International Journal of Medical Informatics (2004) **73**, 291—295

ELSEVIER

International Journal of Medical Informatics

www.intl.elsevierhealth.com/journals/ijmi

A cross-platform model for secure Electronic Health Record communication

Pekka Ruotsalainen

National Research and Development Centre for Welfare and Health (Stakes), Centre of Excellence for ICT, Helsinki, Finland

KEYWORDS
Secure platform;
Security infrastructure;
Security domains;
Grid security;
Secure communication;
Distributed information system;
Health information systems

Summary During the past decade, there have been many regional, national and European projects focused on the development of platforms for secure access and sharing of distributed patient information. A platform is needed because present local or enterprise-wide information systems are typically not intended for cross-organisational secure access of patient data. Most of the present secure platforms are local or regional. Commonly used platform types in the health care environment vary from secure point-to-point communication systems to internet-based portals. This paper defines an enhanced cross-security platform which makes it possible for different kinds of local, regional, and national health information systems to communicate in a secure way. The proposed evolutionary way interconnects regional or national security domains with the help of a cross-platform zone. A more revolutionary model based on peer-to-peer Grid like networks and dynamic security credentials is also discussed. The proposed evolutionary model uses cross-domain security and interoperability services to ensure secure communication and interoperability between different security domains. The platform supports both communication defined beforehand and adhoc dynamic access to distributed electronic health records (EHRs). The internet is proposed as the ''glue'' between different regional or national security domains.

1. Introduction

E-health and telemedicine services are promising business areas in Europe. It is clear that e-health products and services will be sold and ordered from a distance and over national borders in the future. Typical cross-organisational e-health applications are:

- sharing of patient records among different healthcare professionals;
- access to distributed EHRs any place and any time;
- on-line teleconsultation, telemonitoring and assistance;
- patient—doctor consultation services;
- patients' access to their own EHRs.

Health professionals are also anticipating that e-health systems will support new ways of working (e.g. shared care, work-flow management).

The types of present health information systems vary from distributed to centralised systems. Most of the distributed systems are based on the messaging approach, Grid-like linking directory approach or are portals with clearinghouse functions [1,2]. Centralised systems typically have one centralised patient repository. This repository can be also a portable personal health record [2]. A mechanism is needed for building trust and ensuring communication between different health information systems.

E-health and telemedicine applications and services require not only cross-organisational but also trans-border data flow. At present, a few enterprise-wide information systems have security

1386-5056/$ — see front matter
doi:10.1016/j.ijmedinf.2003.12.012

services aimed at cross-organisational communication. In many cases, policy on trust, privacy and confidentiality is not harmonised even at national level. Hence, to make it possible to develop plug-and-play e-health services, a secure cross-platform is needed.

2. Definitions

Security means that personal information can be communicated or stored in such a manner that access is limited to authorised parties. The *security framework* gives general rules and limitations for the processing of confidential health data [3]. The *security infrastructure* defines components that support users or applications to exchange sensitive information in a secure way. A PKI infrastructure is a typical secure infrastructure [2]. *Security platform* means a platform where different health applications can run securely and exchange data and money privately. *Security services* are the services provided by a system for implementing the security policy of an organisation. They can be classified into basic, infrastructural and value-added security services [4].

Every security platform can include one or more security domains [3,4]. Inside a domain there are common security schemes and common security services. The most common security domain (a basic domain) is a health care unit or enterprise. When two or more security domains share information, additional infrastructural security services are needed. Cross-border communication forms the widest security domain. It makes it possible to share sensitive information across borders in a trusted way.

For interoperability, both semantic and technical interoperability are needed. Elements of semantic interoperability are language, terminology and clinical coding, information structures, clinical protocols, and processes. With regard to interoperability levels of interoperability domains can also be distinguished. The basic domain exists at local or regional level. The most demanding level is the cross-border interoperability domain.

3. Barriers for cross-organisational communication

There are many barriers for secure cross-organisational communication [5]. The goal of a secure cross-organisational platform is to make communication possible between different platforms and across borders in spite of those barriers. The major security barriers are the lack of

- a harmonised legal and ethical framework;
- a harmonised policy on trust, privacy and confidentiality;
- security services for trans-border communication;
- common security standards.

Those barriers exist both between regions and between countries in Europe.

4. Current situation of secure platforms in Europe

Most health platforms in Europe are used for the integration of distributed health information systems. They are typically regional, although some national solutions also exist. Among the EU countries, UK, France, Germany, The Netherlands, Finland, Denmark, Slovenia and the Czech Republic use or are planning to implement national secure infrastructures and platforms [2].

