A Generic Secure Internet-Based Facility to Support Multiple Registries using Modern Encryption Technology and Client Certificates

WRM Dassen, ED Gommer[1], CCW Bonnemayer, HJ Spruijt[1], WA Dijk[1], MH Baljon[1]

Maastricht University, Dept. of Cardiology, Maastricht, the Netherlands, [1] Interuniversity Cardiology Institute of the Netherlands, Utrecht, the Netherlands

Abstract

For the management of their disease chronic patients are alternately dependent on the care of the general practitioner, (specialized) nurses or the specialist. For optimally coordinated communication there is a strong need for one single patient record containing all necessary medical information in order to get a complete overview of the condition of the patient for all healthcare providers.

In this feasibility study we demonstrated that using current methods for data security and encryption over the Internet an electronic patient record could be employed to be used by only those care providers that have legitimate access to the data.

The data security and encryption technology can also be used to employ various other registries not necessary requiring the same level of security.

1. Introduction

Tuning of a given treatment for chronic patients involves more and more the close cooperation between various care providers. Depending on the condition of the patient he is investigated / treated by the general practitioner, a specialist or (specialized) nurse. To optimize the tuning of information transfer between these care providers there is a need for a shared patient record in which the information from the different patient contacts can be stored. Sharing this data via the Internet seems to be a straightforward approach because it is widely available and easy accessible. However, one has to take good care of protecting the privacy and integrity of the information. After all it concerns medical data and (deliberate) changes in the data can lead to incorrect diagnosis and/or treatment of the patient. Transferring medical data over the Internet requires consideration of the following aspects. One has to be sure about the authenticity of the information provider and the information retriever/sender, about the integrity of the data and about the authorization of the information retriever/sender. Measures have to be taken to prevent unauthorized persons from intercepting the data.

The MAastricht Heart failure Study (MAHS) is an example of a project where such a shared patient record proved to be very helpful. The aim of this project was to improve the care for heart failure patients by improving the coordination between cardiologists, general practitioners and specialized heart failure nurses. The importance of sharing the patient record data in a fast and unambiguous way is eminent. An easy electronic facility is not (yet) available.

In a pilot project it was shown that using the current techniques for data encryption and server security, the Internet could be the suitable medium to transfer this patient data. The project assessed the facilities that have to be arranged to secure the data and its transfer.

2. Security structure

Many documents have been produced on the protection of data. Firstly there are a number of European and Dutch guidelines and pre-standards like SEISMED [1], NEN-ISO/IEC 10181 [2], NVN-ENV 12924 [3] and NVN-ENV 13608 [4]. These guidelines indicate the boundary conditions for the national laws. In the Netherlands at least two laws are of importance within the framework of privacy protection and data security. These are the *law on protection of personal data* and the *law on the medical treatment agreement*. These laws arrange among other things the rights of the patient concerning his personal medical record of which he is legally the owner. The patient has the right to browse through his medical data and his consent is required for collecting data not directly necessary for his diagnosis/treatment; e.g. clinical data gathered for research.

In line with the national laws the medical center, responsible for the organization of such a database, together with those participating healthcare professionals that will store their patient data in such a system, have to write down a policy on how to implement the national laws in the daily practice. This policy has to state which information is accessible to whom and how it has to be secured for illegitimate access. In the Maastricht University Hospital such a policy exists and it was applied for this project.

0276−6547/02 $17.00 © 2002 IEEE

3. Security implementation

After it is clearly defined who may view, modify, and/or delete which data, this needs to be technically implemented. The implementation needs to be done in a way that the user is aware of the fact that access restrictions are set (according to his personal profile) but without the need for him to perform many extra actions. However for security reasons a minimum set of measures needs to be taken.

Firstly the user requesting information needs to be sure about the authenticity of the information system he communicates with. The user needs to be able to ascertain that the information system he gets is the information system he requested. He needs to ascertain that his connection is not diverted to a different server pretending to be the desired information system.

Secondly the information system needs to be sure about the authenticity of the user. It needs to ascertain the validity of the user identification and check the privileges the user has to view, modify and delete data.

Thirdly it needs to be ascertained that data was not changed during transport. Checks are needed to assure that the sent data and the received data are identical.

