Security in the Dutch Electronic Patient Record System

Guido van 't Noordende
System and Network Engineering Group
University of Amsterdam
Science Park 107, 1098XG Amsterdam, the Netherlands
guido @ science.uva.nl

ABSTRACT

In this article, we analyze the security architecture of the Dutch Electronic Patient Dossier (EPD) system. Intended as a mandatory infrastructure for exchanging medical records of most if not all patients in the Netherlands among authorized parties (particularly, physicians), the EPD has to address a number of requirements, ranging from scalability and performance to security and privacy – as well as usability in practice. The EPD is partially centralized. Patient records are stored decentrally, while a central component takes care of authentication and authorization of health professionals and of the mechanics required for exchanging patient records.

The requirements for the EPD, as well as high-level descriptions of solutions and protocols, are described in a set of documents that are publicly available. This paper describes the security and privacy implications of the EPD design, argues where it falls short, and briefly discusses some improvements that may alleviate some of the risks that exist in the current design.

Categories and Subject Descriptors

J.3 [**Computer Applications**]: Life and Medical Sciences – *Medical Information Systems, Health*; K.6.5 [**Computing Milieux**]: Security and Protection; K.4.1 [**Computers and Society**]: Public Policy Issues – *Privacy*

General Terms

Security, Design

1. INTRODUCTION

The Dutch EPD is being mandated by law as the infrastructure to use for exchanging patient information in the Netherlands. The proposed law governing the use and introduction of the EPD is currently discussed in the Senate. The system has been in use since 2008-2010, initially through pilot projects, but subsequently more and more as a production infrastructure.

The EPD is designed by the Dutch National IT Institute for Healthcare (NICTIZ), under supervision of the ministry of health. The overall architectural design of the EPD system is published under the name AORTA [1]. One of the most notable and widely referred-to features of the EPD design, is that it is developed as a partially decentralized system, in contast to, for example, the NPfIT system developed in the U.K [2] which is fully centralized. Here, all patient records are stored in a central database managed by the National Health Service.

Dutch regulations do not favor storage of patient information in a central infrastructure [3, 4, 5]. This is due to legal, security, and privacy concerns raised by a centralized approach. The legal argument that favors decentralization over centralization, is that, in the Netherlands, the physician (and healthcare organization) who has a treatment relationship with a patient is responsible for managing the patient's dossiers [6]. Handing over control of management over patient records to a third party is in conflict with these regulations [3, 5]. The approach taken by the EPD is that patient records are not stored centrally, but instead remain stored in the information system of the hospital, GP, or other party responsible for managing the patient record(s) of a given patient. To allow for finding and retrieving patient information using the EPD, a central *reference index (verwijsindex, VWI)* maintains a set of pointers to the patient records of each patient, using which the records can be retrieved.

Despite decentralized storage of patient records, authentication and authorization (to control access to patient records) in the EPD are fully centralized in the current design. Furthermore, some patient related information *has* to be stored in a central part of the system (such as the VWI), for the EPD to function. Because the EPD contains -in principle-information about all patients in the Netherlands, the privacy risks related to a potential security breach of the central components of the EPD are quite significant.

This paper discusses the architectural design and the mechanisms of the EPD, and evaluates some of the risks associated with the chosen approach. We also briefly discuss some ways to alleviate some of these risks using improvements to the architectural design of the EPD.

2. APPROACH AND ARCHITECTURE

The primary function of the EPD is to couple the decentrally stored patient records such that health professionals throughout the Netherlands can find and fetch patient

SPIMACS'10, October 8, 2010, Chicago, Illinois, USA.
Copyright 2010 ACM 978-1-4503-0094-0/10/10 ...$10.00.

records that are relevant, provided that they are authorized to see these records. Patient records are stored *decentrally*, i.e., only in the information systems of the care providers (such as hospitals and GPs) that have a treatment relation with the patients. The (central) EPD infrastructure provides the mechanisms for retrieving the decentrally stored patient records.

References to all patient records that are accessible through the EPD are registered in the VWI. The VWI references (index lines) describe the available patient records to health professionals, and allow them to locate relevant patient records for retrieval. Alternatively, physicians may specify a *query* to let the EPD find and retrieve a set of records based on information stored in the VWI. Patients are identified using a unique number (the 'burgerservicenummer' or *BSN*, formerly known as the Dutch social security number), which can be looked up by means of a separate *BSN verification service* [7, 8]. VWI index lines and patient records are only visible or queryable to health professionals which are authorized to access the patient record in question.

2.1 Connecting to the EPD

Decentral information systems located at the care providers (e.g., hospitals, GPs, and pharmacies) are connected to a central part of the EPD infrastructure, called *Landelijk Schakel Punt (LSP, literal translation National Switching Point)*. All interactions required for finding and accessing patient records in the EPD go through the LSP. The LSP authorizes and logs all attempts to access information in the EPD.

Information systems must meet some general (security) requirements before they can obtain the credentials required to connect to the LSP [9]. These requirements are, to a large extent, organizational in nature and emphazise aspects such as management and maintenance procedures. Systems that meet these requirements are termed *GBZ*, which, translated from Dutch, stands for *well-managed care system.*

Although the GBZ requirements are an important (first) step towards improving the security of systems that are part of the EPD, it is obviously not possible to guarantee correctness of all systems hardware, operating systems, application programs, and usage of all systems that are part of the EPD – especially because the EPD is an very large system consisting of a large number of GBZ systems which themselves may consist of a large number of (sub)systems and (desktop) PCs. Therefore, the GBZ requirements should not be viewed as a complete answer regarding the security of GBZ systems, even though they are sometimes presented as such.

The connections between (decentral) GBZ systems and the LSP are cryptographically protected to avoid that outside attackers can listen in on the communication channels between GBZ and LSP. Information is currently passing through the GBZ or LSP systems in unencrypted form. Some of the components inside GBZ and LSP are shown in Fig 1.

2.2 Authentication

The LSP is a central component of the EPD infrastructure, which by design requires all systems that participate in the EPD to trust it. In particular, the LSP authorizes all requests in the system. Examples of requests are the retrieval of index lines from the VWI and requests for retrieving patient records. Underlying authorization lies an authentication mechanism which is also centralized. An authorization service (AUT, Fig. 1) located in the LSP takes care of authenticating requests and enforcing (role-based) access control rules.

