HØGSKOLEN I AGDER

Agder College

Security in the Wireless Application Protocol

Postgraduate Thesis
in
Information and Communication
Technology

By

Monica Storfjord

Grimstad, June 2000

Abstract

The necessity of being online wherever you are and at any time, have brought foreword the WAP technology. Solution based on banking, industry, and sale among others, is services and application that are on the market to day. Like in all new technologies the security issues in WAP is of great interest. The interest lies on both possible intruders and company that want to make a profit out of it by offering services. This assignment enlightens possible security problems in the WAP architecture, both in the security layer Wireless Transport Layer of Security (WTLS) and the WAP infrastructure.

The report is a result of the investigation and will be used as information on new technology for my employer, The Norwegian Intelligence Service (NIS).

In the version that exist as of to day (version 1.1 and version 1.2) the security-leaks in the security layer are to many, and to easy for an intruder to attack. Some of the security problems is a consequence of a cipher-suit on 40 bits, this is considered week in all literature about crypto-analysis. The designers of WAP applications got the responsibility to implement as much security as required into the solution. As of 14.January 2000 the export of strong encryption is regardless of their strength or type of technology. This means that the designers can implement cipher-suites bigger than 40 bits into the solution.

To avoid a lesser probability of man-in-the-middle attacks in the infrastructure a company should invest in a WAP Gateway or WAP Server. This will surround the WAP architecture with the security infrastructure inside a company. Based on the research in this report it is possible to draw the conclusion; independence is the key to maximum security. This will also be the preferable solution for NIS if operations goes wireless, but it is recommended that NIS carries out a comprehensive evaluation on WAP and type of bearer before even considering implementing the WAP technology.

The use of eXtended Markup Language as a base for the interfaces shown for the user is fully supported by the means of Wireless Markup Language and extended Style Language. The powerful style language makes it possible to implement more powerful features. This is verified in the demo application.

Preface

This postgraduate thesis is a part of the master of engineering degree in Information and Communication Technology (ICT) at the Agder University College. This last assignment is a closure on the education that lead to the title Master of Engineering.

This thesis is written for the Norwegian Intelligence Service (NIS) as information on the security issues in the Wireless Application Protocol. It has been a comprehensive and challenging task that required a lot of information gathering and understanding.

During the process Project Coordinator Rune Fensli has been my supervisor at the collage. He has been a big help structuring the report. I would like to thank him for giving me advice and guidance throughout the project. Another person who also contributed to the end result in this report is Senior Engineer Jon Robert Dohmen. He helped with the revision of the report at the end.

Grimstad
Spring 2000

Monica Storfjord

Contents

Lists of figures and tables

1 Introduction

The recent and significant changes in the business environment have been the growing demand for mobility. The mobility fills the needs that the employee might have to access the information at the organization wherever and whenever they fell like it. As a result of this, the Wireless Application Protocol (WAP) was developed.

WAP is a platform for cellular phones and other portable terminals, which provides an open universal standard for bringing Internet content and advanced value added services a user. Different mobile communications technologies are used in the military environment to maintain “real-time” communications between headquarter and the field, and the Norwegian Intelligence Service (NIS) wish to expand their knowledge within this area. The main focus of this assignment is the security issues in the WAP technology.

This report is made to enlighten the Norwegian Intelligence Service on new wireless technology. The choice of technology felt upon the Wireless Application Protocol. The main reason for this is that WAP is an entirely new technology on the market that is said to offer improved security, it supports multiple bearers and it is very straightforward to implement in existing applications and IT systems to the mobile environment.

An application has been made to demonstrate the technology against a remote-access database. The interaction between eXtended Markup Language and the Wireless Markup Language, which is the programming language used in WAP has been tested. The results of this will be available in the report.

