A SECURE WEB SERVICE

Specification on how to implement a secure Web service in a health care environment

Bill Andreas
Persson Robert

Jun 2005
A SECURE WEB SERVICE

Specification on how to implement a secure Web service in a health care environment

Authors:
Bill Andreas
Persson Robert

Supervisor:
Werner Jonas

Examinator:
Gäre Klas
Abstract

Course: IVC730
Title: Specification on how to implement a secure Web service in a health care environment
Authors: Robert Persson, Andreas Bill
Level: Bachelor of Science in informatics
Tutor: Jonas Werner
Examiner: Klas Gäre
Date: 2005-05-10
Language: English
Key words: Web service, Security, XML, SOAP, UDDI, WSDL, Web service security, XML signature, and XML encryption, SAML

Background: With Web service growing popularity more and more companies chose to apply Web service in their organisation. With the rising usage of the concept the demands rise with it. For companies that deal with vulnerable information for example hospitals, there needs to be strong security measures taken.

Purpose: The aim of the report is to examine different security functions that can help developers to secure Web service applications. The report will be written so that organisations such as health care organisation can get insight on how to use a secure Web services in their line of work.

Method: One of the main methods used in this report is a qualitative hermeneutic way of thinking. The research process will apply Wallace’s model. The theoretical study is achieved with research on the subject through literature studies and published articles. Interviews that are used to gain knowledge are structured as quality orientated science surveys with semi-standardised questions.

Conclusions: We believe the time has come for hospitals to investigate if Web service can help their organization. In case they choose to use Web services, we advise them to follow Web service Security’s recommendations to produce a web service that is adapted to their security needs.
List of content

1. INTRODUCTION ................................................................................................................................. 1
   1.1 BACKGROUND ................................................................................................................................. 1
   1.2 CARELINK AND REGIONSKÅNE ....................................................................................................... 2
   1.3 PURPOSE ......................................................................................................................................... 2
   1.4 PROBLEM DISCUSSION .................................................................................................................. 2
      Problem formulation ............................................................................................................................. 3
   1.5 TARGET GROUP ............................................................................................................................. 3
   1.6 DELIMITATION .............................................................................................................................. 3
   1.7 OUTLINE ......................................................................................................................................... 4
   1.8 CASE “PATIENT CASE” DESCRIPTION .......................................................................................... 4
   1.9 QUALITY ASSESSMENT .................................................................................................................. 5
   1.10 RELEVANT SOURCES ................................................................................................................... 5

2. RESEARCH METHOD ............................................................................................................................. 7

3. PREVIOUS RESEARCH .......................................................................................................................... 8
   3.1 WEB SERVICES ............................................................................................................................... 8
      3.1.1 WEB SERVICE DEFINITIONS ................................................................................................. 9
         3.1.2 Extensible Markup Language .................................................................................................. 10
         3.1.3 Simple Object Access Protocol ............................................................................................. 10
         3.1.4 Web Services Description Language ....................................................................................... 11
         3.1.5 The Universal Description, Discovery and Integration .......................................................... 11
   3.2 FUNCTIONS TO SECURE WEB SERVICE ....................................................................................... 12
      3.2.1 Web service Security ................................................................................................................ 12
      3.2.2 Message Time Stamps ............................................................................................................. 14
      3.2.3 Digital Signature ..................................................................................................................... 15
      3.2.4 XML Signature ......................................................................................................................... 16
      3.2.5 Encryption ................................................................................................................................ 17
      3.2.6 XML Encryption ....................................................................................................................... 17
      3.2.7 XML Encryption and XML Signature ......................................................................................... 18
      3.2.8 Secure Socket Layer and Transport Layer Security ................................................................. 18
      3.2.9 Security Assertion Markup Language ...................................................................................... 19

4. EMPIRICAL STUDIES ............................................................................................................................ 21
   4.1 ANALYSE OF EMPIRICAL STUDIES ............................................................................................. 21
   4.2 INTERVIEW DESCRIPTION ............................................................................................................ 21
   4.3 MEETING WITH RICHARD LINDVALL AND PER TORLÖF .......................................................... 22
   4.4 INTERVIEW WITH RICHARD LINDVALL AND PER TORLÖF ....................................................... 22
      Result of the interview with Richard Lindvall and Per Torlöf ............................................................ 23
   4.5 INTERVIEW WITH PR. LÖWE ......................................................................................................... 23
      Result of the interview with Pr. Löwe ................................................................................................ 24

5. RESULT AND DISCUSSION .................................................................................................................... 25
   5.1 DESCRIPTION FOR THE IT-POLICY ............................................................................................. 25
   5.2 IT-POLICY FOR IMPLEMENTING A WEB SERVICE ......................................................................... 25
   5.3 CASE “PATIENT CASE” ................................................................................................................. 27
      5.3.1 Scenario “Patient case” ............................................................................................................ 28
      5.3.2 User case .................................................................................................................................. 29
   5.4 RESULT .......................................................................................................................................... 30
   5.5 SUMMARISED RESULT ................................................................................................................... 32
   5.6 DISCUSSION .................................................................................................................................... 33

6. TEXT REFERENCES ............................................................................................................................... 36
   FIGURE REFERENCE ............................................................................................................................. 37
   TABLE REFERENCE ............................................................................................................................... 37

APPENDIX “INTERVIEW WITH RICHARD LINDVALL AND PER TORLÖF” AND ANSWERS ...... 38
APPENDIX “INTERVIEW WITH PR. LÖWE” AND ANSWERS ........................................................... 40
1. Introduction

1.1 Background

Web services is a concept that is used to connect systems on the Internet and intranet to exchange information in real-time. Behind Web services there is a set of standards that has been developed by W3C. The aim is to find services on the Internet that makes it easier for the exchange of data between web applications. The technology can also be used within a company’s intranet systems, therefore Web service can be referred as the new method for system integration. Fredholm (2002). Four technologies from the basics of Web services are explained in this quotation.

“XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available and UDDI is used for listing what services are available.”

- Webopedia, (2005)

Rosenberg and Remy (2004) explains in the process of making a Web service secure, there are some security components that have to be considered: confidentiality, authentication, authorisation, integrity, non-repudiation. Rosenberg and Remy describes further that confidentiality means that the message is not decrypted by anyone else then the recipient and can be solved by XML-encryption. An authentication determines the identity of the user and the function that can determine the identity can be SAML. Authorisation determines what a user can do in the system. Integrity ensures that the message is not altered during the transaction and to guarantee this, different tunnelling techniques can be used. Non-repudiation ensures that the message was sent. The solution to integrity and non-repudiation problem can be solved using an XML-signature. In the chapter Functions to secure Web service it is possible to read Saikali (2002) interpretation the same four components in Web service Security.
1.2 Carelink and Regionskåne

Carelink works to support IT more efficient for the patient as well as for the personnel. Carelink invites people involved from all counties and regions organisations to be members. Together with members Carelink works for the evolvement of IT usage within Swedish health care. Carelink also work for a common, homogeneous, national platform of information safety, were they could exchange care information over a health care intranet or Internet. Their goal is to use systems for patient administration, journal management etc. and to ensure that the information can be referenced to the source, they are currently using digital signature. Sixteen counties including Regionskåne has joined to sign a letter of intent concerning a jointly policy regarding electronic identification and signing that is called the SITH-model. In the chapter “Result and Discussion” we have made a case study where we produce a scenario, which is based on our meeting with Richard Lindvall and Per Torlöf at Regionskåne in Lund. The case is also based on our theoretical knowledge of security functions that are described in the theoretical part of this thesis.