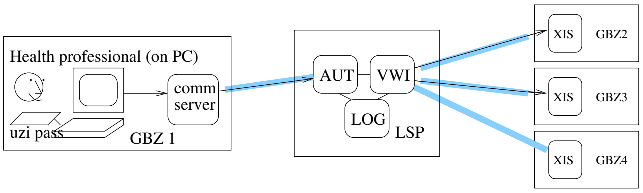

Figure 1: Overview of the EPD, showing how the different components are connected. Several GBZ systems are shown, each connected to the central LSP system by means of encrypted, authenticated SSL connections (thick grey lines). In GBZ 1, a physician is shown who issues a request; this request is sent over a communication server and then forwarded to the LSP (arrows). Authentication and authorization takes place in the LSP (AUT); LOG is the component responsible for logging all requests. Using information from the VWI, the request is forwarded to two information systems (XIS) in different GBZs. Note that the SSL connections cannot prevent the GBZ or LSP components from reading or interfering with traffic that passes through them. The exact internal architecture of the LSP is not described in detail in the public AORTA documentation.

Health professionals can access the EPD using a personal smartcard that contains a public/private keypair. This smartcard is protected by a PIN code, and it is called a *Unique Healthcare provider Identification (UZI)* pass. Each smartcard contains a certificate containing information about the (medical) title, specialization, and function of the health professional, issued by a PKI based on Dutch professional registries. This information is used by the EPD for (role-based) access control.

All data in the EPD (messages, requests, patient records) are transfered as part of a *Health Level 7 version 3 (HL7v3)* (request) message [10] . HL7v3 is a standard supported by many existing healthcare related information systems.

Each request that is sent to the LSP is associated with a token. A token is a data structure, separate from the HL7v3 request message, which contains information used by the LSP to verify the authenticity of the request. The LSP compares the content of the token with the HL7v3 message. The token contains the *BSN* of the patient whom a request concerns, the *information category* that the request is concerned with, and some information to prevent replay. A token is signed by the health professional using his or her UZI pass before a request is sent to the LSP. Using the signature over the token, the LSP can authenticate (verify) which health professional made the request. Normally, a physician signs a token, but it is also possible that a token is signed by a mandated employee or co-worker (Section 4.3). The token is removed by the LSP after authentication and is *not* forwarded to the information system(s) that contain the patient record(s).

2.3 Access Control

The EPD defines two authorization policies to mediate

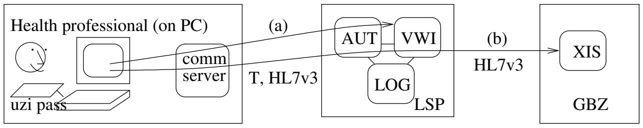

Figure 2: Method invocation and token authentication overview. A request for (a) inspecting VWI index lines, or (b) retrieving a patient record, originates from a physician who signs a token *T* using his or her UZI pass. The token is sent along with the request *HL7v3*. In some cases, part of the request may be adapted (e.g., XML canonicalization) on a communication server in the GBZ before it is sent to the LSP; this does not invalidate the token. (a) depicts the protocol for requesting index lines from the VWI. In case (b), a patient record is retrieved. The LSP authenticates and authorizes the request (using the authentication service AUT), and forwards the HL7v3 request to the VWI, or to the decentral information system(s) (XIS) where the patient record(s) is or are stored. Replies (containing VWI index lines or patient records) take the same route back.

access to patient records. These policies also apply to the VWI index lines for these records: if a health professional is not allowed to access a patient record, he or she cannot obtain the index lines regarding those records either.

First, an *authorization protocol* defines per class of health professional (e.g., General Practitioner (GP), gyneacologist, pharmacist) whether that class is authorized to access a specific type of patient record. For example, a GP is allowed to inspect records created by a pharmacist, as well as records created by other GPs for patients that he or she has a treatment relation with. A pharmacist, on the other hand, is never allowed to see a GP patient record. The authorization protocol is agreed upon nationally by physicians and health organizations, and is enforced by the LSP.

Second, patients are able to define a fine-grained *authorisation profile*, which allows them to define *(restrict)* which health professionals or which care providers (hospitals or other organizations) may access their records. Details on the authorization profile are somewhat vague. In later sections, we will derive some limitations of the authorization profile based on what we know of the current AORTA authentication protocols and delegation mechanism.

3. SECURITY AND PRIVACY

This section focuses on technical aspects of the EPD. We describe some security weaknesses and risks in the current LSP design, both inherent risks and risk that can be alleviated by an improved protocol design.

3.1 Threat Assumptions

Because of its central role in authentication and authorization and the exchange of patient records, the LSP could be an attractive target for attackers. There are obvious rewards in targeting the EPD to obtain private information from it; (financial) incentives could range from selling information concerning TV personalities to a magazine, to blackmailing high-profile people with a sexually transmittable and/or stigmatizing disease such as HIV. Other reasons for attack may be to modify records to influence treatment, or perhaps for other reasons left to the imagination of the reader.

In this paper, an important *threat assumption* is that attackers may penetrate parts of the system, such as the LSP or a GBZ system, with the aim to obtain or modify information regarding (specific) individuals. Attacks could come from outsiders, but also from insiders who have access to parts of the system, or who have extensive knowledge of its inner workings. Insiders have played a role in many real-world attacks [11]. Resourceful attackers or insiders may be able to compromize core components of the LSP, from which they may be able to bypass regular access control checks. Assuming (insider) threats or accidents is not unrealistic, certainly for a system in whose development, implementation, and deployment many people are involved [12, 13].

In this paper, we analyze the security architecture of the EPD for its ability to cope with possible attacks on components in hospitals or the LSP. Examples of components in a GBZ system are an application or a communication server in a hospital, or a router for handling traffic in the LSP. Information pertaining to many patients is exchanged over these systems. Even a passive attack (i.e., listening to and possibly copying, but not changing any messages) may result in large amounts of information being available to malicious software running on these components. The risks of these and more active attacks are evaluated in the remainder of this paper.

3.2 Inherent Risks

Although the EPD does not store all patient information in a single central system, central components such as the VWI still contain privacy sensitive information. For example, in each VWI index line, information about the hospital or organization that a patient visited is recorded, as well as information concerning the physician who registered the reference and the record type (e.g., GP or psychiatrist record, or lab result), is stored. Depending on how the EPD is used, there may also be references to lab results[1] in the VWI. VWI information in itself is sensitive in many cases, for example, think of a record at a cancer institute, a mental institute, or a rehab clinic. Treatment relation information should also be considered privacy sensitive.

Normally, only authorized parties can see VWI index lines, but if an attacker manages to break into the central LSP infrastructure, all index lines of a given individual could be directly obtainable. Because the VWI is required for the functioning of the EPD, this is an *inherent risk* in the current design of the EPD infrastructure.

It is arguable that the VWI could contain less information than what is described above; however, the proposed law describes all the above content of the VWI explicitly and in detail. This makes it unlikely that less information will be embedded in the VWI in the near future; the detailed description of the VWI content in a law is a curious artefact originating from the development of the EPD as a government infrastructure, whose usage is mandated by law.