In Europe, health platforms typically consist of one security and interoperability domain, but there are also some regional and cross-regional platforms [1,2]. They are based on closed networks and they offer limited security service (e.g. NHS Net, MedCom, Sjunet and HealthNet in Iceland). Many countries are also investigating PKI services, but no large scale solutions exist in health care yet. Lately, even in the case of a closed network, Internet access has been added. As an example, the French RSS-net provides Internet access and the Danish MedCom system is moving towards VPN networks and to the Internet-like platform [6].

The general trend is the use of Internet-like technology and portals as ''glue'' between different regional platforms or enterprise-wide domains and the utilisation of web browsers as middleware [7–9]. For example, many of projects in the 5th EU Framework are using the Internet as middleware. The RESHEN project uses PKI-services at the regional level and has plans for cross-regional certification services. It also uses a web-client for communication [9]. The PICNIC-platform uses inter-enterprise common services to enable interoperability between regional and enterprise-wide applications. The HARP security platform is another model in the trial phase [4]. Its Internet-based security system is composed of a secure client environment, a policy server, an attribute certificate server, and a database server storing all medical data. Commercial web-based personal electronic record

solutions are already available or under development [10].

5. Security requirements of an interoperable cross-platform model

It is rather unlikely or legally impossible for users from different organisations to know or trust each other. Hence, we need both a mechanism to build trust between partners (organisations, persons and entities) and to fulfil security requirements. Because a platform typically integrates two or more security domains having different internal security schemes, it has to offer common security bridging services for connected domains. The platform must also support both data transfer (e.g. messaging) and the data access modes of communication. In both models, the data controller inside a security domain has the responsibility to check that all necessary conditions for data transfer or access are met. The platform can simply ''open a point-to-point secure channel'' between the data controller and the data processor or it can interconnect security domains and certify that they have the same level of security policy.

Generally, the secure cross-platform has to support:

- security policy bridging between security domains;
- (static)certificates for access on a pre-request basis;
- digital credentials with privilege attributes for dynamic access;
- both centralised and distributed managed security;
- both brokered and pure peer-to-peer communication;
- both data transfer and data access communication models;
- cross-platform identification;
- both internet access and access from the terminals of any legacy system;
- different EHR realisations (including personal records on the Internet);
- migration to pure Internet-based EHR solutions;
- cross-platform language interpretation;
- terminology and clinical coding mapping;
- mapping of different information structures.

From a practical and economic perspective the cross-platform model has to use existing commercial security solutions and services where available. The platform also has to be defined in such a way that minimum changes are needed for present regional or enterprise-wide health information systems.

6. A proposed model for cross-platform security

Some ongoing European projects have proposed candidate solutions for secure inter-organisational communication and information sharing. One of the most interesting is the HARP model. Its original platform has been upgraded to a middleware-like common secure cross-platform [4]. For cross-platform communication, the HARP project has defined an enhanced Trusted Third Party (TTP) server with security policy mapping features. For internet access, the HARP model proposes that the user security profile, which determines all access rights in the client terminal, could be dynamically downloaded to the client.

The E-Europe Trailblazer 11 group has proposed a cross-platform integration model using secure communication via the Internet and the utilisation of a smart card for security. The MEDITRAV EU-project has defined a multilingual portable personal health record [2] for cross-border communication.

All of the aforementioned candidate solutions have restrictions for secure and interoperable cross-platform communication. We are proposing two possible ways forward: an evolutionary and a revolutionary roads. In the evolutionary model we first have to integrate enterprise-wide and regional platforms and form a national secure and interoperable platform. After this stage we can integrate different national platforms with the help of cross-platform security and interoperability services. The revolutionary platform is a Grid-like peer network that dynamically connects national security domains. Security is archived through the use of digital credentials, with expanded attributes for dynamic access and privilege management control [11].

The evolutionary model seems to be the most practical cross-platform integration method [2,11]. Fig. 1 shows the architecture of the evolutionary cross platform model. The platform integrates regional and national security domains with the help of an inter-domain zone. This zone offers common security and interoperability services for all connected domains. The main task of the platform is to offer centrally managed security services for cross-organisational pre-defined communication.