1.3 Purpose

The aim of the report is to investigate functions to secure Web service applications in a health care environment. The report will be written so that organisations can get insight on how to use a secure Web services in their business.

1.4 Problem discussion

Web services have been applied in many fields, but in the field of health care there have not yet been any satisfying security measures. With new technologies such as web services security, the security has advanced to a level that is satisfying for this type of vulnerable information. We will examine Richard Lindvalls proposed requirements on how to make a
secure Web service in a health care environment. We have made a problem formulation with consideration of Backman’s (1998) questions and intentions.

We will consider Backman (1998), page 70:

- Generalisation, the question of how sure we are of the assumption on the chosen study.
- Causality, the relationship between cause and effect.
- Theorize, is the study evolving forwards both theoretically and the conceptually to a greater understanding.
- Application, the question of how to apply the knowledge in a practical solution.

**Problem formulation**

How can security measures be used to secure a Web service application within a health care environment?

**1.5 Target group**

This report is aimed to be read by people with basic insight in the subject of computer science knowledge and those who are employed to manage IT systems. We write this report with the wish that persons in the field of system management can use it as a proposal on how to implement secure Web services.

**1.6 Delimitation**

This is a theoretical study and the thesis will not include any practical work. Nor will we include any advanced implementation examples in this thesis. The report will not consist of any other functions then security function in Web service applications. We will not write any
details in theoretical part about how hospitals handle their information. To get this information we will ask Richard Lindvall and Per Torlöf. The questions are about how information is sent with consideration of security at hospitals under Regionskåne.

1.7 Outline

The four components in this report are mainly introduction, previous research, empirical studies and result and discussion. We started with an introduction chapter were we focuses on telling the reader the background and the reason why we have chosen our line of work. In the same chapter we have reasoned a problem formulation under the header “Problem discussion”. To make a clear reservation against what this report will exclude, we wrote a legible delimitation. After we identified the purpose and the delimitations of the report we took a great deal of project time to chose a suitable method to affect our research. To assure a good quality on the report we will maintain a close contact with our supervisor and obtain continues dialog with Richard Lindvall at Regionskåne. This and more details on how we will try to maintain our goal of a quality report can be read in the section quality assessments. In the next chapter “Previous research” we make a short description of the Web service technology. Further on we take a look on the recent advances that is available when making a secure Web services. We will also consider Richard Lindvall at Regionskåne advice on how to make Web service secure. In the last chapter of the report we will evaluate our theoretical and empirical studies and write a conclusion in the chapter result and discussion.

1.8 Case “Patient case” description

To exemplify our study we have made a case, were we explain how a communication between actors in a hospital can work. To refer to our report we will explain security measures that have to be considered when implementing a Web service in such an environment. To specify the “Patient case” we have made a user case specification by the rules of UML.
1.9 Quality assessment

Background knowledge about Web services is partly gained through lecture by Lars-Erik Ljung, Jesper Andersson and Professor Welf Löwe (Pr. Löwe) in the course IVC 741 on the University of Växjö. Theoretical knowledge is accomplished through literature concerning the subject. In depth and practical knowledge are studied in literature and published articles on the Internet. Basic knowledge in system architecture and other fundamental computer science orientated studies where achieved during the five terms that we have studied at the University of Växjö. For further quality assessment we have discussed the subject with Professor Per Flensborg at MSI, Växjö University. To get a view on how Regionskåne practise their work we have conducted a quality interview with Richard Lindvall and Per Torlòf at Regionskåne in Lund. To follow up this interview we have formulated a quality orientated science survey with structured, semi-standardised and follow-up questions. The goal of the interview is to be able to analyze the result of the information given in the interview. To get a better view on the subject of Web services we will try to book a meeting with Pr. Löwe how is a Professor in computer science.

1.10 Relevant sources

To get an understanding in the subject of relevant sources we have mainly studied Thurén’s books on source criticism were he claims that. “All the knowledge we receive is based on knowledge sources. The task of source criticism is to validate these sources, evaluate their credibility.” Thurén, (1997), page 7.

Our principles for the choice of literature sources.

- Authenticity - The source shall be what it claims to be.
• Time relation - The reliability of the source depends on the time between the publication of the source and the time you read it.
• Independent - The reference should come from the original author so that opinion in the reference not changes.
• Rehabilitée - there should not be any suspicion that the source does not portrait the reality, do to any personal, economical, political or any other interest that may distort the reality.

Our principles for the choice of Internet sources.
When choosing Internet references it is not always sufficient to apply the rules that we mention previously. Therefore we apply an additional set of rules that Leth and Thurén (2000) recommends for Internet.

• The tendency of applying the world and knowledge view - The source must be objective and in some sense the culture aspect plays a role.
• Reliability – The problem with Internet is that it contains great amount of information therefore it is important to sort out unreliable sources.
• The source prerequisite and properties – The issue of the source authentification depends on how we judge its information.

In the report the reference model is taken from Erikson’s “Litteraturreferenser enligt Harvard-systemet”.
2. Research method

One of the main methods used in this report is a qualitative hermeneutic way of thinking. Hermeneutic is the theory of interpretation and understanding. Hermeneutic understanding of a subject means that we do not just grasp reality from our senses. What seems to be a pure sense impression also contains a portion of interpretation. The term of fact in this case can be referred as theory impregnated. The research to this report can be compared to the conception of a hermeneutic spiral in the sense that understanding demands empathy i.e. the ability to familiarize in other persons situations. Thuren (2002)

The research process will apply Wallace’s model. In the way that we think of this project as a cycle were we gain new knowledge and audit incorrect knowledge. Järvinen, (1999)

With the belief that people reading this report has knowledge of the concept of Web service. We would like to go beyond this “understanding horizon” as Johansson describes it, and think out of the box on how a company can secure a Web service. Johansson, (2003)

We think that after making researches that a hermeneutic approach will be the best solution to our problem and will give the most truthful result. With the background knowledge that we posses in the subject of Web services we think that hermeneutic method is the right choice. To draw conclusions in this report we will use positivistic hypothetical – deductive method. This we will do through empirical induction and logic deduction.

Thuren (2002) refers empirical studies as observations through our five senses. It is with the help of the five senses we establish facts. A positivistic point of view is that after reviewing and examining the facts, one can draw a conclusion on its credibility.