[1] AORTA also provides a mechanism for secure message transport as a replacement for e-mail, which may be safer and more suitable for exchanging lab results than a (more permanent and more visible) registration in the EPD ; however, public examples for using the EPD include registeration of lab results in the EPD [14], so we describe the possibility here.

By specification and by proposed law, the LSP is required to keep historical (traffic/access) information, and to allow the VWI to be restored to a previous state, until some *reconstruction horizon* in the past [1]. This may be for a period of 15 years, matching the period of time in which physicians are required by law to keep their records [15].

The reconstruction requirement implies that references which were explicitly removed from the EPD, may remain stored in the central LSP infrastructure to allow for reconstruction of the VWI. Traffic information relates to patient records, and may thus (implicitly) contain information about those records. Especially for explicitly removed information, this is a curious situation, as references may have been removed from the EPD precisely because they were considered privacy sensitive by the patient. As a result, complete removal of information from the LSP is difficult or impossible, making this information potentially vulnerable to attacks on the infrastructure.

Patients are allowed to remove records from the EPD. However, removal of information from the EPD is currently not instantaneous, since patients cannot directly remove references to patient records from the VWI: the decentral systems (e.g., hospitals) are responsible for removing information and references from the LSP, possibly involving explicit action from the responsible physician. This may complicate timely removal of information from the EPD, and makes this information at least temporarily vulnerable even without considering attacks on the EPD infrastructure. In addition, time may pass before a patient even notices that (new) information was registered in the EPD. Finally, as indicated above, when references are removed from the LSP, logging and reconstruction information related to those references are currently not fully removed. This means that if an attacker obtains logging (or reconstruction) information, he or she may obtain sensitive information regarding a patient's medical history, including information that the patient explicitly wanted to be removed.

3.3 Trusting LSP for Authorization

An important shortcoming of the token based authentication protocol, is that it does not permit for *end-to-end authentication*: the endpoint information systems where patient records are stored are unable to authenticate incoming requests independently, and thus cannot establish that a request is legitimate and originates from an actual health professional. This means that information systems cannot distinguish a forged message that originates from malicious software in the LSP from a legitimate request.

As a consequence, any malicious code strategically positioned in the LSP can obtain any patient record from any information system connected to the EPD, *without* being questioned. The potential impact is high: a succesful attack on the LSP core infrastructure may allow an attacker to actively retrieve *any* patient record stored in any decentral information system connected to the EPD, without being questioned.

The lack of end-to-end authentication of patient retrieval requests is an important shortcoming of the current EPD design – a simple forwarding of authentication tokens together with the request messages to the decentralized information systems would suffice for these systems to instantly detect any forged messages originating from the LSP - assuming that sufficient information is embedded in the tokens (Section 3.4). The AORTA specification does describe some XML headers to support end-to-end authentication protocols and (payload) encryption for future use. However, these protocols are not currently used for the AORTA *EPD* application.

Note that healthcare providers such as hospitals are legally responsible for ensuring appropriate protection of data – including access control [6]. Therefore, *autonomy* of information systems to implement access control policies independently from the LSP is an important property; this, however, is not currently possible due to the fact that the EPD centralizes authorization in the LSP. End-to-end authentication would allow GBZ systems to independently check the integrity of each request, allowing them to detect attacks as well as potential mistakes in the authorization logic of the LSP. It would also also them to enforce access control rules independently from the LSP (e.g., to block access to some patient records).

3.4 Binding Tokens to Requests

A token is a data structure that contains a (minimal) set of information that allows the LSP to verify the authenticity and integrity of an incoming request. The token is signed using the smartcard of the health professional (or mandated employee, Section 4.3) who made the request. A token allows the LSP to determine the validity of a request, and to authorize the request. Access control rules currently only consider BSN and information categories, and do not enforce policies at the level of individual patient records.

Each token contains the category of the requested information, the BSN number of the patient that the request is concerned with, and a nonce and an expiry date to avoid replay. The LSP verifies whether the information in each token corresponds to information in the HL7v3 request. Tokens are only seen by the LSP and not forwarded; only the HL7v3 request is forwarded to the decentral XIS systems (Figure 2).

Tokens do not contain an identifier for a specific patient record; in fact, the LSP implements a protocol where a request or query regarding a specific BSN and information category is forwarded (replicated) to all information systems that contain a patient record of the BSN and type that matches the query, and have the LSP collect the results before returning them back to the requestor. Thus, a single token can theoretically be used to request *all* records of a given patient (BSN) and information class in a single operation.

Any field in a request message which is not in the token, can be manipulated along the way from the requestor to the LSP without the requestor being aware of it, or the LSP being able to detect it. For example, record identifiers or query parameters are currently not embedded in the token. Suppose a physician wants to obtain all records of a given type up until a year ago, but nothing further back in the past. Malicious software on a communication server can change the query such that *all* available records of this patient and information category are retrieved. On return of the information, the malicious software may read the obtained data, and return only the requested information to the requestor.

The problem explored here is that insufficient information is embedded in the tokens used in the EPD, making it possible to expand requests to obtain a larger set of patient records than the physician intended. This problem is exacerbated by the very large scale of the EPD. Officially, patient records must be kept for about 15 years [6], with discussions taking place to extend this period to 30 years; indeed, the EPD is intended as a *longitudinal* healthcare record. Therefore, it may be normal to find references to patient records many years back in the EPD. As a consequence, even a slight change to a query may make a very large number of (historical) records available to a potential attacker.

In general, it is important that physicians retrieve only information which they require, preferably based on selecting VWI index lines. Recording the precise request (parameters, record identifiers) in the token, avoids that malicious software on the way from physician to LSP can manipulate the request message to obtain more records than the physician intended. Furthermore, embedding more information in the token would allow for enforcing more fine-grained access control rules in a patient's authorization profile, possibly on a per-record basis.

Including sufficient information in a token is also required to achieve the property of *non-repudiation* [12]: only for information signed by a requestor can it be shown (in court) that the requestor made this request - i.e., that no intermediate party (or software on an intermediate system) could have changed the request without the signer's knowledge.

4. AUTHORIZATION

The authorization model of the EPD is based on legal constraints. First, existing regulations concerning patient treatment and patient treatment teams provide a guideline on who may access medical data in the course of medical treatment [6]. Second, patients have a right to decide who may access which information, as defined in European and Dutch data protection regulations [16, 5]. This section describes some aspects of authorization in the EPD which relate to these constraints.

4.1 The Authorization Model

Regulations regarding treatment relations and treatment teams constitute an implicit authorization policy which underlies all access control decisions in the EPD. Figure 3 shows the authorization model.

