2009-01-01

Identity Management to Support Access Control in E-Health Systems

Xu Chen
Dublin Institute of Technology, xu.chen@dit.ie

Damon Berry
Dublin Institute of Technology, damon.berry@dit.ie

William Grimson
Trinity College of Dublin, william.grimson@dit.ie

Identity Management to Support Access Control in E-Health Systems

Xu Chen, Damon Berry and William Grimson

School of Electrical Engineering Systems, Dublin Institute of Technology, Dublin, Ireland

Abstract— **The related and often challenging topics of identity management and access control form an essential foundation for e-health infrastructure. Several approaches and supporting specifications for electronic healthcare record system (EHR-S) communication have been proposed by research projects and standards development organizations in recent years. For instance, part four of the CEN TC251 EN13606 EHRcom standard and the HL7 Role Based Access Control Draft Standard for Trial Use have helped to specify the nature of access control behaviour in relation to EHR communication within and between healthcare organisations. Access control services are a core component not only of the integrated care EHR-S but also for other information systems in the e-health domain. To underpin functionality of this type in a distributed environment, it is necessary to provide access to scalable, secure and uniform ID domains for users and patients.**

This paper considers the use of part four of the EHRcom standard in the context of the availability (or lack thereof) of national identification systems for patients and for users of an integrated care EHR-S. This work begins with a brief summary of the state-of-the-art in identity management and access control in the health domain and a description of approaches that could lead to a secure and interoperable identification mechanism. To address the identification problem, the authors describe well known EHR access control viewpoints that are compatible with the CEN standard for EHR communication, EN13606 and describe how an identification service can support this functionality.

Keywords— **Electronic Healthcare record system, Identity management, ID domain, EHRcom standard, Access control**

I. Introduction

We live in a mobile civilization with free movement of citizens between cities and towns and across many national boundaries. Patients visit different public and private medical institutions to get treatment for different medical conditions, and are increasingly referred by primary physicians to various specialists in a process known as shared care. The modern day health process must cope with the effects of this mobility. Therefore a growing need for the sharing of health care information has arisen and it has become the part of health informatics strategy in many countries.

The paper is organized as follows. Section two introduces a state of the art on identity management and access control for health information and attempts to answer whether there is a strong need for national identification systems in order to support shared care on a regional or national scale. Section three discussed several popular access control "viewpoints" for access to health information. Section four gives a brief introduction to EHRcom - the European and ISO standard for EHR communications and also summarizes the security requirements associated with access to health information. Section five proposes the idea of integrated EHR system and interaction with large-scale regional national system.

II. Patient identification and identifiers

The effective exchange of health care information to support shared care depends upon rapid, usable and accurate electronic health-care record identification and this will not be implemented with efficiency unless there is a shared identification system.

A. National Identifier and Health Identifier Systems

With the evolution of the discipline of health informatics, there has been drive to leverage information technology to deliver high quality and cost effective health care, leading to increased productivity and enhanced patient safety [1]. In the meantime, the effective and efficient exchange of health-care information has also been proposed and requested from different geographical organisations such as hospital, general practitioner practice or physician.

However, the exchange of health information within and between health enterprises has long been problematic. Today in many countries, the absence of a national identifier has meant that healthcare organizations must develop their own identification systems and separate identification domains. Many of these systems use the same or similar trait attributes to help the identification process (e.g., patient name, date of birth) but the information may not be stored in identical formats at participating healthcare sites. In order to allow IDs from the numerous ID domains to be matched, in the worst case scenario the resulting mapping problem would need to be solved for every pair of sites, resulting in the classic n-squared/2 mapping problem.

This situation is simplified if each site could refer to a national identifier domain. By simplifying the process of

linking identifiers at different health sites, unique national identifiers facilitate the integration of health information. The resulting multi-site access to historical and other health information represents an important enhancement of healthcare quality and a major step towards a regional EHR system.