Empirical studies will be conducted through interviews. The interviews are structured as quality orientated science surveys with semi-standardised questions. The goal of the interviews is to be able to analyze the result of the information given in the interviews.
3. Previous research

3.1 Web Services

A Web service can be described as an application system which sole purpose is to integrate computers over a network. Web services use Simple Object Access Protocol –messages (SOAP), often conveyed by HTTP with a series of XML and other Web-related standards. Hugo Haas (2004)

Ramachandran (2004) stats two fundamental criteria for defining what Web services should be able to do:

- A Web service should be able to service requests from any client regardless of the platform on which the client is implemented.
- A client should be able to find and use any Web service regardless of the services’ implementation details or the platform on which it runs.

Web service is a technique in the sense that it makes it possible to connect different functions. This service can be employed in an intranet as well as on Internet. A Web Service is programming language neutral and platform independent. This is a new type of Web application that is self-supporting and self-descriptive application that can be published and integrated over the Internet. A Web service can rejoin everything from a small calculation to powerful complex business systems. This makes Web service a dynamic tool that can be adapted for the customers needs.
3.1.1 Web service definitions

Because Web service is a relatively new technology it is sometimes hard to define. Below there are some examples from the major actors of Web service development, whom attempting to specify what Web service is:

“A Web service is a software system designed to support interoperable machine-to-machine interaction over a network.”


“Web Service is a piece of logic that applications can access over a network via a standardized interface, in a platform independent and language-neutral way.”


“Web Services are a message-oriented communication framework that is designed to be very interoperable and extensible.”

  Advisory Software engineer, IBM
3.1.2 Extensible Markup Language

Extensible Markup Language (XML) is the cornerstone of a XML based web service. XML is a language that allows providers and requestors to communicate with each other independent of platform or technology. This is done through Internet protocol such as HTTP.

In an Internet article published on www.informit.com written by Ramachandran (2004), it is declared that XML is independent in the choice of proprietary platform or technology. Furthermore Ramachandran describe messaging with XML.

“Because XML is a product of the World Wide Web Consortium (W3C) body, changes to it will be supported by all leading players. This ensures that as XML evolves, Web services can also evolve without backward compatibility concerns.”


XML is as HTML a mark up language, but it is different in the way of presenting data. HTML is used for displaying data and XML is designed for describing data. W3schools by Refsnes Data (2005)

“XML is the foundation of the Web service standards. All standards for describing, discovering and invoking Web service are based on XML.” Rosenberg, Remy, (2004), page 6.

Rosenberg and Remy (2004) stats that XML programmers usually apply a schema to describe the rules for a XML instance. The schema is constructed to control the XML document.

3.1.3 Simple Object Access Protocol


SOAP is according to HP (2005) and W3C (2005) a lightweight mechanism. Further more HP explains that SOAP provides a structured exchange type that distributes information using XML. W3C declare that SOAP consists of three parts. The first one is an envelope that describes what a message withhold and what to do with the message. Second of it is a set of rules for encoding that express instances of application-defined data types. And then there is a convention for representing remote procedure calls and responses.
W3C (2005) declares that SOAP can be combined with other protocols but most of the time it is combined with HTTP. SOAP does not have strict application semantics. Instead it is defined as simple mechanisms for encoding data within modules. This gives the developer the liberty to use SOAP in a large variety of systems ranging from simple messages to advanced Remote Procedure Call (RPC).

“Although these parts are described together as part of SOAP, they are functionally orthogonal. In particular, the envelope and the encoding rules are defined in different namespaces in order to promote simplicity through modularity.”

- W3C, DevelopMentor, (2000)

### 3.1.4 Web Services Description Language

“The XML language used to describe a Web service and to specify how to communicate with it.” Oracle, (2005)

W3C, (2001) determines that Web Services Description Language (WSDL) is an XML format for describing web services as a set of network endpoints that operate on messages. A WSDL service description contains an abstract of definition for a set of operations and messages, a concrete protocol binding these operations and messages, and a network endpoint specification for the binding.

IBM (2001) claims that WSDL has a lot of versatility in the use of methods. This is especially noticeable when it works with Universal Description, Discovery and Integration (UDDI) registries in many different ways. The developers have the liberty to adjust WSDL depending on the requirements on the application.

### 3.1.5 The Universal Description, Discovery and Integration

Universal Description Discovery and Integration (UDDI) give the user the method for finding service descriptions and publishing it.

Intel (2005) describes UDDI as a centralized location for storing a listing of available Web services. It is later described as a big advertisement place where the customer finds what he/she wants and then the UDDI registry broadcast the means of interoperating with an application designed to fulfill the service. UDDI provides support for many different types of service descriptions both business and service information. This means that there is no exact
support for WSDL or any other mechanism. The UDDI organization has therefor published a document titled Using WSDL in a UDDI Registry 1.05 IBM (2002) on how one best practice UDDI and WSDL interaction.

3.2 Functions to secure Web service

When using Web services in organisations where the information needs to be dealt with extra caution, like for example about a patient at a hospital. When taking these security precautions it is possible to use different functions, which we describe in this section.

3.2.1 Web service Security

Web Service Security was approved as an OASIS open standard in April 2004. It is originally a standard proposed by Microsoft, IBM, and VeriSign in April 2002, and later that year the standard become part of OASIS standards body. It was establish as an OASIS open standard in April 2004. Web service Security (WSS) is a security standard developed by the WSS Technical Committee. WSS created the standard with the aim to be able to send secure SOAP messages. OASIS (2004)

“The goals of Web-services security are pretty straightforward, actually: to provide confidentiality, authenticity, integrity, and nonrepudiation of business transactions performed using Web services. “

- Oracle, Saikali (2002)

Saikali (2002) describes four rules for business transactions:

Confidentiality requires a safe communication between a client and Web service. For example, a Web service that sends a journal between two hospitals needs to ensure that the patient’s information is not exposed to anyone beside the receiver.

Authenticity requires that the client knows the Web service identity and that the Web service knows the identity of the client. For example, a Web service that manage journals
needs to make sure that it knows which hospital that is receiving the journal, and the hospital receiving the journal needs to be sure which hospital that is sending.

**Integrity** depends on the communication between the Web service and the client to be secure from tampering while in transfer. For example, the hospital receiving a journal needs to be confident that the information they receive has not been altered with.

**Non-repudiation** means that a client cannot deny the request he/she sent to the Web service and the Web service cannot deny the replies it sent back.

The Web service Security supplies a method that allows you to digitally sign your SOAP messages with an XML Signature. There is also a method that allows you to encrypt all or part of a SOAP message by using XML Encryption. Other security technologies that are included in Web service Security are X.509 certificates and SAML assertions. Web services Security also has functions to pass information in the SOAP header that contains the encryption keys required to decrypt the message or verify the digital signature. The standard does not apply with any new security technologies instead; it focuses on applying existing security technologies. To show the basic functions on how Web service Security is applied, we have taken an example from Rosenberg and Remy (2004).
This example illustrates a security header, often referred with the namespace prefix WSSE (Web service -Security extension), which has three children. The first one of these children is Security Tokens that shows a UsernameToken. The second one is Signatures that can sign all or parts of the SOAP body and the last is ReferenceList or EncryptedKey that have the EncryptedData element that can exist for each element encrypted. To strenghten these elements you can use ReferenceList or an EncryptedKey to point at the entire EncryptedData element. In this way Web service Security can read the SOAP header and then decrypt the data to which EncryptedData points to.