The *treatment relation* between patient and physician implies authorization of the physician with regard to the patient's EPD records - modulo that the physician's role must match the record type. The physician claims and registers a treatment relationship in the local information system. After a physician has claimed a treatment relation, he can access any record of this patient which is registered in the LSP, provided he is not explicitly excluded from accessing the record by the patient's authorization profile.

An employee within a physician's *treatment team* is -by current regulations- authorized to access a patient's records on behalf of the physician. In the context of the EPD, this extends to authorization of employees to access or modify *all* EPD records that the mandating physician has access to.

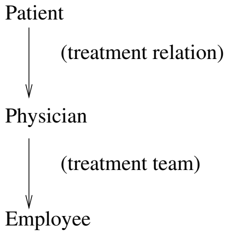

Figure 3: The authorization model which underlies access control in the EPD. Physicians are (implicitly) authorized to access a patient's EPD when they become involved with the patient's treatment. Employees are authorized (implicitly) when they are part of the patient's treatment team. The arrows indicate authorizations; these are not explicitly verifyable in the LSP at the time when an access control decision is made.

4.2 Patient Treatment Relation

When a physician becomes involved in the treatment of a patient, he or she must declare to have a treatment relationship with the patient [17]. The treatment relation is registered locally, in the physician's information system. When a physician accesses a patient record for the first time, the LSP takes this as an (implicit) declaration of a treatment relation, without any further verification: the LSP simply assumes that the treatment relation exists, and that this is somehow verified by or recorded in the physician's local information system. Similarly, the LSP assumes that a treatment relation exists when a physician registers a reference in the LSP[2].

Patients can use the access logs of the EPD to verify who accessed which data, and take (legal) action when detecting that a physician outside a treatment relation accessed their patient record(s). Because treatment relations are currently not explicitly confirmed by patients, it is not possible to *automatically* verify the validity of a claimed treatment relation in the LSP, or to *prevent* illegitimate access.

Because the LSP cannot verify at the time of invoking an operation whether a treatment relation actually exists, the validity of a treatment relation can only be verified after the fact. Patients will in the future be able to access their patient records, adapt their authorization profile, and inspect logging information about who accessed which information of their EPD using a *patient portal* [18]. Patients can thus verify whether access to their EPD by (or on behalf of) a particular health professional was legitimate, that is, if those health professionals indeed had a treatment relationship with the patient at the time of obtaining a patient record [6, 18]. Not all patients may be willing or able to inspect the access logs of their EPD, though, or do so in a timely manner. Also, the composition of a treatment team will not be clear to a patient in general, so it is questionable how effective the use of access logs will be to detect illegitimate access by employees who claim to be mandated by a given physician. In all, the approach seems rather weak.

4.3 Delegation

AORTA provides a model that allows authorized health professionals to *delegate* authority to access the EPD to employees or co-workers. From a legal perspective, this is a

[2] It may be straightfoward for an employee to register information regarding a patient to claim a treatment relationship in prepation of an attack. Also, registering information in the EPD may be critical not just to security, but also to integrity of patient records. For these reasons, we believe that these operations should be reserved for physicians alone.

valid operation: multiple people including co-workers and employees may be part of a patient's *treatment team*, and are in that role authorized to access the patient's patient record(s) [6]. The overseeing physician(s) are responsible for their employee's actions.

AORTA has a decentralized delegation model (called *"mandatering"* in the EPD specification). Every care provider (GBZ) that makes use of delegation, must maintain a *delegation table*. The delegation table describes which employees are allowed to access the EPD on behalf of which health professional(s).

Employees of care organizations can have a personal UZI pass similar to those of health professionals, except that the certificate on this pass contains only the employee's name, and not a medical title. Normally, this pass may only be used for low-security tasks, such as verification of a patient's BSN number [7][3], except when a physician delegates authority to access the EPD to this employee. Physicians can delegate authority to access a patient's records to any employee that has a UZI pass.

Employee passes can be used for obtaining any patient record of any information class on behalf of any physician, as long as the mandating physician is authorized to access this record. The LSP assigns exactly the same rights to a mandated employee, as to the mandating physician.

The EPD also allows usage of employee UZI passes that have a role encoded on them, instead of a name. These passes can apparently be shared freely within a ward; obviously, this has severe consequences for auditability and tracking of possible mis-use of these UZI passes, as these passes are not bound to a specific individual. Using such passes is very dangerous from a privacy and security perspective; we would recommend to immediately stop issuing and using such passes.

4.4 Issues related to Delegation

The delegation mechanism is implemented as follows. A mandated employee signs a token for the request message using his or her UZI pass. The health professional on behalf of whom the EPD interaction takes place, is noted as the *overseer* in a field of the HL7v3 message. This field is not present in the token. Based on the overseer field, the LSP derives who the mandating physician is, and based on this information decides if the request is allowed.

The delegation table is used as an auditing tool that allows maintainers of the EPD to verify *after-the-fact* whether an interaction of an employee could have been made on behalf of the physician specified in the overseer field. However, there currently is no way for the LSP to verify *at invocation time* whether an employee truly acted on behalf of a given physician or not: there exists no way for either the employee or the physician to prove to the LSP that an employee is indeed mandated by the physician.

AORTA fully relies on security of the GBZ system's delegation tables, and, if required, on inspection of LSP audit logs after the fact. Working schedules or agenda entries can be used in addition to delegation tables to establish whether a particular employee could have accessed an EPD patient record legitimately on behalf of this physician or not [1]. It is unclear how or how often such auditing takes place. Note that it may be possible to tamper with delegation tables to cover up mistakes - for example in case of a hospital or physician that wants to avoid getting a bad reputation.

The delegation system is vulnerable to an attack that combines malicious code within a GBZ with a (stolen) employee pass together with a PIN code. Employee UZI passes can be used to access the EPD on behalf of any physician in the same organization. The mandating physician is indicated in a field of the HL7v3 message; if the local information system is working properly and is not tampered with, this information system may take care that only valid physicians (corresponding to information in the delegation table) can be filled in in the overseer field. However, if an attacker breaks into an information system, he can simply construct any HL7v3 message and token, sign it with an arbitrary UZI pass, and inject it into the system and send it to the LSP.

By constructing a HL7v3 message with a suitable overseer field and a token with a matching information category, an *arbitrary* (stolen) UZI pass can be used to retrieve patient records behalf of effectively any physician in a given GBZ, say a hospital. This is a direct consequence of the fact that the EPD relies on security of the decentralized systems to handle delegation (and patient administration) correctly. For large organizations with many physicians and a large number of (potentially vulnerable) systems, this poses a significant risk.

The problem is that the delegation mechanism is not limited in any way. Should there be a mechanism that binds a specific (stolen) UZI pass to a specific health professional at a specific time, or at least to a role, the power of the abovementioned attack would be much limited. In this case, an employee pass would not be usable to claim an arbitrary mandate, but only be usable to misuse an existing mandate for already existing treatment relationships - or at a minimum stay limited to a specific role. Solutions along these lines are discussed in Section 6.