1.1 The original task description

Project title:

Security in Wireless Application Protocol (WAP)

Description of the project:

The Norwegian Intelligence Service (NIS) wishes to expand their knowledge in mobile communication. Thus the new technology Wireless Application Protocol (WAP) is of great interest. The focus of this thesis will be the security from the mobile unit over the wireless interface and the end-to-end encryption.

A software application will be made as a demonstration of the functionality of WAP's ability to communicate with remote-access databases. This will happen as an insert and search in a database. The programming language will be in WML (Wireless Markup Language). This application will, if possible, be tested against reliability and functionality in the data transmission.

The application will be evaluated in relation to *i*Portal. *i*Portal is a common interface that lies over all the databases in the organization, thus making it easier for an employee to get access to the right databases. A part of the XML- structure (eXtensible Markup Language) between *i*Portal and the databases has been changed and released in connection to this thesis. The purpose of this is to make a realistic demonstration of the WAP technology connected up against the military needs.

1.2 A description of the assignment

In the WAP architecture of today there are several physical problems. Many of these problems occur because of the physical limitation that lies in the wireless area. Others are because of the GSM architecture (Global System for Mobile Communication).

The main goal of this thesis is to uncover possible security-problems and enlighten the reader upon the most secure solution concerning the infrastructure.

The task can be divided into three different parts;

1. Security issues in WAP
2. The evaluation on WAP in accordance to NIS
3. The design of an demo application

The more accurate description on these assignments will be described in the next subchapters.

1.2.1 Security issues in WAP

Costumer investing in new technology wishes to implement the system with optimized security on the infrastructure. WAP will be used in many e-commerce solutions and security is essential. Figure 1 shows the different parts in the WAP architecture where this report focus on security.

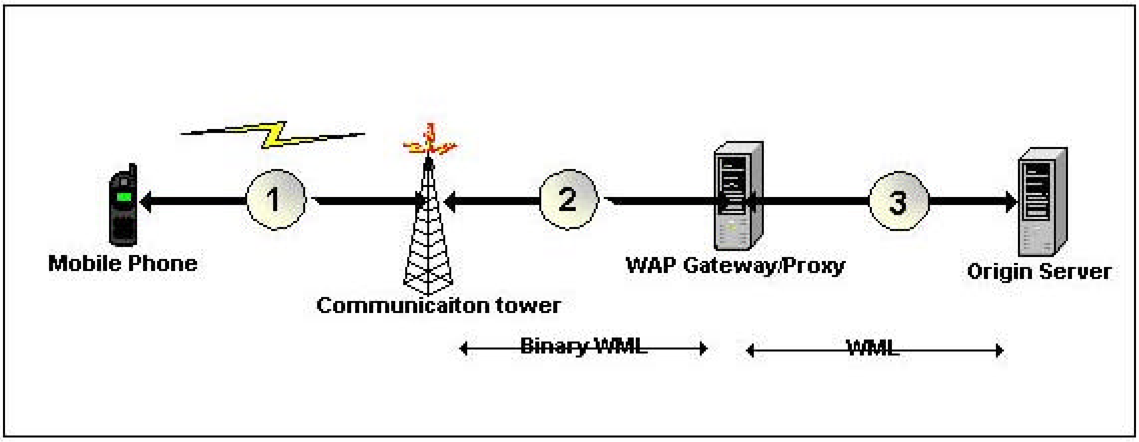


Figure 1 The security aspect in the WAP architecture

The different devices in Figure 1 are the hardware that is the basis in a WAP infrastructure. The mobile phone can also be any portable device supporting WAP. The mobile phone sends requests to the WAP Gateway/Proxy through the bearer. The WAP Gateway/Proxy gets the information of from the origin server and send the response to back to the mobile phone.

The numbers in Figure 1 indicates the main areas where security should be focused on. All of the three areas must be taken into consideration in this thesis. The three areas is described further underneath:

1. Security between the mobile phone and the antenna. Which security consideration that lies in the WAP technology regarding this issue.
2. Security between the antenna and the WAP gateway. Security considerations that lies in the WAP technology regarding this issue, and considerations that must be taken on the environment.