The adoption of a single standard identifier should also lead to more efficient processes and improved patient safety. If a unique identifier is independently introduced and is not just an extension of an existing number, it may avoid recognized problems from earlier identifier systems. For these reasons, it is important that the scope of intended use of the identifier is carefully considered.

Clearly, a unique national identifier would serve many purposes in e-health. In particular it is expected that a national health identifier would enhance the provision of quality health care services by facilitating the accurate and rapid identification and compilation of an individual's health records. An independently assigned identifier would require the creation of a new system for assigning and maintaining the numbers as well as separate technology infrastructure and administrative structures so the development and implementation would require a huge investment. Nevertheless, the positive attributes are still leading those of negative side on the basis of many countries' experience [2].

B. Existing identity management service specifications

It has been noted above that communication between health care information systems is the key to securing closer co-operation in a shared care setting, improving handling of patients in terms of quality and continuity of care and patient safety. To ensure that health care professionals have access to information about an individual patient by different privilege division of work, several standard specifications to support identity management have been developed over the last few years. A brief summary of some of the main innovations in identity management follows.

The *Person Identification Service* (PIDS) is a service specification that has been adopted by the Health Domain Taskforce of the Object Management Group (OMG) [22] for managing identities of persons within a particular domain. The PIDS standard includes an interface that supports the ability to connect multiple PIDS components/servers together in a federated manner. These PIDS components were designed and validated for interoperability with a variety of pre-existing person-model and record-format standards though healthcare. This was to ensure that the specification could permit most preexisting person identifier management systems and interfaces to participate as members of a complex integration environment.

Entity Identification Service (EIS) [23], under a joint agreement between HL7 and OMG, the Healthcare Services Specification Project (HSSP) has sought to provide to a mechanism to develop standard specifications to support the improved provision of health care. The Entity Identification Service (EIS) is one of the constituent services of the HSSP which provides a set of service interfaces to uniquely identify various kinds of entities (e.g. people: patients, providers etc., devices) within disparate systems within a single enterprise and/or across a set of collaborating health organizations.

The EIS specification could be seen as a superset of PIDS, and in the Authors' view it is moving in the right direction which is more powerful and flexible use of identification of abstracted entities rather than the single patients. However, EIS specification is still work in progress at time of writing.

Integrating the Health Enterprise (IHE) PIX/PDQ Profiles, Integrating the Healthcare Enterprise is aimed at stimulating integration of healthcare information resources and IHE technical framework. IHE have defined several profiles for interdepartmental communication [3].

Patient Identifier Cross-referencing (PIX) [24] provides cross-referencing of patient identifiers from multiple Patient Identifier Domains by supporting the transmission between an identity source to the PIX manager and correlating information about a single patient from sources that know the patient by different identifiers [4] has described the relationship between the interfaces specified in the IHE PIX profile and a implementation of a master patient index and how to link to identity domains.

Patient Demographics Query (PDQ) [24] supports the distributed applications to query a central patient information server and retrieve the patients' demographics information (such as when and how to search or visit the information).

NHS *Personal Demographics Service (PDS)* is part of the NHS Care Record Service which supports access control and identity management in the United Kingdom [5] [6]. The demographic information will be form part of each person's electronic NHS Care Record. The PDS is the national electronic demographic service and it allows a patient to be identified by NHS staff. The PDS it is hoped will provide secure, efficient and convenient access to demographic information for 50 million patients in UK [25] within the NHS Connecting for Health Initiative which in turn is part of the National Programme for IT [26].

In many cases, patients' demographic and identity information is stored local databases from where it can only be accessed within the same organization or geographical

area. This can result in delays in identifying a patient, accessing their correct medical information or even in providing treatment. Becker has noted that the specification and development of the NHS SPINE and the Personal Demographics Service [25], is quite open leaving room for differing and therefore possibly conflicting interpretations [7].