The above assumes a *software attack*. However, depending on the implementation of the local information system, easier ways to abuse the delegation mechanism are conceivable. For example, it may be possible to simply choose an overseering physician using some drop-box of the local information system, to interact with the EPD on the chosen physician's behalf. When such illegitimate use of delegation does not take place too often, it may well go undetected, because a patient who checks the access logs will often not be able to tell which employees were part of his or her treatment team at a particular time.

It may often not be clear to patients who is a valid member of a treatment team. This makes it very difficult for patients to assess whether access to the EPD by a particular employee on behalf of a given physician was legitimate or not, even when detailed access logs are available[4].

Currently, misuse of the delegation mechanism can only be prevented by a patient by blocking a complete care organization in the authorization profile, which may not be

[3] Note that patient treatment relationships may be derived from the verification logs, by inferring information about who requested BSN verification for which patients. Care should be taken to protect the access logs of the BSN verification service accordingly, and to destroy these logs timely.

[4] It is unclear if the names / details of mandated employees are included in the access logs visible to patients, or whether the authorization profile will contain functionality to deny access to (specific) employees. In fact, discussions are ongoing on whether the privacy of employees (as identifyable from the access logs) should be protected.

practical; otherwise, there are few limits to the attack. The attack may be particularly powerful because delegation can also be used to claim a treatment relationship, as far as the LSP is concerned [15]. Mandated employees may even request or register a (new) record of a new patient – operations that we would expect to be reserved to physicians.

4.5 A Fundamental Problem

At a high level of abstraction, the fundamental problem is that the authorization model is *reversed*: instead of a patient actively authorizing physicians, who then actively authorize co-workers or employees directly involved in treating a patient (Fig. 3), employees not known to the LSP can claim to work for any given physician by simply having the system fill in an arbitrary physician in the overseer field, and the physician (and consequently, an employee), can claim a treatment relationship – all without the patient's involvement.

The LSP assumes that a physician who invokes an operation on the EPD, has (locally) declared a treatment relationship with this patient. Also, the LSP assigns all rights of the physician to any employee who claims to work for this physician. Because of this, malicious employees or attackers may obtain practically any patient record from the EPD system using an arbitrary (stolen) UZI pass. Combined with verification after the fact, this model may have severe consequences for patient privacy.

Allowing physicians to claim a patient treatment relationship and then allowing them to access a patient's records based on this claim may be defendable: physicians are registered and held to professional ethics, have a reputation to uphold, and they can be held accountable for their actions by means of professional sanctions. Some degree of trust in physicians seems inevitable. In particular, confirmation of treatment relationships after the fact may be necessary when information is required for urgent medical treatment.

There may be emergency scenario's where the lack of prior treatment confirmation by a patient is defendable; however, it seems unacceptably risky to assign all the rights -including the right to claim a treatment relation- to any employee who claims to work on behalf of a physician, especially without any possibility to verify this claim in the LSP and prevent access in case that a treatment or delegation relation is not confirmed. Note that for specifically privacy-sensitive information such as psychiatric information, delegation may have to be forbidden altogether.

Generally, emergency scenarios should not be regarded as the norm, but as an exception. Explicit treatment confirmation by patients should take place for all non-emergency cases, to ensure that information leakage to unauthorized parties can be *prevented* rather than (at best) detected after the fact. Emergency scenario's are probably not the most common medical scenario for which the EPD offers a solution. In fact, from discussions in the Senate it appears that increased mobility of patients due to competition in healthcare (e.g., where insurers may require patients to migrate to another clinic based on for example pricing or waiting list information) and the need for persistently storing information regarding, e.g., chronic patients, may be the most important use-cases for the EPD [19]. In these and other scenario's, it seems a feasible model to only permit access after explicit, prior confirmation of a treatment relationship, i.e., after explicit authorization, by a patient.

Note that this paper has not included possible risks due to malware on Desktop PCs used by physicians or other healthcare professionals. When these are considered, the above claim of relative safety of trusting physicians may be seen in a different light, since malware may be able to divert the smartcard into signing requests which the physician did not intend to make. This is another scenario where explicit treatment confirmation by patients may be useful, since a careful design can make sure that an attack on the UZI pass based authentication mechanism becomes much more difficult to execute, since patient authorization is then required as well.

4.6 Auditing

The proposed law regarding the EPD emphasizes extensive logging and auditing of these logs as a cornerstone of EPD security [18]. However, the lack of verifiability of delegation and patient treatment relations complicates auditing, and limits the probability that abuse is detected in time or at all. Key questions are:

- *How can the LSP or an auditor establish whether an overseer field is valid, when the responsible physician has not explicitly confirmed that the employee or co-worker is mandated?*
- *How can the LSP or an auditor distinguish a genuine claim of a treatment relation from an illegitimate one when a patient has not confirmed this relation in the EPD?*

Because of the lack of (automatic) verifiability of the above relations, the EPD must depend on heuristics, 'intelligence', or manual procedures -after the fact- to distinguish valid treatment and working relations of physicians or employees from invalid ones. It is easy to envision how malicious software can evade detection by letting the misuse exhibit behaviour which is infrequent or difficult to distinguish from normal usage behaviour.

An important assumption of the *trust model* that underlies authorization in the EPD, is that one can always address the responsible physician (overseer) when something goes wrong. However, the analysis in this paper shows that this assumption does not hold, because any overseer can be filled in in a HL7v3 message *without involving the physician.* It will be difficult to hold a physician accountable when the overseer field –which points to this physician as the party responsible for a given employee‘s actions– cannot be verified as being valid, and when the physician is not involved in constructing or validating the message or the underlying delegation relation.

The basic problem is that the 'chain of involvement' with a patient's treatment - or in other words, the chain of authorization from treating physician to delegated employee as shown in Fig. 3- is not clearly reflected in the authorization mechanisms.

Because of the inherent lack of verifyability of the basic relations that underly all authorization decisions in the EPD, the LSP loses out on the possibility to filter out confirmed (completely authorized) operations. This would allow auditing to focus attention on suspicious operations, rather than having to (also) distinguish potentially false delegation or patient treatment relation claims from legitimate ones, which is difficult or impossible.

Delegation relations should become explicit and verifiable not just for prevention, but also for auditability of the system. In other words, a care organisation has to *prove* to the LSP that a particular mandate is valid. The reason is simple: authorization should flow 'down' – from patients to physicians to employees. Allowing access to some record simply because an employee says (by means of a HL7v3 field) that he or she is mandated by a physician (who is automatically assumed by the LSP to have a treatment relation with the patient when he or she invokes an EPD operation), simply places too much trust in an employee who does not have a medical title, and who is not known to the system and who has no direct professional relationship with the patient.

