription will be stored in a centralized database — naturally with agreement of the patient. In a further step the database will be supplemented with over–the–counter drugs, so the full medication history of a patient will be placed at the disposal. So for prescription the health care provider is able to check the selected medicament with means of this existing data pool supported by additional tools and indexes e.g. the SIS specialties information system (index of pharmaceutical products). This information could help significantly to avoid medication errors as already discussed in chapter 4.2. Additionally this database could be an excellent source for providing pseudonymized/anonymized reports about consumption of drugs in Austria (cf. [52]).

For the first phase of implementation the estimated numbers of participants are approximately 8 millions of patients, 1.200 public pharmacies, 18.400 resident doctors and 19.100 doctors in hospitals. The next step is the supplemental connection to the doctor's and hospital dispensaries, which is calculated with 1000 extra participants. Altogether public pharmacies hand out about 163 millions of pharmaceuticals within a year, 90 millions of it — which can be converted into 46 millions of prescriptions — are passed to account by the pharmaceutical salary cash office of Austria (cf. [52]).

ELGA is only responsible for the authorization check for the eMedication database, the data itself is stored at an external location. For sequenced requests during a doctor's advice only one authorization check is executed. The outcome of this is an estimated number of 120 millions of authorization checks, which will be executed by ELGA within a year (cf. [53]).

Pilot projects

One of the first launched prototypes for the eMedication core component of ELGA is Health@Net, which is the model– and reference project of a research group of the Austrian eHealth Initiative. The basic idea behind Health@Net is to create a lifelong electronic health record for patients in Tyrol (cf. [52]).

Another example of a pilot project for eMedication is the "Arzneimittelsicherheitsgurt", the idea of this prototype was born in the course of the plans of the Pharmaceutical Salary Fund and the Chamber of Pharmacists for the creation of an eMedication database, which should contain all filled prescription data. This decision was triggered by the legal regulation — coming into effect on 1.01.2005 — that public pharmacies are obliged to do electronic billing with all social insurance agencies belonging to the Association of Social Insurance Agency (cf. [33]).

As operational area for the first prototype of "Arzneimittelsicherheitsgurt" the province of Salzburg was chosen. Out of 76 public pharmacies in Salzburg 71 of them could be won over for participation in the pilot scheme. The starting signal was on 22.02.2007 and the testing time should last till 30.06.2008 (cf. [33]).

The results of the pilot scheme in March 2008 showed a total of 9.218 patients which participated in the project. The 71 pharmacies dispensed 88.625 medications (23.250 of them over–

the–counter drugs) and 14.588 interaction problems were notified, furthermore 4.212 double medications and 7.382 compliance problems were detected (cf. [89]).

The experience gained from the prototype Arzneimittelsicherheitsgurt was passed on the development of the ELGA core component e–Medikation which has started operations in April 2011 — ([108]). It is described in more detail in the following chapter.

e–Medikation

In March 2009 the Austrian "Bundesgesundheitskommission" authorized the Association of Social Insurance Agency to realize the project e–Medikation together with the Austrian Chamber of Pharmacists, the Medical Association and the Federal Ministry of Health. In June 2009 the project management committee came to an agreement about the project handling, the definition and functional scope of e–Medikation and so the project will be realized as the first ELGA core application (cf. [17]).

Since the authorization for realizing the project e–Medikation in March 2009 was given, work on the respective position paper has started, in which detailed information regarding system architecture, scope and functionality of e–Medikation and planning of the pilot phase were specified ([106].
In this position paper the evaluation results from the previous pilot project Arzneimittelsicherheitsgurt were included ([107]).

After the policy agreement on 08.03.2010, the finishing of requirements analysis was reached in the end of April 2010, followed by the finishing of the system specification in the end of June 2010. The participating project partners are the same as in the project Arzneimittelgurt (cf. [106]).

The project goals of e–Medikation are enhancing the patient safety as well as increasing effcency in the prescription processes. This will be achieved by

- completeness and readability of administered medication
- avoidance of multiple prescriptions
- avoidance of unwanted drug interactions
- future inclusion of relevant information such as allergies, diagnostics and other vital data
- drug server as data foundation of all admitted drugs in Austria
- possibility for the patient to get a print–out of her medication list
- full comprehension of the patient (cf. [106], [18]).

All e–Medikation services are supposed to be integrated in the software systems the project participants are using. The interfaces are geared to international standards, the implementation of an IHE–interface is planned (cf. [106]).

The usage of the IHE–standard was also supported by the FEEI/FV UBIT — the trade association of the electrical and electronic industry, that published a position paper in August 2010. In this paper the trade association approved the realization of e–Medikation and offered its support and participating in the project (cf. [26]).

Also some advices were offered regarding to the investment protection (cf. [26]):

- Consideration of the IHE–conform components like master patient index, HCP–index and the planned pharmacy profile in the pilot project in preparation for the Austrian–wide rollout.
- If the IHE–conformity cannot be considered in all components yet, the development of an integration concept and migration scenarios to the IHE–standard is necessary. The resultant consequences in technical, economical and organizational regard have to be announced to the project participants as part of the acceptance management for all involved parties.
- A collective project overview for the Austrian–wide rollout has to be provided,which considers IHE–conformity, benefits for the patient, costs and deadlines.

The piloting of e–Medikation is divided into two phases. The first phase contains the pilot operations itself, which is supposed to be 9 months in total, and the following evaluation of its development. The piloting includes the checking of multiple prescriptions and unwanted drug interactions. Participants are supposed to be all e–card users (patients), physicians and hospitals in the e–card–system and pharmacies (to be connected to the e–card–system) (cf. [107]).

The prototype functionality includes (cf. [107]):

- Medication database and prescription database, which build on prescribed and administered medication
- Calculation of reach
- Printing of medication overview for the patient at the pharmacy or physician
- Protocol of all transaction data

The medication database that is the foundation of the e–Medikation–checks is composed of

- 12.882 drugs, only available on prescription, which represents 100 % of the permitted pharmaceutical products in Austria
- 4.040 over–the–counter drugs (31 %)

- 336 over–the–counter drugs, which are relevant for drug interaction (2,6 %) (cf. [105]).

The medication list doesn't contain the over–the–counter drugs, which are not relevant for drug interaction, so the printed medication overview for the patient or respectively for the physician or pharmacist doesn't show them either (cf. [105]).

The second phase of the pilot operations considers the evaluation results and adaptions and optimizations based on those results are supposed to be made to the software. The Austrian–wide rollout and the further usage of the ELGA base components also depends on the experiences of the pilot operations (cf. [107]).

Goals of the piloting (cf. [107]):

- Practicable use of e–Medikation
  The test run of e–Medikation should point out what problems occur during the e–Medikation process. Also the room of improvement can be detected according to performance, data quality, usability and alerts. In addition it will test the waters how the health care providers and the patients are accepting the new technology.

- Potential savings and room of improvement in quality assurance
  Attention should be paid to the first ordination of a patient and admission in hospitals.

- Reporting of found problems regarding to the patients safety
  Check of drug interactions and multiple prescriptions, for the latter it could be calculated how many prescriptions were avoided and how much of them would have been covered by the social insurance agency. Also there would be reports available concerning the total number of checks or grouped by how many checks were executed at the hospital, the pharmacy or the physician.

Every patient, who participates in the piloting operations, which is voluntary and free of charge, gets a prescription account. In this account all the prescribed medication or purchased pharmaceutical products are journalized and stored for intake duration and the following 6 months. At the pharmacy or the physician a medication check is possible using the e–card. There is no data stored onto the e–card itself, instead the data is stored in the prescription account and the e–card is used as a key to have access to this data (cf. [108]).

Before going into detail of the architecture and infrastructure of e–Medikation some general information about the Austrian e–card system, which is a core element of the project, is provided.

e–card system

The Austrian electronic health card is a key–card which gives access to eHealth applications for either the card owner or a third party, the latter needs a special second key–card e.g. for physicians (o–card) or for pharmacists (a–card). The e–card only holds some personal and insurance data of the owner like national insurance number and the owner's name. More detailed health insurance data is not stored on the card but in the data center of the e–card system. The card also contains all necessary signature features to use it — after activation of the appropriate certificate — as an Austrian Citizen Card. The patient has to bring the e–card to every consultation of a medical facility to give the physician access to the corresponding data e.g. whether the patient is covered by insurance at all and which health insurance company she is member of respectively (cf. [104]).

The o–card (surgery card) is the key–card and therefore the electronic signature of the physician. The physician also needs a GINA–Box (GINA stands for Health Information Net Adapter) for using the e–card system in her surgery. This is a mini–computer, on which all necessary eHealth applications are installed and with both — the GINA–Box and the appropriate software in combination — the communication with the e–card server can be established. Naturally also a card reader is necessary for getting access to the key–card data. The LAN–CCR is a network–compatible card reader which is usable with one or more GINA–Boxes (cf. [104]).

Of course medical data is not transmitted via the Internet but via the GIN (Health Information Net), a highly secure broadband network only accessible for health service providers. For hospitals there is a separate network connection according to their greater need for bandwidth and redundant network connections — the eHi–Net. The e–card data center is due to reasons of reliability and performance distributed to two different locations (cf. [104]).

The following graphic shows an overview of the services and connections that GIN is providing:

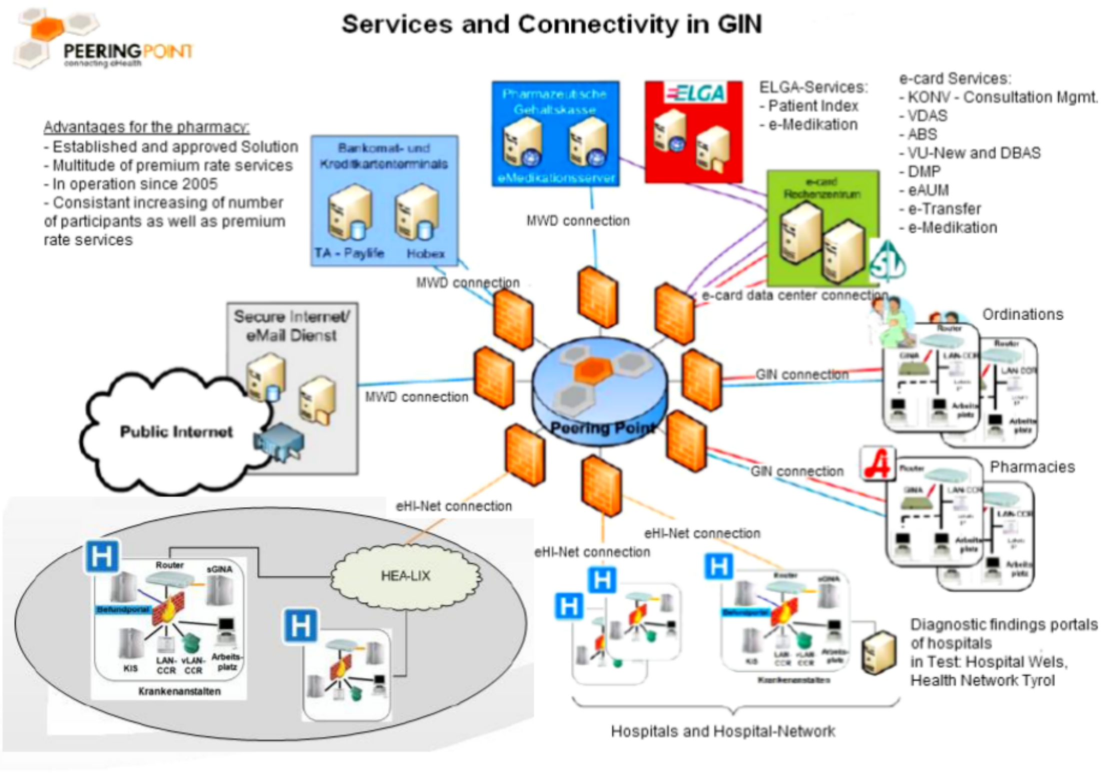

Services and Connectivity in GIN
PEERINGPOINT
connecting eHealth
Advantages for the pharmacy:
- Established and approved Solution
- Multitude of premium rate services
- In operation since 2005
- Consistant increasing of number of participants as well as premium rate services
Bankomat- und Kreditkartenterminals
TA - Paylife
Hobex
Pharmazeutische Gehaltskasse
eMedikationsserver
ELGA
ELGA-Services:
- Patient Index
- e-Medikation
e-card Services:
- KONV - Consultation Mgmt.
- VDAS
- ABS
- VU-New and DBAS
- DMP
- eAUM
- e-Transfer
- e-Medikation
e-card Rechenzentrum
MWD connection
MWD connection
e-card data center connection
Secure Internet/ eMail Dienst
Public Internet
MWD connection
Peering Point
GIN connection
Ordinations
GIN connection
Pharmacies
eHI-Net connection
eHI-Net connection
eHI-Net connection
HEA-LIX
Router
sGINA
Befundportal
KIS
LAN-CCR
vLAN-CCR
Arbeitsplatz
Krankenanstalten
Diagnostic findings portals of hospitals in Test: Hospital Wels, Health Network Tyrol
Hospitals and Hospital-Network

Figure 5.3: Services and Connectivity in GIN [107]

The graphic below shows how the components of the e–card system explained further above and the involved health service providers are networked among each other (cf. [89]).

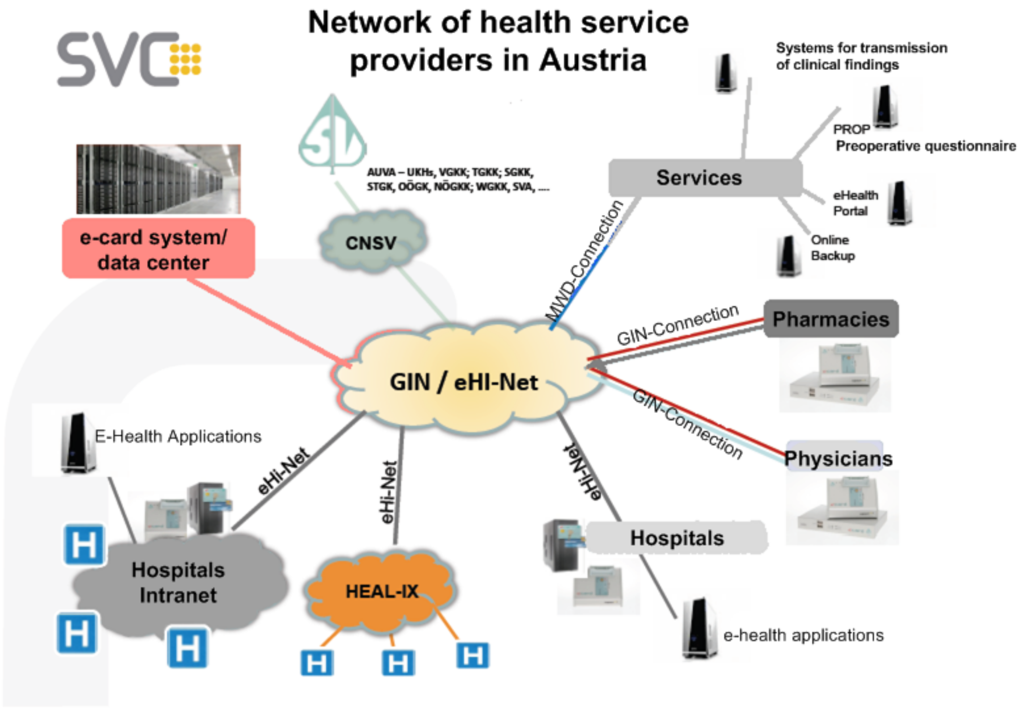


Figure 5.4: Network of health service providers in Austria [65]

e–Medikation architecture details

The project e–Medikation is based on the e–card infrastructure ([105]) — similar to the pilot project Arzneimittelgurt..

The pharmacies, physicians and hospitals have a star–shaped connection using GIN, eHI–net or HEALIX ([105]), which is illustrated in the following graphic (cf. [106]).

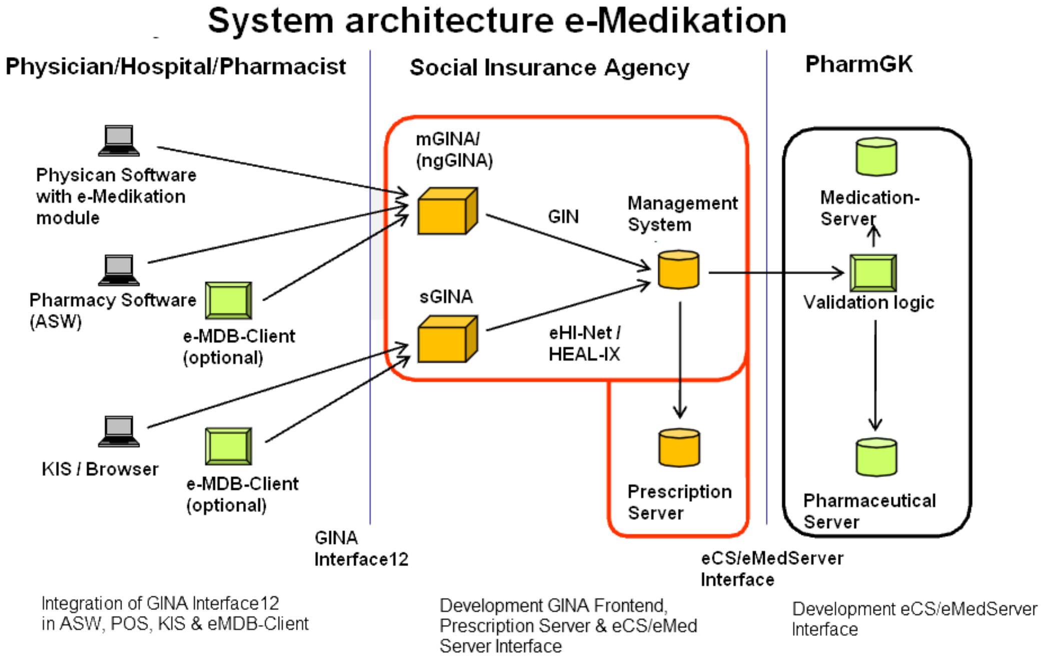


Figure 5.5: System architecture e–Medikation [106]

E–Medikation combines two information network systems. From the data protection view the ordering parties are the participating health care providers. The information network system “prescribed pharmaceutical products” is operated by the Association of Social Insurance Agency, the Sozialversicherungs–Chipkarten–Betriebs– und Errichtungsgesellschaft m.b.H — SVC is the service provider. The information network system “administered pharmaceutical products” is operated by the Pharmaceutical Salary Fund (cf. [29]).

The check for drug interaction is based on SIS (“Spezialitäten–Informations–System”), which is the default standard in the German–speaking world. SIS allows for the physician to request information concerning the patient information sheets, drug composition or intake information. Also it provides an interaction check that is able to compare two or more drugs with each other and recognizes possible interactions. The used data is provided by the Austrian Pharmacists Publisher and is updated on a regular basis (cf. [43]).

It is possible for the e–Medikation functionality to be included in the physician–, pharmacist– or hospital–Software or to be used as a stand–alone client (cf. [105]).

For the pilot project a special e–Medikation client application was implemented, which could load the prescription data from the pharmacy software and execute the e–Medikation functions. Also for hospitals an extra–implementation of an e–Medikation client software was necessary due to the different hospital software systems, though they could only display the patient's medication list and didn't have write access (except one hospital). For physicians the e–Medikation module was integrated in their medical practice–software. The e–Medikation clients are connected to the back–end software via the GINA–interface. The back–end software consists of the management system, which has direct access to the ePrescription server and is connected to the medication server (prescribed medication), the validation logic and the drug server (all admitted drugs in Austria) via the eMed–interface (cf. [18]).

e–Medikation security details

The Austrian Data Protection Commission has in its 196. sitting on 25.05.2010 concordantly agreed to approve the pilot project e–Medikation, based on the position paper, which was filed by the Association of Social Insurance Agency. In its statement the Austrian Data Protection Commission remarked that the pilot project needs the explicit acceptance of the affected persons and after finishing the pilot operations a solid legal foundation has to be created for the e–Medikation component. The wording of this legal foundation has to be paid particular thoughtfulness according to its intrusion in a basic right (cf. [16], 2.4).

The participation in the pilot project is voluntarily and free of charge, the patients have to sign once a declaration of approval, which can be withdrawn at any time. With this declaration of approval the patient complies that pharmacists and physicians are allowed to gain insight into her medication data and to update it (cf. [108]).

The agreement for participating in e–Medikation is given in the following way (cf. [106]):

- Finding a health care provider, who is participating in e–Medikation
- The patient has to bring a signed declaration of approval and her e–card
- Going through the activation dialogue in software with e–Medikation integration
- Signing with e–card

The withdrawal of the participation requires similar steps, but the patient has to announce her cancellation and the appropriate dialogue in the software has to be run through ([106]).

Data, which is gained during the pilot operations is only allowed to be used in anonymized form for statistical reports. Also the data is only used for drug interaction validation and is not handed over to third parties, not even the general practitioner, the patient alone decides who is able to have insight to her data. With the declaration of improvement the patient gives a general agreement to usage of her data in the information network system, which lies behind e–Medikation. But she has to approve in every single case of using e–Medikation by a given request of the pharmacist/physician and the provision of her e–card (cf. [29]).

The topic data protection is a principal point in e–Medikation. Particularly between the physicians and the Association of Social Insurance Agency this is an issue, which has caused a lot of trouble. The Medical Association criticizes the fact, that the patient is able to block access to any part of her medical data, because it is necessary to have the overview of the complete data for a decent treatment. On the other side the Association of Social Insurance Agency states, that the patient must have the decision which of her medical data is visible to others, everything else would violate the data protection law (cf. [102]).

A main issue regarding to data protection is according to the Austrian Society for Privacy and Data Protection the number of persons who have access to this sensible medical data, which is totally incalculable. Many of the medical staff members have access to this kind of data and don't subject to the obligation of secrecy (cf. [102]).

An example for this kind of security leak was given in a discussion organized by the Austrian General Practitioners Association on 08.06.2010, where one of the speakers referred to a personal experience in this matter. A male nurse was taken to the hospital — the one he worked in — by the ambulance, because of a serious accident. This hospital has a total of 1600 employees and within several days the patient's records were inspected about 1400 times. It is doubtful, that so many accesses were necessary because of medical reasons and the assumption stands to reason that curiosity has taken over (cf. [77]).

e–Medikation ePrescription process details

The following graphics are showing the run of the e–Medikation process in different surroundings. At first the standard process at the physician is shown, which starts with the obligatory agreement of the patient to give access to her medication data via her e–card. The one–time agreement necessary for participating e–Medikation is not shown in the graphics. Afterwards the physician loads the patients medication data using the e–card system. After prescribing the necessary drugs, the validation check is executed and the result is displayed. The physician can either accept the result or automatically document the warnings. If interactions were found the physician is able to correct her prescription and go back to the previous prescription planning part of the process. The prescription is stored in the medication database and printed for the patient (cf. [105], [106]).

The e–Medikation process at the pharmacy is different depending on whether the medication is an over–the–counter product and if a previous validation check has already been executed. If the patient has had her prescription validated by the physician no further check is necessary and the process is executed as shown in the graphic 5.7. The prescribed medication is read in and the prescription is filled and stored in den medication database. The process is finished after handing over the prescribed medication (cf. [105], [106]).

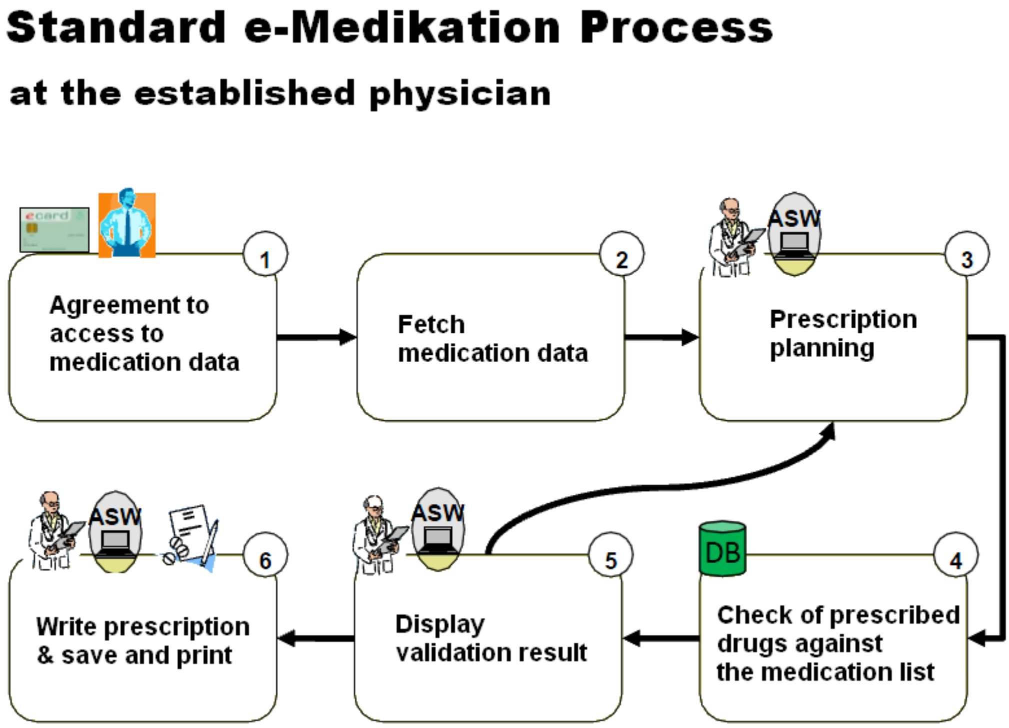

Standard e-Medikation Process
at the established physician
ecard
1
Agreement to access to medication data
2
Fetch medication data
ASW
3
Prescription planning
DB
4
Check of prescribed drugs against the medication list
ASW
5
Display validation result
ASW
6
Write prescription & save and print

Figure 5.6: Standard e–Medikation Process Physician [106]

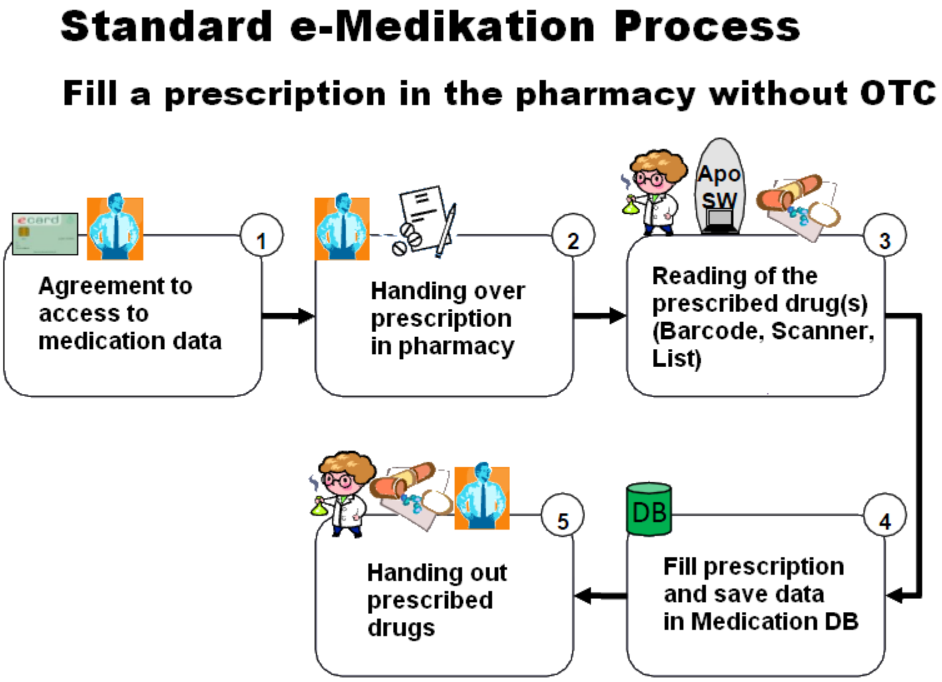

Standard e-Medikation Process
Fill a prescription in the pharmacy without OTC
ecard
1
Agreement to access to medication data
2
Handing over prescription in pharmacy
Apo SW
3
Reading of the prescribed drug(s) (Barcode, Scanner, List)
DB
4
Fill prescription and save data in Medication DB
5
Handing out prescribed drugs

Figure 5.7: Standard e–Medikation Process Pharmacy without OTC [106]

But if the validation check wasn't executed by the physician because of a home visit or over–the–counter products are purchased, the e–Medikation process at the pharmacy is executed as shown in the next graphic, which is very similar to the one regarding the physician (cf. [105], [106]).