C. Identifying the health professional health organization and other actors in the care process

The primary identity in the health care process is the subject of care. However, identification and identifiers are also needed to categorize and uniquely identify a long list of other roles in the health process including EHR authorship committal and attestation, responsible health professionals, the associated health care organizations and health care units, diagnostic devices and pharmaceutical products. All of these entities play a part in establishing an EHR system in which the main protagonists are "clearly visible". It is likely that EIS will support identification of these parties at the service level while ISO OIDs [8] can be utilized with the appropriate standardization of domains, to provide hierarchical identification for health organizations and units as well as information sources and devices.

III. MULTIPLE VIEWS ON ACCESS CONTROL

Access to a paper chart is obviously constrained to those individuals who can because of their roles, pick up the chart. Access is limited by the nature of the medium. The electronic health record is intended to be shared widely to the right persons but unless care is taken, access could be much wider. Of course the record needs to be accessed in order for health professionals to do their job, but there are sensitivities which need to be considered. Whiddett, R [9] investigated the attitudes of patients to disclosure of health information and found that patient's responses varied. As one would expect, respondents were more accepting of sharing of less sensitive data and anonymised data with only 6% of respondents permitting sharing of sensitive data with other government departments, while 70% agreed to share sensitive health information with doctor or nurse. The study identified general denial with specific consent [10] as an appropriate access control approach to answer the concerns of respondents.

Two basic mechanisms underpin access to an electronic health record. *Authentication* the "*...process of reliably identifying security subjects by securely associating an identifier and its authenticator...*" [11] *Authorization* the process of granting rights for access to information resources [12].

Blobel [13] has described an interesting series of model viewpoints which can be used when considering access to health information from different perspectives. These model viewpoints are summarized below.

The *domain viewpoint* allows information resources to be grouped into communication *domains* that share an agreed security policy. Domains can be aggregated into super-domains or broken into sub-domains.

The *policy viewpoint* facilitates a range of different policy types. For instance authorization policies contain sets of permitted actions; event-based obligation policies define actions which must be performed when certain conditions are met; refrain policies declare actions the subjects must not perform; delegation policies define which authorizations can be delegated and to whom.

The *role viewpoint* allows privileges to be indirectly assigned to users as individuals are given roles and roles are associated with a set of privileges. This separation allows privileges associated with a role to be updated without needing to modify the role membership.

The *document viewpoint*, Processes, entity roles, etc. must be documented and signed expressing the particular relations between entities and processes. The combination of processes and relations leads to multiple signatures (e.g. in the case of delegation) [13].

The *privilege management viewpoint* is used by ISO PMAC specification and it allows the system authority to assign the privilege to individual actors or to groups of individual actors which can be a human user, a system or application etc., and playing the closed role to role viewpoint [14].

The *authorization viewpoint*, used by OMG RAD specification and authorization logic is encapsulated within an authorization facility that is external to the application. In order to perform an application-level access control to clinical object, an application requests an authorization decision from such a facility and enforces that decision [27].

The *control viewpoint*, illustrates how control is exerted over access to a sensitive object operation [15].

The *delegation viewpoint*, a source authority can delegate to certain delegation administrators the privileges to create and manage the identity management for an authorization entity [12].

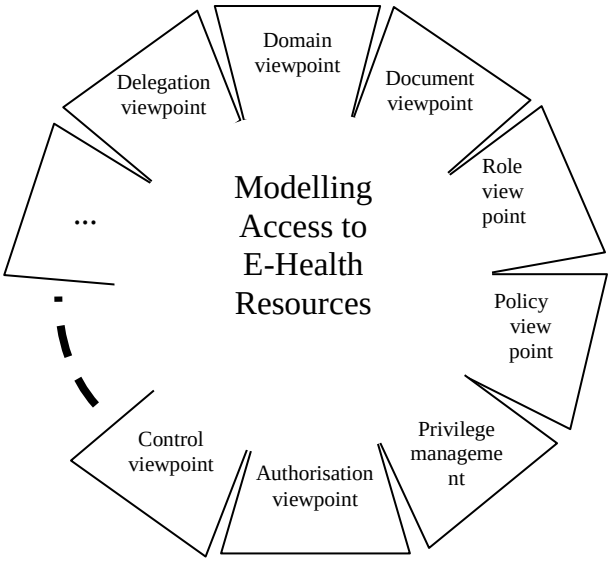

Fig. 1 Different model viewpoints on access control [14][15]