To assure these three demands the Secure Socket Layer protocol was developed [5]. The current version is 3.0. The three items are now discussed in more detail. Firstly data encryption and the data integrity check are illustrated.

3.1. Encryption and integrity check

To send data in a way that interception is prevented the data should be encrypted before sending. Suppose Alice wants to send an encrypted message to Bob. Alice and Bob then have to agree on the encryption algorithm (which key) they want to use. Alice encrypts the message with this key and Bob decrypts it with the same key, as shown in figure 1. This method, called symmetric-key encryption, is fast but the disadvantage of this method is the fact that both Alice and Bob need to have this key at their disposal and they need to prevent others from getting this key. Because possessing this key, means one can decrypt the message.

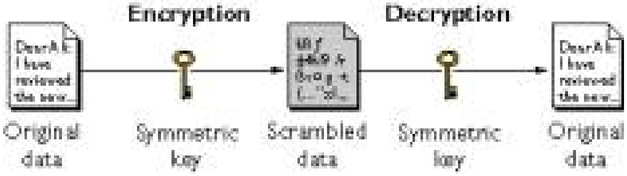

Figure 1 Symmetric-key encryption.

To simplify the complicated key maintenance for symmetric-key encryption a new encryption technique was developed where the key is split in two parts, one private key and one public key [6]. When Alice now wants to send an encrypted message to Bob she encrypts it with Bob's public key after which Bob can decrypt it with his private key (see figure 2). Bob can without any trouble distribute his public key to anyone who wants to send him encrypted messages. He only needs to protect his private key from falling in the wrong hands. The disadvantage of this technique called asymmetric-key or public-key encryption compared to symmetric-key encryption is that more calculation time is required and therefore communication speed is decreased.

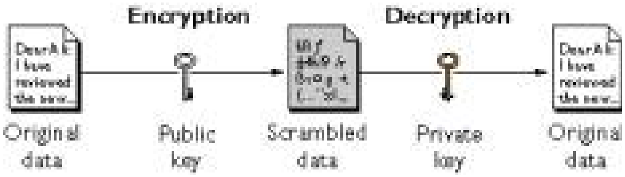

Figure 2 Asymmetric-key encryption.

Bob and Alice now also want to guarantee the integrity of the message and ascertain that the message was not changed during transport. To check this a digital signature is created. By a so-called hash-filter a digest of the message is taken and this is encrypted with the sender's private key. This produced digital signature is attached to the original message. Using the same hash-filter Bob also creates a digest from the message. Secondly he decrypts the attached digital signature using the sender's public key. The result needs to be identical to his primary created message digest. If not, the message was changed during transport. Figure 3 shows a graphical representation of this integrity check.

The combination of public-key encryption and digital signing of the messages is a sufficient guarantee for secure communication and data integrity.

3.2. Server authentication

For the user to be sure about the server's identity he needs to check the server certificate's authenticity. The used Internet browser does this automatically after referring to the URL. The identity of the server is registered in the server certificate. Such a certificate contains among other things the following items:

Certificate details	
Version	Version
Serial number	Number
Signature algorithm	Algorithm for signature
Issuer	Name, address etc. CA
Valid from	Start date certificate
Valid to	End data certificate
Subject	Name, address etc. server
Public key	Public key for encryption
Thumbprint algorithm	Hash algorithm
Thumbprint	Digest of public key

A certificate authority (CA) issues the server certificate. This certificate authority is a Trusted Third Party (TTP) for both the data sender and the receiver.