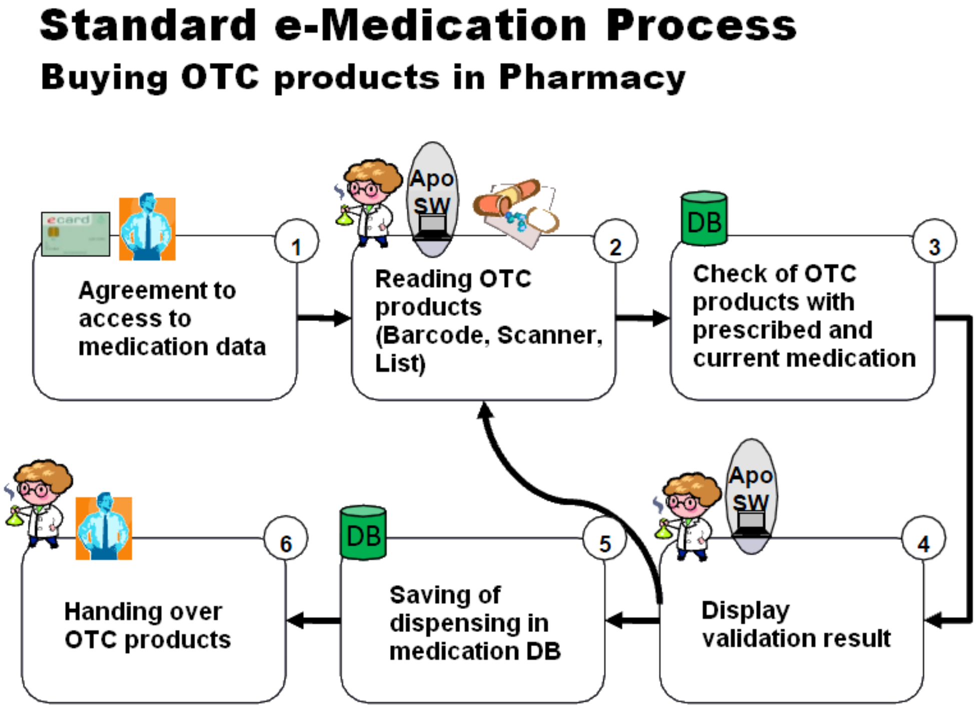

Standard e-Medication Process
Buying OTC products in Pharmacy
ecard
1
Agreement to access to medication data
Apo SW
2
Reading OTC products (Barcode, Scanner, List)
DB
3
Check of OTC products with prescribed and current medication
Apo SW
4
Display validation result
DB
5
Saving of dispensing in medication DB
6
Handing over OTC products

Figure 5.8: Standard e–Medikation Process Pharmacy with OTC [106]

The e–Medikation process at the hospital starts with the agreement of the patient at the admission. Whether the hospital software has KIS integration or not, one of the following two process variations are run through (cf. [106]).

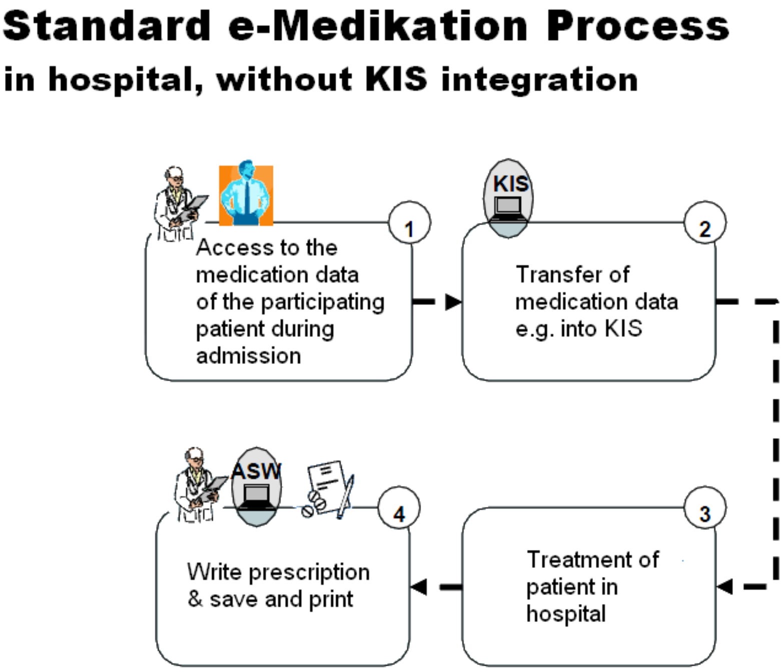

Standard e-Medikation Process
in hospital, without KIS integration
1
Access to the medication data of the participating patient during admission
KIS
2
Transfer of medication data e.g. into KIS
3
Treatment of patient in hospital
ASW
4
Write prescription & save and print

Figure 5.9: Standard e–Medikation Process Hospital without KIS [106]

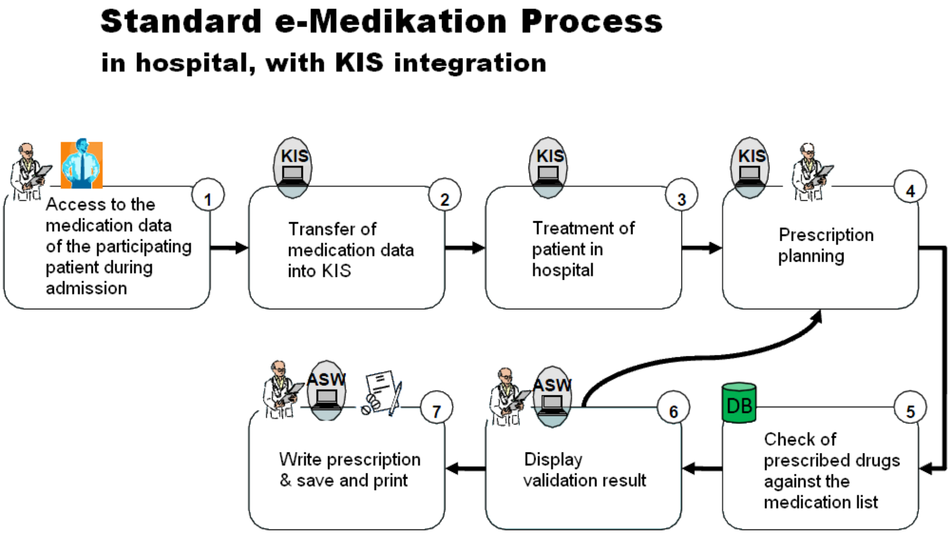
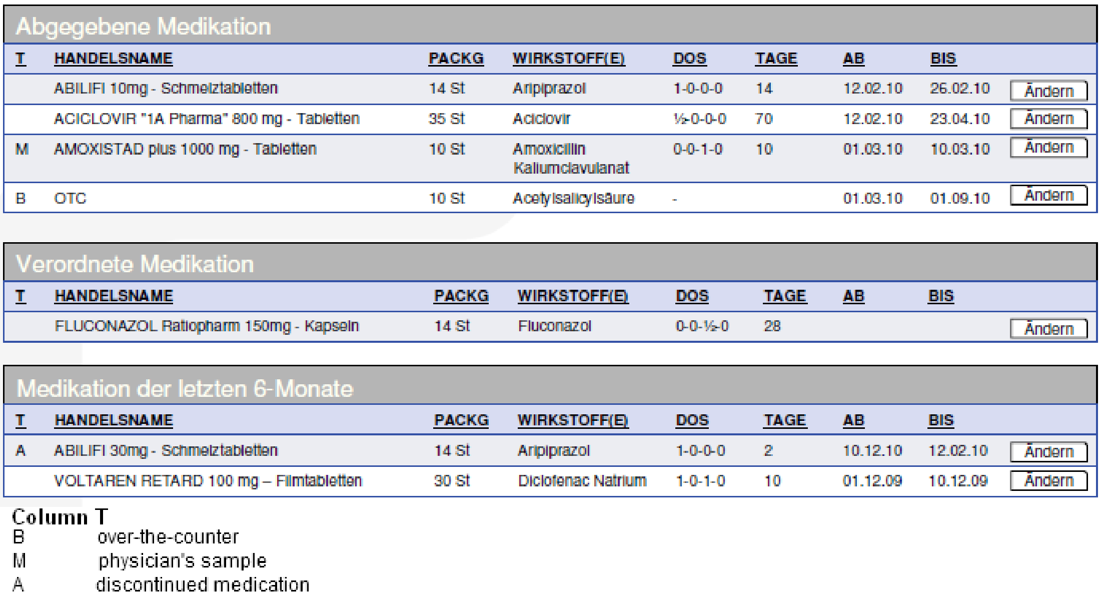

Standard e-Medikation Process
in hospital, with KIS integration
1
Access to the medication data of the participating patient during admission
KIS
2
Transfer of medication data into KIS
KIS
3
Treatment of patient in hospital
KIS
4
Prescription planning
DB
5
Check of prescribed drugs against the medication list
ASW
6
Display validation result
ASW
7
Write prescription & save and print

Figure 5.10: Standard e–Medikation Process Hospital with KIS [106]

Since December 2010 the company INNOMED, which develops medical software applications,works on the integration of the e–Medikation component into their products. The installation and delivery of the new software starts with April 2011 (cf. [32]).



Abgegebene Medikation

T	HANDELSNAME	PACKG	WIRKSTOFF(E)	DOS	TAGE	AB	BIS	
	ABILIFI 10mg - Schmelztabletten	14 St	Aripiprazol	1-0-0-0	14	12.02.10	26.02.10	Ändern
	ACICLOVIR "1A Pharma" 800 mg - Tabletten	35 St	Aciclovir	½-0-0-0	70	12.02.10	23.04.10	Ändern
M	AMOXISTAD plus 1000 mg - Tabletten	10 St	Amoxicillin Kaliumclavulanat	0-0-1-0	10	01.03.10	10.03.10	Ändern
B	OTC	10 St	Acetylsalicylsäure	-		01.03.10	01.09.10	Ändern

Verordnete Medikation

T	HANDELSNAME	PACKG	WIRKSTOFF(E)	DOS	TAGE	AB	BIS	
	FLUCONAZOL Ratiopharm 150mg - Kapseln	14 St	Fluconazol	0-0-½-0	28			Ändern

Medikation der letzten 6-Monate

T	HANDELSNAME	PACKG	WIRKSTOFF(E)	DOS	TAGE	AB	BIS	
A	ABILIFI 30mg - Schmelztabletten	14 St	Aripiprazol	1-0-0-0	2	10.12.10	12.02.10	Ändern
	VOLTAREN RETARD 100 mg – Filmtabletten	30 St	Diclofenac Natrium	1-0-1-0	10	01.12.09	10.12.09	Ändern

Column T

B	over-the-counter
M	physician's sample
A	discontinued medication

Figure 5.11: software–integrated medication list [105]

e–Medikation status

As already mentioned in the previous chapter the pilot operations of e–Medikation has started in April 2011 ([108]).
It is supposed to has a total run duration of 9 months, in which the first 3 months are considered as warm–up time and the remaining 6 months are used for evaluation. The evaluation results in turn are used for planning future steps of an Austrian–wide rollout ([105]).

The following Austrian regions are used for pilot operations ([108]):

- Vienna (21. and 22. area)
- Upper Austria (Wels–Stadt, Wels–Land, Grieskirchen, Eferding)
- Tyrol (Reutte, Imst, Landeck)

In addition also in some hospitals e–Medikation is provided ([108]):

- Vienna (SMZ Donauspital, SMZ Floridsdorf)

- Upper Austria (Klinikum Wels–Grieskirchen)
- Tyrol (Bezirkskrankenhaus Reutte, Krankenhaus St. Vinzenz Zams, Uniklinik Innsbruck)

So in total up to April 2011 there are 6 hospitals, more than 50 pharmacies and about 100 physicians participating in this pilot project which are able to register patients since the start of the project operations ([108]).

On 16.05.2011 a press conference took place, initiated by the Association of Social Insurance Agency and the Austrian Medical Association according to a first retrospection of the pilot project. Whereas the Association of Social Insurance Agency stated contentment with the development and only admitted to minor shortcomings to the pilot project, the Medical Association raised concerns over it — the main point of criticism being the securing of the patient's data privacy protection (cf. [62]).

A big issue concerning the further development of the pilot operations is the fact, that the Association of Social Insurance Agency didn't make a public announcement regarding the installation of the needed software for e–Medikation. This led to a court decision initiated by the Federal Public Procurement Office (BVA), which led to a fine of € 24.000 and the nullification of the contracts with the hired software companies. The Medical Association even went to such lengths as requiring to stop the pilot project (unsuccessfully) (cf. [62]).

The evaluation of the pilot project stated a positive performance and recommended the continuation of e–Medikation in consideration of some suggestions of improvement, also the majority of the participating pharmacists, patients and physicians reviewed e–Medikation as good and useful for the patients. Naturally the evaluation contained also the negative comments of the pilot project participants and other problems and shortcomings, that occurred during the pilot. Critical points were the quality of the client software, long response times, long processing times, bad usability and quality of training, some of those complaints varied strongly between the different client software applications, which contained the e–Medikation module. Software integration in pharmacies needs to be improved, the pharmacists suggested to integrate the e–Medikation module into the pharmacy software, instead of a stand–alone client. In general there were concerns if the e–Medikation software is ready for use according to the performance and stability problems in the pilot, also a better integration of e–Medikation into the processes at the pharmacy of the physician's office is necessary (cf. [18]).

The pilot project evaluation pointed out how important it is to give patients the possibility to access their medication lists personally, not only due to patient safety but also because patients, who have used this service once will usually continue using it. A main critical point was the incomplete storage of prescription data which is crucial for the benefit of ePrescription, so an area–wide roll–out involving all healthcare professionals (public, private, hospitals, ambulances etc.) is necessary for achieving a complete collection of all dispenses. In this context the possibility of excluding certain drugs from the medication list by the patient was considered unreasonable. The including of over–the–counter drugs was positively observed because of the big amount of drug–interaction warnings they generated (cf. [18]).

Furthermore it was noted that the e–Medikation modules for the client applications hardly used international standards like IHE or CDA, despite the Austrian eHealth strategy determined the use of IHE profiles. 5 out of 7 software manufacturers, who developed the clients for the pilot, didn't use those mentioned standards, 3 of them didn't even know what IHE was. According to privacy primarily the physicians worried about abuse of patients' data, there was also apprehension, that the prescription data could be used for spying on the healthcare professionals and their prescription habits (cf. [18]).

The Association of Social Insurance Agency was instructed to accomplish the nation–wide roll–out and start–up of e–Medikation in Austria until 31.12.2014. At the earliest — depending on the due–process completion of the necessary ELGA components — storing of e–Medikation data is possible from 01.01.2015 for public hospitals and will be gradually expanded to other medical institutions (pharmacies, physicians etc.) (cf. [109]).

Current status

In 2006 the Austrian Federation, the Austrian social insurance agencies and the Austrian "Bundesgesundheitskommission" decided in the 15a–agreement that ELGA should be realized as a public infrastructure. A feasibility study for ELGA was successfully finished in 2007, a following study concretized the ELGA system components and a master–plan for realization. Further milestones were the harmonization of the necessary document standards, cost–benefit–calculations and the legal regulations (cf. [53], [30]);

After passing the ELGA Act in 2012 (2.4) the necessary legal requirements for ELGA were provided, e.g. defining the opt–out possibility for citizens, who don't want to participate in ELGA and the access to an Internet portal, where citizens have insight into their medical data (cf. §§15,16 ELGA–G, [30]). Both the Internet portal and opt–out offices have to be provided until 31.12.2013, which is also the start date for the official use of ELGA (cf. §27 ELGA–G).

The following deadlines are defined for obligatory storing of medical data via ELGA (as far as the technical realization of ELGA components allows it) (cf. §27 ELGA–G, [30]):

- 01.01.2015 public hospitals (redundancy letters)
- 01.07.2016 pharmacies, physicians and ambulances (e–Medikation, lab reports, X–ray reports)
- 01.01.2017 private hospitals, living wills, medical registers
- 01.01.2022 dentists

For the planned eMedication core application in ELGA some prototypes were already launched. In 2011 the latest pilot project “e–Medikation“ has started operations in some selected regions of Austria ([108]).

5.2 Electronic Health Insurance Card (Germany)

The Electronic Health Insurance Card (abbr. eGK) — with electronic prescription as one of its basic components — was planned to be established in Germany in 2006. Since 1999 preparations for launching the new Health Insurance Card were in progress and influenced different legal regulations for providing the conditions and infrastructure for electronically networked health care (cf. [92]).

The German Federal Act GMG (GKV–Modernisierungsgesetz) determines the upgrading of the conventional health insurance card to an Electronic Health Insurance Card until 1. January 2006. Furthermore it contains detailed specifications about the card functions, the interaction with the patient, processing of medical data and data transparency. In addition the introduction of healthcare profession identity cards is defined (cf. [64]).

In September 2003 the Federal Ministry of Health entrusted an industry consortium with the specification of a telematics architecture, which represents the foundation of the introduction of the eGK. In April 2004 protego.net (project telematics for health organizations) was founded, a project group which has the function to develop an improved architecture. The next big step was the foundation of the business organization “gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“ in the beginning of 2005 with involvement of the head organizations in public health sector. The composition of these head organizations consists in equal shares of cost–bearers and care providers (e.g. pharmacy association, physicians etc.). The main function of the business organization gematik mbH is the development and introduction of the eGK and its core applications e.g. the electronic prescription (cf. [92]).

Currently about 80 % of the 700 millions of prescriptions per year were already created electronically, but printed thereafter for the patient’s use. Later the prescriptions were digitized again in the pharmacy, so there are some unnecessary and cost–generating breaks between hard–copy and digital format, which could be avoided by using the eGK (cf. [4]).

The healthcare profession identity cards play a major role in the introduction process of the eGK. They represent the interface to the sensitive medical data on the eGK and so the equipment of health care professionals with these cards has a high priority (cf. [92]).

In total there are about 80 millions of insured persons who will use the eGK. Together with about 270.000 physicians, 65.000 dentists, 2.200 hospitals and 21.000 pharmacies and 300 private and compulsory health insurance funds they will be connected among each other and use the established infrastructure around the eGK (cf. [4]).

Thereby efficient data exchange and flexible data access between different institutions is possible. So a powerful infrastructure is necessary as a solid base for the eGK and the protection of the managed data has to be assured. This infrastructure has to be realized within certain boundaries, which are predetermined by many requirements and legal regulations regarding privacy protection. Also the business processes should remain as unchanged as possible, otherwise the acceptance of the users would be at risk. Furthermore the efficiency of the work routines has to persist. In addition filling ePrescriptions should be possible in online pharmacies just as well as in conventional pharmacies, the physical presence of the patient must not be required in such cases. Supplementary the already existing infrastructure, e.g. the IT–systems, which are in use in medical practices or the document management systems in hospitals are planned to be tied to the telematics infrastructure to a large extent in order to keep down migration costs (cf. [11]).

In general there are two types of planned applications which will be realized in the course of the eGK. Obligatory applications (e.g. ePrescription), which are intended to save costs and reduce administrative work and optional applications (e.g. emergency data record, medication history), which should improve the interaction between the health care professionals and the involvement of the patient in the medical process (cf. [11]).

Architecture and technical details

The telematics infrastructure has to be very flexible to satisfy all the requested requirements. Already existing infrastructure and responsibilities should be respected. Nevertheless the operating of the infrastructure and the health care organizations are not meant to be too intimately connected with each other, it should be possible that also non–healthcare companies are able to conduct system components of the infrastructure e.g. the personalization of the smart cards will be sourced out to an external service provider (cf. [11]).

Due to the requested flexibility of the system according to projected further applications and storage locations of data the telematics infrastructure was planned as a service–oriented architecture (SOA). Though some restrictions concerning the design of the architecture had to be regarded:

- Because some data is stored locally on the card it is necessary that some processes are also executed on the client side.
- Regarding security and performance no dynamic service binding via UDDI is used.
- RPCs are used for communication between the services, a document–oriented process model was rejected due to performance and availability weaknesses (cf. [11]).

The graphic below gives a survey at the architecture of the telematics infrastructure:

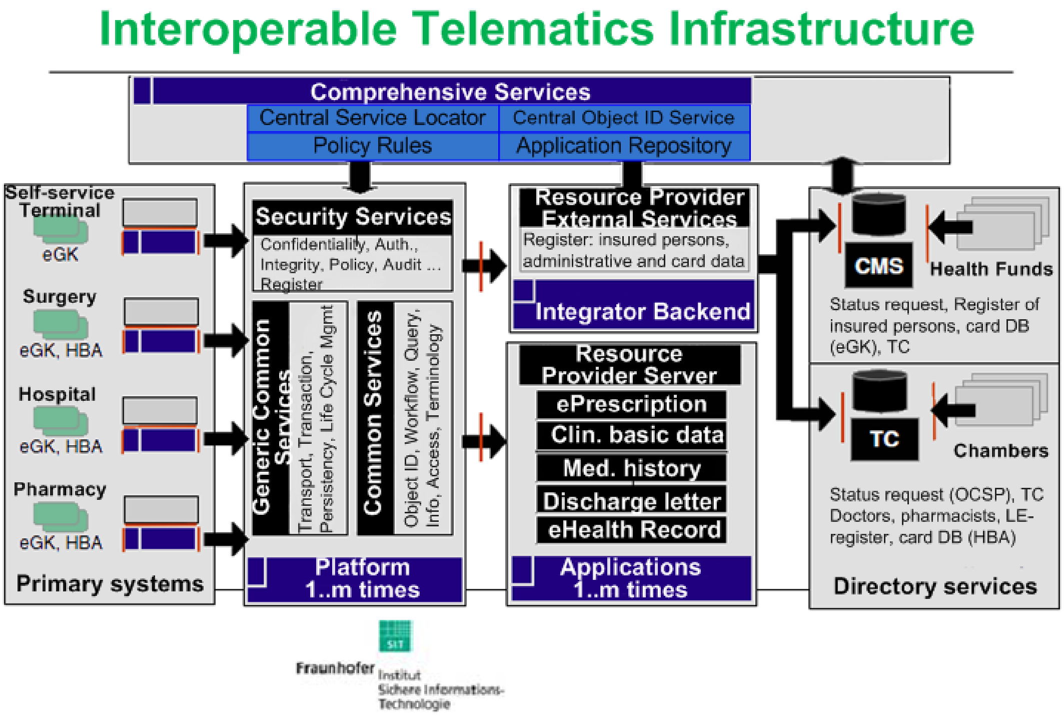

Interoperable Telematics Infrastructure
Comprehensive Services
Central Service Locator
Central Object ID Service
Policy Rules
Application Repository
Self-service Terminal
eGK
Surgery
eGK, HBA
Hospital
eGK, HBA
Pharmacy
eGK, HBA
Primary systems
Security Services
Confidentiality, Auth., Integrity, Policy, Audit ... Register
Generic Common Services
Transport, Transaction, Persistency, Life Cycle Mgmt
Common Services
Object ID, Workflow, Query, Info, Access, Terminology
Platform 1..m times
Resource Provider External Services
Register: insured persons, administrative and card data
Integrator Backend
Resource Provider Server
ePrescription
Clin. basic data
Med. history
Discharge letter
eHealth Record
Applications 1..m times
CMS
Health Funds
Status request, Register of insured persons, card DB (eGK), TC
TC
Chambers
Status request (OCSP), TC Doctors, pharmacists, LE-register, card DB (HBA)
Directory services
SIT
Fraunhofer Institut Sichere Informations-Technologie

Figure 5.12: Architecture telematics infrastructure [103]

On the left side there are shown the pharmacies, the medical centers, the hospitals and the patients, who have access to their medical data via the self–service terminals. They are using their health profession identity cards (HBA) and the eGK to access the telematics infrastructure and the included services and applications via the connector links. In the back–end structure is on the one hand the card management system, which is in the responsibility of the health funds and the trust center, which is supporting the security functions (cf. [103]).

The architecture is divided into several layers to which the different system functions are allocated (cf. [11]).

1. Presentation (primary system)
2. Business processes (concatenation of single services, set up decentrally in primary system)
3. Services (encapsulation of functions)
4. Applications (implementation of business logic)
5. Infrastructure (data storage, system management)

The services layer is split into two parts, the topmost of them is realized in the primary system and acts therefore on the client side. To connect those decentral services with the base infrastructure and the central services a connector has to be used. Therewith the primary system has secure access to the functions of the service bus, which means in succession secure access to the central services and applications. An example for a central service, which could be used via the connector is the validation check of an ePrescription, which includes checks of format, date and signature of the prescription. This service is realized as a re–loadable proxy in the connector, that has access to the appropriate service implementation in the base infrastructure. Also the user of the primary system is not able to see if data, that is stored on the card, is read out by the virtual file system of the connector or by a server–side service. Another concept is the use of consistent services, which means a cascading of services with the bottom service implemented at the connector (cf. [11]).