3. Security between WAP gateway and WAP server. Security consideration within the WAP technology regarding this theme and security within the Internet technology. Consideration concerning the environment regarding this issue.

The security theory and the solution will be of a general art taken mostly from the standardization organization, WAPForum.

Some commercial solutions that are on the market will be evaluated against the solution and compared to each other. The commercial solutions will be packages from RSA Security, VeriSign and Baltimore Technologies. RSA Security has collaboration with Ericsson on end-to-end security. VeriSign delivers WAP Server Certificate to organizations to enable secure connections with wireless devices. Baltimore Technologies delivers a package that lets the developer integrate the security layer (WTLS) into the application.

There will be different secure solution that will be supported by the documentation in this thesis. The secure solutions will, when it is possible, take into consideration different commercial security solutions that are on the marked.

1.2.2 Evaluation on WAP in accordance to NIS

To use WAP- or equivalent technologies NIS demands high security. There are lots of requirements that must come into consideration. Information regarding this is gathered from the Internet. [32: Datasikkerhetsdirektivet] This reference consists of the information regarding the Computer Security Directive in Norway. These will be the only documentation used to see if WAP is secure enough for NIS.

1.2.3 Designing a demo application

Following this report there is an application that will be a demonstration on how WAP is used in a secure environment. The security package Baltimore telepathy from Baltimore Technologies will be used to implement the security layer of WAP.

XML will be used to describe the actually content and structure of a document and individual applications interpret how the document is to be viewed. WML (Wireless Markup Language) will be used to display the information held in XML documents. The document will consist of information regarding field scenarios in NIS.

The solution between XML and WML will only be theoretically.

1.3 Limitations of the assignment

1.3.1 Security issues in WAP

This thesis will not mention how GSM can be configured in the most secure way. The reason for this is that GSM itself is a large issue.

1.3.2 Evaluation in WAP in accordance to NIS

Because of the limited documentation that is on the demands that NIS has on wireless communication, the solution mentioned in this report is compared to the rules found on Internet regarding common information security in the military. Thus this chapter will not be entirely correct compared to how new technology is evaluated and accepted or rejected in NIS.

1.3.3 Designing a demo application

The security features will not be integrated into the demo application. A login routing will be the only security feature that will occur in the solution. The application will be a demonstration for my employer on how the WAP-technology works in the real world.

2 Documentation

This chapter will consist of the theoretical documentation that will support the results in chapter four and the discussion in chapter five. First there will be a brief introduction of the WAP architecture.

2.1 An introduction to the Wireless Application Protocol

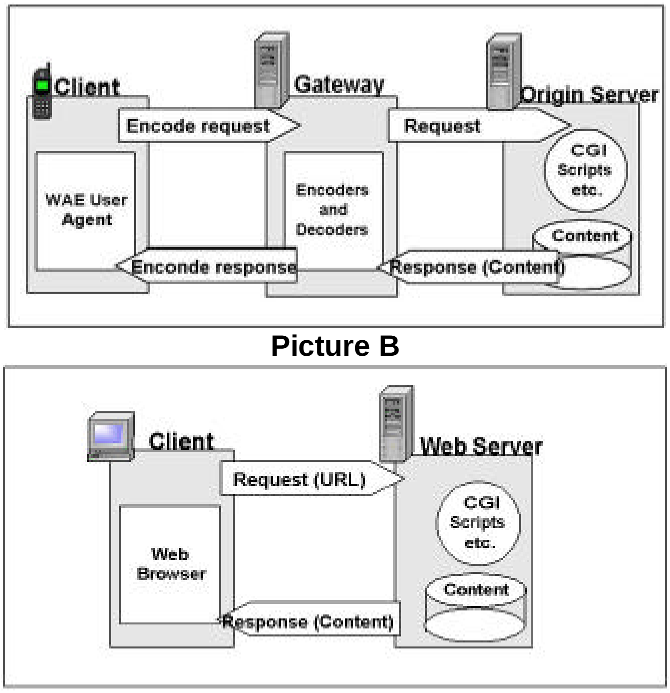
The WAP architecture is a result contributed by several major companies. All of the companies are members of WAPForum, who started the specification of WAP. In the beginning the only members of WAPForum were Nokia, Ericsson, Motorola and a little company called Phone.com. According to the WAPForum's web page the number of member in WAPForum, as of the third of May 2000, exceed 400 members. This number contains full- and associated members.