Three principal variations on the access control model have been widely used commercially: the discretionary access control (DAC) in which access is determined by the system rather than the owner and is the basis for access control on UNIX and Linux, mandatory access control (MAC) which is often employed within database management systems, and role-based access control (RBAC) [13]. RBAC is probably the most popular access control scheme in use today and controls collections of permissions relating to everything from complex operations such as an e-commerce transaction, to simple as read and write operations.

RBAC separates the user from specific authorization, in the design of RBAC, the user must have the authority to adopt specific roles to be set, so different abstract descriptions of the licensing authority can be made to easily specify a different role in the collection for each user and give users different levels of the most detailed collection of authority. In addition, it reduces the amount of administrative work needed to add or delete users.

Despite being the most popular access control scheme RBAC alone is probably not sufficient for providing a comprehensive and satisfactory access control solution for a working shared electronic health record. For example as Becker [7] points out, the security and confidentiality requirements as described in the NPfIT output-based specification OBS and subsequent documentation *"are highly challenging and beyond the capabilities of current access control technologies including role-based access control (RBAC)."*

Other access control schemes have been described for the health domain. *Identity based access control* (IBAC) Gaute M. [16] also means that, regardless of where or when an individual appears on the network, policy appropriate for that individual can be enforced. In addition, policy based on the individual means that non-trusted users can be prevented from accessing the network even though they connect through a seemingly legitimate connection point. Identity-based access control makes it possible for mobile users to roam throughout the network, and yet continue to have the appropriate access to the resources based on business need. *Process Based Access Control* (PBAC) [13] is an authorization system where each (web) service publishes a list of operations that it can perform and PBAC determines which operations can be called by each user in different contexts.

The *information distance model* applies increased restrictions depending on the "information distance" between the information and an actor who seeks to interact with it. The originator (subject of care) is "closest" followed by the producer (author/interpreter) of the information next comes the administrator (user) of information.

Lovis et. Al [17] described zones of medical responsibility and physical location to indicate medical responsibility and therapeutic relationships which can supplement more general role assignment so that the EHR of subjects of care who enter the care flow of a particular heath unit can be accessed by HCPs with appropriate roles within that health care unit.

Distribution rules define the behavior of an access control component, and the attributes of an access control policy can be categorized into who, when, where, why and how. Sucurovic [18] indicated that for the purposes of calculating access control decisions the attributes governing access across these categories can be processed using logical AND operations, while attributes within a single category can be processed using logical OR operations.

The progress towards the electronic health record has led to a significant "fading of boundaries" between health information systems [19]. Among the basic functionality requited to support this trend, it is necessary to provide integrated identity management and access control facilities.

IV. Identity and Access Control Features of an EHR System

A number of EHR research projects have developed sets of requirements electronic health record architectures. These requirements have been refined into the ISO technical specification 18308 Requirements for an electronic health record architecture [20] which is being revised at time of writing. The ISO work has suggested that apart from the

management of clinical information, an EHR system must provide integrated support for recording the main identifying traits for the subject of care. It should also provide support for unique identification of authors and other users of the EHR as well as supporting informed consent and audit trails and not least various forms of access control.