The infrastructure contains several basic services (e.g. for unique ID creation) and security services that could be used by the application services, which provide the functionality of the applications. These application services are able to use each other for performing more complex tasks. Due to the low interconnection of the different services it is easy to integrate additional services. Indeed every service has to implement two base interfaces:

- a CRUD interface (CRUD = create, read, update, delete) for access to the medical data objects
- an authorization–management interface for administration of access rights to the medical data objects (cf. [11]).

Security and authorization details

In the German Social Security Act (Sozialgesetzbuch SGB) the patient's right of data sovereignty is stated, it is also defined, that the card must support a qualified electronic signature and secure authentication. The use of the patient's medical data without consent is restricted to emergency cases or matters of organ donation, when the patient isn't amenable to treatment. The gematik organization is responsible for ensuring the patients' rights and to maintain their privacy according to the legal specifications within the telematics infrastructure (cf. §§291a, 291b SGB). Beside the Social Security Act the legal requirements for privacy within the telematics infrastructure consist of the European Community Directive 95/46/EG and the German Data Protection Act (cf. [36]).

Correspondingly privacy protection was one of the cornerstones for the architecture of the telematics infrastructure, voluntariness and transparency towards the patient has priority. In this context the use of pseudonymization and anonymization is intended as privacy supporting techniques. The Fraunhofer institute developed the pseudonymization approach for the eGK on the authority of the Ministry of Health (cf. [36], [11]).

A pseudonym has to be unique and is created by using a cryptographic hash function, which takes a part of the social security number, the last name of the citizen and a random value as input. The pseudonym is always connected to a certain eGK, if a new eGK is issued a new pseudonym has to be created. A patient has a different pseudonym certificate with a private key for authentication and for encryption respectively and so the pseudonym can be used for signing the patient's messages and using the audit service. The audit data cannot be assigned to a certain patient without knowing the pseudonym. A de–pseudonymization isn't necessary for several of the planned eHealth services and therefore isn't allowed for them. The outcome of this is that for example ePrescriptions cannot be reassigned to a patient after a eGK-change. It's not possible to pick up an ePrescription from the old eGK and transferring it to the new one (cf. [36]).

Supervising data protection and social security administration is in the scope of duties of the Data Protection Commissioner, there is one on the federal level and one in each of the 16 German states, who are operating on the state level. Data linkage is subject to the strict legal restrictions and is only done on a state level, not on a national level, but it is possible to extract medical data within the individual health care organization and provide them anonymized or pseudonymized for research projects with the purpose of improving health care quality (cf. [67]).

For example the national cancer registry in Germany gets the collected data regarding registered cancer cases from each state. Pseudonymization is done with a national algorithm, therefore it is possible for the national cancer registry to check the data for completeness and possible bias and to provide reports on a national level. Researchers and data analysts only have access to pseudonymized or anonymized data and employees of the institution, that is in charge of pseudonymizing data have to deal with strong access restrictions and to follow data confidentiality rules. Pseudonymized data doesn't contain any names, but possibly other identifying information like date or place of birth if the research project can justify the need of this data and the potential of re–identification is low. To make re–identification less likely it is possible to decrease the level of detail (cf. [67]).

Using medical data of different states or linking it further with other data sources needs to be approved from each involved state, which makes national research projects cost and time intensive. Data from the electronic healthcare record is not used as data source for quality improving research, because it doesn't cover enough health care processes at the moment (cf. [67]).

The eGK plays a central role in the telematics infrastructure. It contains a smart card with a micro processor, a storage unit and communication interfaces and is able to do the authorization by means of a personal identification number (PIN), which is chosen by the patient. The encrypted PIN is stored on the card and protects the data against unauthorized access. Additionally the last 50 access attempts are stored on the card (cf. [35]).

The card also serves as data storage for information required by European regulations, so that the eGK can be used EU–wide as health insurance card. This is a mandatory feature by regulation (German Federal Act GMG), as is the administrative data on the card the information of possible private health insurance (cf. [97]).

All the data on the card is encrypted with the RSA cryptographic system which has been recommended by the Federal Office for Information Security. The length of the private key was chosen with 2048 bit and therefore cannot be cracked in a reasonable period of time by present technology. Furthermore the private key is stored in a especially secured data area of the card which is protected against active and passive electronic eavesdropping and physical manipulations (cf. [35]).

As a matter of principle in the telematics infrastructure sensitive data is used strongly earmarked. It is defined precisely which data is necessary for which purpose. Due to the additional pseudonymization it is made sure that no unauthorized people have data access or could draw a conclusion to the patient's identity (cf. [35]).

In order to be responsive to the technological improvement the telematics infrastructure is checked every year in collaboration with the Federal Office for Information Security concerning the used cryptographic mechanisms. If security deficiencies are found the appropriate adaptions regarding to the hardware, software and smart cards are made. Anyway every six years the smart cards are going to be replaced (cf. [35]).

The connector represents the interface between the medical practice and the telematics infrastructure. On that account security is a big issue and the connectors are checked and certified in this regard with special care. The following picture shows how the connector, the eGK and the HBA ("Heilberufsausweis") are working together during the process of data encryption [35].

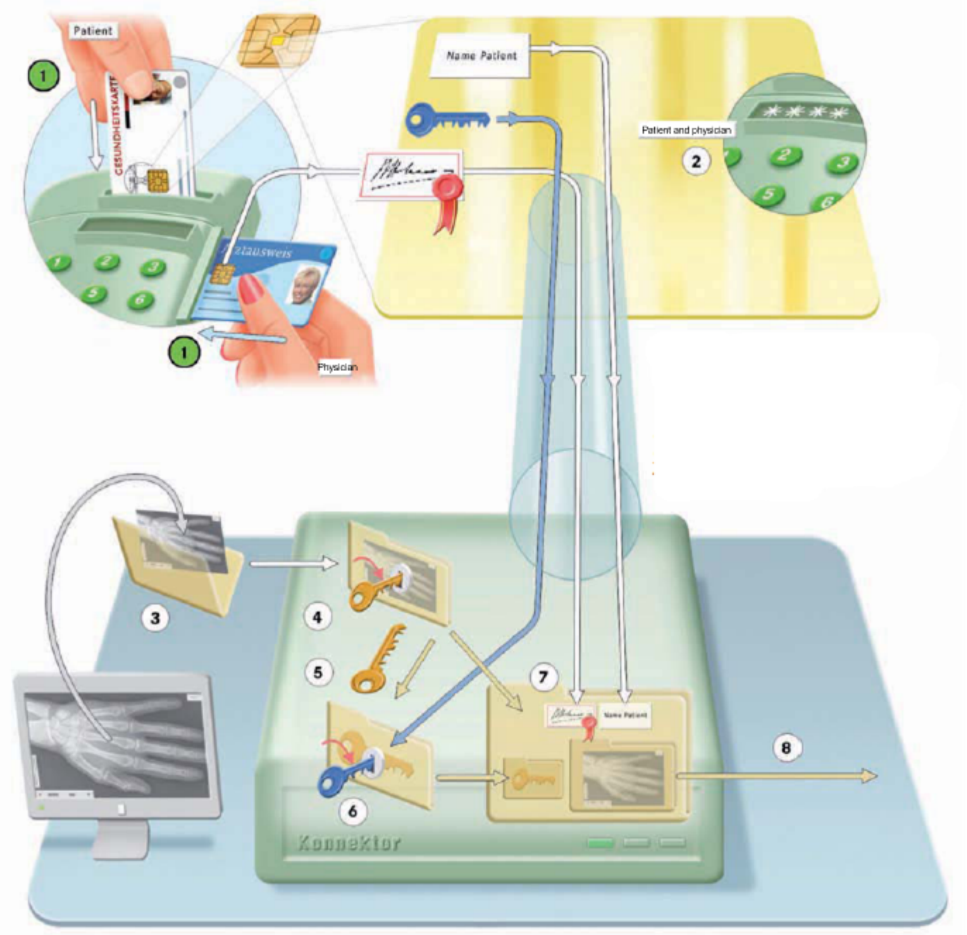


Figure 5.13: Encryption of medical data in telematics infrastructure [35]

For gaining access to the telematics infrastructure it is necessary that both the eGK and the HBA are inserted in the card reader. Afterwards their owners have to enter their PINs, which is shown in the top half of the picture. After successful PIN validation medical data (e.g. X–rays) can be sent to the connector, which encrypts the data symmetrically with a randomly generated secret key that is in turn encrypted asymmetrically with the public key of the eGK. This secret key can only be used once for decryption (cf. [35]).

This security technique is called Challenge–Response and the idea behind this authentication method is that a person has to solve a riddle whose solution only she and no one else is able to know. Transferred to the telematics infrastructure only the eGK whose public key is used for encryption of the random number is able to decrypt it with its private key and therefore provide the solution for the riddle (cf. [10]).

For integrity check the connector calculates a check–sum of the medical data to assure that nobody can manipulate it. The check–sum is signed in the smart card of the HBA, which additionally attaches the physician's certificate for proof of authenticity (cf. [35]). The used certificates can be allocated to the different health care providers by group identification [10]. After all these security checks the medical data is ready for being sent to the telematics infrastructure [35].

In case of the other way round when medical data in the telematics infrastructure is going to be interrogated from outside the encrypted secret key is sent to the eGK where the internal card processor decrypts it with its private key. Afterwards the decrypted secret key goes to the connector which uses it for further decryption of the medical data. Afterwards the secret key is deleted. Naturally also in this case both PINs of the cards have to be validated first. This hybrid encryption technique is supposed to provide a higher level of security for the eGK (cf. [35]).

In this scenario the connector has to provide a secure transport channel between connector and card terminal and between connector and telematics infrastructure to make this whole process work. The medical data is already encrypted on application layer by using the Secure Sockets Layer Protocol (SSL). Using the Internet Protocol Security method the data is once more divided into smaller data packets that are individually encrypted again by the connector. Within the telematics infrastructure the medical data is received by a broker that is checking every data packet in the regard, that it had been transmitted by an active, certified connector (cf. [35]). For both connectors and HBAs black lists are existing, so stolen or broken cards and connectors cannot be misused [11]. Furthermore brokers provide functions for protecting the system from denial of service attacks [35].

Naturally the owner of the eGK has to be able to trace when and by whom her medical data has been accessed. The audit service is responsible for logging these events, the protocols themselves are encrypted with the public key of the patient's eGK to assure that only the card owner has access to this protocol data. Of course the audit service does not store any medical data in the protocol not even in encrypted form (cf. [35]).

Apart from the security level which is tried to be realized by technology there are some legal regulations that are assuring privacy from the legal perspective. The patient decides if she wants to gain access to her medical data und who is allowed to see which information. So the patient is able to specify which information is visible for each of her individual physicians e.g. she can make accessible her complete electronic health record except to Dr. X who is only allowed to see the medication history (cf. [4], [11]).

So such access restrictions can be made in very complex combinations by the patient herself. When a HBA is trying to gain access to the patient's medical data the role allocation is checked by using the HBAs certificate and private key for identification and authorization. Usually a default definition of access authorization is assigned for every set of medical data, additionally the patient can define her own authorization rules, which are extending or restricting the default ones for certain persons or health care provider groups (cf. [10]).

ePrescription component details

In 2003 the representatives of the German Pharmacist Association made the proposal to use a mailbox system for the ePrescription process. So for getting and filling an ePrescription physical presence would not be necessary anymore. Every patient has a kind of mailbox where the ePrescriptions are stored and which is accessible by the eGK. The eGK is the foundation of the concept because it provides the authorization and encryption functions (cf. [9]).

The following graphic illustrates the run of ePrescription process:

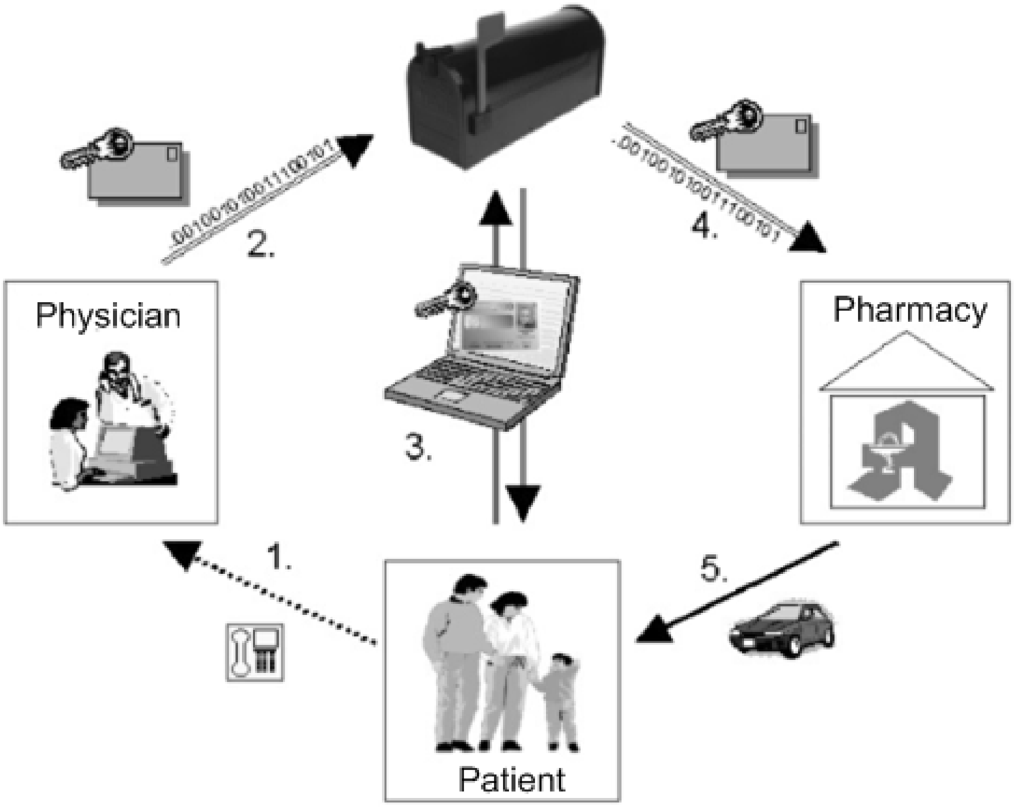


Figure 5.14: eGK ePrescription process [9]

Primarily the patient requests an ePrescription from her physician e.g. via telephone. The physician sends the encrypted prescription to the patient's mailbox where the patient in turn can inspect the prescription and forwards it to any pharmacy. In the latter case the prescription is encrypted with the public key of the pharmacy so no other pharmacy is able to read the prescription data (cf. [9]).

The ePrescription develops its full advantage in combination with the optional applications of the eGK e.g. medication history. Negative interactions with other pharmaceuticals or with documented allergies of the patient could be discovered immediately when the prescription is created (cf. [9]).

Because of the used smart cards the physician do not need to send the prescription to a server where the patient in turn is able to access it. It is also possible to store the prescription directly on the card, which also provides the usage of ePrescription when no connection to the telematics infrastructure is available (cf. [9], [38]).

If prescriptions are locally written on the eGK the prescription data is stored encrypted and compressed together with the certificate of the health service provider. Without this certificate the prescription is useless similar to a paper prescription without the signature of the physician (cf. [37]).

In general particular attention is paid to all the security and privacy aspects of the telematics infrastructure. Relating to the security needs of ePrescription these are classified in the following way :

Basic Value	Confidentiality	Integrity	Availability	Authenticity	Non–repudiation
Security Needs	very high	very high	high	very high	very high

Table 5.1: Security needs of ePrescription [38]

Current status

After the foundation of the gematik organization in 2005 different legal regulations were made over the years and a lot of preparation was done for the introduction of eGK. In 2005 a Decree for testing procedures for the introduction of the eGK in Germany was passed, which was extended in 2006, 2009 and 2011. It extends the first testing phase by adding the ePrescription component and the emergency data record. After the successful completion of the lab tests for the introduction of the telematics infrastructure, field tests were started at the end of 2006 in Sachsen and Schleswig–Holstein, Wolfsburg followed at 12.11.2007. A planned expansion of the test regions didn't happen, because of problems in the test runs and the changed political climate after the election of 2009 (cf. [28]).

Though on 26.10.2009 the governing parties signed a coalition agreement about construction of the telematics infrastructure and analysis of the results from the test regions. In 2010 it was decided to restrict the eGK to three applications (online insurance management, storing of emergency data and a safe communication infrastructure with the health service providers (cf. [28]).

The eGK has been distributed by the health insurance companies since October 2011 and was received by about 50 millions of insurants until the end of 2012 (cf. [31]).

5.3 KanTa — National Archive of Health Information (Finland)

The Finnish healthcare system has a high level of decentralization and is divided into 3 different systems, each of them has its own standards according to provided services, user fees and the like:

- municipal healthcare
- private healthcare
- occupational healthcare (cf. [21]).

The situation is further complicated by the different administrative levels in the Finnish state, because the responsibilities are distributed to the central level (including the national ministries and the central authorities, the regional level (including amongst others the Regional State Administrative Agency and the Center for Economic Development) and the municipal level. Also the major part of the Finnish population is living in the south of the country where the biggest cities are located, whereas big parts of the country are sparsely populated (cf. [21]).

The financing of the healthcare system is mostly based on tax revenue and is on authority of the public sector, nevertheless providing the municipal health services is a challenge for the local authorities particularly due to the big range in municipal population which varies from 804 inhabitants to 580 000. To help with those and other difficulties the PARAS project for restructuring the municipal services — which include not only health services but also for example educational and social services — is running since 2007 and is planned to be completed in 2012 (cf. [21]).

In 1996 Finland set the first milestone regarding to eHealth policy development in publishing the “Strategy for utilizing information technology in the field of social welfare and healthcare in Finland” by the Ministry of Social Affairs and Health, which has its main focus on developing citizen–centered, seamless chains by working with new technologies and new types of information system architectures. In 1998 the strategy was updated with focus on developing digital patient records and the interoperability between legacy systems while maintaining privacy protection (cf. [21]).

In 2002 the introduction of digital patient records was decided, which resulted in a nation–wide electronic patient record system development project that was running from 2003 to 2007. Until then every service provider has its own patient record system, none of them were interoperable with each other. In 2004 a minimum data set to be used in all electronic health records was specified which included basic patient information and basic clinical data. This data set was extended by several components until 2009, e.g. dental health, psychiatry and occupational health (cf. [21]).

In December 2006 it was decided to release a nation–wide EHR–Archive (eArchive) for easier access and exchange of health data between healthcare providers. The ePrescription and

National Pharmaceutical database, the eArchive and an online portal for patients to access their medical data are supposed to be part of KanTa, the National Archive of Health Information (cf. [21]).

Based on the eHealth Action Plan of the European Union of 2004 the Finnish eHealth road–map was published in 2007 by the Ministry of Social Affairs and Health, which summarizes the previous development of eHealth structure in Finland, implementation strategies, infrastructural data and future challenges (cf. [21]).

The following parties are the main stakeholders in implementing the planned eHealth structure (cf. [21]):

- Ministry of Social Affairs and Health
  Party in charge of eHealth policy and responsible for developing the national architecture, regulatory framework and semantic and technical definitions.
- KELA (Social Insurance Institution of Finland)
  In authority for the central architecture (KanTa) which contains eArchive, eView/eAccess and the ePrescription center.
- VALVIRA (National Supervisory Authority for Welfare and Health)
  Responsible for strong authentication of healthcare professionals, using smart cards and electronic signature.
- THL (National Institute for Health and Welfare)
  Supports development of structured EHR systems and maintains national code center.
- KUNTALIITTO (Kommunförbundet, League of Local Authorities)
  Organizes the co–operation of clusters and communities on a local level.

There are many more involved parties to which further information can be found in [21].

One of the key services in Finnish eHealth is KanTa, the National Archive of Health Information, which represents the core services for patients ([111]).

Those core services contains (cf. [91], [101])

- ePrescription (includes medication summary and handling prescribing as a fully electronic process)
- eArchive (centralized and real–time data store that permits secure data transfer between healthcare providers)
- eAccess (patients have access to their medical data)
- Patient Care Summary (for healthcare professionals)

The SAINI concept — the Electronic Healthcare Services Concept — which represents a road–map for implementing electronic healthcare services for citizens and is coordinated by Sitra and the Ministry of Social Affairs and Health (amongst others), has centered the KanTa services and uses it as a base for other value–add services (cf. [111]).

This road–map refers to the EU program "eHealth Impact", which evaluated the success factors of different pilot projects running in Europe and tries to take this output into consideration. The main focus lies on the acceptance of the user groups, on the one hand the citizen, who has to be encouraged to use the new services and to take a more active role in her own health. On the other hand the healthcare professional, whose acceptance is a decisive factor, which influences the success of the services. Also it is stated, that the required changes in organizational and operational structures may take years and therefore a lot of patience is required (cf. [111]).

Architecture and technical details

A big challenge is the great diversity of used IT–systems in Finland (15–20 major systems), because of the decentralized health care systems, they all have to be connected to the KanTa infrastructure. As the graphic 5.15 is showing, the architecture is divided into the central parts on the right side, which represents the heart of the national infrastructure and the connected decentralized components on the left side. (cf. [91]).

For establishing an eHealth infrastructure it is necessary to be able to uniquely identify patients and healthcare professionals. Health care professionals are authorized by VALVIRA the National Supervisory Authority for Welfare and Health, which handles not only the licensing of healthcare professionals but also the using of occupational titles e.g. chiropractor or psychotherapist (cf. [21]).

As general identifier acts the Finnish personal identity code (FINUID) which is given to every citizen by the Population Register Center and is based on the birth certificate. There is a mapping between the FINUID and the Social Security Identity Number, which on its part is also an unique identifier regarding to eGovernment services. The FINUID is not only given to citizens who are born in Finland but to everyone who stays in Finland for longer than a year and is also needed for bank transactions, appliances for pensions or the payment of salaries (cf. [21]).

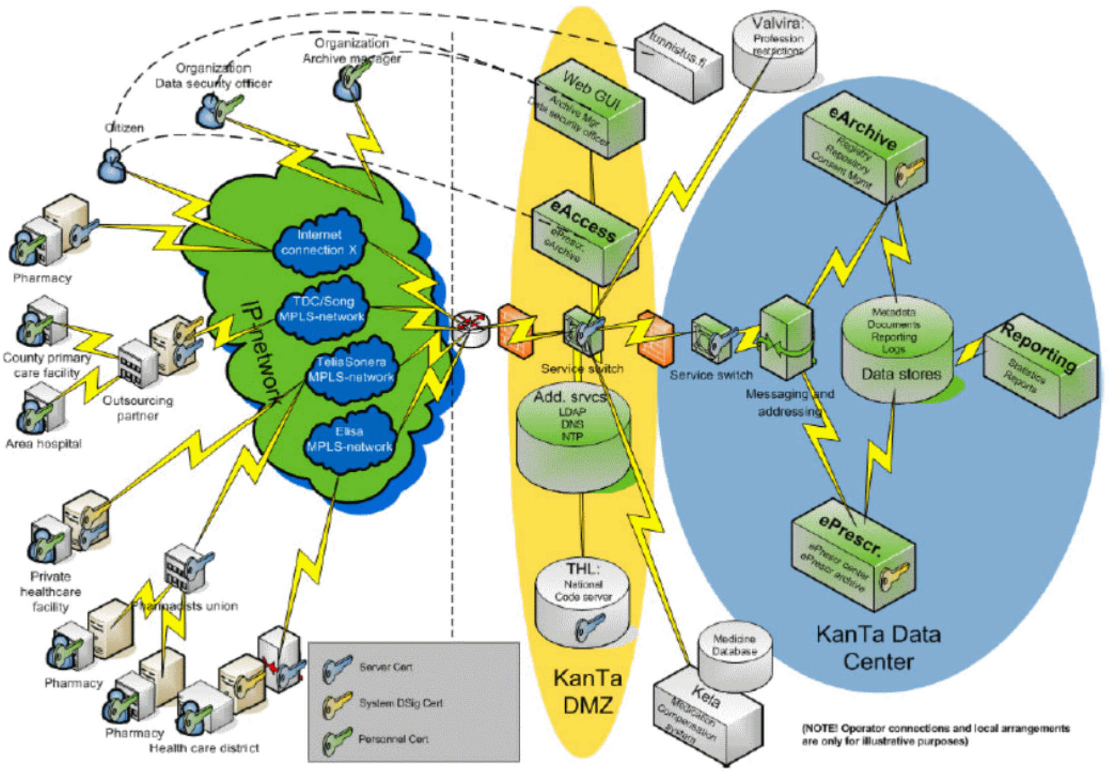


Figure 5.15: Network view of the KanTa architecture [91]

Together with the FINUID the Population Register Center creates an electronic identity (FINEID), which is necessary for electronic user identification and online transactions. It is further used for Citizen Certificates, which contains next to the FINEID other data, e.g. the citizen's name. Such a Citizen Certificate could be handed over to a person for example on a chip ID card.

There are different types of e–cards available in Finland (cf. [21]):

- FINEID card
  To get this card a person has to apply for it explicitly. A FINEID card is a smart Citizen ID–card with a PKI–based certificate, which is distributed by the local police. Because getting a FINEID card is a voluntary action only a small number of people have one in June 2009, but at that time there doesn't exist many services for using it.

- KELA card
  This is a health insurance card and everyone who is member of the Finnish social security system gets one automatically and for free. When presenting this card in pharmacies or private hospitals the patient gets a discount in the amount of the KELA coverage.

- combined ID card
  It is possible to combine the FINEID card with health insurance data and therefore use the card also as a KELA card. But for this service a fee is required and validity is limited to 5 years.

- European Health Insurance card
  This card is similar to the normal KELA card available for everyone in the Finnish health insurance system.

- VALVIRA smart card
  This card is necessary for access to KanTa applications and health related data. It is necessary for the identification of healthcare professionals and is also handed out by the Population Register Center.

In Finland e–cards are only used for identification, it is prohibited by law to store any health related data on the cards (cf. [21]). Alternatively identification can also be done by using internet banking IDs, which is far more common than e–cards (cf. [91]). The Citizen Certification is the foundation for user identification and authorization in eHealth in the SAINI concept (cf. [111]).

The SAINI integration concept relies on open standardized interfaces and plans the integration of the National Electronic Health Record Services by using a national messaging service. Web Services and SOAP interfaces will allow flexible connections to the client systems (cf. [111]).

HL7 (Health Level Seven International — the authority on standards for interoperability) collaborated in developing implementation guidelines for the interfaces of the services e.g. ePrescription (cf. [111], [112]).

KELA — the Social Insurance Institution of Finland — which is responsible for developing the ePrescription center and the eArchive for patient records, has developed the functional and data requirements for ePrescribing (eRx) (cf. [82]).