5. INFORMED CONSENT

By the end of 2008, the Dutch Minister of Health issued a letter informing the general public about the introduction of the EPD. This letter -addressed to home addresses rather than individuals- included a form using which Dutch citizens could object *(opt-out)* to the use of the EPD for exchanging their health-related information. If citizens do not object, their consent for using the EPD to access and transports their health information is automatically assumed. At the time of writing, about half a million of the 16.5 million Dutch citizens opted out [20].

The 'informed consent' is a *general* consent: it is not possible to request or obtain consent for individual registrations of information in the EPD, but rather it is only possible to opt-out from using the EPD system as a whole or per care organization - with the possible addition of being able to opt-out per information category in the future.

The EPD's opt-out model explicitly allows for an interpretation of the lack of an opt-out as an *assumed consent.* This means that the physician, or even the local system used by the physician may interpret the lack of an opt-out for a patient as permission to register information in the LSP. Such registration may take place without the patient or even physician being aware of it.

As an example of how assumed consent may work in practice, the director of Nictiz has suggested that information may be extracted from local GP records automatically in some cases [21]. This implies that the EPD may become so well-integrated with local information systems, that physicians may barely notice when information is registered in the EPD in the future. This may make it hard to say no to registration of a (possibly automatically extracted) *professional summary* in the EPD in time in specific cases, for example when a GP consultation regarded a sexually transmittable disease or some psychological problem.

It has also been reported that batch jobs have been run to register medication information from hospital pharmacies in the LSP [22]. Medication information may be rather privacy sensitive, since it is often straightforward to derive a patient's medical condition from this information - think of for example antidepressants.

It is an open question whether an opt-out remains feasible in the future. The EPD may become so commonplace that an opt-out becomes impractical. Health professionals may come to depend on using the EPD for so many tasks (not just for storing patient records, but also for secure message transport, for example), that patients eventually may feel pressured to opt-in to the EPD for exchanging health related information. It may even become harder to get effective (efficient) treatment if one does not allow usage of the EPD for exchanging health related information, when the use of the EPD becomes pervasive in medical practice. In this case, the general nature of consent is a severe disadvantage for patient privacy.

6. POSSIBLE SOLUTIONS

This section briefly discusses some possible solutions to the problems outlined in this paper. Although these solutions may also have limitations, they preclude a number of significant threats which were described in this paper.

6.1 Technical Issues

Solving the technical problems is relatively straightforward. End-to-end authentication can be achieved by forwarding the signed tokens to the endpoints such that these endpoints can independently authenticate (and possibly authorize) incoming messages; embedding additional information regarding the requestor's original request in the authentication tokens can restrict the scope of attacks that involve tampering with a request. Also, including for example record names in the requests may enable the use of fine-grained policies on a per-record basis in the authorization profile. End-to-end encryption is a logical next step -based on end-to-end authentication- to prevent information leakage through compromised systems between requestor and the system where a patient record is stored.

The problem of storing historical (traffic, logging, reconstruction) information in the LSP can be solved by allowing complete, unconditional, and undelayed deletion of all information related to a specific patient record or treatment relation from the LSP, including logging information. A less rigorous approach would be to encrypt all historical traffic and VWI information using a key associated with the patient, possibly after a short period during which (traffic) analysis and auditing may still take place. Encryption could take place efficiently using a symmetric key that can be decrypted only by the patient. Such a solution could be securely manageable when patients have access to a patient identification smartcard similar to an UZI pass, or possibly a future electronic National Identity Card (eNIC) [23][5].

6.2 Delegation and Patient Treatment

A possible way to implement delegation confirmation, is to create a *delegation certificate* for each possible mandatee, which has to be shipped with each message and token and can be checked by the LSP. Delegation certificates can be signed by a physician, or by someone authorized for this task. Preparation of delegation certificates may be straightforwardly automated using the (existing) delegation tables, possibly using working schedules. Delegation certificates usage can be constrained, for example by making them valid only for a limited time interval or for a limited number of operations.

Although delegation certificates are not infallible – for example, the process of creating and signing delegation certificates may be manipulated, as well as delegation tables and schedules – but at least attacks are made more difficult

[5] Introducing a patient identification pass with cryptographic capabilities can additionally alleviate some risks related to patient access to the EPD through a patient portal. Here, a (centralized) attack is possible due to -again- a lack of end-to-end authentication of, in this case, patients [23].

and less powerful. An additional security measure is to constrain employee UZI passes such that they can only obtain records of an information category that matches the specialization of the physician(s) that the employee is working for - i.e., employee UZI passes could have a role encoded upon them, not just a name. Note that in cases where (timely) creation of a delegation certificate for a given employee is not possible, access should not be permitted. In this case, a health professional can always interact with the EPD in person without delegation.

In terms of enforcement, it is imperative that *only* physicians should be allowed to claim a treatment relation in the LSP – either explicitly or implicitly by invoking the first request to obtain a record of a patient or by registering a record in the LSP. These rights should not be delegatable. Only this way can physicians be held accountable for false patient treatment claims in all cases.

To facilitate auditing, patients could sign an explicit *treatment confirmation message*, which is verifiable by the LSP. Using treatment confirmation, it becomes visible which treatment relations are legitimate, allowing auditing to focus on unconfirmed cases. As a side-effect of explicit confirmation, (logging) information in the LSP related to confirmed treatments may be encrypted or removed after treatment confirmation, since transactions related to confirmed treatments are generally not suspect. If necessary, encrypted information can be decrypted when the patient cooperates.

Treatment relations may in certain cases be confirmed *eventually*, that is, after the fact. Eventual confirmation may be relevant for emergency information, but not for psychatric information, for example. For effective privacy protection, confirmation should generally be required *before* allowing access to patient records. In case of eventual confirmation, if some time after access to the EPD a patient has not confirmed the treatment relation, the system could send a letter to a patient requesting confirmation, or to the patient's family or to the hospital where an exception took place[6]. Such procedures ensure that (written or electronic) confirmation eventually takes place to facilitate auditing.

6.3 Explicit Consent

Avoiding registration of information in the EPD (LSP) is a simple and effective way for patients to ensure that information can never be leaked to unauthorized parties through the EPD without their knowledge. For patients, this gives improved certainty that no information can leak from the EPD, simply because it is never registered in the first place.

A solution is to provide a mechanism for *explicit consent* as part of the EPD. *Explicit consent* means that a physician has to ask a patient for permission to register any information in the EPD; this is a 'no unless' setting, in contrast to the current ('yes unless') assumed consent model.