A. CEN TC251 prEN13606 EHRcom

One recent piece of standardization by the "EHRcom" project team of CEN Technical Committee 251 has sought to fulfill the ISO requirements. This standard is called prEN13606 - "EHRcom". This is a five part standard which defines and describes various critical aspects of the exchange of electronic healthcare records. EHRcom consist of five parts:

1. The reference model
2. Archetype interchange specification
3. Reference archetypes and term lists
4. Security requirement and distribution rules
5. Exchange model

The prEN13606 EHR standard is intended to support sharing of health records on a regional or national scale ultimately leading to a shared national EHR system. EHRcom supports the two-level modeling approach which is intended to make health information systems more adaptable and more under the control of domain experts through the use of archetypes.

The five parts of EHRcom are mostly complete at time of writing and are at various stages of the CEN-ISO standardization process and will incorporate a representation of EHR access policies which are dealt with in part 4 of the standard which also deals with EHRcom defines a representation for EHR access policies which were introduced in part 4. A large number of EHR-specific medico-legal and ethical requirements are also expressed within ISO TS 18308. The following are those security requirements that apply most specifically to part 4 of the standard [21]. An electronic health record architecture such as EHRcom should support,

- citizens' right of access to EHRs
- citizens' ability to incorporate and record information in EHRs
- an audit trail of exchange processes,
- the labeling of the whole and/or sections of EHRs
- privacy and confidentiality restrictions
- retrieval, recording and tracking the status of access
- recording all consent with the associated time frames
- measure to define, attach, modify and remove of access rights for whole EHR section
- measures to enable and restrict access to whole EHR section with access rules
- measures to separately control authorities to add/modify the EHRs from the control of authorities to access the EHR
- recording of an audit trail of access to and modifications of EHR access privilege
- recording the access and/or modification of EHRs
- storage and retrieval of whole EHR information, the minimum requirement is to allow for the recording of the data on disclosures and consent