At the same time HL7 worked out the technical specifications which have to cover the following use–cases delivered by KELA (cf. [82]):

EPRs / eRxing use–cases:

- Browse prescriptions, dispenses and renewal requests
- Write prescription
- Send signed prescriptions and corrections
- Release a held prescription

Pharmacy systems use–cases:

- Update prescription status information (hold, lock ...)
- Dispense a prescription
- Correct a dispense
- Repudiate a dispense
- Select prescriptions for dispense

Shared use–cases:

- Repudiate a prescription
- Correct a prescription
- Print overview of prescriptions
- Print patient instructions for a prescription
- Add and process renewal requests (simplified, includes other use–cases)

ePrescriptions and messaging are based on a centralized repository service. It will be a service–oriented solution which uses synchronous web service interfaces for message sending. Two–way authenticated SSL/TLS–connections are used for data encryption as well as Web Services Security X.509 token profile for third party service providers. The international standard HL7 v3 was the basis for the architecture, which includes CDA R2 (for prescription and dispense information), W3 XML (digital signatures), Medical Records DSTU (communication) and the X.509 certificate–based infrastructure for the ISO 7816–* compliant smart cards. Further used standards are DICOM (imaging) and Object Identifiers (OID), the IHE XDS profile family for cross–enterprise data sharing is currently under development. PikaXML (referral–report process automation) is an EDIFACT standard derived from the MEDCOM MEDDIS profile of Denmark (cf. [82], [91]).

The image below shows an overview of the KanTa infrastructure with its services, standards and interfaces:

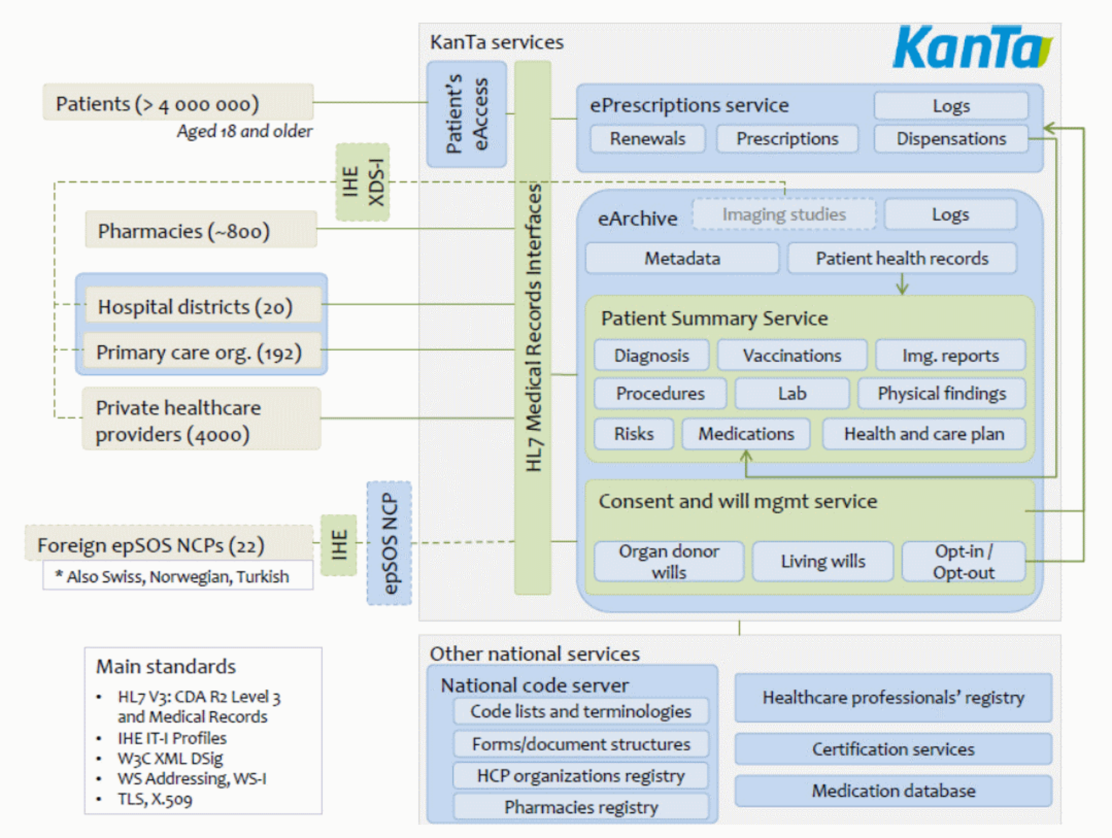


Figure 5.16: schematic View of KanTa [91]

eAccess is a possibility for the patient to get insight in her medical data, mainly the electronic health record and ePrescription but also registering for organ donation, living wills and so on. Consent management is also done by eAccess, patients have an opt–in possibility, but they are limited in regulating who has access to which type of data though they can use the audit facility for access monitoring (cf. [91]).

Security and authorization details

Over the time several legal regulations were made in Finland due to making eHealth applications possible and simultaneously ensuring data protection and privacy of the users (cf. [21]):

- Personal Data Act from 1999
  The objectives of this Act are to ensure the privacy and data protection of the individual when processing personal data and to set conditions due to duration of data storage and data exchange.

- Act on Experiments with Seamless Service Chains in Social Welfare and Care Services from 2000

The main focus of this Act was to support the building of seamless services on a regional level. It defines under which circumstances health data can be disclosed e.g. with written consent of the patient or for scientific research purposes. It was in force until the end of 2003 and was then extended to the whole country until the end of 2005.

- Decree on the Storing of Patient Data from 2001
  The Decree defines how medical records and related documents are stored, who has access to read or change this data and which kind of data has to be registered at least for a patient.

- Act on the Use of Electronic Social and Healthcare Client and Patient Information from 2007, also called the Client Data Act
  This Act defines that the patient has access to her own medical record as well as to its related access log and healthcare professionals have access to the patient's medical data, if they are involved in her treatment. It also states a deadline for all health care units, who don't have a paper–based archive until they have to join the eArchive system.

- Legislation on the Use of ePrescription from 2007
  This Legislation went into effect in January 2008 and allows the use of electronic prescriptions. KELA was stated as responsible party for the centralized nation–wide electronic prescription database. Also it indicates that service providers are obliged to use electronic prescriptions by 2011.

- Health Care Act (1326/2010)
  This Act came into force in May 2011 and is supposed to enforce a large reform in healthcare in improving quality and patient's safety as well as providing the right to freely choose a service provider. It is planned to be expanded so that the patient is able to choose among all national public or private service providers. The Act also declares that social and health care sectors should be handled as one entity, which is the leading principle of the planned reformation in those sectors (cf. [59]).

- Act on Information Management Governance in Public Administration (634/2011)
  This law enforces an enterprise architecture approach and promotes standards and interoperability in public health care (cf. [59]).

- Social Welfare Act (proposal 2014)
  The current Social Welfare Act is already over 30 years old and needs to be reformed to support a preventive approach towards welfare and offer more client–oriented services. The goal is to present the draft to the Parliament in 2014, so at the earliest the law could come into effect in 2015 (cf. [59]).

- Decree on Nationwide Health Care Information System Services (165/2012)
  This Decree specifies several deadlines for entering medical data into KanTa. At 01.09.2014 this should be the case for personal patient data, medical notes, lab reports, diagnoses, information on medical risk factors, living wills, organ donor etc., at 01.09.2016 vaccinations, oral diseases, medical statements and certificates should follow, a few other medical data types are allowed to follow later (cf. [91]).

After enacting the Client Data Act a national digital archiving service was provided for the health service providers, in which every organization has its own patient record archive with an uniform structure. Health service providers are obliged to join the system within the deadlines mentioned above (cf. [21]).

Because paper–based archives aren't in use anymore, the patient cannot refuse the electronic health record, which is a critical point. At least it is possible to forbid sharing it with other healthcare professionals. If this is not the case accessed healthcare providers have a three–months access period to the patient's data (psychiatric diseases are an exception) (cf. [91]).

In the first phase only a defined set of data will be available in the eArchive, but it will be extended step by step. As former mentioned all patient record archives which join the eArchive have to use a predefined structure using international classification systems e.g. ICD–10 and ICPC–2 (cf. [21]).

Electronic health services are supposed to use a central identification and authentication routine like the VETUMA service which is already in production use and is provided by the ministry of finance and is run by Fujitsu Services Ltd. For using the VETUMA service with a web browser session cookies and JavaScript execution have to be enabled. Also SSL version 3.0 or TLS version 1.0 have to be supported and a minimum 128–bit–connection is required. Furthermore the http–protocol versions 1.0 or 1.1 have to be supported (cf. [111]).

VETUMA provides an interface with 3 different identification methods (cf. [111]):

- Identification and authentication based on the Citizen Certificate (can be located on a smart card or a SIM–card)
- Identification and authentication based on user id and password (using a web browser or a mobile phone)
- Identification and authentication service in the internet offered by the banks

The Tunnistus.fi–service, provided by KELA can also be used for secure user identification and authentication. It requires a chip identity card and a card reader or net–banking credentials, the identification takes place over the internet and is using an encrypted connection (cf. [111]).

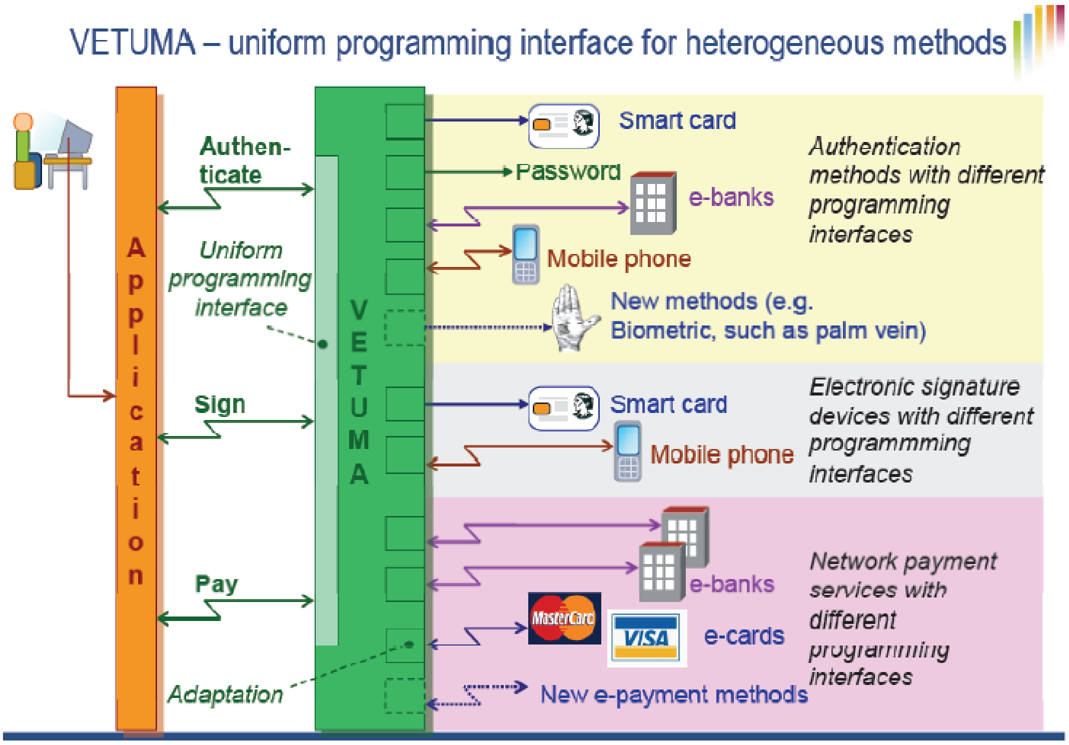

VETUMA – uniform programming interface for heterogeneous methods
Application
Authen-ticate
Uniform programming interface
Sign
Pay
Adaptation
VETUMA
Smart card
Password
e-banks
Mobile phone
New methods (e.g. Biometric, such as palm vein)
Authentication methods with different programming interfaces
Smart card
Mobile phone
Electronic signature devices with different programmming interfaces
e-banks
MasterCard
VISA
e-cards
New e-payment methods
Network payment services with different programming interfaces

Figure 5.17: VETUMA uniform programming interface [111]

In the peer review of the Finnish eHealth strategy and action plan it was stated that Finland has to increase privacy and data protection for the benefit of the citizens and therefore pseudonymization in the eHealth infrastructure has to be improved (cf. [91]).

The National Institute for Health and Welfare (THL) is legally authorized to collect and process medical data, within this institution a research ethics board is responsible for approving research projects involving data linkage with registry data. If Statistics Finland is serving as data source an application process takes place there as well and they are conferring with the Finland National Data Protection Authority if necessary. The use of registry and mortality data, as well as data linkages doesn't require the patients' consent (cf. [67]).

The Personal Identity code (FINUID) serves as unique identifier and is encrypted as well as the names (the same algorithm is used for all databases with linked data), the original data is then removed and given to the THL employees who are in charge of the record linkage with the encrypted identifiers or to external researchers. However the pseudonymized data contains some addresses and dates with potential for re–identification. Access to this data is strongly restricted and data is secured by physical and virtual security measures. Only one person within THL has access to the encryption technique for the original data and the original data is also stored separately. Employees have to follow strict data confidentiality rules (cf. [67]).

Finland is using data from electronic health records regularly for analysis of health care quality and efficiency, typically this happens on a local or regional level, at a national level the existing registries are used. Although it is unusual external researchers also might get approval for accessing identifying data. Each registry in Finland has one responsible person for approving research projects with data linkage, if data from more than one registry is required for the research project, each of the registries has to approve. This approval process is the same for requests from inside or outside the government. If the approval was given the Data Protection Authority has the final say in that matter (cf. [67]).

Requests with a commercial purpose are ruled out on principle. Generally when a researcher is applying for a project approval she has to present how she and her institution are regarding data protection requirements. In case the request is granted the applicant receives the encrypted data on a compact disk and the encryption key on a separate communication channel. Only named and approved people are granted access to this data (cf. [67]).

ePrescription component details

The conventional ePrescription process in Finland used to process prescription data at least 3 times and caused a big amount of paperwork. Annually there are in total 37 millions of prescriptions written in Finland, 27 millions of them are filed for reimbursement to KELA, which needs further processing (cf. [112]).

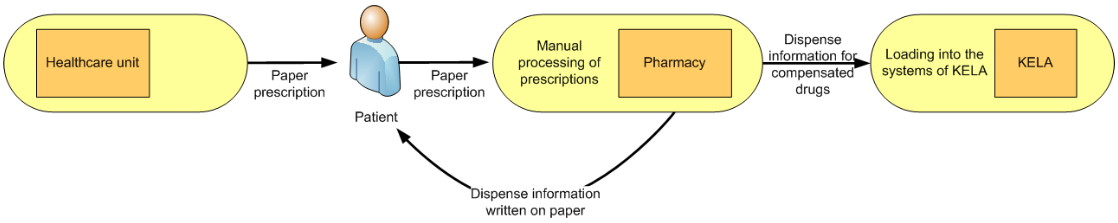

Healthcare unit
Paper prescription
Patient
Paper prescription
Manual processing of prescriptions
Pharmacy
Dispense information for compensated drugs
Loading into the systems of KELA
KELA
Dispense information written on paper

Figure 5.18: Conventional ePrescription Process [112]

The following graphic shows how the new ePrescription process is operated and how the information is flowing:

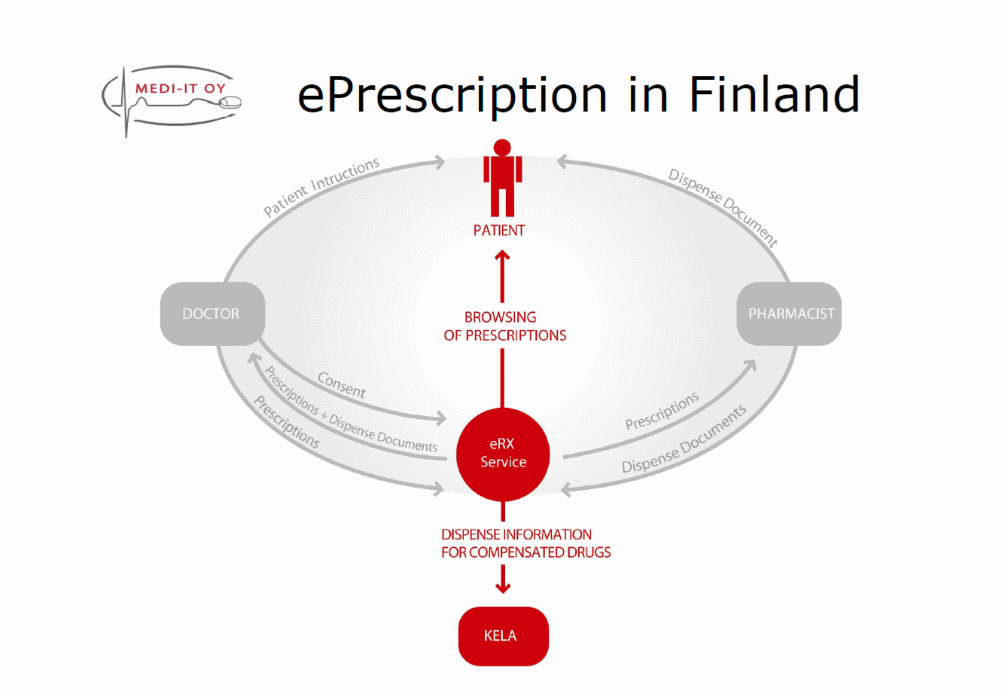


Figure 5.19: KanTa ePrescription functionality [112]

At first the healthcare unit is writing a prescription electronically and sends it to the ePrescription Center, the patient can optionally ask for a printed document with a bar–code and all necessary information to the prescribed medication. With this document the patient is able to get the prescribed medication dispensed at every pharmacy, that is using the ePrescription system, alternatively if the patient is not using a print–version it is also possible for the pharmacist to determine undispensed medication using the national person id number of the patient. When the prescribed medication was handed out the dispense information is retransmitted to the prescription center. The patient has secure access to her prescription data on the web and is able to print out a medication summary. To access the web portal the online access codes from the patient's bank are necessary or a citizen PKI card (cf. [82]).

ePrescriptions are stored actively in the ePrescription center for 30 months, afterwards they are transferred to an electronic archive, where they are stored for another 10 years, after that the destruction of the prescription data is scheduled (cf. [21]).

The patient is also able to make renewal requests at the healthcare unit or the pharmacy when the original prescription wasn't issued longer than 16 months ago. The renewal request could be sent electronically by the pharmacist to the healthcare unit and the healthcare provider will process the request within 8 days. Indeed it is up to the attending physician if the renewal request is successful or not and if previously a physical examination is necessary. The resulting information regarding a renewal request can be sent in a SMS message to the patient. Normally prescriptions are valid for a year (cf. [82], [72]).

This new electronic prescription process implicates several benefits for the patient (cf. [82]):

- Prescriptions cannot get lost
- Errors in prescribing and dispensing medication are minimized
- Information to prescription renewals can be received via SMS
- Prescription renewals can be requested at the healthcare unit or the pharmacy
- In a later phase easier handling of renewals is planned via eAccess portal

With the patient's consent health personnel is allowed to view the patient's medication history to prevent drug interactions or multiple prescriptions. They also have access to a Pharmaceutical Database to look up information about prices, interchangeable products and ingredients (cf. [21]).

Patients always have the choice to use paper–based prescription instead of ePrescription, data from paper–based prescriptions is not included in the ePrescription center. Without the patient's consent health care units and pharmacies are not allowed to use ePrescription, though once permission is given in an ongoing treatment or in emergencies the health personnel doesn't need to ask for the patient's consent (cf. [72]).

Admittedly there are several remaining challenges which have to be addressed (cf. [21]):

- How will the new ePrescription system influence the operational procedures?
- Part of the health personnel has a negative attitude towards ePrescription.
- The old and the new prescription system will have overlapping time in use.
- Nobody can say for sure if the new system will come up to everybody's expectations and all the expected benefits are realized.

Current status

The first national ePrescription pilot in Finland could handle the electronic transfer of prescriptions to pharmacies and provided some decision support. It was tested in 2002, but never made it to implementation phase. Nevertheless the experiences from this prototype were evaluated and poured into the development of another pilot project, which started in 2004. After passing the law of Use of ePrescription in 2007, which scheduled a central ePrescription database in the custody of KELA, major steps towards the development of KanTa — the National Archive of Health Information — were made. After the functionality of the central ePrescription database was provided, new ePrescription pilots started their testing phase in May 2010 (cf. [21]).

The ePrescription service of KanTa started its production use in Turku in May 2010 and involved one health care unit and one pharmacy. Afterwards the use of ePrescription was geographically expanded by using hospital districts. Since 31.03.2013 ePrescription is obligatory by law for public health care, the deadline for pharmacies already was at 31.03.2012. About 170 organizations have already joined the system. In total about 1,6 million people got 7,9 million ePrescriptions and about 530.000 people used the online access to view their prescription information online. The use of the ePrescription service is closely monitored, so in March 2013 about 1,1 million ePrescriptions were issued and they were filled at the pharmacies about 1,4 million times. The utilization rate lies between 34 and 93 % depending on the region. The deadline for using ePrescription for the private health sector is 31.03.2014 (cf. [58], [91]).

The feedback of patients and organizations that are using ePrescription are quite positive, which is also attributed to the systematic action plan of the country. The physicians appreciated the fact that a prescription is always readable and cannot get lost or falsified, the increased patient safety, the good performance of the ePrescription process and the provided tools for cooperating with other health care institutions (cf. [91]).

The eArchive service of KanTa is ready for use as a national service. The Decree (165/2012) states September 2014 and 2016 as obligatory start–up dates for using KanTa for storing most types of medical data. The work, that has to be done to accomplish these goals is defined in a road–map and a part of it has already started. Although the deadline of 2014 could be stressful for some of the tasks, others are going to be finished already in 2013 (cf. [91]).

In the peer report of the Finnish eHealth strategy several possible threats of the system were discovered (cf. [91]):

- Timeliness and responsiveness of service provision of healthcare providers have to be increased
- Risk of data overload due to the complexity of the system, which can decrease effectiveness and effcency.
- Awareness of threats to the information system has to be increased (hacking and intervention). Enhancement of risk management, security, and patient safety.
- Technological and organizational design errors (e.g. alternative for specialized smart cards for healthcare professionals, guidelines or regulations for roles of public authorities and private vendors)
- Technological issues with identification, health data, legacy systems and interoperability:
  - Linkability of de–identified patient data threatens patient's privacy
  - Management of patient–entered data in the medical record (recommendation of authentication of data records with electronic signatures to mark the records from non–healthcare professionals)

  - Data migration from legacy systems
  - Improvement of interoperability necessary

5.4 Shared Medication Record (Denmark)

In Denmark the responsibilities for public healthcare are allocated to three different levels: the state, the regions and the municipalities, thereby the state is responsible for the legal framework, the five regions for the primary and secondary care such as hospitals and the practice sector and the 98 municipalities for other types of care such as rehabilitation, home nursing and school health service. The financing of the public healthcare in Denmark is tax–based, the inhabitants have the possibility of free choice of a general practitioner or a hospital (cf. [19]).

In 2007 a big structural reform was implemented which reduced the number of municipalities from 275 to 98 and the regional authorities from the former 14 counties were consolidated into five regions. In the process the financing of public health care was reorganized — most notably on the regional level — to create more transparency for the taxpayers (cf. [19]).

In 1996 Denmark already started the development of Electronic Health Records, which was further upgraded after the published eHealth strategy of 2003, which introduced the importance of shared information as foundation for the future healthcare service. It was planned to provide a central ePrescription server, which serves as database for a personal medication profile (cf. [19]).

The organization "Connected Digital Health in Denmark" developed the current Danish road–map for eHealth. This is already the forth paper in the history of Danish eHealth strategies and it concentrates on the digitalization of the Danish healthcare. The road–map describes several action plans which in turn consists of different projects, that are supposed to implement the road–map's strategy within the time frame from 2008 to 2012 (cf. [19]).

The organization of the Danish eHealth project was reformed in summer 2010, the following participants are essentially involved (cf. [19]):

- Ministry of the Interior and Health
  Whereas the regions and municipalities are responsible for their own projects, the Ministry is in charge of the main organization and the coordination between the different participants. It is also responsible for decisions according to a national level such as standards or infrastructure.

- MedCom
  MedCom is a non–profit organization on a national level, that was founded for assistance in the development of electronic communication in the health sector. Key issues are the project implementation, communication networks and health data networks. The financing of MedCom is provided by different governmental instances e.g. the Danish National

Board of Health. In 2007 the extension MedCom International was established, that has its focus on international healthcare collaboration. MedCom also provides the Danish Health Data Network, which allows secure data exchange between healthcare organizations e.g. prescriptions, lab results, referrals etc. In June 2007 4 million messages were sent via the network. An upgrading of the network is necessary if all requirements regarding to security, capacity and other areas should be fulfilled ([19], [54]).

- Sundhed.dk
  Sundhed.dk is an official eHealth portal, which was introduced in 2003 by all public instances regarding health in Denmark. Citizens and professionals have access to the portal via digital signature and gain insight into health data according to the Danish data protection terms. The portal allows interaction between patients, their relatives and healthcare professionals, the patients thereby have the possibility to gain a more active role in their medical treatment and prevention. Further development of the portal is planned until 2012, all self–service solutions, that are available at Sundhed.dk will also be provided at borger.dk — a portal for government services — which has a collaboration with Sundhed.dk since 2009 (cf. [19], [54]).

- National Board of eHealth (NSI)
  The NSI was founded in 2011 and is responsible for the medical databases and registries, the management of cross-sectoral projects and planning strategies in healthcare. Furthermore an important task is setting interoperability standards for the electronic health record and for making sure, that a uniform medical terminology is used (cf. [67]).

The Danish National Patient Registry (DNRP) is used since 1977 in hospitals to collect patient data like diagnoses, surgical codes and the like. This collected data base was used for developing the National Patient Index (NPI) — the Danish version of a Patient Summary — which provides access to medical patient data for citizens and healthcare professionals (cf. [19]).

The already existing service on Sundhed.dk "My Health Summary" will be replaced by the National Patient Index, which should be ready for use in 2013. The NPI will be based on various data sources aside from the National Patient Registry e.g. medication history, personal wishes of the patient regarding organ donation and so on, laboratory test states and more (cf. [19]).

A huge problem in the Danish health sector is the local storage of data, which affects medication records, lab results and any other kind of medical data. Also the use of different IT systems in public healthcare makes the situation more complicated, in 2007 there were 23 Electronic Patient Record landscapes, 13 practice systems and 4 Electronic Care Record systems. The goal is to downsize the amount of different IT systems as soon as possible, in 2010 the number of Electronic Patient Record landscapes was 17 and in the end of 2013 it should be reduced to 5 — each for one of the Danish hospital regions (cf. [19]).

Naturally the Electronic Patient Records should replace any paper–based records in the future and present a central source of the patient's medical data. The principle "one hospital region

— one Electronic Health Record" serves as a base for developing a cross–region Electronic Patient Record for hospitals and in the future for all healthcare services(cf. [19]).