A simple solution is to have patients define an optional *consent setting* in the LSP. The information system used by a physician can consult the LSP to check the patient's consent preference. If the patient has set an explicit consent option, a pop-up box may be presented to the physician indicating that the physician should ask the patient for consent every time the physician wants to register a new record with the EPD. The physician would then be legally obliged to ask the patient for consent. An alternative would be to register the information temporarily, but to only commit this registration after the patient agreed to it. This could be implemented through the patient portal.

A more practical approach may be to simply require care organizations (health professionals) to inform the patient of what will be registered in the LSP; a simple second TFT screen on the physician's desk (which is often already present) would suffice for this. When the patient has not set a consent preference, the patient would allow physicians (or systems) to register medical information at their discretion based on assumed consent, identical to the current situation.

Explicit consent may be particularly important in the future, when systems may register information almost invisibly based on assumed consent. One of the reasons that patient-doctor confidentiality is part of the Hippocratic oath, is that this ensures that patients are comfortable in sharing all information that may be relevant to his or her health or the health of others, also when this information may be of a sensitive nature. Such confidence in confidentiality may be eroded by technology which which may silently register information in an infrastructure which -essentially- is intended for sharing this information with others, and thus cannot ever protect privacy optimally.

An explicit consent mechanism allows patients that wish so, to control what information is stored in the EPD, while setting the preference to 'yes unless' makes the EPD system efficiently usable when the patient agrees - i.e., in case the patient leaves it up to the physician to decide which information is shared through the EPD infrastructure.

The gained transparency (and the resulting pressure on IT providers to provide transparency before registering information in the EPD - or in any large-scale system for that matter) is very important to ensure that patients and physicians remain aware of the transition point between the relatively trusted local environment and the potentially more risky external environment, which is in the end designed for sharing information with other health professionals.

7. RELATED WORK

Various approaches to build Electronic Healthcare Record (EHR) systems are taken around the world. This section higlights a few examples to exemplify the differences between some characteristic approaches; space precludes a full overview.

Google Health [24] and Microsoft HealthVault [25] are well-known examples of *personal health records*. The main difference between these approaches and approaches such as the EPD, is that here the patient is responsible for managing the content of the health records. This is not reconcilable with legal regulations which govern the way in which medical records must be maintained by physicians in many countries. Indeed, if patients were able to manipulate information written by physicians, this could give rise to major (medical) problems - or mistakes. For this reason, it seems unlikely that personal health records will easily replace the healthcare records used by physicians, where the physicians and/or care organizations are responsible for managing and maintaining the patient records – although they may be a useful addition to the health records kept by physicians.

In the U.K. NPfIT system [2], a curious situation is reported with regard to responsibility for managing healthcare records [26]: here, a wikipedia-style model of 'collective

[6] Currently, patients only get a letter for the *very first registration* of information in the EPD, to ensure that citizens are aware of the possibility of opting out of the EPD.

authorship' was planned for the Detailed Care Record, a record to which multiple care professionals can contribute. This project is in trouble, being late and over budget, and may be cancelled. However, there are already shared local records to which multiple clinicians and even social care staff contribute. A problem here is that no-one is actually responsible for maintaining the overall quality of the record. This will undoubtedly lead to problems when mistakes occur due to erroneous content stored in the system. The NPfIT also contains a basic Summary Care Record for unplanned care use; this accumulates data from GPs and elsewhere. It has been reported to contain a significant number of errors [27].

The U.K. system uses a 'consent to view' approach where data *is* collected by default, but made available to clinicians only if a treatment relation exists and the phycisian claims that the patient has consented. This model is similar to the Dutch EPD's consent model in that it ignores the fact that collected (registered) information is vulnerable in case of a succesful attack on the central infrastructure or other misuse - in contrast to a model where patients would have to consent *before* information is registered in the first place.

The German *gesundheitskarte* (health card) places a strong emphasis on privacy protection and prevention of misuse, by avoiding centralized storage of information as much as possible. Here, a certain amount of medical information can be stored on the smartcard, and remaining information may be stored centrally in an unreadable (encrypted) form, such that it is only readable to a physicians after the patient explicitly consented in the information being read (decrypted). Emergency information is readable without prior confirmation of the treatment relation by the patient, but requires access to the physical card. A related approach is a USB stick that contains public and protected health information[7].

It is interesting to consider the technical differences between the Dutch and the German system. Since in the german system, information is either stored in a central system or on the card of the patient, it is important to encrypt of information stored centrally to achieve effective protection. Since in the Dutch EPD system information (with the exception of references, authorization rules, and logging information) is not stored centrally, encryption of data is less relevant here. Still, the Dutch system also contains privacy-sensitive information centrally, of which encryption could be relevant in some cases (e.g., see Sections 3.2 and 6). Clearly, some concerns overlap, and there exist conceptual similarities between the approaches, even though the implementations differ widely.

8. DISCUSSION

This paper highlighted some design, deployment and organizational issues of the EPD which may have an impact on the security it provides. Effectively, we distinguish three overall problems in the current design:

- Technically: a lack of end-to-end authentication combined with incomplete and insufficient information embedded in tokens.

- Policy/organizatorial and implemention-wise: there exists no mechanism in the LSP for immediate confirmation of delegation relations and (eventual) confirmation of patient treatment relations.

- An inherent risk of information leakage: attacks on VWI and historical information stored in the LSP may allow attackers to obtain this information directly. In particular for historical information, this may be an important risk.

The basic technology which underlies this infrastructure seems solid enough: the system uses a proper PKI with smartcards for authentication of (registered) health professionals, it uses decentralized storage of patient records 'at the source' rather than a potentially more risky centralized approach, and it uses a central infrastructure to control access to those patient records, including access by patients[8].

However, in its details the current system's architecture falls short. A number of implementation aspects, such as a lack of end-to-end authentication (or encryption) of requests and embedding of insufficient information in the authentication tokens used in the system unnecessarily increase the potential impact of an attack. Furthermore, a large amount of privacy-senstive information is stored centrally in the system - including logging information, treatment relations, and rather detailed references to patient records - in contrast to the government's statements that the central system contains no medical information at all.

Of particular importance is that the authorization policies are not supported by sufficient (verifiable) confirmation of patient treatment and delegation relations that underlie authorization in the EPD. This makes validation of, in particular, delegation very difficult in practice. This issue undermines the effectiveness of the authorization policies embedded in the EPD, and limits auditability of the system.

Overall, the Dutch EPD appears biased towards (emergency) use-cases which require immediate, unhindered access to patient records as a default, whereas the mainstay of records in the system and privacy protection may benefit from a much more conservative approach where access is not permitted unless after explicit authorization by the patient. We believe that -within the current framework- more secure approaches are neccessary and possible for most if not all usage scenarios's. This can achieve much stronger protection of privacy-sensitive patient information than currently possible.