### 3.2.2 Message Time Stamps

A time stamp makes it possible for the recipient to determine the freshness of a security semantic. If the security semantic is outdated, depending on the context it is possible that a recipient may choose to ignore it. When using Web service Security you use Time Stamp to secure the freshness of a SOAP header. All times should be in UTC format so that time difference between the sender and the receiver not will be a problem.
As illustrated above the message sender have initialised a time frame with a creation time and an expiration time. When the message tag `wsu:Expires` time and date has expired, then the content of the message is outdated.

### 3.2.3 Digital Signature

Before describing XML Signature we will make a short introduction about digital signing. The basic function with this method is to protect the message from being changed during the transmission to its recipient. To accomplish this, the sender signs the message with his or hers private key and the receiver opens the message with the corresponding public key. This protects the sender from malicious users that are pretending to be someone else or in some way want to alter or replace the message.

On Microsoft (2004) webpage they describe how to create a digital signature. The first step is to hash the message you are signing employing a cryptographic hash function. When inputting any length of value a cryptographic hash function returns a defined set of bits described as the hash value. The next step is to sign the hash value by using a signing algorithm and the use of a private key to create a signature value. Now you create the signature with your private key so that the recipient who has the public key can approve it. When the message is sent to the recipient an authentication process starts. If the signature and the calculated hash match, then the signature is real. If the hash does not match the data or the signature, the information has been changed.
3.2.4 XML Signature

XML Signature is a W3C standard that makes it possible to sign any kind of data represented in an XML document. The Standard is very flexible when it allows you to filter and transform the data before it is signed. Microsoft (2004)

“The purpose with XML Signature is to provide a mechanism for message integrity.” Rosenberg, Remy, (2004), page 19. This means that no one except the creator has changed the message. Rosenberg and Remy describes four major components of XML Signature, with the third and forth as optional:

- A set of pointers to things to be signed
- The actual signature
- The key to verifying the signature [Optional]
- An Object tag that contains miscellaneous items not included in the first three items [Optional].

Table 3. XML Signature example, Rosenberg, Remy, (2004)

```
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <Reference URI="http://www.foo.com/secureDocument.html"/>
  </SignedInfo>
  <SignatureValue>…..</SignatureValue>
  <KeyInfo>…..</KeyInfo>
</Signature>
```

The example above is explained by Rosenberg and Remy (2004). There are three children element of the parent element Signature. The SignedInfo element consists of information of what is being signed. The SignatureValue element contains the actual signature bits and the last element KeyInfo contains information about the public key that is required to validate this digital signature. This is a very simplified example but it describes the most significant three elements within a XML Signature. When using security methods it is always good to use it with a critical attitude. In the XML Signature standard there are some security considerations to be aware of.

“…you can change (transform) the information being signed in a hidden way (by an algorithmic process) before it is digitally signed.” Rosenberg, Remy, (2004), page 140.
A transform algorithm can change anything in the original XML document. One example of using transforms is when you need to remove a signature that is there to create/validate an Enveloped Signature. Rosenberg and Remy describes transforms to be necessary in some situation but you have to be careful when using them.

### 3.2.5 Encryption

W3C (2005) explains the encryption as a process of securing information. They claim that while it is available to a community, for example when it is accessible on your hard drive or network, it is not meaningful to those undeliberate eavesdroppers.

### 3.2.6 XML Encryption

The purpose of encryption is that unauthorised persons shall not have access to the data. To maintain this security the message have to be protected at all time, this means that after the message has been transferred in a secure way it must also be secure while it rests on the node. XML Encryption can be thought as a tool to compliment SSL and is not created to replace it.

<table>
<thead>
<tr>
<th>Table 4. XML encryption example, IBM (2002)</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;purchaseOrder&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Order&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Item&gt;book&lt;/Item&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Id&gt;123-958-74598&lt;/Id&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Quantity&gt;12&lt;/Quantity&gt;</code></td>
</tr>
<tr>
<td><code>/Order&gt;</code></td>
</tr>
<tr>
<td><code>&lt;Payment&gt;</code></td>
</tr>
<tr>
<td><code>&lt;CardId&gt;123654-8988889-9996874&lt;/CardId&gt;</code></td>
</tr>
<tr>
<td><code>&lt;CardName&gt;visa&lt;/CardName&gt;</code></td>
</tr>
<tr>
<td><code>&lt;ValidDate&gt;12-10-2004&lt;/ValidDate&gt;</code></td>
</tr>
<tr>
<td><code>/Payment&gt;</code></td>
</tr>
<tr>
<td><code>/purchaseOrder&gt;</code></td>
</tr>
</tbody>
</table>

IBM (2002) suggests that if you are to publish a XML file like the one described above, you have to be carfull with the credit card information in `CardId`. For this communication you should use a secure connection to protect sensitive data. To do this you can use SSL, if you want to protect the information even more you can use XML Encryption.
3.2.7 XML Encryption and XML Signature

Rosenberg, Remy, (2004) declares that XML Encryption go hand in hand with XML signatures in the extent that they are sharing the same concept, terminology and XML elements.

In many cases you want to be able to use two or more technologies together. The combination of XML signature and XML encryption are easy to fuse together perhaps because the two standards are developed by the same organisation W3C. The two committees are also sharing some of the members. Rosenberg, Remy, (2004)

This gives the two standards similar functions. XML encryption can encrypt all or parts of an XML document either internally or externally, just like XML Signature can. They can both use one or multiple keys to decrypt or verify signatures in a document. The most striking similarity is that both techniques share the $KeyInfo$ element. Even thou the structure of these technique many times resemble each other, the usage are quite different. First of we explain that the signing of a document has to do with integrity assurance and the acknowledgement that the signature is authentic. The usage of encryption also allows the user to hide confidential information from anyone other than the private key holder.

“...with secure XML and Web service you need to both encrypt a message to a recipient as well as sign the message to confirm your identity and verify that the message you sent is the message that received.”

Rosenberg, Remy, (2004), page 148

3.2.8 Secure Socket Layer and Transport Layer Security

When using Secure Socket Layer (SSL) for transferring, SSL developers guarantees that the message is securely encrypted, but what about when it is received at the first destination, where it is open for insight. This is a big vulnerability. Further more SSL does not address the problem of maintaining a secure sessions with multiple participants. With the new de facto standard for secure communication over Internet former developers of SSL have introduced Transport Layer Security (TLS). SSL was designed for Netscape version 3.0 by the Internet Engineering Task Force (IETF) which later adapted the SSL protocol to the secure and reliable protocol TLS. TLS is an end-to-end security protocol that runs secure sessions between two parties.
3.2.9 Security Assertion Markup Language

Rosenberg, Remy, (2004) describes the Security Assertion Markup Language (SAML) as an XML-based structure for exchanging security information. This OASIS standard makes it possible to express security attributes about individuals when sending information between two organisations. SAML is described as the notion of portable trust and which solves the problem of transporting identity. SAML is three XML-based methods that are: a set of bindings, a protocol and assertions.