Another shared service is the "Personal Medicine Profile", which is an electronic summary of medication data, the registration is mandatory and automatically. It is planned to extend this service to interact with local solutions e.g. integrating medication systems of hospitals with the Personal Medicine Profile. The Shared Medicine Record is supposed to be the output of a patient's collected medication history and should be available for healthcare staff at hospitals, old people's homes, the physicians and any other medical place where this information might be of use. A further closely related service is the drug interaction and allergy check (cf. [19]).

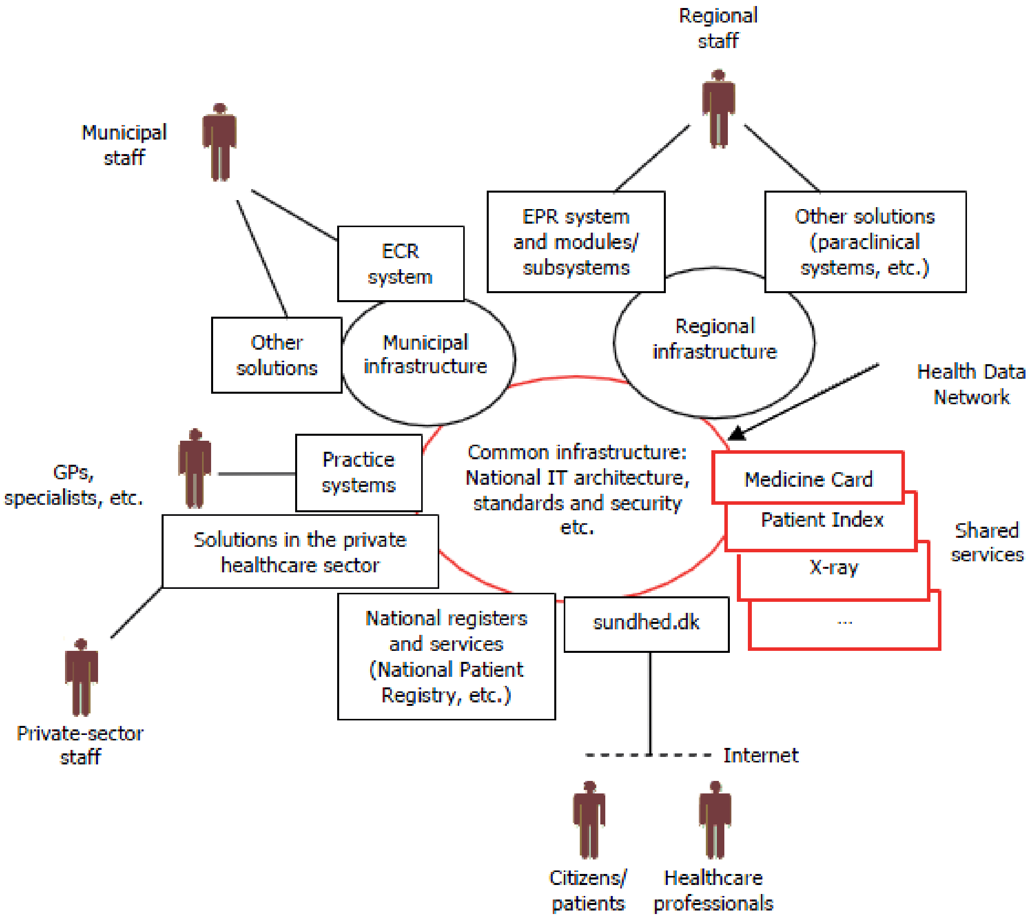


Figure 5.20: Coherent IT in the healthcare service [54]

Architecture and technical details

The goal is to connect the Danish health care sector in a way that all health care professionals have access to medical patient data and the different medical services. Therefore it was decided to realize this with a national service–oriented architecture (SOA) via SOAP based web services over HTTP. Furthermore a single sign on (SSO) system was required, so that healthcare professionals are able to authenticate themselves with single credentials to have access to all needed systems. For the identity management SAML 2.0 was chosen as framework because it is a highly supported specification (cf. [14]).

The Danish road–map for eHealth emphasizes the importance of using international, market–driven common public standards. In Denmark such standards are in common use, for example for laboratory data and imaging the DICOM standard is used or classifications and terminologies in the health sector like ICD10, ICPC and SnomedCT (cf. [19].
HL7 v2 was under discussion as messaging standard, however EDIFACT was chosen in the end, but currently the format is being changed to XML messages (cf. [55]). In primary and secondary care terminology standards are different, which makes definition of a national standard necessary (cf. [67]).

MedCom — the Danish healthcare organization — is responsible for development and deployment of these standards. In doing so two approaches are used: on the one hand the "inside–out" standardization, which means that a standard is specified for a smaller area that is step–by–step extended, on the other hand the "outside–in" standardization, which goes the other way round. MedCom develops its standards based upon CEN standards (European Committee for Standardization) (cf. [19]).

However because the five regions of Denmark are using many different IT systems — several of them not using international standards — it will be very time–consuming and expensive to implement one common set of standards for the whole country. While there are efforts to adapt those systems to increase interoperability, it's often the case that the Danish adaptions of standards are not strict enough to ensure complete interoperability (cf. [6]).

A basic principle of using eHealth services is the ability of securely identifying a person, who wants to access this service. Therefore it is necessary to have unique identifiers for patients and healthcare professionals. In Denmark since 1968 the CPR (Central Person Register) is in use, which every person born or with place of residence in Denmark must have. This is a 10–digit number, where the first six digits are the date of birth followed by a 4–digit serial number, this number is registered in the central National Register and is linked with basic information about the citizen like name, address and birth information, but no medical data (cf. [19]).

The CPR is used as an identifier not only in the public and finance sector, but also in the healthcare sector and has to be included in the patient records. However the CPR was not available on an identity card until 2007 the Health Card was introduced as a substitute of the social security card (cf. [19]).

Healthcare professionals are registered in a central register of the National Board of Health, in which every healthcare professional is registered with an authorization identification number (cf. [19]).

Denmark has decided against e–cards and uses digital signatures instead. The reason behind this decision is on the one hand that digital signatures are very cost–effective and on the other hand that it will be in widespread use more quickly than other solutions. The citizens should be able to interact with all public authorities securely and free of charge from home by using the same identification method for all public services they consume — in this case a software–based digital signature from an official source (cf. [19]).

Therefore they are able to access the eServices provided, for example by Sundhed.dk, such as online booking of appointments at physicians or renewing prescriptions. Also healthcare professionals have the possibility — by using special security certificates — to access medical data of patients and other resources such as clinical pathways (cf. [19]).

Security and authorization details

The Danish road–map of eHealth strategy also brought into focus the importance of ensuring data security and patient privacy and therefore several legal regulations were processed (cf. [19]):

- Act on Processing of Personal Data
  This Act came already into effect in 2000 and since then it was amended several times.
- Consolidation Act on Legal Protection and Administration in Social Matters
  Regulates the automatic information exchange between hospitals and home care providers
- Health Act
  This Act came into effect in 2007 and defines the purpose of the healthcare service and the requirements regarding to an easy and user–friendly way to access medical information, a top–quality treatment and maintaining integrity and the right of self–determination for the patient. Also it allocates the responsibilities of providing the healthcare services to the regions and municipalities and defines rules of action for accessing and transferring patient data by health professionals as well as the right of the patient to see her own data. The Act was explicitly adapted to electronic medical data, because its predecessor was designed for paper–based medical data (cf. [19], [54]).

The Danish Health Act is significant in handling patient rights. In general health information can be collected without the explicit approval of the patient, but the patient has to be informed and has the right to object. The patient also has to give her consent when personal data is shared with people outside of the healthcare sector (cf. [19]).

Despite of this the participating in health and social care registries is mandatory and cannot be reversed by the citizen, which is conforming to the law. Also identifiable medical data can be shared for certain projects with data linkages, e.g. Statistics Denmark. The de–identification of data consists of removing names and addresses but not the Central Person Register Number, which reveals the data of birth and gender. Requests for data linkage projects are accepted from within and outside the government, at first by the Danish Data Protection Agency, then by the National Board of Health and Welfare. The latter is audited regularly by the Danish Data Protection Agency and sometimes by the Danish National Audit Office to assure that their databases are meeting the legal requirements. If a data linkage project was approved the Danish Data Protection Agency will instruct the researcher about data security measures, which includes a certain time period in which the data can be used, then it has to be deleted or used in a de–identified version. It is forbidden to link it with data from other sources or share it further. In general those data linkage projects provided a range of important results which are serving as basis of decisions for medical policies e.g. for human resource planning or the effectiveness of treatment approaches. The secondary use of data from electronic health records is restricted to using it for treatment decisions in the primary care sector (cf. [67]).

Within a treatment or following steps of care no explicit consent of the patient is needed, otherwise the patient has to approve the access to her personal data. This should avoid that third parties, for example the patient's employer, are able to gain access to personal data without the knowledge of the patient. Also the patient always has the right to see her own medical data and the responsible healthcare professional is obliged to explain the medical content. Medical records after January 2010 are electronically accessible (cf. [19]).

The use of standards is widespread in Denmark, also because of security requirements. Therefore the DS 484 information security standard was chosen as foundation for digitalization (cf. [54]).

Some main concerns of a secure architecture are the confidentiality, the integrity and the availability. The latter can be achieved by providing redundant critical components and communication lines, the others by using encryption techniques. The VPN–based health care network SDN, which already connected a lot of health care organizations in Denmark before, was reused for the SOSI project (Service–Oriented System Integration). The main task of SOSI was to evaluate technologies and standards for authentication within an eHealth network and provide valuable feedback during the testing phase. SDN provides a secure transport mechanism, which maintains confidentiality and integrity and can be used for web services (cf. [14]).

The Danish national certificate initiative (OCES) provides components, which are suitable for web service integration and is able to allocate a nationally implemented X509–based public key infrastructure for issuing certificates, which are used for verifying the digital signatures of the participants of the eHealth network. The transported XML messages must contain the information of their sender, which is realized via the embedded credentials provided by the digital signatures. The SSO mechanism uses a trusted third party for verifying the credentials — the Security Token Server (STS) — by using WS–Trust messages. The OCES certificate is linked to the citizen's CPR number (which is used as an identifier) and when the citizen is using the SSO a SAML assertion is issued. While SAML assertions and X509 certificates are classified as very secure a weakness of SAML assertions is, that the issuer is aware of the user's identity — even if pseudonyms are used in the SAML assertion — and therefore is able to retrace all of the user's actions and used services (cf. [14], [56]).

The digital signature serves as central access point to various services using it for the SSO mechanism. If an attacker is able to compromise the digital signature she has access to the data in all systems that are using it, which also implies the possibility of identity theft. The fact, that the CPR number of a citizen is used as identifier and is embedded into the digital signature increases this risk, because the CPR number has to be given at numerous occasions due to most governmental facilities using it for citizen services. In this case a pseudonymization system where a citizen is authenticated with a different identifier in every system would provide more security, even if one system was compromised the data within the other systems would be safe and because the hacked system uses the pseudonym as identifier the intruder couldn't find out the real identity of the citizen (cf. [6]).

A further weak point in privacy protection in the Danish healthcare is the insufficient regulation of role–based access to medical data. For example at the eHealth portal Sundhed.dk, any doctor can access any patient's medical data, because in emergency cases they must be able to do so. This is similar to most of the hospital EHR systems where doctors can access any patient's data without repercussions. But when there is no emergency the access should be restricted to patients they are currently treating (cf. [6]).

ePrescription component details

In Denmark primary healthcare providers are using ePrescription at a rate of nearly 100 %, they can choose if the prescription should be issued paper–based, electronically, via fax or telephone ([19]). This way the prescribed medicine can be ordered in any pharmacy in Denmark and it is already waiting for the patient when she arrives there ([48]).

The process of ePrescription consists of the following steps (cf. [51]):

1. The Physician writes the electronic prescription in her medical practice system.
2. The Physician sends the electronic prescription via the secure VANS network (value added network service) to the ePrescription server.
3. The Pharmacist downloads the electronic prescription from the central ePrescription server into her pharmacy system.

ePrescription for primary healthcare providers were made mandatory in 2007. The first step towards ePrescription was made in 2007, when a central ePrescription server was provided by the Danish Medicines Agency, that was able to send prescriptions from physicians to pharmacies (cf. [19]).

Since then several projects were developed and introduced (cf. [19]):

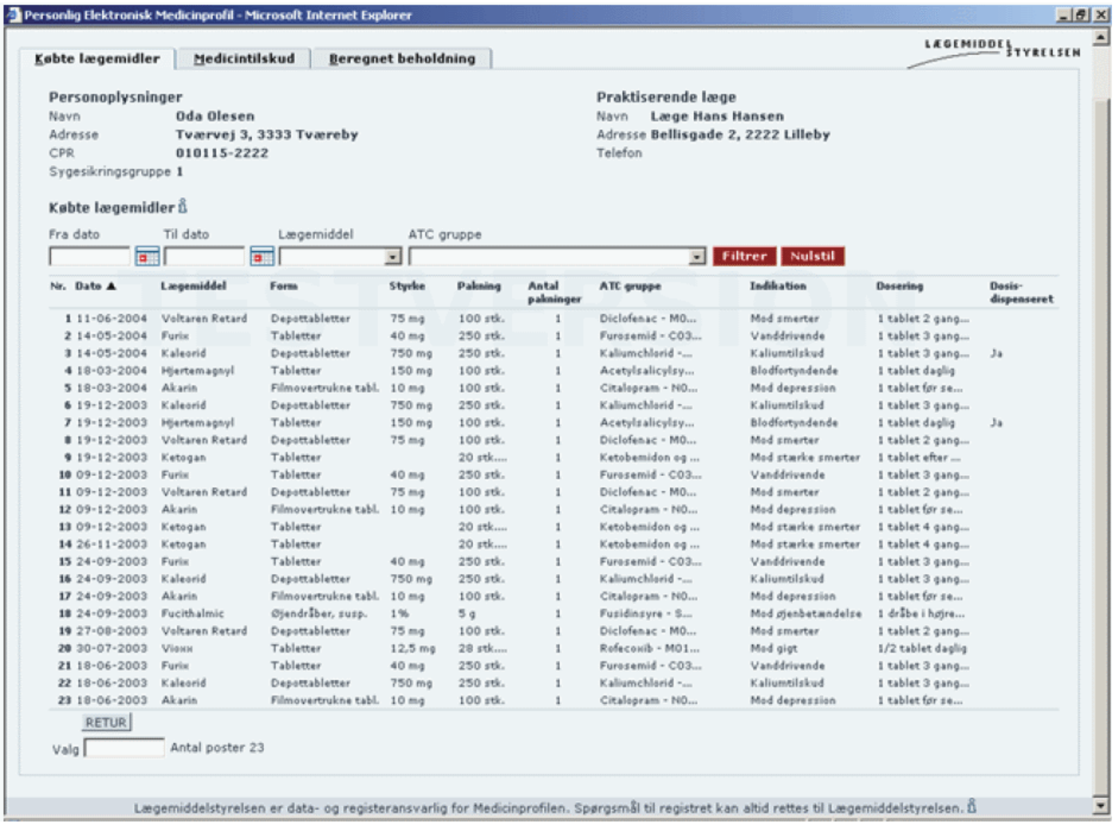
- Apoteket.dk
  Apoteket.dk is an online portal, provided by the Pharmacy Association, where patients can buy drugs online for delivery or pick–up at the pharmacy. The patients have to use again digital signature to buy medication and the portal also offers additional features e.g. online consultation of pharmacists via chat or email.

- Medicinkombination.dk
  Another online portal, also provided by the Pharmacy Association, where patients are able to inform themselves about drug interactions.

- Medicine Profile
  This is a service, which is also available at Sundhed.dk, and provides an overview of all prescribed medication of a patient. The service can be used by the patient herself or a pharmacist or another healthcare professional. When purchasing a drug it is registered in the Medicine Profile, whether the prescription is issued via telephone, fax or paper–based, and healthcare professionals are able to check the patient's medication history to avoid drug interactions or double medication).
  Healthcare professionals are also able to add data to the profile, for example a note, that the patient didn't tolerate a certain drug. The prescriptions, which are sent to National Health Portal as XML messages can be accessed via Sundhed.dk or via www.medicin–it.dk. Citizens need to install a personal digital signature, health professionals need additionally a special employee certificate to access the medical data of patients. Every access to the data is logged and visible for the patient (cf. [19], [48]).

- Shared Medication Record (SMR)
  This record is a data set which contains the medical data of a patient within the last two years, so all healthcare professionals can have access to necessary information to give the patient the optimum treatment. The record is also available for the citizens for looking up their medical data and can be accessed via electronic signature on Sundhed.dk. The Shared Medication Record gains its data from the central prescription server and the Medicine Profile (cf. [47]).

The following graphics are showing screen–shots of the Medicine Profile:



Personoplysninger

Navn	Oda Olesen
Adresse	Tværvej 3, 3333 Tværeby
CPR	010115-2222
Sygesikringsgruppe	1

Praktiserende læge

Navn	Læge Hans Hansen
Adresse	Bellisgade 2, 2222 Lilleby
Telefon	

Købte lægemidler

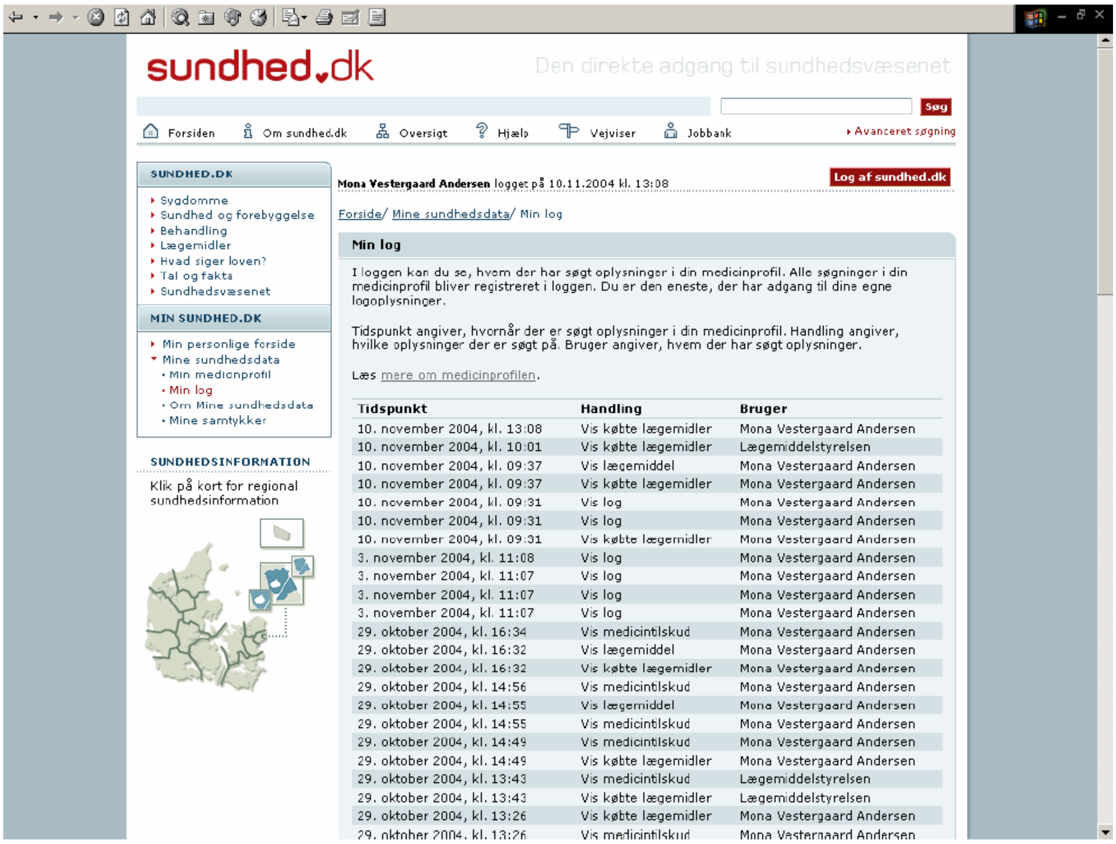
Fra dato | Til dato | Lægemiddel | ATC gruppe

Nr.	Dato ▲	Lægemiddel	Form	Styrke	Pakning	Antal pakninger	ATC gruppe	Indikation	Dosering	Dosis-dispenseret
1	11-06-2004	Voltaren Retard	Depottabletter	75 mg	100 stk.	1	Diclofenac - M0...	Mod smerter	1 tablet 2 gang...	
2	14-05-2004	Furix	Tabletter	40 mg	250 stk.	1	Furosemid - C03...	Vanddrivende	1 tablet 3 gang...	
3	14-05-2004	Kaleorid	Depottabletter	750 mg	250 stk.	1	Kaliumchlorid -...	Kaliumtilskud	1 tablet 3 gang...	Ja
4	18-03-2004	Hjertemagnyl	Tabletter	150 mg	100 stk.	1	Acetylsalicylsy...	Blodfortyndende	1 tablet daglig	
5	18-03-2004	Akarin	Filmovertrukne tabl.	10 mg	100 stk.	1	Citalopram - N0...	Mod depression	1 tablet før se...	
6	19-12-2003	Kaleorid	Depottabletter	750 mg	250 stk.	1	Kaliumchlorid -...	Kaliumtilskud	1 tablet 3 gang...	
7	19-12-2003	Hjertemagnyl	Tabletter	150 mg	100 stk.	1	Acetylsalicylsy...	Blodfortyndende	1 tablet daglig	Ja
8	19-12-2003	Voltaren Retard	Depottabletter	75 mg	100 stk.	1	Diclofenac - M0...	Mod smerter	1 tablet 2 gang...	
9	19-12-2003	Ketogan	Tabletter		20 stk....	1	Ketobemidon og ...	Mod stærke smerter	1 tablet efter ...	
10	09-12-2003	Furix	Tabletter	40 mg	250 stk.	1	Furosemid - C03...	Vanddrivende	1 tablet 3 gang...	
11	09-12-2003	Voltaren Retard	Depottabletter	75 mg	100 stk.	1	Diclofenac - M0...	Mod smerter	1 tablet 2 gang...	
12	09-12-2003	Akarin	Filmovertrukne tabl.	10 mg	100 stk.	1	Citalopram - N0...	Mod depression	1 tablet før se...	
13	09-12-2003	Ketogan	Tabletter		20 stk....	1	Ketobemidon og ...	Mod stærke smerter	1 tablet 4 gang...	
14	26-11-2003	Ketogan	Tabletter		20 stk....	1	Ketobemidon og ...	Mod stærke smerter	1 tablet 4 gang...	
15	24-09-2003	Furix	Tabletter	40 mg	250 stk.	1	Furosemid - C03...	Vanddrivende	1 tablet 3 gang...	
16	24-09-2003	Kaleorid	Depottabletter	750 mg	250 stk.	1	Kaliumchlorid -...	Kaliumtilskud	1 tablet 3 gang...	
17	24-09-2003	Akarin	Filmovertrukne tabl.	10 mg	100 stk.	1	Citalopram - N0...	Mod depression	1 tablet før se...	
18	24-09-2003	Fucithalmic	Øjendråber, susp.	1%	5 g	1	Fusidinsyre - S...	Mod øjenbetændelse	1 dråbe i højre...	
19	27-08-2003	Voltaren Retard	Depottabletter	75 mg	100 stk.	1	Diclofenac - M0...	Mod smerter	1 tablet 2 gang...	
20	30-07-2003	Vioxx	Tabletter	12,5 mg	28 stk....	1	Rofecoxib - M01...	Mod gigt	1/2 tablet daglig	
21	18-06-2003	Furix	Tabletter	40 mg	250 stk.	1	Furosemid - C03...	Vanddrivende	1 tablet 3 gang...	
22	18-06-2003	Kaleorid	Depottabletter	750 mg	250 stk.	1	Kaliumchlorid -...	Kaliumtilskud	1 tablet 3 gang...	
23	18-06-2003	Akarin	Filmovertrukne tabl.	10 mg	100 stk.	1	Citalopram - N0...	Mod depression	1 tablet før se...	

Valg Antal poster 23

Lægemiddelstyrelsen er data- og registeransvarlig for Medicinprofilen. Spørgsmål til registret kan altid rettes til Lægemiddelstyrelsen.

Figure 5.21: Screenshot Medication Profile Overview [51]



Mona Vestergaard Andersen logget på 10.11.2004 kl. 13:08

Forside/ Mine sundhedsdata/ Min log

Min log

I loggen kan du se, hvem der har søgt oplysninger i din medicinprofil. Alle søgninger i din medicinprofil bliver registreret i loggen. Du er den eneste, der har adgang til dine egne logoplysninger.

Tidspunkt angiver, hvornår der er søgt oplysninger i din medicinprofil. Handling angiver, hvilke oplysninger der er søgt på. Bruger angiver, hvem der har søgt oplysninger.

Læs mere om medicinprofilen.