Finally, we believe that an (optional) explicit consent policy is important for patients who -for whatever reason- feel they need more transparency and control over what becomes registered in the EPD than is currently possible. An explicit consent option would allow patients to *prevent*, on a per-case basis, that particular medical information gets (automatically) registered in the EPD. This is important in future scenario's when an opt-out may no longer be practical, while at the same time the EPD becomes increasingly integrated with the information systems that physicians use.

[7] For example, `http://www.sosguard.com.au/`

[8] The Dutch government commits to providing patient access to the EPD in the proposed law governing the EPD. Although this helps to provide transparency, patient access to the EPD may also create a number of security and privacy issues: can information in the EPD actually be useful and comprehensible to patients and physicians at the same time? Can patients also add information to the EPD? And can we prevent that patients are coerced into providing access to their records through the patient portal - for example by angry husbands, law enforcement agencies, or health insurers?

The current debate

A technical report about this research was made public early 2010, after which the author took part in a discussion in the Senate [19]. The ministry's main response was that the assumption that the LSP or the decentral information systems could be hacked was invalid, since extensive (non-public) audits and hacker tests take place on a regular basis. We wrote a response indicating that hacker testing (penetration tests) and audits cannot replace a good systems design - nor guarantee prevention of attacks for that matter. Indeed, insider threats were already taken as a grounding point for an earlier critique on the NHS system in 1995-1997 [28]; unfortunately, the situation is not likely to have improved since [11, 29].

At the time of this writing, it is unclear if the law mandating the use of the EPD will be approved by the senate.

Acknowledgements

Thanks for Niels Sijm for taking the first steps into this research [30]. Thanks to the (anonymous) reviewers who took the time to read early drafts of this paper and provided valuable comments that improved the paper. Special thanks go to Marie-José Bonthuis and Matthijs Koot for reviewing very early drafts of this paper. Thanks to Nictiz for elaborating on some points of the EPD design which were unclear from reading the public documentation.

9. REFERENCES

[1] Nictiz. AORTA Documentation Release. *http://www.infoepd.nl/informatiepunt_com/ aorta-documentatierelease_2008_totaal.php*, October 2008.

[2] U.K. National Health Service (NHS). SPINE - NHS Connecting for Health. *http://www.connectingforhealth.nhs.uk/ systemsandservices/spine.*

[3] J.C.J. Dute et al. Rapport Evalutatie WGBo. 2003.

[4] Working Party Article 29. Working Document 131 regarding the processing of personal data relating to health in electronic health records (EHR). *http://ec.europa.eu/justice_home/fsj/ privacy/workinggroup/wpdocs/2007_en.htm*, February 2007.

[5] Marie-José Bonthuis. Privacy en het Landelijk Electronisch Patientendossier (EPD), Universiteit Groningen. 2007.

[6] Dutch ministry of health, welfare and sports (VWS). Wet op de Geneeskundige BehandelingsOvereenkomst (WGBO). *http://www.hulpgids.nl/wetten/wgbo.htm*, 1994.

[7] Sectorale Berichten Voorziening in de Zorg (SBV-Z). *http://www.sbv-z.nl/*, 2009.

[8] Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de electronische informatieuitwisseling in de zorg (31-466). *Eerste Kamer 31 466, A, SDU publishers*, 2008-2009.

[9] Nictiz. Programma van Eisen aan een GBZ (PvE GBZ). *http://www.aortarelease.nl/content/inf/ Programma_van_Eisen_GBZ.html*, 2007.

[10] Health Level 7 standards for interoperability of health information technology. *http://www.hl7.org/.*

[11] D. Cappelli, A. Moore, R. Trzeciak, T. Shimeall. Common Sense Guide to Prevention and Detection of Insider Threats, 3d edition - v3.1. *CERT Report, Carnegie-Mellon University*, January 2009.

[12] Ross Anderson. Security Engineering, 2nd edition. *Wiley*, 2008.

[13] Ken Thompson. Reflections on Trusting Trust (Turing award Lecture). *Communications of the ACM Vol.27(8)*, August 1984.

[14] Ministerie van VWS. Informatie en bezwaarschrift EPD. 2008.

[15] Nictiz. Personal communication. 2010.

[16] European Parliament and the Council. Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *http://ec.europa.eu/justice_home/fsj/ privacy/docs/ 95-46-ce/dir1995-46_part1_en.pdf*, October 1995.

[17] Nictiz. Memo behandelrelatie en additionele GBZ-eisen. april 2009.

[18] Minister A. Klink. Memorie van antwoord bij de Wijziging van de Wet gebruik burgerservicenummer in de zorg in verband met de electronische informatieuitwisseling in de zorg (31-466). *Eerste kamer der staten-Generaal*, September 2009.

[19] Stenographic report of the EPD Roundtable meeting in the Dutch Senate. *Eerste Kamer der Staten-Generaal*, March 2010.

[20] M. Katzenbauer. Te vroeg voor landelijk EPD. *medisch contact 64 nr.20*, pages 880–883, May 2009.

[21] Stenographic report of the EPD Expertmeeting in the Dutch Senate. *Eerste Kamer der Staten-Generaal*, December 2009.

[22] CSC - Internal protection of the Dutch LSP. *Talk at the Dutch Organization of Hospitals (NVZ)*, Dec. 2009.

[23] B. Jacobs, S. Nouwt, A. de Bruijn, O. Vermeulen, R. van der Knaap, C. de Bie. Beveiligingseisen ten aanzien van identificatie en authenticatie voor toegang zorgconsument tot het Electronisch Patientendossier (EPD). *Report by PriceWaterhouseCoopers, Radboud Universiteit Nijmegen, and Universiteit van Tilburg*, December 2008.

[24] Google Health. *https://www.google.com/health.*

[25] Microsoft Health Vault. *http://www.healthvault.com/.*

[26] R. Anderson, I. Brown, T. Dowty, P. Inglesant, W. Heath, A. Sasse. Database State. *Report commissioned by the J. Rowntree Reform Trust*, 2010.

[27] T. Greenhalgh, K. Stramer, T. Bratan, E. Byrne, J. Russell, S. Hinder, H. Potts. The devil's in the detail: Final report of the independent evaluation of the Summary Care Record and HealthSpace programmes. *University College London*, May 2010.

[28] R. Anderson. A Security Policy Model for Clinical Information Systems. *IEEE Symposium on Security and Privacy, Oakland*, 1996.

[29] Office of the Auditor General of British Columbia. The PARIS System for Community Care Services: Access and Security. *On: http://www.bcauditor.com/*, 2010.

[30] Niels Sijm. Onderzoeksrapport LSP. *https://www.os3.nl/_media/2007-2008/courses/rp2/ ns-report.pdf*, 2008.