This example illustrates the fundamental of how SAML is built. The mechanism protocol is a Request/Response protocol that looks for the type of assertions. The three methods of SAML assertions send a request which the SAML protocol respond to. The information is carried in the SOAP body over HTTP binding. To ensure that the SAML is secure in the SOAP payload Web service Security specifies an SAML profile. The Web service Security profile contains a
SOAP message that has a linked SAML assertion in the header. Assertions in SAML are programmed in a XML Schema that contains basic information and the statement that the requestor is suggesting.

**Assertions** - The security information in SAML is described in the form of assertions about subjects, where subjects either are humans or computers that are described as entities that have identities in some security domain.

There are three types of assertions according to Rosenberg and Remy (2004):

**Authentication** - is an assertion that a subject is who he/she claims to be.

**Authorization** - is an assertion that the subjects’ identity is legitimate to execute a specific action, and it must be confirmed before the requested action is approved.

**Attributes** – This assertion supplies information concerning an authorization or authentication.
4. Empirical studies

In this section of the report we will discuss the way of collecting data through interviews among other things. To do this we will make a tactical plan for gathering information in the analyse part.

4.1 Analyse of empirical studies

Our approaches for empirical studies are based on our theoretical assumptions. To get a better understanding on how to apply a secure Web service in hospital environment, we met and interviewed Richard Lindvall of Regionskåne. To get an insight on how to implement a Web service we will ask Welf Löwe professor in computer science to answer some question in an interview.

4.2 Interview description

We have conducted two interviews. To get an overview of Regionskåne organisation and their expectations on this project, we met Richard Lindvall and Per Torlöf. This meeting contained a discussion on which security level they request for a Web service. To follow-up this meeting we made structured questionnaire that we mailed to Richard for further information. The questions asked were about his web service experience and security knowledge in his current work as a project leader of information security at Regionskåne. For further insight on web services applications, we interviewed Pr. Löwe in the form of a survey. The survey was quality orientated science survey with structured, semi-standardised and follow-up questions.
4.3 Meeting with Richard Lindvall and Per Torlöf

The first meeting with Richard Lindvall was done at his office in Lund. Per Torlöf was also present during this meeting. The first part of the meeting Richard Lindvall and Per Torlöf introduced us to their organisation and their post description at Regionskåne and Carelink. After that we had some prepared questions that we asked to Richard Lindvall and Per Torlöf about present security measures and desired future security wishes. We explained what our goal with the report is. After identifying their organisation we discussed how we wanted the project to evolve. We came to the conclusion that we wanted to write this report with considerations on how to secure a Web services in their field, but also to describe the different security functions that are available for any organisation or company. Their wishes on a web service applied in their organisation were that it must be encrypted and signed before any communication is made. Their demands on the encryption were that it should be asymmetric. Further on they would appreciate such functions as single sign on and a freshness confirmation function. To confirm the time the message were sent they recommended the usage of time stamping. To ensure that the messages are authentic they suggested the use of protection against compromised messages. To secure the message integrity digital signatures should be used. After we analysed these suggestions on how they wanted a Web service to be secure we had some follow-up questions that we mailed Richard Lindvall later during the project, witch will be presented later in the report under “Interview with Richard”

4.4 Interview with Richard Lindvall and Per Torlöf

On the 14th of April we sent Richard Lindvall a questionnaire via mail. The questionnaire contained questions about his position at Regionskåne and his experience of Web service. The questionnaire also asked questions on how he wanted to secure a Web service application.
Richard Lindvall answers the first question about his current work situation at Regionskåne, that he is a project leader of information security. Per Torlöf also works as a project leader of information security and standardisation. Richard has worked for ten years with IT-security related jobs and has contributed with implementing Secure IT-solution. In the second section of the interview we ask Richard Lindvall what Web service means to him. He describes Web services as loosely connected services with Service Oriented Architecture (SOA). With Web service he wants a standardised and message based interface. He believes that Web service Security can provide an IT-support of information in a hospital. When we ask Richard Lindvall and Per Torlöf what obstacles there can be when implementing Web services, they answers that the biggest problem is to get started with a new infrastructure. In the third part of the interview we asked them what security functions in WS they desire. Richard Lindvall and Per Torlöf mentions that XML encryption and XML signature etc. is wanted. When we ask them what information that is most vulnerable at a hospital, they answers that all information is equally important to protect and should be handled with regards of secrecy laws. Richard Lindvall and Per Torlöf think that it is the right time to implement a WS and they explain that there are good tools like .Net for example. When we ask them which functions that can secure vulnerable information, they suggest Web service Security’s solution of XML signature and encryptions. They also mention SAML for legitimacy controls and XACML.

4.5 Interview with Pr. Löwe

The interview with Professor Löwe at the School of Mathematics and Systems Engineering was conducted in Pr. Löwe’s office on the 21st of April. The interview questions are mostly about his experience in implementing Web services. We also asked him about his role at the University of Växjö.
Result of the interview with Pr. Löwe

Pr. Löwe starts the interview by telling us that he is a professor of Computer science since three years back at Växjö University. He is currently involved in the organisation WCSS that is a competence cluster. WCSS works together with W3C and OASIS to develop standards. When we ask him why Web service has become such a successful concept he replays that Web service (WS) is good at solving two problems. The first problem is that WS works independent of platform and gives the programmer great freedom. The second is that WS offers good distribution possibilities that can contribute to faster communications and transactions. Pr. Löwe continues that WS is relatively easy to learn and understand. This makes it easy to start programming. Another factor to the successes of WS is that it has got a lot of attention lately. When we asked Pr. Löwe what is important to think about when implementing a WS he answers: That you should first think of what the problem is, then of what tool for solving it. Maybe WS can be a solution to the problem, maybe another development tool is more suitable. Pr. Löwe mentions two aspects to think about when implementing WS, which are security and performance, these could be more expensive to implement after. Many times the orderer thinks of the security but neglects the performance. Some aspects of performance can be to know which multitude of data that is transferred and how many users that are utilizing the system. We asked Pr. Löwe what he believes are the biggest distinction between traditional system development and development of WS. Pr. Löwe explains that there are no big differences, although there are some advantages of using a standard. One advantage is the maintenance of the system is easier even though new system managers are employed they can understand the system. It is also easy for the head management to understand the basics of the system. One negative aspect is if the data amount is big and complex then the WS application becomes slow. If you want a system that handles big and complex data amounts it is better to use for example Enterprise java beans. Pr. Löwe mentions that you can calculate the time it takes to use an XML transaction with the factors of the amount of data and users. These calculations can be a good basis when choosing application. If you are uncertain of which platform to use for your WS CORBA has developed software called Modelling Driven Architect (MDA) to help you. When we asked Pr Löwe if he has had any experience in implementing WS at a hospital, he answers that he has not.
5. Result and discussion

5.1 Description for the IT-policy

This Web service (WS) policy establishes how the service should work in a health care environment, with the consideration of safety and secrecy. The policy applies to the whole organisation and everyone employed in the organisation or any other business with contract to the organisation. The Policy also comprises entrepreneurs, consultants and suppliers that are hired by the organisation. All those that are included above will have knowledge and responsibility for the use of Web services. All personnel employed must have knowledge of the policy and how it implies on him or her. It is also important to have an employed that is responsible for education and follow-up of the IT-policy. The IT-policy is constructed with consideration of our theoretical and empirical studies.