V. A DESCRIPTION OF THE PROPOSED SYSTEM

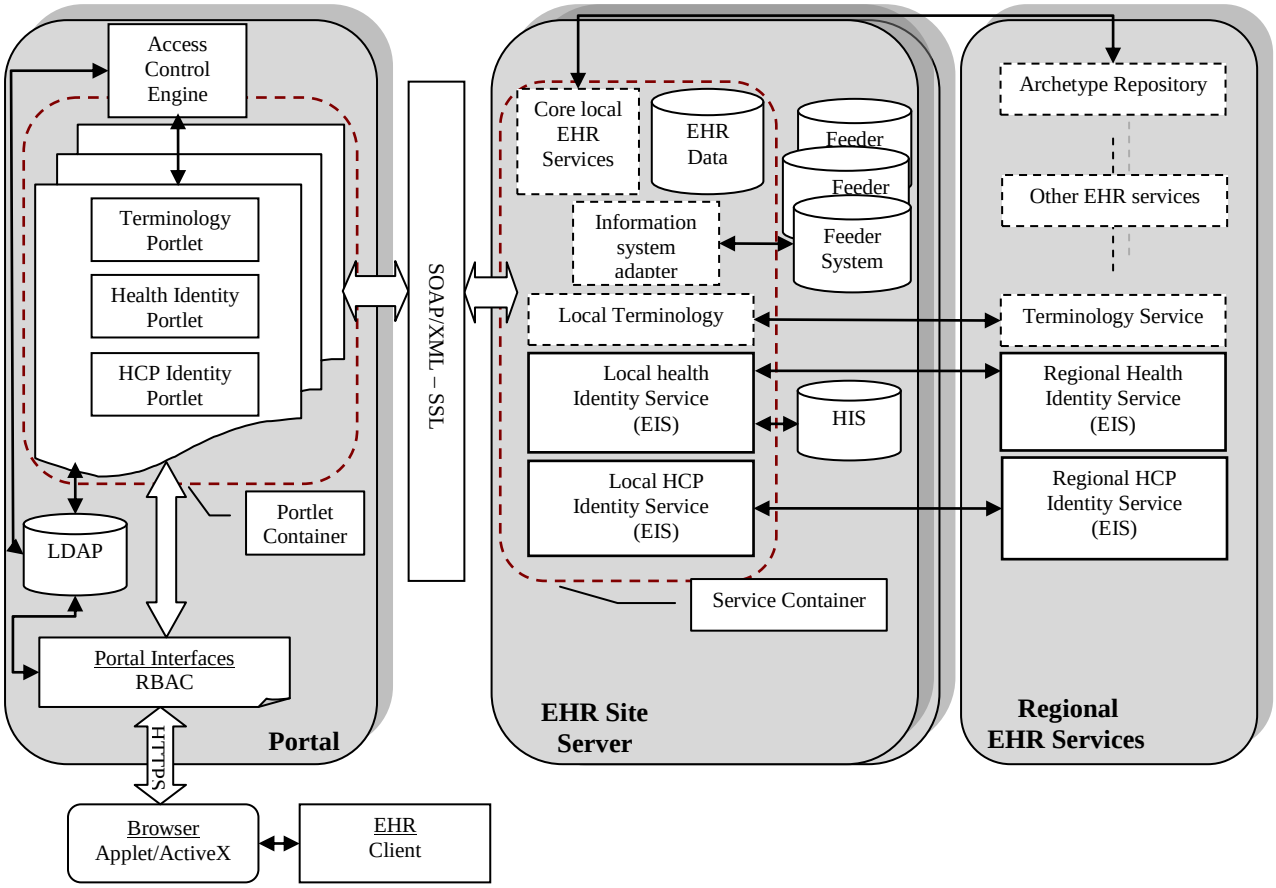

Fig. 2 The proposed system

A shared EHR system requires supporting components at both a national level at each EHR "site". In the proposed system, regional EHR-S services while supporting archetype repositories and terminology services would provide access to registers of identities for patients (Regional Health Identity Service) and health professionals (Regional HCP Identity service) Each EHR-S site would have access to these regional resources. In addition to the clinical information services at each EHR-S site local identity services would support the mapping of the local patient and health care provider identities to the regional equivalents.

The portal of proposed system, is a web-based application that integrates various services (such as terminology service and health identity service as shown in Figure 2) provided by multiple hospitals and other medical organizations. The feature of web service based services is that these services exposes their interfaces as web services and the portlet communicates with the backend service via SOAP which enables the interoperability. An end user, such as a patient or doctor, uses a web browser to the portal server. The portal server displays a webpage, namely, portal interface to the user. The portlets inside each portal interface correspond to a collection of correlated services provided by medical organizations (such as national HCP identity service corresponding to HCP registration portlet).

The system will provide a uniform and easy-to-use interface to users by hiding implementation details of services and their providers. It also enables remote services which will be instantiated to the correspond portlet. These portlets will be definitely under control of security mechanisms and these access control policies will be produced by an access control engine which gathers certain policy data from the LDAP server.

The portlet container provides a runtime environment for portlets to be instantiated, used and finally destroyed. The separation of portal interfaces from portlets allows portal administrators to easily customize the source of services using a content management system.

VI. Conclusions

There is no doubt that the provision of secure widely-shared patient records which can nevertheless only be appropriately accessed by the right health professionals at the right time is a complex goal which requires complex solutions. One solution could be considered as a composite of identity management and access control to support record communication using prEN13606 EHRcom.

In addition to a problems associated with the integration of legacy systems including the harmonization of access control approaches and linking of identity domains to support interoperability between clinical information systems there are numerous access control issues which general solutions have yet to be found including identification of medical devices and pharmaceutical products, health organizations or units. The system proposed in this paper attempts to provide a general architecture for identity management and access control to support national-level EHR-S corresponding to the back-end regional EHR service.

Although the prEN13606 EHRcom are still being developed by the health informatics community, the authors will explore further and implement the prototype system based on identity management and access control to facilitate the procedures of national EHR-S development.