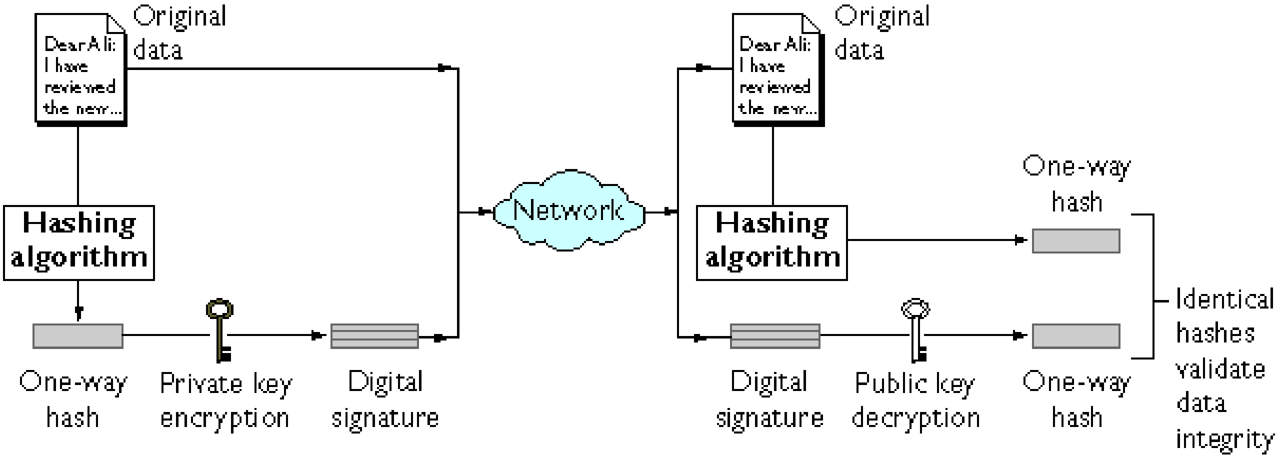

Figure 3 Data integrity check using digital signatures.

Before signing such a certificate the CA will ensure the organization requesting a server certificate can be undoubtedly identified. This certificate authority can be one of the dedicated worldwide CA's such as Verisign (www.verisign.com) or alternatively Globalsign (www.globalsign.com). But when the group of users is small and known by the institute running the server with the information system one can create its own certificate authority. The default Internet browser will not recognize such a small certificate authority and the browser will therefore present a warning that the CA does not belong to the group of trusted certificate authorities.

The verification of server authenticity by the Internet browser is shown in figure 4. It is checked if today is within the validity period of the certificate, if the browser trusts the issuer (CA), if the issuer's public key validates its digital signature and if the URL corresponds with the certificate's subject. If this is all OK an encrypted link can be established using the SSL protocol.

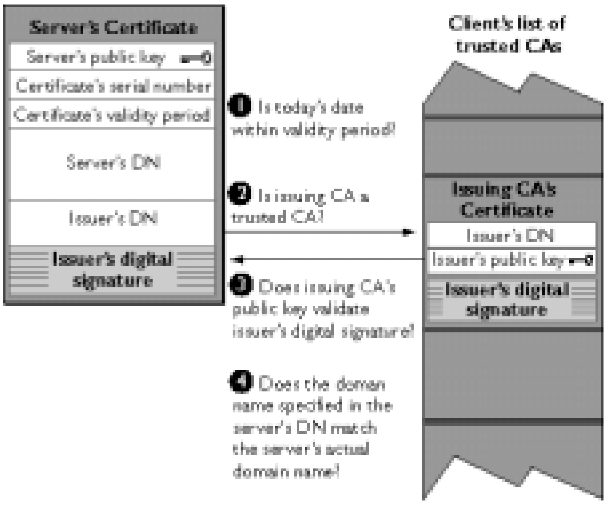
Server's Certificate
Server's public key
Certificate's serial number
Certificate's validity period
Server's DN
Issuer's DN
Issuer's digital signature
Client's list of trusted CAs
1 Is today's date within validity period?
2 Is issuing CA a trusted CA?
3 Does issuing CA's public key validate issuer's digital signature?
4 Does the domain name specified in the server's DN match the server's actual domain name?
Issuing CA's Certificate
Issuer's DN
Issuer's public key
Issuer's digital signature

Figure 4 Steps to authenticate a server's identity.

3.3. Client authentication

For the server to check the identity of the user it can require the user to authenticate itself by presenting his client certificate. The client certificate contains the same items as a server certificate; only the subject contains the name and address of the user. The issuer can be the same CA as for the server certificate.

The steps of authenticity check by the server are shown in figure 5. It checks if the client's public key validates its digital signature and if today is within the validity period of the certificate. Furthermore if the issuer is trusted by the server, if the issuer's public key validates its digital signature and if the client certificate is listed in the authorized users of the server. If all is OK the server allows the client to access the information system. The user now can view, edit and insert data corresponding his privileges.