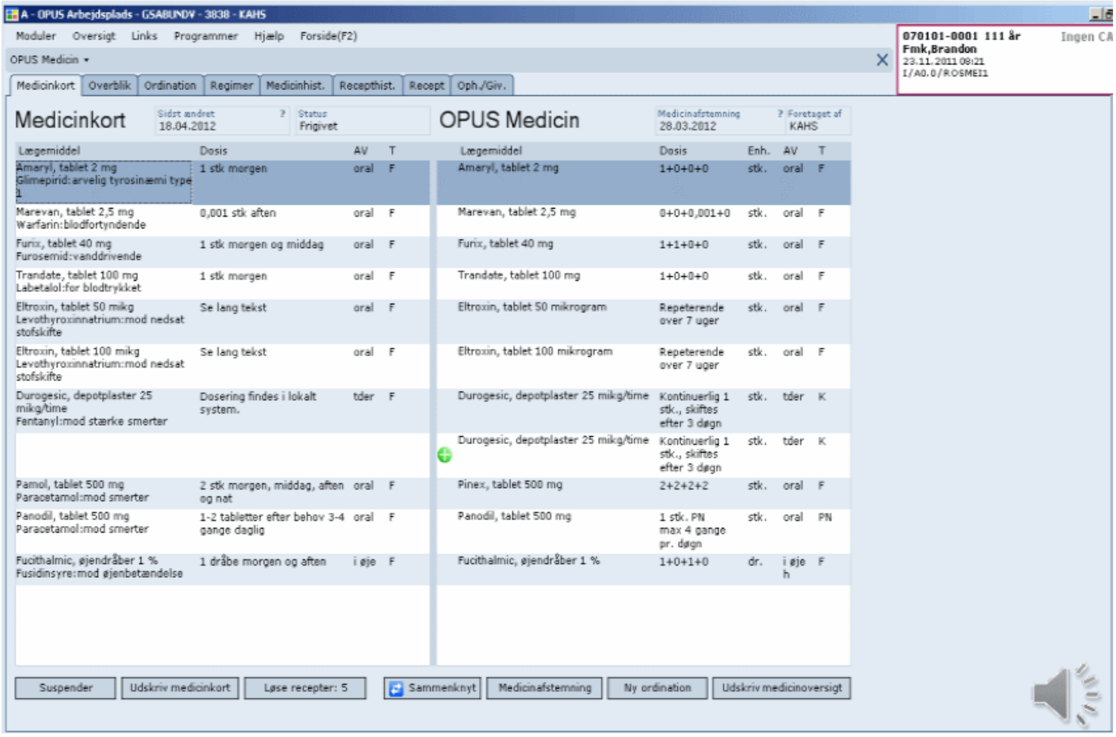
Tidspunkt	Handling	Bruger
10. november 2004, kl. 13:08	Vis købte lægemidler	Mona Vestergaard Andersen
10. november 2004, kl. 10:01	Vis købte lægemidler	Lægemiddelstyrelsen
10. november 2004, kl. 09:37	Vis lægemiddel	Mona Vestergaard Andersen
10. november 2004, kl. 09:37	Vis købte lægemidler	Mona Vestergaard Andersen
10. november 2004, kl. 09:31	Vis log	Mona Vestergaard Andersen
10. november 2004, kl. 09:31	Vis log	Mona Vestergaard Andersen
10. november 2004, kl. 09:31	Vis købte lægemidler	Mona Vestergaard Andersen
3. november 2004, kl. 11:08	Vis log	Mona Vestergaard Andersen
3. november 2004, kl. 11:07	Vis log	Mona Vestergaard Andersen
3. november 2004, kl. 11:07	Vis log	Mona Vestergaard Andersen
3. november 2004, kl. 11:07	Vis log	Mona Vestergaard Andersen
29. oktober 2004, kl. 16:34	Vis medicintilskud	Mona Vestergaard Andersen
29. oktober 2004, kl. 16:32	Vis lægemiddel	Mona Vestergaard Andersen
29. oktober 2004, kl. 16:32	Vis købte lægemidler	Mona Vestergaard Andersen
29. oktober 2004, kl. 14:56	Vis medicintilskud	Mona Vestergaard Andersen
29. oktober 2004, kl. 14:55	Vis lægemiddel	Mona Vestergaard Andersen
29. oktober 2004, kl. 14:55	Vis medicintilskud	Mona Vestergaard Andersen
29. oktober 2004, kl. 14:49	Vis medicintilskud	Mona Vestergaard Andersen
29. oktober 2004, kl. 14:49	Vis købte lægemidler	Mona Vestergaard Andersen
29. oktober 2004, kl. 13:43	Vis medicintilskud	Lægemiddelstyrelsen
29. oktober 2004, kl. 13:43	Vis købte lægemidler	Lægemiddelstyrelsen
29. oktober 2004, kl. 13:26	Vis købte lægemidler	Mona Vestergaard Andersen
29. oktober 2004, kl. 13:26	Vis medicintilskud	Mona Vestergaard Andersen

Figure 5.22: Screenshot Medication Profile Security Log [51]

The Shared Medication Record (SMR) can be used by hospitals and physicians who access it with their local EHR systems and connect via the secure healthcare network with the central SMR service. All healthcare professionals which are involved in the treatment of the patient have access to the medication data in the SMR, in this way it is possible to share a medical standardized documentation across sectors, which at the same time represents a value chain, because healthcare professionals are able to double–check the treatment (cf. [73]).

The following graphics are showing some screen–shots of the SMR:

The physician at the hospital opens the Shared Medication Record with the hospital IT system and sees on the right side an overview of the patient's medication record of the hospital and on the left side the patient's current medication record from the SMR. The physician is now able to synchronize the medical data (cf. [73]).



070101-0001 111 år Ingen CA
Fmk,Brandon
23.11.2011 08:21
I/A0.0/ROSMEI1

Medicinkort

Sidst ændret: 18.04.2012

Status: Frigivet

Lægemiddel	Dosis	AV	T
Amaryl, tablet 2 mg Glimepirid:arvelig tyrosinæmi type 1	1 stk morgen	oral	F
Marevan, tablet 2,5 mg Warfarin:blodfortyndende	0,001 stk aften	oral	F
Furix, tablet 40 mg Furosemid:vanddrivende	1 stk morgen og middag	oral	F
Trandate, tablet 100 mg Labetalol:for blodtrykket	1 stk morgen	oral	F
Eltroxin, tablet 50 mikg Levothyroxinnatrium:mod nedsat stofskifte	Se lang tekst	oral	F
Eltroxin, tablet 100 mikg Levothyroxinnatrium:mod nedsat stofskifte	Se lang tekst	oral	F
Durogesic, depotplaster 25 mikg/time Fentanyl:mod stærke smerter	Dosering findes i lokalt system.	tder	F
Pamol, tablet 500 mg Paracetamol:mod smerter	2 stk morgen, middag, aften og nat	oral	F
Panodil, tablet 500 mg Paracetamol:mod smerter	1-2 tabletter efter behov 3-4 gange daglig	oral	F
Fucithalmic, øjendråber 1 % Fusidinsyre:mod øjenbetændelse	1 dråbe morgen og aften	i øje	F

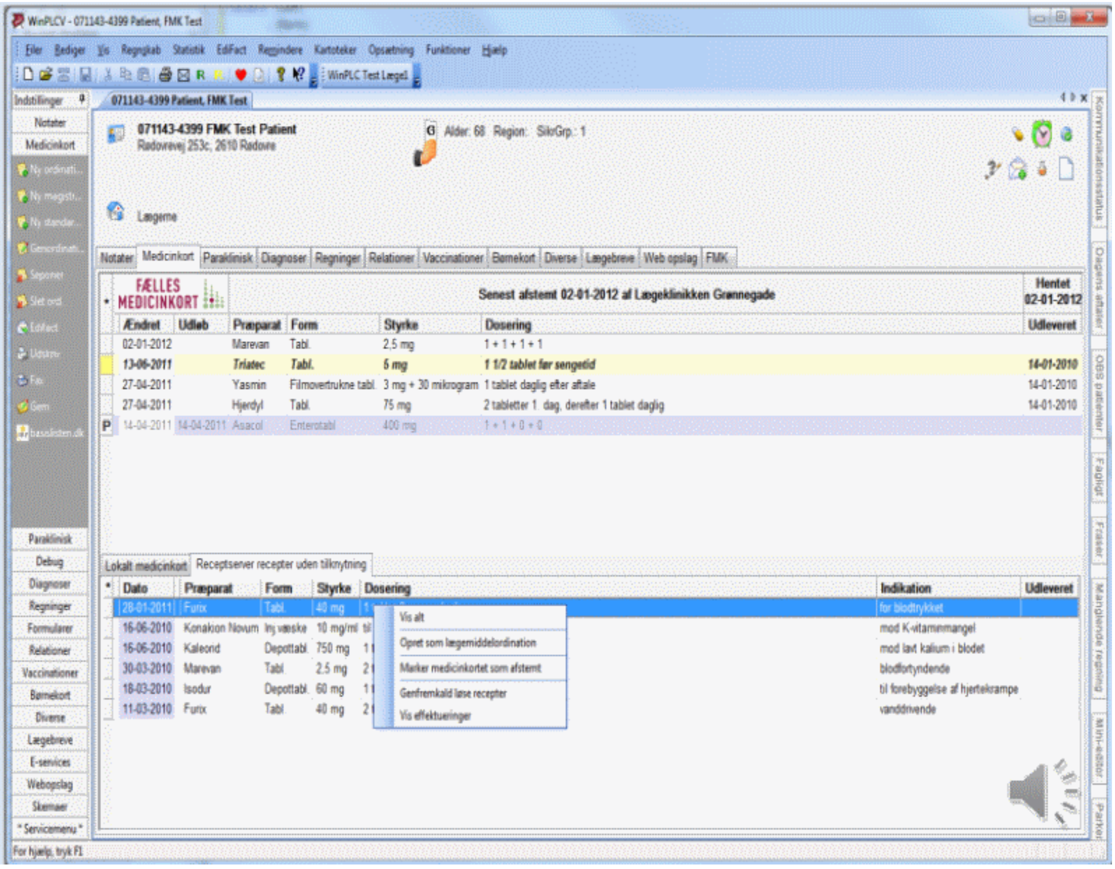
OPUS Medicin

Medicinafstemning: 28.03.2012

Foretaget af: KAHS

Lægemiddel	Dosis	Enh.	AV	T
Amaryl, tablet 2 mg	1+0+0+0	stk.	oral	F
Marevan, tablet 2,5 mg	0+0+0,001+0	stk.	oral	F
Furix, tablet 40 mg	1+1+0+0	stk.	oral	F
Trandate, tablet 100 mg	1+0+0+0	stk.	oral	F
Eltroxin, tablet 50 mikrogram	Repeterende over 7 uger	stk.	oral	F
Eltroxin, tablet 100 mikrogram	Repeterende over 7 uger	stk.	oral	F
Durogesic, depotplaster 25 mikg/time	Kontinuerlig 1 stk., skiftes efter 3 døgn	stk.	tder	K
⊕ Durogesic, depotplaster 25 mikg/time	Kontinuerlig 1 stk., skiftes efter 3 døgn	stk.	tder	K
Pinex, tablet 500 mg	2+2+2+2	stk.	oral	F
Panodil, tablet 500 mg	1 stk. PN max 4 gange pr. døgn	stk.	oral	PN
Fucithalmic, øjendråber 1 %	1+0+1+0	dr.	i øje h	F

Figure 5.23: Local medication record at hospital [73]



WinPLCV - 071143-4399 Patient, FMK Test

071143-4399 FMK Test Patient
Rødovrevej 253c, 2610 Rødovre

Alder: 68 Region: SikrGrp.: 1

Lægerne

FÆLLES MEDICINKORT — Senest afstemt 02-01-2012 af Lægeklinikken Grønnegade — Hentet 02-01-2012

	Ændret	Udløb	Præparat	Form	Styrke	Dosering	Udleveret
	02-01-2012		Marevan	Tabl.	2,5 mg	1 + 1 + 1 + 1	
	13-06-2011		Triatec	Tabl.	5 mg	1 1/2 tablet før sengetid	14-01-2010
	27-04-2011		Yasmin	Filmovertrukne tabl.	3 mg + 30 mikrogram	1 tablet dagligt efter aftale	14-01-2010
	27-04-2011		Hjerdyl	Tabl.	75 mg	2 tabletter 1. dag, derefter 1 tablet daglig	14-01-2010
P	14-04-2011	14-04-2011	Asacol	Enterotabl	400 mg	1 + 1 + 0 + 0	

Lokalt medicinkort | Receptserver recepter uden tilknytning

Dato	Præparat	Form	Styrke	Dosering	Indikation	Udleveret
28-01-2011	Furix	Tabl.	40 mg	1	for blodtrykket	
16-06-2010	Konakion Novum	Inj.væske	10 mg/ml	til	mod K-vitaminmangel	
16-06-2010	Kaleorid	Depottabl.	750 mg	1	mod lavt kalium i blodet	
30-03-2010	Marevan	Tabl.	2.5 mg	2	blodfortyndende	
18-03-2010	Isodur	Depottabl.	60 mg	1	til forebyggelse af hjertekrampe	
11-03-2010	Furix	Tabl.	40 mg	2	vanddrivende	

Figure 5.24: Local medication record at physician [73]

Current status

The company Computer Sciences Corporation (CSC) developed — in close collaboration with the Danish National Board of Health and Danish hospitals — a web–based ePrescription solution, which is applicable for use across all other European countries. The Solution is based on CSC's Opus Medication solutions (medication record), Home Care solutions and CSC's Vitae Suite (coordination of mobile services), which support an interface to the National ePrescription Repository provided by the Danish National Board of Health. CSC wants to adapt all three components, to make them suitable to meet other countries requirements (cf. [49], [19]).

Altogether it is worked on completing digital exchange of medical data of most text–based messages e.g. prescriptions, referrals, lab test orders, discharge letters. More than 60 million messages were digitally exchanged in 2011, 75 % of the prescriptions between physicians and pharmacies are already sent electronically. The next step is to digitalize the messages sent between hospitals and home nursing, which should be completed at the end of 2012. Also the start–up date for using the Shared Medication Record in all Danish hospitals was set within 2012 (cf. [68]).

5.5 eRecept (Sweden)

Sweden has divided the healthcare responsibility among three independent levels — the national level, the county level and the municipality level — each of them has the possibility to choose between delivering the care themselves or to commission private companies, the latter possibility is well received recently with up to 10 % of the county healthcare. The 290 municipalities have the main focus on the nursing–homecare, the 21 counties are responsible for the health and medical services. The counties again are grouped into regions, so medical services can be further classified into primary care, regional and county medical care (cf. [20]).

In 2009 the Swedish parliament (Riksdag) decided that from January 2010 the Swedish population has free choice of healthcare, so they can select between private and public health centers. In July 2009 the pharmacy monopoly of the state Sweden ended and since then everybody can run a pharmacy but prescribers and pharmaceutical manufactures (cf. [20]).

In 2006 the National strategy for eHealth was published, which focused on creating the legal and technical infrastructure for eHealth solutions and their adaption to patient needs. All of the county councils and regions of Sweden agreed within six months to integrate the National strategy into their own activities. Since then this strategy was further developed — the latest version was finalized in June 2010 — and several status reports were published to inform about the development and status of the eHealth solutions (cf. [20], [69]).

The latest version of the National strategy for eHealth has its main focus on accessible and secure information in health and social care. Because a new phase of eHealth implementation has been entered the action areas of the strategy were adapted and the priority issues were reorganized. High priority and great importance were given to the fact, that every citizen should have secure access to her personal health data, the patient should be able to document and share her medical data in an user–friendly way (cf. [69]).

The National Patient Summary and therefore the patient's full drug history should be fully accessible throughout the healthcare services. Training of medical staff and documentation methods should be improved regarding to eHealth knowledge and collaboration. Also in the sector of standardization, information structure and interdisciplinary terminology a lot of further development is needed to ensure that all eHealth information data can be used, stored and managed appropriately (cf. [69]).

There are several parties involved in eHealth organization in Sweden (cf. [20]):

- Ministry of Health and Social Affairs
  On the national level the Swedish Ministry of Health and Social Affairs (Socialdepartementet) is the main institution in charge of the healthcare system, it cooperates with Ministry of Industry, Employment and Communications, the Ministry for Education and Research, the Ministry of Finance and participates in international eHealth information exchange.

- National Board of Health and Welfare
  The government agency National Board of Health and Welfare (Socialstyrelsen) is responsible for planning the information structure, classifications and documentation procedures in the processes of monitoring, accessing and structuring patient data.

- Apotekens Service AB
  The Apotekens Service AB is the connection between pharmacies and the public healthcare sector. It is responsible for national drug statistics, maintaining the ePrescription database and other national registers e.g. the reimbursement system or the pharmaceutical product register.

- Swedish Association of Local Authorities and Regions
  The Swedish Association of Local Authorities and Regions (SALAR) acts as a representation of interests for the Swedish municipalities and counties. An important part of SALAR is the Center for eHealth in Sweden (CeHIS) which participates in implementation management, coordination and strategy planning of eHealth solution development and which collaborates also with the private health and social care providers. The company Inera AB, which is developing national eHealth solutions, also belongs to SALAR.

There are several eHealth projects scheduled by the National strategy which are in different implementation stages in the various regions and counties (cf. [69]), the most important are described in more detail further below:

- Sjunet — digital communication channel of the care sector
- Video — Video/distance meeting service via Sjunet
- HSA — Health Services Address Registry
- SITHS — Secure IT in Health Services
- 1177.se — Website, which provides information about healthcare
- NEF — National Format for ePrescriptions, managed by Apotekens Service AB
- SIL — Swedish Drug Information Database
- NPÖ — National Patient Summary
- 1177 — health and advise service by telephone
- RGS Web — Decision–making support for health advice over Sjunet

The National Patient Summary (NPÖ) is used in several counties in Sweden since April 2008 under the prerequisite of patient consent. It contains the patient's medical data including medical alert information and chronic diseases. Healthcare staff has access to the NPÖ with the patient's acknowledgment, the patient herself can access her own data through the internet (cf. [20], [69]).

The Läkemedelsförteckningen database (Swedish Prescribed Drug Register) is also part of the NPÖ and is basically a list of the patient's dispensed drugs, which is provided by the Apotekens Service. The prescription data is stored for 15 months and accessible to the prescriber, the pharmacist and the patient, each access is logged and can be reviewed by the patient (cf. [20]).

The project Pascal (Comprehensive information on patients' drug prescriptions) gives prescribers access to the patient's entire drug history and uses existing information from Swedish Prescribed Drug Register, the National Prescription Database and the National Dose Register. It was planned for 2010 to provide a pilot system which gives access to those services (cf. [69]).

In 2006 the Swedish Drug Information Database (SIL) — which provides quality–assured drug information — was introduced in the first county and since then several more counties joined in using it, the remaining counties agreed to integrate SIL into their health records until 2012 (cf. [69]).

Architecture and technical details

The National eHealth strategy for Sweden turned attention regarding to the technical infrastructure to the use of global standards to ensure secure and efficient exchange of sensitive information (cf. [69]). An important benefit of using standards is the increase of interoperability within the eHealth components on the technical level (cf. [74]).

The National Board of Health and Welfare initiated two projects in the standardization sector, which are part of the National regulatory framework (cf. [69]):

- National Information Structure (NI) (2007 — 2009)
  The NI specifies what kind of information is generally needed and how it has to be structured to cover all the necessary use–cases in processing and managing this data. In 2009 NI was successfully tested by several health authorities, for 2011 the development of a NI guidance document is scheduled as foundation for future regulations.

- National Interdisciplinary Terminology (NF) (2007 — 2011)
  The NF includes national and international classifications, concepts and terms. The most important one is the international reference terminology SNOMED Clinical Terms, which was translated into Swedish in 2010. It is planned to use SNOMED on a national level, but the implementation is still in progress (cf. [67]).

Other used standards are HL7 v3, Tveksamt, DICOM däremot, EN 13606 and ICD 10, the Swedish translation for ICD 10 was finished in 1997. For the ePrescription standard ENV 13607 was used as basis (cf. [20]).

Every Swedish citizen is registered with a national citizen ID — the "personnummer" in the population register. This personal ID is also used as electronic healthcare ID. For the identification of healthcare professionals exists also a central register managed by the Swedish National Board of Health and Welfare (cf. [20]).

A further centralized information register is the HSA (Health Service Address Registry) which provides information about healthcare staff duties and roles. It will serve as a basis of decision–making in regards to access medical information. In October 2010 HSA contained about 320 000 items and was implemented in almost all counties (cf. [20], [69]).

SITHS (Secure IT in the Healthcare Sector) is a solution for secure communication and electronic identification. Healthcare professionals use their SITHS cards for identification, SITHS was also introduced by all county counsels in 2010 and will be given to municipalities and private healthcare companies in a bundle with HSA and Sjunet, the national network for secure communication between healthcare services (cf. [20], [69]).

The eCard for healthcare professionals, which is provided by SITHS, contains a Public Key Infrastructure certificate (PKI) for identification and authorization. In October 2010 about 205 000 cards have to be distributed, 15 of 21 counties and 8 municipalities have already joined (cf. [20]).

The eCard is used by patients and healthcare professionals since 2005, not only for healthcare services, but also for banking business and other services. Every person, which has a national ID and is older than 13 can apply for an eCard. It is planned to add an electronic circuit to the card for a secure electronic identification routine (e–ID). Every card user has her own key– and security code (cf. [20]).

Security and authorization details

Over the years several legal acts were passed to ensure data integrity and protection for patients' electronically stored medical data (cf. [20]):

- Patient Data Act (Patientdatalagen)
  Was passed in July 2008 and replaces the Patient Record Act (Patientjournallagen) and the Healthcare Register Act (Lagen om vårdregister). It regulates cross–organizational and nation–wide digital access of patient's medical history through different healthcare services. Additionally it specifies the patient's rights of approval which parts of her medical data are shared and who is allowed to access them. In general only people who are part of the treatment chain are allowed to access the patient's medical data, the patient's consent is obligatory, if she wants she is able to choose to block parts of her medical information.
  The healthcare providers are obliged to inform the patient about all accesses to her medical data and intended purpose of data processing. So patients are able to review all access logs and always have the possibility of digital access to their own data. Also according to the Act patients can benefit from the care choice models, which means, that patients have the free choice of healthcare providers and the providers have free choice of estab-

lishment. Naturally these care choice models increased the need of a cross–organizational access to patient's medical data.
The Act strictly specifies in which cases medical data of patients is allowed to be accessed and in which cases an explicit consent or objection of the patient is needed.

- Act of the Prescription Database (receptregister)
  Administers the handling of sensitive data in the national ePrescription database and the national database of dispensed drugs by Apotekens Service.
- Act of Medication Summary (Lagen om läkemedelsförteckning)
  Governs the management of private medical data regarding the national ePrescription and dispensed drug databases.
- Personal Data Act (Personuppgiftslagen)
- Digital Signatures Act (Lagen om kvalificerade elektroniska signaturer)

The task of the Social Services Personal Data Inquiry was to examine how the regulation of processing medical data, statistics and monitoring activities has to be handled and in which scope these processes are taking place. The inquiry results were transferred to the government for further analysis in March 2009. An important area for the future affects the requirements of the national legal framework to provide healthcare across national and organizational borders (cf. [69]).

The National Board of Health and Welfare and the Swedish Data Inspection Board published a manual for applying the rules of the Patient Data Act practically to the medical services. SALAR (Swedish Association of Local Authorities and Regions) organizes training programs for legal advisers on county or municipality level, so that the Act is legally correct implemented (cf. [69]).

To fulfill the requirements of the legal regulations the BIF (basic services for information management) provides the possibilities for secure communication and role– and authentication management across organizational boundaries. This includes the use of Sjunet (the secure communication channel between healthcare providers), the Health Service Address Registry (HSA) and Secure IT in the Healthcare Sector (SITHS). The introduction of BIF was done during 2010 with regard to the introduction of the National Patient Index (NPÖ) (cf. [69]).

In Sweden the National Board of Health and Welfare is legally allowed to process medical data for the purpose of improving national quality registers, which have to be linked to the Patient Registry (a national health database) for creating significant statements. There are several quality registers for different care sectors e.g. stroke care, cardiac care and so on. To provide the best possible medical treatment it is often necessary to link medical data of different treatments of a patient. For example a cardiac treatment may require medication that might cause side effects like gastric bleeding. This causal connection is important because it influences the effectiveness of the cardiac treatment and therefore the medical care of the patient (cf. [67]).

Access to the identifying data and executing the data linkage is under strict surveillance of a security officer and data confidentiality rules, it is specified who has access to the identifying data and how long and where it has to be stored. This includes providing a secure building, encrypted data transport channels and protected computers, so no unauthorized access is possible. New employees are trained in data security and confidentiality requirements. Data analysts only have access to pseudonymized data, so that no backtracking to a certain patient is possible. Data is considered pseudonymized when full names, addresses, national identity numbers and dates of birth are removed, a study number is serving as pseudonym and some personal data regarding gender, age and home community is provided. Participating in those registers is mandatory for the patient, but there is the possibility of being removed by appealing to the Board (cf. [67]).

The National Board of Health and Welfare is also in charge of approving requests of research proposals no matter if they are coming from the government or from external researchers. Requests for commercial use are not ruled out on principle but there are concerns how to determine if a request is in the public's interest and there is the idea of legally regulating these decisions more clearly. It is considered likely that data from the national electronic health record will be used for those quality registers within the next five years (cf. [67]).

ePrescription component details

Since the 1990s ePrescription was prioritized in Sweden, which led to the installation of the "Healthcare–digital–network", an IP–based broadband network which connects hospitals, primary care centers and other health care services. It is separated from the internet and allows secure transfer of medical data and images. At first the network was part of the Swedish internet as a virtual private network (VPN), but since 2003 it is based on VLAN technology and therefore separated from the internet. It is highly secured against breakdown and has an excellent availability (cf. [20]).

Since July 2009 Apotekens Service AB is responsible for the National ePrescription Format (NEF), which has already been implemented in all counties. With it the ePrescription service is adapted to meet its organizational and qualitative requirements (cf. [69]).

The new ePrescription format replaced the old EDIFACT format with XML messages, which made format control via the XML scheme possible. The ePrescription messages were extended with the name of the prescribing EHR system, the version and a unique prescription identifier, the latter made it possible to rule out occurring technical duplicates of the prescription system. Furthermore ePrescriptions were validated against completeness and a bunch of 24 prescription rules — most of them concerning legal formality and agreed code of practice between the prescription process participants (e.g. valid packaging and identification of drugs, reimbursement etc.). With this improvements the most frequent types of errors in the ePrescription system (with the old ePrescription format) — format and prescription rule errors — could be resolved and the interoperability of the system was increased immensely. When using the old ePrescription format 98,6 % of all prescriptions contained errors, whereas with NEF the error rate was reduced to 0,9 % (cf. [74]).

An eRecept is transmitted from the prescriber (a physician or a hospital system) electronically to the pharmacy over Sjunet,the secure healthcare communication channel. This can happen either by using a primary care electronic record system with the appropriate software module for sending an eRecept or by using secure web–based prescription over the internet (cf. [93]).

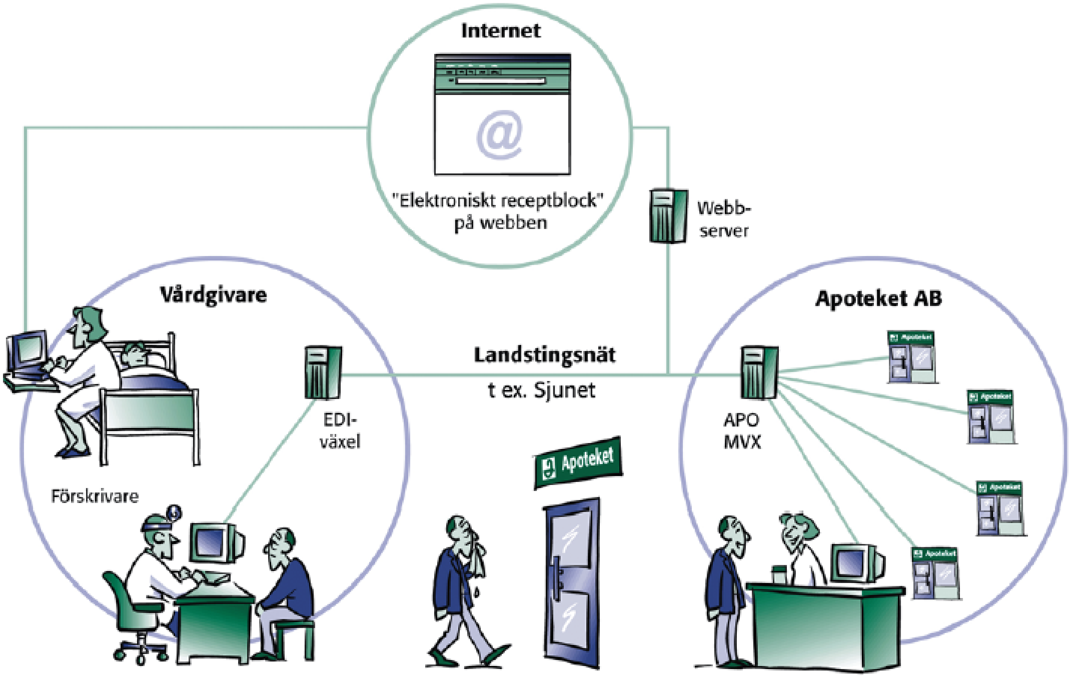


Figure 5.25: Journey of ePrescription [93]

The traditional way of prescribing was very inefficient and time–consuming for the patient, who had to go to the primary care unit taking the prescription by herself to a pharmacy. With eRecept it is possible to send the prescription electronically to a pharmacy or to the National Mailbox. There are about 900 pharmacies in Sweden which are able to access this mailbox, when the patient doesn't want to specify the dispensing pharmacy at the time of the prescription generation, but wants to choose on short notice where to dispense her prescription (cf. [93]).