Acknowledgment

This material forms part of the work of the EHRland project and is supported by interim Health Information and Quality Authority of Ireland (iHIQA).

References

1. William A. Yasnoff, Patrick W. O'Carroll, Denise Koo, Robert W. Linkins, and Edwin M. Kilbourne (2000) Public Health Informatics: Improving and Transforming Public Health in the Information Age, journal of public health management and practice
2. Graham I (1994) informatics enhancing health, Health Informatics Society of Australia, Melbourne Hannan T 1991 Medical informatics - an Australian perspective. Australian and New Zealand Journal of Medicine 21:363-378
3. ACC (2005) HIMSS and RSNA Integrating the Healthcare Enterprise IHE IT Infrastructure Planning Roadmap
4. Baksi D. (2008) Integrating MPI and reduplication engines: A software architecture roadmap international journal of medical informatics Awaiting Publication
5. Integrated Care Records Service Part I – NATIONAL SERVICES Output Based Specification version 2 NPfIT (2006) at www.dh.gov.uk/en
6. Integrated Care Records Service Part II - LSP SERVICES Output Based Specification Second Iteration NPfIT (2006) at www.dh.gov.uk/en
7. Becker M (2007) Information governance in NHS's NPfIT: A case for policy specification. International Journal of Medical Informatics , Volume 76 , Issue 5 - 6 , Pages 432 – 437
8. Werner Ceusters and Barry Smith (2006) Strategies for referent tracking in electronic health records, Journal of Biomedical Informatics Volume 39, Issue 3
9. Whiddett, R, Hunter I, Engelbrecht, J., Handy, J (2006) Patients' attitudes towards sharing their health information, International Journal of Medical Informatics 75, 530—541
10. Coiera, E. Clarke, R. (2004) e-Consent: the design and implementation of consumer consent mechanisms in an electronic environment, J. Am. Med. Inf. Assoc. 11 (4) 129—140.tation of consumer consent mechanisms in an electronic
11. ISO (1989) ISO 7498-2: Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture
12. ISO (2006) Health informatics -- Privilege management and access control -- Part 1: Overview and policy management, ISO/TS 22600-1:2006
13. Blobel B. (2004) Authorization and access control for electronic health record systems International Journal of Medical Informatics 73, 251—257
14. Bernd Blobel, Ragnar Nordbergb, John Mike Davisc, Peter Pharowa (2006) Modeling privilege management and access control, International Journal of Medical Informatics 75, 597—623
15. Bernd Blobel, Ragnar Nordberg (2003), Health informatics - Privilege management and access control - Part 3: Access control management
16. Gaute Magnussen, Stig Stavik (2006) Access Control in Heterogeneous Health Care Systems - A comparison of Role Based Access Control Versus Decision Based Access Control
17. Lovis, C. Spahni, S. Cassoni, N. Geissbuhler, A. (2007) Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks international journal of medical informatics 76 466–470
18. Sucurovic S. (2007) Implementing security in a distributed web-based EHCR international journal of medical informatics 76 491–496
19. Hammond W.E (2003) Making the boundaries clearer: revisiting information systems with fading boundaries International Journal of Medical Informatics 26 99-104
20. ISO/TS 18308 (2004) Health Informatics – Requirements for an Electronic Health Record Architecture
21. CEN (2004) prEN 13606 part 4, Health informatics-Electronic health record communication, European Committee for Standardization, Brussels, Belgium
22. OMG Person Identification Service Specification v1.1 at www.omg.org
23. OMG Entity Identification Service Specification v0.5 at hssp-rlus-rfpsubmission.wikispaces.com
24. PIX and PDQ at www.interoperabilityshowcase.org
25. Personal Demographics Service (PDS) A guide for general practice, at www.nhscarerecords.nhs.uk
26. National Programme for IT at www.connectingforhealth.nhs.uk/itprogrammes
27. Resource Access Decision specification, at www.omg.org/cgi-bin/doc?formal/2001-04-01d