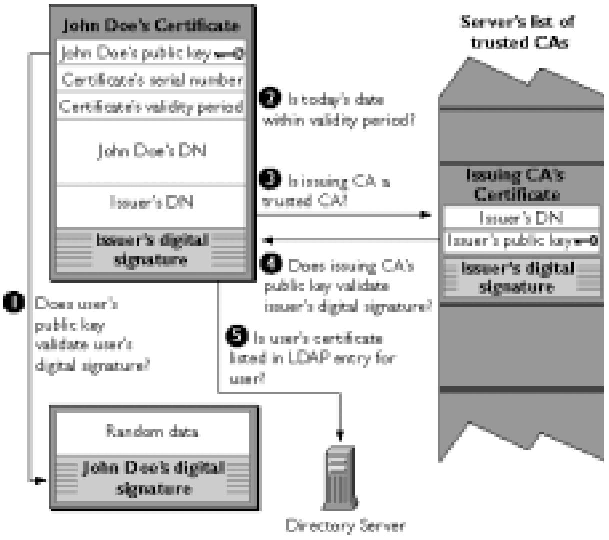
John Doe's Certificate
John Doe's public key
Certificate's serial number
Certificate's validity period
John Doe's DN
Issuer's DN
Issuer's digital signature
Server's list of trusted CAs
2 Is today's date within validity period?
3 Is issuing CA a trusted CA?
4 Does issuing CA's public key validate issuer's digital signature?
1 Does user's public key validate user's digital signature?
5 Is user's certificate listed in LDAP entry for user?
Issuing CA's Certificate
Issuer's DN
Issuer's public key
Issuer's digital signature
Random data
John Doe's digital signature
Directory Server

Figure 5 Steps to authenticate the client's identity.

4. Pilot project

Within the framework of a pilot project an information system for the treatment of heart failure patients is setup by means of an Internet database server. The server is equipped with SSL-modules and a server certificate signed by an own certificate authority. The server is setup to require client validation. The client certificate needs to be issued by the same certificate authority. In the pilot phase the server was inside the intranet of the hospital and could not be accessed from outside the hospital network's firewall. For the pilot project all security measures were taken as if it was accessible via the Internet.

For the technical implementation the Apache web server [7] was chosen on a Linux platform. Linux is a freeware operating system for which much open source software is available. Worldwide more than half of the web servers are run by Apache. For the implementation of the SSL-protocol the combination of mod_ssl [8] and OpenSSL [9] were chosen. The implementation was documented and an Internet security consultancy company was invited to assess this setup. The implementation was considered to be in accordance with the state of the art encryption and security technology. With this implementation also all requirements from the concerning guidelines are met.

5. Discussion

This pilot project showed that using the current technical possibilities for information security it is feasible to set up an medical information system on the Internet where the privacy of the data is sufficiently protected. The implementation required a minimum of user actions, is very user friendly and still ensures sufficient protection of the patient data.

The system can be extended with decision support software. For example it is possible to guide the users through implemented guidelines for treatment and diagnoses. Also this facility can be used to support multi-center clinical trials, where all data are stored on a central database server. Interactive checks can be implemented to validate the entered data automatically.

References

[1] AIM (Advanced Informatics in Medicine) Secure Environment for Information Systems in MEDicine. SEISMED(A2033) / SP14 / HILD / DEL / 05.07.95.

[2] NEN-ISO/IEC 10181:1996 Information technology; Open system interfacing (OSI); Security structures for open systems. Part 1-7.

[3] NVN-ENV 12924:1997 Medical informatics; Division of security and protection of information systems in health care.

[4] NVN-ENV 13608:2000 Medical informatics; Security of communication in health care. Part 1-3.

[5] Introduction to SSL: http://developer.netscape.com/docs/manuals/security/sslin/contents.htm.

[6] Introduction to Public-Key Cryptography: http://developer.netscape.com/docs/manuals/security/pkin/index.htm.

[7] Apache HTTPD Project - The Apache HTTP Server Project: http://httpd.apache.org.

[8] mod_ssl: The Apache Interface to OpenSSL:

[9] OpenSSL: The Open Source toolkit for SSL/TLS: http://www.openssl.org.

Address for correspondence.

Willem R.M. Dassen
Maastricht University Hospital
P.O. Box 5800
6202 AZ Maastricht
the Netherlands
w.dassen@cardio.azm.nl