5.2 IT-policy for implementing a Web service

This IT-policy for implementing a Web service (WS) establishes how the service should work in a health care environment, with the consideration of safety and secrecy. The policy applies to the whole organisation and everyone employed in the organisation or any other business with contract to the organisation. The Policy also comprises entrepreneurs, consultants and suppliers, which are hired by the organisation. All those that are included above will have knowledge and responsibility for the use of Web services. All personnel employed must have knowledge of the policy and how it implies on him or her.

Goals

The goal of this IT-policy is to contribute tactic guidelines to efficient and develop Web service applications, so that it simplifies the organisations business. The following points should be considered:
• With the help of WS the care chain within the health care shall be greatly improved, so that the organisation can use their resources more efficient.
• WS will promote that the information concerning a patient will follow her/him through the whole care chain.
• WS shall be used as tool for the personnel to give the patient a good service.
• To contribute for a more efficient business the organisation shall work for better cooperation with its business partners.

Web service
The Web services application should:

• Be supported and make existing resources more proficient.
• Be Patient-orientated.
• Support information exchange within and between organisations.
• Be applied so that the personnel’s rolls and tasks can be carried out.

Security when using Web Service
Users shall comply with following rules:

• Use encryption with a public key.
• Use signatures to identify the sender.
• Use the authentication tool when login on.
• Time stamped should be considered when taking part of information.
• The organisation shall actively follow the security development of Web services.
• An organisation or a person should be responsible for protecting vulnerable information on patients.
• Reliability of the WS system shall be protected on an adequate level.

Competence when using Web Service
Persons using the WS system shall:

• Be Trained on how WS systems works efficient.
• Ensure that available competence is used.
• Apply with rules and laws when using the system.
5.3 Case “Patient case”

To get a view on how to practice the security functions discussed in the previous research. The functions that we handle are to some extent based on the wishes of Richard Lindvall and Per Torlōf at Regionskåne, that we achieved by talking and interviewing them. The scenario basically involves a doctor and a patient at a hospital. To offer the patient a faster and better service the doctor uses the hospital intranet to get information and service. The hospitals intranet uses an integrated Web service to communicate and make necessary transactions. The communication by the Web service is secured with different security functions that are described in the chapter “Previous research”.
5.3.1 Scenario “Patient case”

Dr. Linqvist receives a patient named Jan that complains about backache and that his legs get numb occasionally. Jan has had this problem for quite a while and wants to get examined. Dr. Lindqvist logs on to a Web service system. Because Jan is registered at another hospital Dr. Lindqvist sends a request for Jan’s journal over the hospitals integrated intranet. The request is signed by Dr. Lindqvist. After the system has verified the signature the system gives access to Dr. Lindqvist to download the journal. Once the journal is downloaded it becomes decrypted. After taking a look at Jan’s journal Dr. Lindqvist examines him and decides that Jan should get an X-ray of his inward curve of the lower part of the back and sends Jan to the X-ray ward. After Jan leaves Dr. Lindqvists office, Dr. Lindqvist sends a description to the X-ray ward through the Web service portal. Before sending the description of what is going to be X-rayed he signs it with his approved E-legitimization. After sending the message he receives a confirmation that the system has approved his legitimacy to order the action. After a short while Dr. Lindqvist receives a reservation for Jan to get an X-Ray. After an hour he receives a picture of Jans injured vertebra by the personnel of the X-ray ward. The pictures are enclosed in a signed message. When verifying the signature Dr. Lindqvist takes a look at the pictures and calls for Jan to meet him again. Dr. Lindqvist explains to Jan that he has a slipped disk and needs rehabilitation by a certified physiotherapist. First he needs medication to reduce the pain. Dr. Linqvist once again uses the Web service portal to prescribe a recipe for Jans condition, Dr. Lindqvist verifies the action by using his ID-card, the recipe are sent to pharmacy on the hospital for Jan to get later. Dr. Lindqvist sends a referral request message to the physiotherapist. The system at the physiotherapist wards replays that there can be a reservation a month from now. Dr. Lindqvist asks Jan if it is appropriate for him that day and time. Jan confirms that its ok and Dr. Lindqvist books the time at the physiotherapist. The message that was sent by Dr. Lindqvist is time stamped so the system can refer the booking a month from now. The Web service is programmed to send a reminder to the patient through email and send a reminder to the administration ward to send out a reminder through mail. The Web service system at the physiotherapist books an appointment and ads it to their schedule.
## 5.3.2 User case

### Use case: Patient case

<table>
<thead>
<tr>
<th>ID: UC01</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actors:</strong></td>
</tr>
<tr>
<td>Doctor, System, Patient</td>
</tr>
<tr>
<td><strong>Preconditions:</strong></td>
</tr>
<tr>
<td>1. The patient has made a reservation to see the doctor</td>
</tr>
</tbody>
</table>

**Flow of events:**

1. The doctor logs on the system by using ID-card and his PIN-code
   - 2.1 The doctor denies access to the system
2. If the PIN-code is not valid or does not match the ID-card
   - 3. If the PIN-code is valid and the ID-card matches
     - 3.1 The doctor gets access to the system
3. While the doctor is logged in, he can access the system
   - 4.1 The doctor confirms his identity by using his ID card
     - 4.1.1 The doctor downloads the patient's journal
     - 4.1.2 Once the journal is downloaded it becomes decrypted
   - 4.2 After examining the patient he orders a X-ray description through the system
     - 4.2.1 The system asks the doctor for his ID-card
     - 4.2.2 If the ID-card is invalid
       - 4.2.2.1 The system ignores the message
     - 4.2.3 If the signature is valid
       - 4.2.3.1 The system reserves an appointment.
   - 4.3. He receives a reservation for the patient from the X-Ray ward.
   - 4.4. A picture arrives enclosed in a message to the doctors inbox
     - 4.4.1 The Doctor verifies the attached signature
     - 4.4.2 If the signature is invalid
       - 4.4.2.1 The Doctor ignores the message
     - 4.4.3 If the signature is valid
       - 4.4.3.1 The doctor looks at the X-Ray picture.
   - 4.5 The doctor prescribes a recipe to the patient at the pharmacy by using his ID-card
   - 4.6 The doctor sends a reserve request message to the physiotherapist by using his ID-card
     - 4.6.1 He receives a suggestion on a reservation at the physiotherapist for the patient
     - 4.6.1.1 The doctor books the appointment.
   - 4.7 The system time stamps the booking message
   - 4.8. The system adds it to the booking to the schedule
   - 4.9 The system sends an email to the patient as a reminder
   - 4.10 The system reminds administration personnel to send a mail to the patient.
5.4 Result

In this result part we answer the problem formulation on how to make a secure Web service in a hospital. Here we make some examples and give suggestions on how to use security functions in a Web service. We also draw conclusions on how to use Web service in a secure way.