Basic security services of the cross-platform domain are security policy bridging, cross-domain

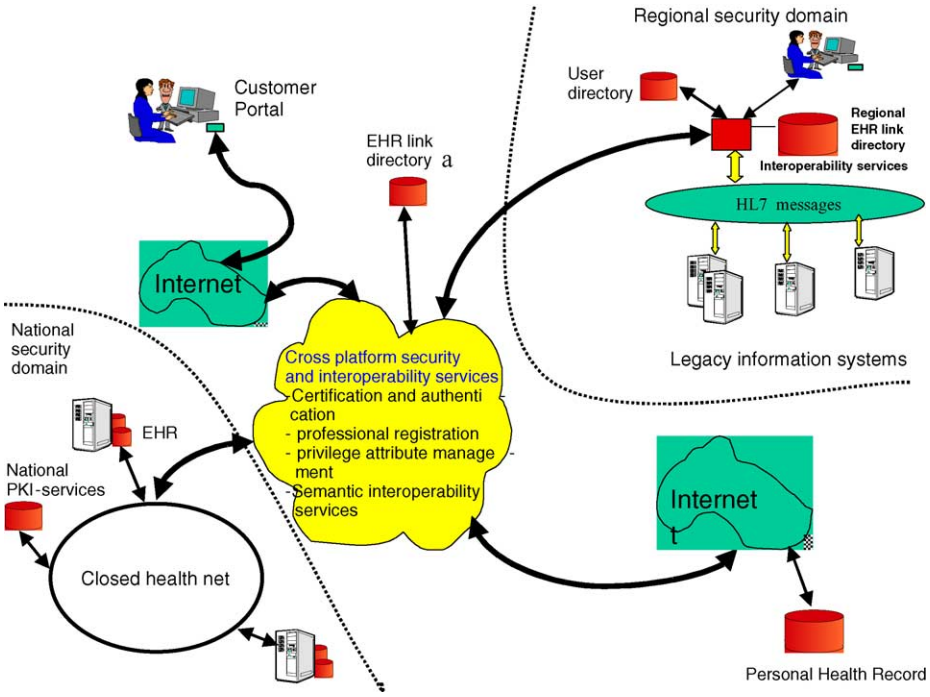

Fig. 1 A secure cross-platform model with interoperability services.

identification and authentication, certification services, static privilege management and auditing services. The platform can use existing PKI-services for authentication where available. To make it possible for external (dynamic) users to access any of the EHRs inside connected domains, the platform can offer automatic security negotiation services.

The interoperability services of the proposed platform consist of semantic services and EHR linking services. To make it possible to use local languages in communication, language clearinghouse services are included. Other interoperability services of the cross-platform are terminology, coding, protocol, and information structure mapping services.

7. Conclusion

To reach European interoperability and ensure secure communication between distributed health care domains, the most practical method is the proposed evolutionary model. First step is to build a national security domain. At the next phase, those national secure and interoperable domains can be linked together with the help of an Internet portal-like common zone. The major benefits of this kind of model are that it requires minimal changes to present legacy systems, it integrates present regional and national networks, and acts as a migration path to future, purely Internet-based health information systems.

References

[1] P. Ruotsalainen, A Secure and Confidential PKI Architecture for Networked Personal Health Records, in: Proceedings of the e-Health Europe 2001 Conference, Maastricht, The Netherlands, 8—10 April 2001.
[2] P. Ruotsalainen, H. Pohjonen, European Ssecurity Frameworks for Health Care, Advanced Health Telematicss and Medicine, the Magdeburg Expert Summit Textbook, IOS Press, 2003.
[3] S. Katsikasaans, S. Kokolakis, High Level Security Policies for Health Care Information Systems, Advanced Health Telematicss and Medicine, the Magdeburg Expert Summit Textbook, IOS Press, 2003.
[4] B. Blobel, Analysis, Designs and Implementation of Secure and Interoperable Distributed Health Information Systems, Studies in Health Technology and Informatics, vol. 89, IOS Press, 2002.
[5] R. Rogers, J. Reardon, Barriers to a Global Information Society for Health Recommendations for International Action, Studies in Health Technology and Informatics, vol. 63, IOS Press, 1999.
[6] PICNIC Professionals and Citizens Network for Integrated Care, http://www.medcom.dk/picnic.
[7] P. Hopner, JAVA-based open platform for distributed health telematics applications, in: International Collaboration to Provide Solution for Advance and Secure Interoperability of Health Information Systems, Magdeburg, 4—6 December 2002.
[8] C. Safran, H. Goldberg, Electronic patient records and the impact of the internet, Int. J. Med. Inform. 60 (2000) 77—83.

[9] A. Georgoulas, RESHEN: the best pracitice approach for secure regional healthcare networks in Europe, in: International Collaboration to Provide Solution for Advance and Secure Interoperability of Health Information Systems, Magdeburg, 4—6 December 2002.

[10] Personal Online Web Electronic Record (POWER), http://www.ascirbe.com,.

[11] MEDITRAV Assessment WP Deliverable 2, Vision and Roadmap towards a Secure and Interoperable European e-Health Platform, October 2003.