The mailbox service was introduced in 2004 and was very well received among patients because of the greater flexibility and other services e.g. home delivery and a 24–hours–available call center for advice. If a specific pharmacy is indicated on the eRecept this pharmacy is able to prepare the medication in advance to be ready for pickup through the patient (cf. [93]).

The ePrescription services generated an economical benefit of 95 million in 2008 in Stockholm county. A core impact of eRecept was the unbroken chain of information between the primary care unit and the pharmacy and therefore a higher degree of security and prescription quality. Prescription and dosage errors could be lessened by 15 %. The healthcare providers and staff are able to save a considerable amount of time due to ePrescription (cf. [93]).

Further benefits of ePrescription were the minimization of illegible prescriptions and prescription falsifications. This is attended by avoidance of double prescribing due to lost prescriptions and of negative medication interaction due to the visible medication history of the electronic patient record (cf. [93]).

One of the most important things, which helped to increase acceptance for ePrescription, was an initiated awareness campaign, organized by the county council and Apotekens Service AB. Therefore a very good cooperation between the involved parties in practicing the eRecept was the main success factor especially the senders and receivers of the eRecepts. Also a thoroughly elaborated implementation strategy in combination with regular reviews helped massively with a successful realization (cf. [93]).

Current status

Since April 2008 a National Patient Summary (NPÖ) is in use in Sweden, which is based on experiences with a previous prototype. In May 2009 the Örebro County Council and the Örebro municipality have agreed to participate, in 2010 the counties Blekinge, Jönköping, Kronoberg, Stockholm, Södermanland and Västra Götaland were following (cf. [20]).
In May 2013 all 21 counties of Sweden and 50 of 290 municipalities have already joined the NPÖ. It is planned to expand the use of the NPÖ to the remaining municipalities until the end of 2013. Currently it is worked on to extend the information the NPÖ is providing and to make further improvements (cf. [71]).

In Sweden ePrescription is in use since before the year 2000 with over 80 % coverage (cf. [20]). At the end of 2010 the efforts were going into the direction of immediate online drug utilization reviews — which was used at that time at 10 % of the pharmacies — and drug interaction control at the prescriber's office, which was in the testing phase back then (cf. [98]). In 2011 more than 90 % of all prescriptions were filled electronically (cf. [74]);

The Personal Health Record is a possibility for the citizens to create their personal medical health records which could contain vaccination lists, medication lists or whatever health information the patients want to put into the record. The patient is able to define not only which information is stored in the records, but which parts are visible to which family members or healthcare providers. This service is run by Apotekens Service and will be introduced in autumn 2013, the full development is expected within 2014 (cf. [70]).

Still there are some interoperability and comparability problems e.g. with the data sharing between the healthcare and social care sectors (cf. [67]).

Chapter 6

Results

At first this chapter gives an overview of the basic facts concerning the evaluated ePrescription systems in chapter 5. Afterwards the results of the evaluation are summarized and interpreted.

	Electronic Health Record
AUT	ELGA, including/planned components are e–Medikation, eDischarge letter, eFinding Laboratory, eFinding Radiology. Legal deadlines for using ELGA are Jan. 2015 for public hospitals, July 2016 for pharmacies, physicians and ambulances, Jan. 2017 for private hospitals, Jan. 2022 for dentists.
GER	eGK (Electronic Health Insurance Card), including/planned components are ePrescription, medication history, eDischarge letter. The distribution of the eGK is in progress since 2011, at the end of 2012 about 50 millions of citizens have received their cards.
FIN	KanTa, including/planned components are eArchive, eAccess, ePrescription, Patient Care Summary. The eArchive service of KanTa is ready for use as a national service, with September 2014 and 2016 most types of medical data are stored via KanTa.
SWE	National Patient Summary (NPÖ), including/planned components are eRecept, Personal Health Record, Swedish Prescribed Drug Register, Swedish Drug Information Database (SIL). The NPÖ is in use since April 2008 and is gradually extended geographically to all counties and municipalities, which should be finished until the end of 2013.
DEN	Shared Medication Record, including/planned components are National Patient Index (NPI), Personal Medicine Profile, Apoteket.dk, Medicinkombination.dk.

Table 6.1: Overview Electronic Health Records

	ePrescription component
AUT	e–Medikation is a core component of ELGA, the Austrian EHR. Successful piloting took place during 2011. Nation–wide roll–out and start–up of e–Medikation has to happen until the end of 2014 for public hospitals, the rest of the medical sectors will gradually follow.
GER	ePrescription was planned as a core component of the eGK, but was put on hold for the time being. The applications of the eGK were reduced to online insurance management, storing of emergency data, safe communication structure for healthcare providers.
FIN	ePrescription is a base component of KanTa, the Finnish EHR. Since 31.03.2013 ePrescription is obligatory by law for public health care, the deadline for pharmacies already was at 31.03.1012. The private health care sector will follow in March 2014.
SWE	eRecept, which is already in use in Sweden for years. In 2011 more than 90 % of all prescriptions were filled electronically.
DEN	ePrescription is included in the Shared Medication Record, its start–up date for using in all Danish hospitals was set within 2012.

Table 6.2: Overview ePrescription component

	Responsible parties
AUT	Association of Social Insurance Agency, Austrian Chamber of Pharmacists, the Medical Association, the Federal Ministry of Health, the Austrian "Bundesgesundheitskommission", ARGE ELGA
GER	Federal Ministry of Health, protego.net, "gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH", German Pharmacist Association
FIN	Ministry of Social Affairs and Health, Social Insurance Institution of Finland (KELA), National Supervisory Authority for Welfare and Health (VALVIRA), National Institute for Health and Welfare (THL), League of Local Authorities (KUNTALIITTO)
SWE	Ministry of Health and Social Affairs, National Board of Health and Welfare, Apotekens Service AB, Swedish Association of Local Authorities and Regions (SALAR)
DEN	Ministry of the Interior and Health, MedCom, Sundhed.dk, National Board of eHealth (NSI)

Table 6.3: Overview responsible parties

	Legal prerequisites
AUT	Data Protection Act (DSG2000), Law of Electronic Health Data Transmission (GTelG), Gesundheitstelematikverordnung (GTelV), Federal Act on Provisions Facilitating Electronic Communications with Public Bodies (E–GovG), ELGA–Law (ELGA–G)
GER	German Federal Act GMG (GKV–Modernisierungsgesetz), German Social Security Act, German Data Protection Act
FIN	Personal Data Act, Act on Experiments with Seamless Service Chains in Social Welfare and Care Services, Decree on the Storing of Patient Data, Client Data Act, Legislation on the Use of ePrescription, Health Care Act, Act on Information Management Governance in Public Administration, Social Welfare Act, Decree on Nationwide Health Care Information System Services
SWE	Patient Data Act, Act of the Prescription Database, Act of Medication Summary, Personal Data Act, Digital Signatures Act
DEN	Act on Processing of Personal Data, Consolidation Act on Legal Protection and Administration in Social Matters, Danish Health Act

Table 6.4: Overview legal prerequisites

	Identification/Authentication
AUT	Every citizen has an e–card for authentication, pharmacies and physicians need a second key card (a–card, o–card). There is no medical data stored on the card (only insurance data and basic data of the patient), it serves as key to the eHealth system.
GER	Every citizen will have an e–card (the eGK) for authentication in combination with a PIN, chosen by the patient. Pharmacies and physicians need a second key card (the HBA). On the card the insurance data and basic data of the patient, the encrypted PIN, the emergency data record and the last 50 access attempts are stored.
FIN	Authentication is done with e–cards (there are different cards for access to KanTa, insurance data and citizen card functions), healthcare professionals have an additional card (VALVIRA card). E–cards are only used for identification and therefore only contain the data needed for this purpose.
SWE	Every citizen can apply for an e–card provided by SITHS (Secure IT in the Healthcare Sector) and has her own key– and security code.
DEN	Every citizen is registered in den Central Person Register with an unique identifier, every healthcare professional is registered in the National Board of Health. Those identifications are stored on the Health Card of every citizen, but for authorization digital signatures and security certificates are used.

Table 6.5: Overview identification/authentication

	Data security
AUT	Data is transmitted via a secure network (the e–Hi Net for hospitals, otherwise the GIN). For secure authentication according to the law role–based access control, the IHE Technical Framework and the profile ATNA Secure Node were used. HL7 delivered an implementation guide for the standardization in ELGA
GER	Telematics infrastructure was planned as service–oriented architecture, RPC (remote procedure calls) were used as communication between services. RSA cryptography is used for encrypting data on the card, there is a role–based access control. SSL (Secure Sockets Layer Protocol) and the Internet Protocol Security method are used for secure transportation of the medical data.
FIN	eHealth system is planned as national messaging system with web services and SOAP interfaces (centralized repository service) and by using open standardized interfaces. Implementation–guidelines were delivered from HL7 to assure the adherence to standards for interoperability. Identification and authorization are based on the citizen certification. Two–way authenticated SSL/TLS–connections as well as Web Services Security X.509 token profile are used for securing medical content.
SWE	The national eHealth network Sjunet is based on VLAN technology and therefore separated from the internet. The e–cards contain a PKI certificate for authentication and identification (role–based), every card user has her own key- and security code. Further standards used are HL7 v3, Tveksamt, DICOM däremot, EN 13606, ICD 10 and ENV 13607 (ePrescription).
DEN	eHealth infrastructure is planned as a national service–oriented architecture via SOAP based web services over HTTP. Data is transmitted via the VPN–based health care network SDN. SAML 2.0 was used as identity framework, further standards are DICOM, ICD10, ICPC and SnomedCT, DS 484 information security standard.

Table 6.6: Overview data security

Although in some Nordic countries ePrescription is already in use for years the realization of electronic health records isn't finished yet. E.g. ePrescription was used in Sweden before 2000 but the electronic health record NPÖ is currently just in the roll-out phase. Because an electronic health record combines so many different types of information from many sources it is much more difficult to link the different data sources and to combine them in a central repository.

The question is how to make sure this central data source is protected from unauthorized access and acts of sabotage. Medical data can be used against the patient and harm her social life and also her job life immensely, insurances or employers have interest in knowing the medical condition of their clients and employees for financial reasons. The disclosure of an abortion or mental health issues could impact a patient's life drastically, so ensuring privacy has to have top priority.

The evaluation of the ePrescription approaches in chapter 5 has its focus on privacy protection measures. For all the evaluated approaches extensive legal adaptions have been made to provide a solid legal foundation for ensuring privacy of citizens' medical data. Table 6.4 provides an overview which laws and regulations were adapted or introduced for each approach to realize this goal. Austria went as far as passing a new law solely for the planned electronic health record (ELGA Act), which defines who has access to patient data and states clearly that misuse of this data will be punished. A comprehensive logging feature makes sure that nobody can access patient data unnoticed and all actions are traceable.

In spite of the legal adaptions not all doubt is cleared. In Austria the Medical Association criticizes the privacy protection of ELGA strongly and tried even to stop the whole pilot project. The acceptance of the population could be better, because the participation in the pilot project was not very high. Also the pilot project got a lot of negative feedback from the doctors due to shortcomings of the software itself, because it was too slow and the integration into the medical practice offices' software was in need of improvement, also there were several stability problems. To increase the acceptance of the users it is absolutely necessary to provide a stable and fast system.

In countries where ePrescription is already in use for some time (e.g. in Finland), the acceptance of people is very good. They appreciate the advantages of ePrescription and are not as wary towards the introduction of an electronic health record. In Finland the good reception was attributed to the the well–thought–out action plan for the introduction of the ePrescription service.

In a country like Austria where ePrescription is a new concept public relations should be increased, so people are better informed what advantages ePrescription and electronic health records can offer them and how their private data is secured and security risks are minimized. Anyway it can be assumed that once ePrescription is established in the country and people got used to it the acceptance towards eHealth will increase.

In addition it has to be said that if the general practitioners are supporting ePrescription or ELGA in general this would have an influence on patients too, because the general practitioners often are the interface between patients and the ePrescription/EHR system and a lot of elderly people or patients who aren't sure what to think of ELGA would ask their opinion.

The ELGA Act defines an Opt–Out opportunity for citizens which means that they can withdraw their participation in ELGA. From a point of view regarding privacy the other way round would be more preferable, which means that the citizen should have an Opt–In opportunity and shouldn't have to make an effort to quit a participation, that she never actively agreed to. Beyond that it would be harder for elderly people, who are generally less experienced with technology or aren't mentally or physically able to do an Opt-Out. The same goes for all kind of people who aren't interested in eHealth matters and therefore don't even notice what's happening with their medical data and who might have access to it. Everyone who participates in this kind of project should agree to it actively and be able to get all information to make an informed decision about it.

Naturally this way is not practical for introducing a project of this size, it would take a long time to get every citizen of a country to agree to a participation and it would increase the cost of introduction immensely. So all the countries in this evaluation don't support an Opt–In, several of them don't even support an Opt–Out (e.g. Finland, Denmark), though the patients can restrict access to parts of their medical information.

An important privacy aspect in EHR systems is access control to medical information, which in Austria is even requested by law (GTelG). An appropriate principle would be RBAC (role–based access control), which is a foundation of ELGA and therefore also for the ePrescription component. So it is possible to give the different parties, who are involved in a treatment process (general practitioner, patient, medical specialists, institute for radiology and so on) different access rights to the same set of data. So they have access to the data they need, but not to data, that isn't important for their role in the treatment.

The role system also makes it possible for the patient to restrict certain medical information not generally but also role–based. The German approach is also based on a strict role–based access control, whereas the Danish approach doesn't support it. An overview how access to medical data is handled and secured can be found in table 6.6.

Another important element of access control is the authorization of the user. To associate the user with her appropriate role it is necessary to use a technology for her secure and unambiguous identification. In the evaluated countries this is mostly done with a physical token e.g.an e–card, which contains the identification data of the user and is used as a key for access to the eHealth system. In Austria there are different types of cards in use depending on the user role, because pharmacists and physicians are using another type of card than the patients . It's also possible to activate the e–card as a citizen's card and use it for authentication for eGovernment services as the social security number, which is stored on the card, is a unique identifier for every Austrian citizen.

The only evaluated country which doesn't use e–cards is Denmark, where the decision was made in favor of electronic signatures. This happened mainly due to financial reasons, because the introduction of e–cards is quite expensive in comparison. It is easier and cheaper for the patients to use it for eHealth services at home compared to Austrian citizens who have to buy a card reader and install the according software on their own to use eGovernment or eHealth services from their own personal computers. Not to mention the administrative effort to activate the card as a citizen's card, which is necessary for example to look at an overview of used health insurance claims or the current state of the prescription fee account [75].

Despite the lower effort and costs that come with using digital certificates they also have their weaknesses. In case of the Danish approach the used SAML assertions make it possible that the issuer of the certificate is aware of the user's identity and therefore able to retrace the user's actions which is a security issue. Also if somebody is able to compromise the digital signature — a risk which is increased by the fact that the unique identifier of the user is embedded in the digital signature — she is able to access all available services with an impersonated identity due to the used SSO mechanism.

Secure access control is also associated with a secure way to transmit data. Usually this is achieved by using certificates, secure protocols and standards and encrypted connections. E.g. Finland provides the Tunnistus.fi–service for a secure authentication and data transmission, Denmark the VPN–based health care network SDN, Sweden provides the secure communication channel Sjunet and Austria the secure network GIN.

Also all the evaluated approaches use a wide range of protocols and standards although not all countries could implement the defined strategy. In Austria the ePrescription prototype got negative feedback in regards of the used standards. Even though the Austrian eHealth strategy determined the use of international standards and IHE profiles most of the software developers working on the prototype didn't use them. Hopefully in the final software version of the ePrescription service this issue will be eliminated. The tables 6.6 and 6.5 provide a more detailed overview of the used authentication techniques and data security measures.

Yet another method to increase security is the decentral storage of sensitive data. If the medical data sources of eHealth applications are evenly distributed and have different physical storage locations, even when an intruder is able to gain access to one of these data sources she wouldn't be able to compromise the others. This approach is used by the Austrian EHR which uses a document registry as an index for medical documents, that only references to the document's physical storage location but doesn't contain actual medical data.

Secondary use of medical data for research purposes or medical quality management is common in the evaluated countries and some of the approaches even provide their medical data for this purpose under specified conditions. This is the case in Finland, where eHealth data from nation–wide and regional registries can be approved for research projects without the patient's consent, although commercial use is not supported. Naturally the data is pseudonymized first, but there are some dates and addresses used in clear text which could potentially be backtracked to a person. Otherwise there are strong rules concerning the issuing of this kind of data in Finland, who is able to use the data and how long this is allowed before the data has to be given back.

In Denmark there are also a lot of health and social registries where medical data is shared for certain research projects and the citizens cannot do anything about it, because it's regulated by law. Although the data is de–identified by removing names and addresses the unique identifier of the patient is not, which contains gender and date of birth. Because of that there is the possibility of re–identification in spite of a set of rules and restrictions how to use the data and on what terms. Secondary use of medical data from EHR is possible but is subject to very restricted conditions. In Sweden the data of registries can also be used for those purposes although the rules seem to be stricter than those of the other mentioned countries. There is a possibility for the patient to apply for a removal from the registries and also the de–identification is more thorough and includes all identifying numbers. Medical data from electronic health records will likely be part of the quality registers in the future.

In Germany it is also possible to use medical data on the state level for research purposes in anonymized or pseudonymized form, but at the moment medical data from the EHR is not included for this purpose. Although it is possible that the de–identified data contains some dates or places which might lead to re–identification the potential for this has to be considered low, otherwise including this kind of information would not be approved by the responsible person. In Austria the EHR is not supposed to provide any information for research projects or other medical reports, the social insurance agencies however are legally obliged to provide pseudonymized diagnostic medical data for the authorities.

Pseudonymization — which is described in greater detail in chapter 3 — could be used in this context to help maintaining privacy in eHealth services. While it is already often used in cases of data linkage and providing de–identified data for secondary use, it has great potential in being included in the management and storage of health data in electronic health records. Although secondary use of medical data often gets by with de–identification of medical data like removing identifiers e.g. names, dates of birth and social security numbers. Often it isn't necessary to re–identify the data by reallocating the pseudonymized data to the original data, whereas in electronic health records this is a necessity.

The German approach of implementing an electronic health record/ePrescription service uses a pseudonymization approach developed by the Fraunhofer institute, which connects the key card (eGK) with an unique pseudonym, which is used for authentication and encryption. A detailed description how this pseudonymization approach works is given here 5.2.

Unfortunately the introduction of the eGK was delayed and is currently in progress with the ePrescription application not included. The process of introduction is very time consuming and expensive, which might be the cause for the huge setback and the pared–down version of the eGK, which was reduced to only support a few basic applications. Although one must admit that looking on the number of inhabitants in Germany in comparison to the evaluated countries, that already did introduce an ePrescription solution, the realization in Germany is on a completely different scale.

The peer review of the Finnish eHealth strategy recommends an increase of pseudonymization to raise privacy and data protection for the benefit of the citizens. Also in Denmark some risks in secondary use of medical data could be eliminated by using an appropriate pseudonymization system as a Danish study of consumer issues stated [6].

PIPE is a pseudonymization approach which was developed especially for securing medical information in electronic health records — in particular the Austrian EHR and the associated e–card as client authentication tool —, and is described in–depth in chapter 3.3. A key feature of PIPE is the separated storage of medical data and patient master data, the two data sets are only related by the used pseudonym. So even when an intruder is able to break into the database she wouldn't be able to connect the two data sets with each other. By using a role–based approach the patient is able to manage the access authorization to her medical data by defined role, she is in control who has access to her data and can revoke this authorization anytime.

Administrators, who have to have access to the system for maintenance purposes are also not able to read the de–pseudonymized data, therefore also sabotage from the inside is prevented. People who have the authority to query pseudonymized data for secondary use are able to do so, but also don't have access to the original data, at the same time the patient is informed about those data queries. Necessary backup strategies for recovering lost or stolen keys involve an algorithm where several persons are necessary to issue a new key. So old keys cannot be used anymore for accessing sensitive data and it isn't possible for one person alone to generate a new key which minimizes the risk of misuse.

Neubauer [66] has extracted a set of requirements for a pseudonymization approach in the eHealth sector in regards to European and American privacy laws and evaluated which approaches are able to meet them. PIPE was the only one among the evaluated approaches that was able to meet all the requirements, second best was the pseudonymization approach used for the German eGK. The only weak point that was discovered was the risk of a data profiling attack due to unencrypted words in the anamnesis data. Neubauer recommends PIPE as the most appropriate approach concerning secondary use. Furthermore PIPE doesn't force the encryption of patient data, but provides it as a feature.

Due to the before mentioned advantages pseudonymization could be a practicable way to increase privacy of sensitive data and meet all necessary requirements. Although there are several possible approaches for pseudonymization (see chapter 3.3 for more information), PIPE seems the most appropriate one because it not only fulfills a lot of requirements, but is also designed for exactly this purpose of securing medical data, so — in contrary to the other approaches – it wouldn't be necessary to adapt it to the eHealth field of activity.

Chapter 7

Conclusion

Electronic health records and ePrescription have a lot of advantages for patients but also for the society. It increases patients' security by avoiding double medication, negative interactions or other medication errors. It also gives an overview of all the medication and over–the–counter drugs a patient is and was consuming in the past, occurred allergies or intolerances and therefore might provide important information for the treatment.

The aging of the population and the decreasing birth rate affects our health care system more and more, the health care costs will increase over time and ways must be found to make the system more economic and to reduce unnecessary expenses. Electronic health records can help to avoid redundant examinations e.g. multiple X–rays because the patient consults different medical specialists. The free choice of medical practitioners makes more sense because every general practitioner is able to access the whole medical history of the patient and therefore no medical knowledge is lost in the change. Also the patient gains more personal responsibility because he is able to access his own medical data, diagnostic findings, X–rays and so on.

In the future the paper–based doctor's office has no place anymore, electronic management and storing of medical data is the way to go, it's a natural progress that cannot be stopped in a long–term view. Therefore the time is more than right to realize this. Naturally the privacy of the patient has to be protected, the legal prerequisites were already created, a lot of countries are already in the middle of the introduction of electronic health records or at least in the planning process.

A lot of critics argument that privacy is threatened by this development and the maintaining of privacy should have priority over the introduction of electronic health records. The privacy argument is also one of the main concerns in the population and reducing the acceptance of ELGA. But on the other hand the health insurance companies already have all the performance data of their patients and are able to derive a lot of information from this data e.g. prescription patterns of doctors, diagnosis and treatments, familial accumulations and things like that. So it seems like a mute point being afraid of ELGA in this regard.

With the technological possibilities discussed in this thesis privacy can be secured on a very high level. Nobody can give a 100 % guarantee that nothing will ever happen, but even in a paper–based doctor's office somebody could break in and gather patient data or a doctor's assistant could leak information. With the appropriate legal framework, a well thought–out implementation strategy and the appropriate technical solution the maintaining of privacy in electronic health records should be accomplishable in the near future.

Bibliography

[1] Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures. In *Lecture Notes In Computer Science: Advances in Cryptology - ASIACRYPT '96*, volume 1163, pages 244–251, 1996.

[2] Mark S. Ackerman, Lorrie F. Cranor, and Joseph Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*, pages 1–8. ACM, 1999.

[3] Giuseppe Ateniese and Breno de Medeiros. Anonymous e-prescriptions. In *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society*, pages 19–31, 2002.

[4] Stefan Bales. Die Einführung der elektronischen Gesundheitskarte in Deutschland. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, 48(7):727–731, 2005. http://www.springerlink.com/content/r75260465807832p [cited 20.10.2013].

[5] Paola Benassi. Truste: an online privacy seal program. *Communications of the ACM*, 42(2):56–59, 1999.

[6] Sahil Bhagat, Danielle Fontaine, and Karl Gibson. Danish healthcare information technology - an analytical study of consumer issues. Project, Worcester Polytechnic Institute, May 2010. http://www.wpi.edu/Pubs/E-project/Available/E-project-051010-054949/unrestricted/Danish_Health_IT_Project_Final_Report.pdf [cited 20.10.2013].

[7] Louis D. Brandeis and Samuel D. Warren. The right to privacy. *Harvard Law Review*, IV.(5):193–220, 1890.

[8] S. Brands. Private credentials. White paper patented by Zero-Knowledge Systems, Inc., Nov. 2000. http://osiris.978.org/~brianr/crypto-research/anon/www.freedom.net/products/whitepapers/credsnew.pdf [cited 20.10.2013].

[9] C. W. Brill, K. Förster, and W. Keil. Patientenfach und elektronisches Rezept. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, 48(7):732–735, July 2005. http://www.springerlink.com/content/g6112305kw515641 [cited 20.10.2013].

[10] Jörg Caumann. Der Patient bleibt Herr seiner Daten Realisierung des eGK-Berechtigungskonzepts über ein ticketbasiertes, virtuelles Dateisystem. *Informatik-Spektrum*, 29(5):323–331, Oct. 2006. http://www.springerlink.com/content/a46463351j0734g4 [cited 20.10.2013].

[11] Jörg Caumann, Herbert Weber, and Arne Fellien. Die eGK-Lösungsarchitektur Architektur zur Unterstützung der Anwendungen der elektronischen Gesundheitskarte. *Informatik-Spektrum*, 29(5):341–348, Oct. 2006. http://www.springerlink.com/content/305k7233n85541x5 [cited 20.10.2013].

[12] David Chaum. Blind signatures for untraceable payments. In *Advances in Cryptology - CRYPTO82*, pages 199–203. Springer Verlag GmbH, 1983.