Web services are well liked because it is platform and language neutral. Another great advantage of web service is the possibility of good distribution that can promote a faster transaction and communication. One of the characteristics of Web service is that it is easy to start developing applications with tutorials and help functions. Pr. Löwe mentions in the interview that developers of Web services should consider the factors of performance. This could be a big problem if it is taking up to much time resources. When using XML for example it has a weakness of taking up a lot of broadband capacity. To examine if Web service is suitable as a solution for transactions, there is a possibility to calculate the performance of the future Web service, by using the variables: multitude of data and users of the system.

When implementing Web services in organisations that handle vulnerable information it is important to protect the information. For example when a person that is certified to get vulnerable information, he or she can use digital signature to ensure him or hers authentication. There are functions and advises available to make sure that this information is not available for uncertified people. To ensure that integrity information is kept from everybody except an authorised person, encryption can preserve the integrity of the information. W3C has developed a XML encryption standard that is developed to compliment SSL. This technique can encrypt part or the whole message package. We have tried to explain how an encryption process might work in our case scenario “patient case”, where a journal is sent encrypted via a Web service application. In the case “patient case” the encrypted message gets decrypted after the doctor’s proved his identity. For the doctor to prove his identity he uses an XML signature. The techniques of XML encryption and XML signature go hand in hand to the level that it involves the same concept. We believe that these two techniques handle the integrity and authentication part of a Web service application in a satisfying way. The techniques have the advantage of sharing the same terminology and XML elements, which provides a good compliment to each other. To identify when a message was sent functions such as Time stamp can be applied. This function provides freshness guarantee on
the message so that the receiver can be sure that the message is updated and valid. To offer portable trust SAML offers identity validation that makes is possible for organizations to share information in a trusted way. In the user case we describe some type of Single Sign On, bypassing additional authentication steps and providing smooth access to resources. This could be supported by SAML trough the concept of federate identities.

To apply all the security measurers that we have explained and exemplified in the sections “Previous research”, “Result and discussion” OASIS has developed the standard Web service Security that involves most of the security functions mentioned in the report. The standard does not apply any new security functions instead it evolves the existing functions. We think that is a good set of rules to practice when developing a Web service. The standard have the reliability of working in the same way and therefore it is accepted among security experts. Big actors in the system development industry such as IBM, Microsoft and HP etc. have participated in the development of Web service Security.

Secure Socket Layer (SSL) is a mean of encrypting messages, but we do not believe that it holds guarantees on adequate safety measure. SSL contains a large vulnerability in the sense that it is open for insight at its first destination. Transport Layer Security (TLS) on the other hand delivers a better solution with end-to-end security protocols that runs secure sessions.

In addition to the Web service Security framework we have produced suggestions on how to secure information within a hospital with an IT-policy. Further on in the IT-policy we recommend that all personnel using the system should have sufficient knowledge on how to use it in a secure way.

After interviewing Richard of Regionskåne and Pr. Löwe and evaluating our theoretical studies, we reflect that with the right kind of security thinking Web service can be implemented in a secure way. When developing web services application there are many good security solutions many of witch are supported by WS Security. In a hospital environment Richard explain that all information is equally vulnerable and should be protected at all times. To do this the Web service needs to be secured by previous mentioned functions.
5.5 Summarised result

Web service has become a large part of system development. One reason for the popularity of Web services is that it is often easier than traditional developing tools. With the increasing amount of supporters using Web services the requirements from the public arises. One of the requirements for the development of web services is that it has to obtain an adequate security level. This requirement mainly comes from organisations that deal with vulnerable information. Because the security aspects have not yet been prioritised, OASIS and W3C and others have developed functions to secure Web service applications. The functions developed by these organisations are means of encryptions, authentication tools and transporting identity through SAML etc. In this report we have addressed some security functions that protect information. The information that needs to be protected is vulnerable information such as patient information, messages that are sent between doctors and hospitals and classified information. To do this we have emphasized some security function that covers these areas. The five security components that Rosenberg and Remy described in the theoretical part of the report are confidentiality, authentication, authorisation, integrity, non-repudiation. We have tried to exemplify these security situations in a case scenario. Further on we have tried to fulfill the requirements of how to protect information by using security measures suggested in the theoretical part of this thesis.
5.6 Discussion

In this section we discuss the subject of how to make a secure Web service in a hospital and to answer the problem formulation:

*How can security measures be used to secure a Web service application within a health care environment?*

We also discuss the time relevance of the concept Web service and the security aspects with the latest security functions available. To make a quality assessment we have evaluated the quality of the report under the header “Quality of the report”. In the conclusion part in this chapter we discuss which functions that can be used to secure a Web service in a hospital. To continue our study we have describes some future studies that may be interesting.

5.6.2 Time perspective

The subject of Web service has got a lot of attention recently. More and more companies implement Web service solutions to their organisation. The security aspect has been neglected, however it has gotten more interest by different organisations lately. Especially hospitals have waited to implement web service solutions, perhaps because they have not believed that the security requirements can be obtained. Possibly now there are sufficient measures to secure Web service applications within hospitals.

5.6.3 Quality of the report

To assure that the report meets our goals of a qualitative report we have discussed the subject early in the project with Professor Per Flensburg at MSI, Växjö University. To get a view on how the company that we have chosen to practise their work, we organised a meeting with Richard Lindvall and Per Torlöf at Regionskåne. To follow-up this meeting we formulated a quality orientated science survey. We achieved our goal with the interview in the sense that we where able to analyze the answers given in the interview and use it in our empirical
studies. We also interviewed Welf Löwe professor of computer science at Växjö University. Pr. Löwe is specialised on the subject of Web service and is Research Coordinator at the Web Services Competence Center (WSCC) an organisation that promote understanding and use of Web Services technology. During the process of writing this report we have had a close contact with our supervisor Jonas Werner that has help us and guided us through the process.

5.6.4 Conclusion

When considering implementing an information system, we believe Web service can be the solution depending on the desired functionality of the system. Before applying a Web service in a company they should think of the factors of performance and security. The factor of performance is notable if the system must handle fast transactions with a large amount of data, then we believe a Web service may not be the best solution. To exemplify different functions that can secure Web service scenarios that might take place in a hospital, we have made a case scenario. We also produced the scenario to imagine how a Web service can be used to make the work routines more efficient. We came to the conclusion that all information in a hospital should be dealt with equal security measures. To be able to this we think that the developers and decision-makers should consider the rule framework of Web service Security. To ensure and complement the Web service Security framework an IT-policy document should be adapted to the Web service application. If this is not possible we believe that the authors of the IT-policy should revaluate or consider recreating the document.