[13] David Chaum and Torben P. Pedersen. Wallet databases with observers. In Shafi Goldwasser, editor, *Advances in Cryptology - CRYPTO '92*, pages 89–105. Springer Verlag GmbH, 1993.

[14] Esben Dalsgaard, Kåre Kjelstrøm, and Jan Riis. A federation of web services for danish health care. In *Proceedings of the 7th symposium on Identity and trust on the Internet*, IDtrust '08, pages 112–121, New York, NY, USA, 2008. ACM.

[15] DSG 2000 (Datenschutzgesetz). Federal act concerning the protection of personal data. BGBl. I No 57/2013, 1999.

[16] Republik Österreich Datenschutzrat. Pilotprojekt e-Medikation Stellungnahme des DSR. http://www.bka.gv.at/DocView.axd?CobId=39787 [cited 20.10.2013], June 2010.

[17] Hauptverband der österreichischen Sozialversicherungsträger. Reformprojekt e-Medikation gestartet. Press release 29/2009 http://www.hauptverband.at/portal27/portal/hvbportal/channel_content/cmsWindow?action=2&p_menuid=69444&p_tabid=2&p_pubid=635945 [cited 20.10.2013], June 2009.

[18] Wolfgang Dorda, Georg Duftschmid, Walter Gall, Stefan Janzek-Hawlat, Elske Ammenwerth, Werner Hackl, Alexander Hörbst, Martin Jung, and Klemens Woertz. Pilotprojekt e-Medikation - Abschlußbericht der Evaluierung. Technical report, Medizinische Universität Wien (MedUni Wien), Zentrum für Medizinische Statistik, Informatik und Intelligente Systeme (CeMSIIS), Priv. Universität für Gesundheitswissenschaften, Medizinische Informatik und Technik (UMIT), May 2012. http://www.elga.gv.at/fileadmin/user_upload/uploads/download_Papers/PR/Langfassung_Pilot_e-Med_Evaluierung.pdf [cited 20.10.2013].

[19] P. Doupi, E. Renko, S. Giest, and J. Dumortier. Country brief: Denmark. Report, European Commission, DG Information Society and Media,

Oct. 2010. http://ehealth-strategies.eu/database/documents/Denmark_CountryBrief_eHStrategies.pdf [cited 20.10.2013].

[20] P. Doupi, E. Renko, S. Giest, and J. Dumortier. Country brief: Sweden. Report, European Commission, DG Information Society and Media, Oct. 2010. http://ehealth-strategies.eu/database/documents/Sweden_CountryBrief_eHStrategies.pdf [cited 20.10.2013].

[21] P. Doupi, E. Renko, P. Hämäläinen, M. Mäkelä, S. Giest, and J. Dumortier. Country brief: Finland. Report, European Commission, DG Information Society and Media,, Oct. 2010. http://ehealth-strategies.eu/database/documents/Finland_CountryBrief_eHStrategies.pdf [cited 20.10.2013].

[22] EC1995. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities of 23. Nov. 1995 No L 281*, 1995.

[23] E-GovG 2004 (EGovernment-Gesetz). Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen. BGBl. I Nr. 10/2004, 2004.

[24] The eHealth Initiative and the Center for Improving Medication Management (CIMM). Electronic prescribing: becoming mainstream practice. http://www.thecimm.org/PDF/eHI_CIMM_ePrescribing_Report_6-10-08.pdf [cited 20.10.2013], June 2008.

[25] ELGA-Gesetz. Elektronische Gesundheitsakte - Gesetz. BGBl. I Nr. 111/2012, Dec. 2012.

[26] FEEI Fachverband der Elektro-und Elektronikindustrie. Positionspapier des FEEI/FV UBIT zu den Pilotierungen e-Medikation. http://www.feei.at/schwerpunktthemen/gesundheit/veroeffentlichungen/?download=4433.pdf [cited 20.10.2013], Aug. 2010.

[27] Dirk Frosch-Wilke. Are e-privacy and e-commerce a contradiction in terms? - an economic examination. In *Proceedings of the 2001 Informing Science*, pages 191–197, 2001.

[28] Bundesbeauftragter für den Datenschutz und die Informationsfreiheit. Elektronische Gesundheitskarte - Historische Entwicklung. http://www.bfdi.bund.de/DE/Schwerpunkte/ElektronischeGesundheitskarte/Artikel/eGK_historische%20Entwicklung.html?nn=409956 [cited 20.10.2013], 2011.

[29] Bundesministerium für Gesundheit. Zustimmungserklärung e-Medikation. http://bmg.gv.at/cms/home/attachments/0/5/8/CH1045/CMS1301392617134/zustimmungserklaerung.pdf [cited 20.10.2013], Mar. 2011.

[30] Bundesministerium für Gesundheit. ELGA-Gesetz -Präsentation zur Regierungsvorlage. http://bmg.gv.at/cms/home/attachments/5/6/5/CH1045/CMS1338460371868/20121009_elga-g_pp.pdf [cited 20.10.2013], Oct. 2012.

[31] Bundesministerium für Gesundheit. Die elektronische Gesundheitskarte. http://www.bmg.bund.de/krankenversicherung/elektronische-gesundheitskarte/allgemeine-informationen-egk.html [cited 20.10.2013], April 2013.

[32] INNOMED Gesellschaft für medizinische Softwareanwendungen GmbH. Erlkönig "e-Medikation". *Innonews*, 23:1, Mar. 2011.

[33] Pharmazeutische Gehaltskasse für Österreich. Arzneimittel-Sicherheitsgurt mit e-card, Pilotprojekt in Salzburg - Teil 1. http://www.gehaltskasse.at/internet/GHK/Infos.nsf/agentEmergency!OpenAgent&p=DD76DB760B568365C12573F500446862&fsn=fsStartHome&iif=0 [cited 20.10.2013], 2008.

[34] Ruth Gavison. Privacy and the limits of law. *The Yale Law Journal*, 89(3):421–471, 1979.

[35] gematik GmbH. Die elektronische Gesundheitskarte - Whitepaper Sicherheit. Whitepaper 3.0, gematik GmbH (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), April 2008. http://www.dkgev.de/media/file/4426.gematik_whitepaper_sicherheit_3571.pdf [cited 20.10.2013].

[36] gematik GmbH. Einführung der Gesundheitskarte - Übergreifendes Datenschutzkonzept in der Gesundheitstelematik. Specification 0.9.0, gematik GmbH (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), July 2008. http://www.gematik.de/cms/media/dokumente/release_2_3_4/release_2_3_4_datenschutz/gematik_DS_Datenschutzkonzept_V090.pdf [cited 20.10.2013].

[37] gematik GmbH. Einführung der Gesundheitskarte - Speicherstrukturen der eGK für Gesundheitsanwendungen. Specification 1.1.0, gematik GmbH (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), July 2009. http://www.gematik.de/cms/media/dokumente/release_4_0_0/eGK_V221ff_101004.zip [cited 20.10.2013].

[38] gematik GmbH. Einführung der Gesundheitskarte - Spezifikation des Regelwerks für die Gültigkeitsprüfung der elektronischen Gesundheitskarte. Specification 1.1.0, gematik GmbH (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH), July 2009. http://www.gematik.de/cms/media/dokumente/release_4_0_0/Fachanwendungen.zip [cited 20.10.2013].

[39] Robert S. Gerstle, Christoph U. Lehmann, and Council on Clinical Information Technology. Electronic prescribing systems in pediatrics: The rationale and functionality requirements. *Pediatrics*, 119(6):1413–1422, 2007.

[40] Arbeitsgemeinschaft Elektronische Gesundheitsakte. Die elektronische Gesundheitsakte in Österreich - Ausblick auf die erste Umsetzungsphase. Report, ARGE ELGA, 2007. `http://www.initiative-elga.at/ELGA/allgemein_infos/Ausblick_elga_umsetzung_phase1_070510.pdf` [cited 20.10.2013].

[41] GTelG 2005 (Gesundheitstelematikgesetz). Bundesgesetz über Telematik im Gesundheitswesen. BGBl. I Nr. 179/2004, 2004.

[42] GTelV 2012 (Gesundheitstelematikverordnung). Gesundheitstelematikverordnung. BGBl. II Nr. 483/2012, 2012.

[43] Dr. Wienzl Informationssysteme GmbH. Ordinationsmanagement für die moderne Arztpraxis! `http://www.wis.at/Service/Dokumente/Handbuch/SIS.pdf` [cited 20.10.2013], 2011.

[44] Orin M. Goldblum. Electronic prescribing: Criteria for evaluating handheld prescribing systems and an evaluation of a new, handheld, wireless wide area network (wwan) prescribing system. In *Proceedings of the 2001 American Medical Informatics Association*, 2001.

[45] Gesellschaft für Versicherungswissenschaft und-gestaltung GVG. Management-Papier “Elektronisches Rezept”. Management paper, GVG, 2001. `http://ehealth.gvg.org/cms/medium/691/Managementpapier010620.pdf` [cited 20.10.2013].

[46] Gesellschaft für Versicherungswissenschaft und-gestaltung GVG. Management-Papier “Pseudonymisierung/Anonymisierung”. Management paper, GVG, 2004. `http://ehealth.gvg.org//cms/medium/712/MP_Pseu.Anon.040503.pdf` [cited 20.10.2013].

[47] Sundhedsstyrelsen Danish Health and Medicines Authority. The shared medication record wins digitisation award. `http://laegemiddelstyrelsen.dk/en/service-menu/about-us/news/the-shared-medication-record-wins-digiti--tion-award` [cited 20.10.2013], April 2011.

[48] Sundhedsstyrelsen Danish Health and Medicines Authority. The Medicine Profile - citizens’ medication overview. `http://laegemiddelstyrelsen.dk/en/service-menu/about-us/the-medicine-profile--citizens-medication-overview` [cited 20.10.2013], January 2013.

[49] CSC Healthcare. Csc announces european eprescription solution to reduce medical errors whilst improving efficiency and patient safety. `http://www.csc.`

com/health_services/press_releases/54910-csc_announces_european_eprescription_solution_to_reduce_medical_errors_whilst_improving_efficiency_and_patient_safety [cited 20.10.2013], June 2010. Press Release.

[50] Johannes Heurix, Thomas Mück, and Thomas Neubauer. Zentralisierte Pseudonymisierung von medizinischen Patientendaten. In *Tagunsgsband eHealth2009 & eHealth Benchmarking 2009*, pages 207–213, 2009. Vortrag: eHealth2009 & eHealth Benchmarking 2009, Wien; 2009-05-07 – 2009-05-08.

[51] Lars Hulbaek. Service Oriented Architecture - a new infrastructure for the electronic exchange of information in Danish healthcare. http://www2.telemed.no/ttec2008/presentations/wednesday/ps13/01_Hulbaek_OK.pdf [cited 20.10.2013], June 2008. tromso telemedicine and ehealth conference 2008.

[52] IBM. Machbarkeitsstudie betreffend Einführung der elektronischen Gesundheitsakte (ELGA) im österreichischen Gesundheitswesen. Feasibility study, IBM, 2006. http://bmg.gv.at/cms/home/attachments/7/2/0/CH1045/CMS1169796766007/machbarkeitsstudie_elga.pdf [cited 20.10.2013].

[53] IBM. Ergebnisbericht - ELGA Systemkomponenten und Masterplan. Report, IBM, 2007. http://bmg.gv.at/cms/home/attachments/7/2/0/CH1045/CMS1169796766007/ergaenzungsstudie.pdf [cited 20.10.2013].

[54] Digital Health Connected Digital Health in Denmark. National strategy for digitalisation of the danish healthcare service 2008-2012. http://www.medcom.dk/dwn3466 [cited 20.10.2013], Dec. 2007.

[55] Health Information and Quality Authority. Eprescribing and electronic transfer of prescriptions: an international review. http://www.hiqa.ie/system/files/Intl-Review-ePrescribing.pdf [cited 20.10.2013], November 2012.

[56] The National IT and Telecom Agency. New digital security models. http://www.digst.dk/Servicemenu/English/IT-Architecture-and-Standards/Cloud-Computing/~/media/Files/English/New%20Digital%20Security%20Models.ashx [cited 20.10.2013], August 2011.

[57] Helmut Ivansits. Nachhaltige Finanzierung und Solidarität im Gesundheitssystem. *Wirtschafts- und sozialpolitische Zeitschrift (WISO)*, 27(3):88–89, 2004.

[58] Valvira KanTa Services in partnership with STM, THL OPER Unit and VRK. Electronic prescription is in extensive use in public healthcare and pharmacies. http://www.kanta.fi/en/tiedotteet?p_auth=Q0u1bJ0b&p_p_id=AnnouncementListing_WAR_newsFetcherPortlets&p_p_lifecycle=1&p_p_state=normal&p_p_mode=view&p_p_col_id=column-2&p_p_col_count=1&_AnnouncementListing_WAR_

newsFetcherPortlets_current=2&_AnnouncementListing_WAR_newsFetcherPortlets_currentId=3513763&_AnnouncementListing_WAR_newsFetcherPortlets_currentPage=0&_AnnouncementListing_WAR_newsFetcherPortlets_javax.portlet.action=naytaUutinen [cited 20.10.2013], April 2013.

[59] Ilmo Karvonen, Sakari & Keskimäki. Annual review 2012. Technical report, National Institute for Health and Welfare, 2012. http://www.thl.fi/thl-client/pdfs/734b5ed8-decc-451f-9dd3-4a19dc4bfa3c [cited 20.10.2013].

[60] Horng-Twu Liaw. A secure electronic voting protocol for general elections. *Journal of Computers & Security*, 23(2):107–119, 2004.

[61] Anna Lysyanskaya, Ronald L. Rivest, Amit Sahai, and Stefan Wolf. Pseudonym systems. In *Proceedings of the 6th Annual International Workshop on Selected Areas in Cryptography*, pages 184–199, 2000.

[62] Ruth Mayrhofer. Pilot-projekt E-Medikation: "Eindeutig geschlampt". *Österreichische Ärztezeitung*, 11, June 2011.

[63] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[64] GMG 2004 (GKV Modernisierungsgesetz). Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen. BGBl. I Nr. 55/2003, Nov. 2003. 291a.

[65] Christian Müller-Uri and Walter M. Bugnar. Arzneimittel-Sicherheitsgurt mit e-card. Con-ect Informunity - eHealth und Krankenhausinformationssysteme http://www.conect.at/uploads/tx_posseminar/Mueller-Uri_Arzneimittelsicherheitsgurt.pdf [cited 20.10.2013], April 2009.

[66] Thomas Neubauer and Mathias Kolb. An evaluation of technologies for the pseudonymization of medical data. In Roger Y. Lee, Gongzhu Hu, and Huaikou Miao, editors, *Computer and Information Science*, volume 208 of *Studies in Computational Intelligence*, pages 47–60. Springer, 2009.

[67] OECD. Strengthening health information infrastructure for health care quality governance. 2013.

[68] Danish Ministry of Health. ehealth in denmark. http://www.sum.dk/~/media/Filer%20-%20Publikationer_i_pdf/2012/Sundheds-IT/Sundheds_IT_juni_web.ashx [cited 20.10.2013], April 2012.

[69] Ministry of Health and Social Affairs. National ehealth - the strategy for accessible and secure information in health and social care. Report S2011.023, Ministry of Health and Social Affairs, May 2011. http://www.sweden.gov.se/content/1/c6/16/79/85/8d4e6161.pdf [cited 20.10.2013].

[70] Ministry of Health and Social Affairs. Swedish strategy for ehealth - a personal health record. Technical report, Ministry of Health and Social Affairs, 2013. http://www.digitalaskrivbordet.se/wohit/Content/upload/files/1018/A%20personal%20health%20record.pdf [cited 20.10.2013].

[71] Ministry of Health and Social Affairs. Swedish strategy for ehealth - the national patient summary. Technical report, Ministry of Health and Social Affairs, May 2013. http://www.digitalaskrivbordet.se/wohit/Content/upload/files/1013/The%20National%20Patient%20Summary,%20NPO%C3%8C%CB%86.pdf [cited 20.10.2013].

[72] KanTa Finnish National Archive of Health Information. Instruction for using electronic prescriptions. http://www.kanta.fi/documents/10180/3444336/eResepti-esite_uusittu_EN_05-13_web.pdf/40737ef5-8393-4af0-899e-2d896a546712 [cited 20.10.2013], May 2013.

[73] World of Health IT Conference & Exhibition. The shared medication record - from sendung to sharing of medical data. http://www.worldofhealthit.org/2012/wp-content/uploads/2012/presentations/2/MIN2_eHealthfortheChronicPatientHypeHopeorReality.pdf [cited 20.10.2013], May 2012. eHealth Week 2012.

[74] Sten-Erik Öhlund, Bengt Åstrand, and Göran Petersson. Improving interoperability in eprescribing. *Journal of Medical Internet Research*, 1(2), November 2012. http://www.i-jmr.org/2012/2/e17/ [cited 20.10.2013].

[75] Bundeskanzleramt Österreich. Formulare mit Signatur, 2013. https://www.help.gv.at/aof/sigliste-flow;jsessionid=70DD50EE81DCEA31A0D72869E7793778.tomcat_help2?execution=e1s2&ortgemeindeliste:_idcl=ortgemeindeliste_j_id32 [cited 20.10.2013].

[76] HL7 Anwendergruppe Österreich. Allgemeiner Implementierungsleitfaden für ELGA CDA Dokumente. http://www.elga.gv.at/fileadmin/user_upload/uploads/download_Papers/Harmonisierungsarbeit/upload220413/HL7_Implementation_Guide_for_CDA_R2_-_Allgemeiner_Implementierungsleitfaden_fuer_ELGA_CDA_Dokumente_V2.01a.pdf [cited 20.10.2013], April 2013.

[77] Österreichischer Hausärzteverband. e-Medikation - Ein Schritt zu mehr Transparenz und Sicherheit oder in die Überwachungsmedizin? (Transkript). http://www.hausaerzteverband.at/down/transkript_08_06_10.pdf [cited 20.10.2013], June 2010.

[78] Andreas Pfitzmann and Margit Hansen. Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management - a consolidated pro-

posal for terminology. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.31.pdf [cited 20.10.2013], 2008.

[79] Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner. Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. *Datenschutz und Datensicherheit*, 14(5-6):243–253, 305–315, 1990.

[80] Klaus Pommerening. *Medizinische Forschung - Ärztliches Handeln*, chapter Pseudonyme - ein Kompromißzwischen Anonymisierung und Personenbezug, pages 229–233. MMV Medizin-Verlag, 1995.

[81] Klaus Pommerening, Michael Reng, Peter Debold, and Sebastian Semler. Pseudonymization in medical research - the generic data protection concept of the tmf. *GMS Medizinische Informatik, Biometrie und Epidemiologie*, 1(3):Doc17, Dec. 2005. http://www.egms.de/en/journals/mibe/2005-1/mibe000017.shtml [cited 20.10.2013].

[82] Jari Porrasmaa, Juha Mykkänena, Timo Tarhonenb, Marko Jalonenc, Petri Kemppainenc, Antero Ensiod, and Vesa Pakarinene. Application of hl7 cda r2 and v3 messaging for national eprescription in finland. http://www.hl7.fi/wp-content/uploads/eResepti_posteri.pdf [cited 20.10.2013], Oct. 2010.

[83] Richard A. Posner. *Philosophical Dimensions of Privacy: An Anthology*, chapter An economic Theory of Privacy, pages 333–345. Cambridge University Press, 1984.

[84] Joseph Reagle and Lorrie F. Cranor. The platform for privacy preferences. *Communications of the ACM*, 42(2):48–55, 1999.

[85] Rezeptpflichtgesetz. Bundesgesetz über die Abgabe von Arzneimitteln auf Grund ärztlicher Verschreibung. BGBl. I Nr. 413/1972, 1972.

[86] Bernhard Riedl, Veronika Grascher, Stefan Fenz, and Thomas Neubauer. Pseudonymization for improving the privacy in e-health applications. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, HICSS '08, pages 255–, Washington, DC, USA, 2008. IEEE Computer Society.

[87] Bernhard Riedl, Veronika Grascher, Mathias Kolb, and Thomas Neubauer. Economic and security aspects of applying a threshold scheme in e-health. In *The Third International Conference on Availability, Reliability and Security*, pages 39–46, 2008.

[88] Bernhard Riedl, Thomas Neubauer, Gernot Goluch, Oswald Boehm, Gert Reinauer, and Alexander Krumboeck. A secure architecture for the pseudonymization of medical data. In *Proceedings of the second International Conference on Availability, Reliablity and Security*, pages 318–324, 2007.

[89] Rainer Schmidradler. e-Medication - gemeinsam mehr Sicherheit für den Patienten. Con-ect Informunity - eHealth und Krankenhausinformationssysteme

http://www.conect.at/uploads/tx_posseminar/Schmidradler_E-Medikation.pdf [cited 20.10.2013], April 2009.

[90] Falk Schubert. Das Elektronische Rezept: Chancen, Risiken und Gestaltungsmöglichkeiten. Master's thesis, University Heidelberg, Germany, 1999.

[91] Diane Schug, S. H & Whitehouse. Peer review - ehealth strategy and action plan of finland in a european context. Report, European Health Telematics Association, February 2013. http://www.stm.fi/c/document_library/get_file?folderId=6556944&name=DLFE-26602.pdf [cited 20.10.2013].

[92] M. Schug, S. H. & Redders. Gesundheitstelematik-Projekte in Deutschland aus Ländersicht. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz*, 48(6):649–656, June 2005. http://www.springerlink.com/content/l28227027674j134 [cited 20.10.2013].

[93] European Commission Information Society and Media. Apoteket and stockholm county council, sweden - erecept, an eprescribing application. http://www.ehealth-impact.org/case_studies/documents/ehealth-impact-7-2.pdf [cited 20.10.2013], Oct. 2006.

[94] R. Song, L. Korba, and G. Yee. *Privacy Protection for E-Services*, chapter Pseudonym Technology for E-Services, pages 141–171. Idea Group Inc., March 2006.

[95] Ronggong Song and Larry Korba. Pay-tv system with strong privacy and non-repudiation protection. In *IEEE Transactions on Consumer Electronics*, volume 49, pages 408–413, 2003.

[96] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 38–47. ACM, 2001.

[97] Karl A. Stroetmann, Jörg Artmann, and Sarah Giest. Country brief: Germany. Technical report, European Commission, DG Information Society and Media,, October 2010. http://www.ehealth-strategies.eu/database/documents/Germany_CountryBrief_eHS_12.pdf [cited 20.10.2013].

[98] Karl A. Stroetmann, Jörg Artmann, and Veli N. Stroetmann. European countries on their journey towards national ehealth infrastructures. Final european progress report, European Commission Information Society, Jan. 2011. http://ehealth-strategies.eu/report/eHealth_Strategies_Final_Report_Web.pdf [cited 20.10.2013].

[99] Alexander Ströher and Wilfried Honekamp. ELGA - die elektronische Gesundheitsakte vor dem Hintergrund von Datenschutz und Datensicherheit. *Wiener Medizinische Wochenschrift*, 161(13-14):341–346, July 2011.

[100] Suchtgiftverordnung. Verordnung der Bundesministerin für Arbeit, Gesundheit und Soziales über den Verkehr und die Gebarung mit Suchtgiften. BGBl. II Nr. 374/1997, 1997.

[101] Teemu Suna. Finnish national archive of health information (kanta): General concepts and information model. *FUJITSU Scientific and Technical Journal*, 47(1):49–57, January 2011. `http://www.fujitsu.com/ee/Images/paper15.pdf` [cited 20.10.2013].

[102] Petra Tempfer. Ärzte warnen vor der e-Medikation. *Wiener Zeitung*, 4. Juni:12, June 2011.

[103] Heinz Thielmann. *eHealth: Innovations- und Wachstumsmotor für Europa*, chapter Datenschutz und Datensicherheit - Kritische Erfolgsfaktoren für eHealth, pages 195–219. Springer Berlin Heidelberg, 2006. `http://www.springerlink.com/content/w2450576wt7w1446` [cited 20.10.2013].

[104] SVC Sozialversicherungs-Chipkarten Betriebs und Errichtungsgesellschaft m.b.H. e-card: Schlüssel zum Gesundheitssystem. `http://www.chipkarte.at/portal27/portal/ecardportal/channel_content/cmsWindow?action=2&p_menuid=51906&p_tabid=4` [cited 20.10.2013], 2009.

[105] Sozialversicherungs-Chipkarten Betriebs und Errichtungsgesellschaft m.b.H. SVC. e-Medikation: Pilotversuch. `http://www.initiative-elga.at/ELGA/e_Medikation_Infos/Praesentation_Herbek_SVC_Siemens.pdf` [cited 20.10.2013], Oct. 2010.

[106] Sozialversicherungs-Chipkarten Betriebs und Errichtungsgesellschaft m.b.H. SVC. e-Medikation Weg zur erfolgreichen Implementierung. `http://www.wko.at/ubit/IT/Pr%C3%A4sentation_e-Medikation_SVC.pdf` [cited 20.10.2013], June 2010.

[107] Sozialversicherungs-Chipkarten Betriebs und Errichtungsgesellschaft m.b.H. SVC. Von der e-card zu e-health. `http://www.yumpu.com/de/document/view/144130/workshop-positition-der-sv-zum-thema-e-medikation` [cited 20.10.2013], June 2010.

[108] Sozialversicherungs-Chipkarten Betriebs und Errichtungsgesellschaft m.b.H. SVC. e-Medikation - es geht los! `http://www.chipkarte.at/mediaDB/775445_PresseunterlageEND` [cited 20.10.2013], Mar. 2011.

[109] Sozialversicherungs-Chipkarten Betriebs und Errichtungsgesellschaft m.b.H. SVC. e-Medikation. `http://www.chipkarte.at/portal27/portal/ecardportal/channel_content/cmsWindow?p_pubid=641673&action=2&p_menuid=51921&p_tabid=5` [cited 20.10.2013], 2013.

[110] General Assembly Resolution United Nations. Universal declaration of human rights (udhr). Resolution 217 A (III) of 10. Dec. 1948, 1948.

[111] Susanne Valkeakari, Jari Forsström, Pauli Kilpikivi, Pekka Kuosmanen, and Marja Pirttivaara. Saini - electronic healthcare services concept. Technical report, Sitra - Finnish Innovation Fund, Oct. 2008. `http://www.sitra.fi/julkaisut/muut%5CSAINI_Final%20Report.pdf?download=` [cited 20.10.2013].

[112] Jaakko (Medi-IT Oy) Vuolasto. Running-in of eprescription. `http://www.sitra.fi/NR/rdonlyres/AD53E8D8-02AD-426C-87A2-CF2B4EE5E9DE/0/Running_inofePrescription.pdf` [cited 20.10.2013], 2009.

[113] Alan F. Westin. *Privacy and Freedom*. New York: Atheneum, 1970.

List of Figures

List of Tables