All the security functions that we have brought up in this report should always be compared to the functionality to the system. We believe that it is also necessary to implement user friendly interfaces. If this is not the case the user may choose to go around the security procedures. We believe that many security flaws can be directly referred to the human factor.

The main reason that hospital have not yet fully implemented Web service solutions can be the consequence of that there has not been any sufficient security measures taken. We believe the time has come for hospitals to investigate if Web service can help their organization. In case they choose to use Web services, we advise them to follow Web service Security’s recommendations to produce a web service that is adapted to their security needs.
5.6.5 Future studies

The time schedule did not allow us to make any application of the concept Web service. This would be an interesting work to do in the future, especially the task of implementing a secure Web service of some sort.
6. Text references


Thuren, Thorsten (1997), Vad är källkritik, Källkritik. Almqvist & Wiksell

Göran Leth och Torsten Thurén (2000), Källkritik för Internet

Torsten Thurén (2002), Vetenskapsteori för nybörjare


**Figure Reference**


Figure 3. “SAML” Rosenberg, Remy, (2004), page 182

**Table reference**

Table 1. “A Web Service Security example” Rosenberg and Remy (2004), page 20

Table 2. “Time Stamp example” Rosenberg and Remy (2004), page 231

Table 3. “XML Signature example” Rosenberg, Remy, (2004), page 108

Intervju
Richard Lindvall och Per Torlöf
05-05-04

Del 1. Presentation

1. Vilken arbetsuppgift/titel har du?

   Jag är Projektledare inom området Informationssäkerhet. Sedan årsskiftet anställd på ITT – InformationsTeknikTjänster, dvs Region Skånes förvaltning för IT.

2. Hur länge har du arbetat med säkerhet inom IT?

   Drygt 10 år. I början mestadels ren IT-säkerhet och bl a ett försök att införa ”säker mail” baserad på X.400. Senaste 5 åren har jag arbetat med införande av ny infrastruktur för Informationssäkerhet, bl a införande av SITHS (Säker IT för Häls- och Sjukvård), dvs gemensam PKI för Vård-Sverige.

3. Har du haft någon tidigare anställning inom IT, så fall vad?

   - Klinisk Fysiologisk avd på UMAS, utveckling av system för fysiologiska undersökningar, bl a bildbehandling för isotopundersökningar.
   - IT-avdelningen UMAS
   - Region Kontoret, Avdelning IT
   - ITT

Del 2. Frågor angående Web services

4. Vad betyder Web services för dig?

   Nya protokoll SOAP, WSDL och UDDI…..
   XML, särskilt XML encryption/signature
   Meddelandebaserade gränssnitt.
   Lösst kopplade tjänster
   Möjlighet till SOA – Service Oriented Architecture (TOA på svenska! TjänsteOrienterad Arkitektur) och tjänster med standardiserade gränssnitt.

5. Vilket/vilka område inom vården anser du kan effektiviseras med Web services?

   Med Web Services Security får vi möjligheten att skapa IT-stöd för vården som uppfyller våra krav på Informationssäkerhet, dvs informationen är
   - signerad och därmed förvanskningsskydda plus att vi vet från vem den kommer (autentiserad)
   - insynsskyddad
   - icke-förnekbar
   - autentiserade användare(och tjänster) – dvs som är kända i den elektroniska världen.
**Med WebServices får vi möjlighet att skapa IT-tjänster i enlighet med intentioner i Carelink Plus dvs tjänster med gemensamma standardiserade gränssnitt (se info www.carelink.se där ni också finner info om SITHS och den gemensamma katalogen HSA där Häls-och sjukvårdscertifikaten publiceras)**

6. Tror du det finns hinder med att implementera Web services i vården?

   *Ja att man inte kan/orkar/förmår ”sätta ner foten” och ta de första stegen in i en ny infrastruktur. Det krävs att vi uppnår viss kritisk massa med bastjänster/stödtjänster.*

**Del 3. Frågor angående säkerhet med Web services**

7. Vilka funktioner inom Web services anser du önskvärda inom sjukvården?

   *Jag är lite osäker på frågeställningen. Menas funktioner/standarder inom WS som t ex WSDL, XML encryption/signature etc eller WebService baserade IT-stöd som sjukvården behöver införa?*

   a. Vilka attribut innehåller ovanstående funktion?

   b. Vilken information anser du vara känslig inom det/de områdena?

   *Vi ser inte anledning att direkt klassificera information. All patientinformation är sekretessbelagd och hanteras därefter.*

8. Vad kan du tänka dig hindrar användningen av Web services inom vården?

   *Se punkt 6*

   a. Anser du att man i dagsläget kan introducera Web Services i vården?

   *Ja*

   b. Motivera


9. Vilka säkerhetsfunktioner anser du kan lösa problemet med att skydda känslig information?

   *WS security med XML Encryption/Signature
   SAML (behörighetsegenskaper, standard - se www.oasis-open.org)
   XACML (regler, se www.oasis-open.org).*

10. Finns det någon annan viktig säkerhetsfråga du vill belysa.

    Inget svar gavs
Appendix "Interview with Pr. Löwe" and answers

Intervju
Pr. Löwe
05-04-21

Del 1. Presentation

1. Vad är du professor i?
   
   Datalogi.

2. Hur länge har du varit professor?

   3 år på Växjö Universitet.

3. Är du eller har du varit involverad i något WS Projekt nyligen?

   Ja, jag är inblandad i WCSS på viduem som är ett kompetens kluster. Vi har samarbete med W3C och Oasis, för att utveckla standards och därmed har ett gemensamt intresse.

Del 2. Frågor angående Web services

1. Varför är Web Services är ett framgångsrikt koncept? Motivera gärna

   Ja, WS löser två problem dels är det plattformsobeornde som ger stor frihet vid implementation. Dels Distributionen som erbjuder snabbare kommuniktion och transaktioner. WS är även relativt lätt att använda, det tar oftast inte lång tid för utvecklaren att komma igång. En annan anledning till att WS är och har blivit mer använt tror jag beror på att det fått mycket plats i media.

2. Vad anser du vara viktigt att tänka på för företag som överväger att införa Web services?

   Man ska inte överväga att införa web service utan först och främst tänka på att lösa problemet, kanske är web service en del av lösningen, kanske är något annat utvecklings verktyg bättre lämpat för att lösa problemet. Två viktiga aspekter när man överväger att implementera en WS är i ett tidigt stadié tänka på säkerhets och prestanda, som oftast är dyrare att anpassa i efterhand. Ofta tänker beställarna på säkerheten men är inte lika medvetna om prestanda kraven. En aspekt är hur många användare WS har och hur stora datamängder som skickas.
3. Vad anser du vara de största skillnaderna mellan traditionell systemutveckling och utveckling med Web services?


4. Har du någon erfarenhet av att implementera Web service i vården?

Nej