The most common devices to be used on WAP will be personal digital assistants (PDA) and cellular phones. These handheld devices tend to have less powerful CPU's, less memory, restricted power consumption, smaller displays and different input devices. At the same time wireless networks tend to have less bandwidth, more latency, less connection stability and less predictable availability. The WAP specification address these network characteristics and service provider needs by including new technology where appropriate and adapting existing network technology. [4: WAP Architecture].

2.1.1 The WAP Model

The obtained information about WAP is mostly from the specification on WAP that is obtainable from WAPForums web page. If necessary more information regarding the WAP model can be gathered on the online web page of WAPForum. This information is partly gathered form the WAP Architecture specification on reference four.

In accordance to the document about the WAP architecture the WAP programming model (Figure 2) is similar to the WWW programming model. This is convenient for the programmers that will meet a well-known interface. Optimizations and extensions have been made in order to match the characteristics of the wireless environment. In some places of the WAP technology, existing standards have been adopted or have been used as a starting-point for the WAP technology.



Picture A

Picture B

Figure 2 Picture A: WAP programming model. Picture B: WWW programming model.

WAP programming model: The content encoders on the client translate WAP content into a compact encoded format to reduce the size of data over the network. When the byte-stream comes to the gateway, the gateway translates requests from the WAP protocol stack to the WWW protocol stack. The request is then sent to the origin server and the client will receive an encoded response.

As shown on picture A in figure 2, the physical devices in the WAP architecture mainly consist of a client, a gateway and an origin server.

Client

A micro browser on the client's wireless terminal consists of the user interface and is just like a standard web browser. The WAP architecture requires that the mobile phones have a micro-browser, and more memory compared to ordinary phones to handle the WAP stack. This browser is the client's interface to the WAP-content on Internet or Intranet.

Gateway

It is also required that the mobile network got a WAP gateway/proxy connected to it. The gateway is very often a WAP proxy. This allows content and applications to be hosted on standard WWW servers and use of WWW technologies.

The WAP gateway provides a transition between the Internet and different non-voice mobile services. These can in accordance to WAPForum FAQ information, be bearers like Short Message Service (SMS), Circuit Switched Data, Terrestrial Trunked Radio (TETRA) and General Packet Radio Service (GPRS). In short the WAP gateway gets information from a web server, process it, and sends it out on the mobile network, which directs it to the WAP client.

Origin Server

The origin Server contains the WML-pages that the clients are able to browse. It is possible to create an origin server with the WAP proxy/gateway functionality. This can be used to support end-to-end security solutions, or applications that require better access control or a guarantee of service, for instance WTA.

2.1.2 Security Model

The security infrastructure in WAP focuses on providing connection security between a WAP client and server. The WAP architecture provides end-to-end security between WAP protocol endpoints. If a client and an origin server desire end-to-end security, they must communicate directly using the WAP protocols. End-to-end security is also achieved if the proxy-gateway is trusted. A proxy-gateway is trusted if it is located on the same secure place as the origin server.

A more elaborated and detailed description on security issues comes in chapter 2.2.

2.1.3 Use of WAP

This is an example taken from the “Official WAP book”, page 19. In this example the physical devices in the WAP architecture expands to contain a computer that serves a HTML filter and a Wireless Telephony Application (WTA) Server as shown in figure 3.

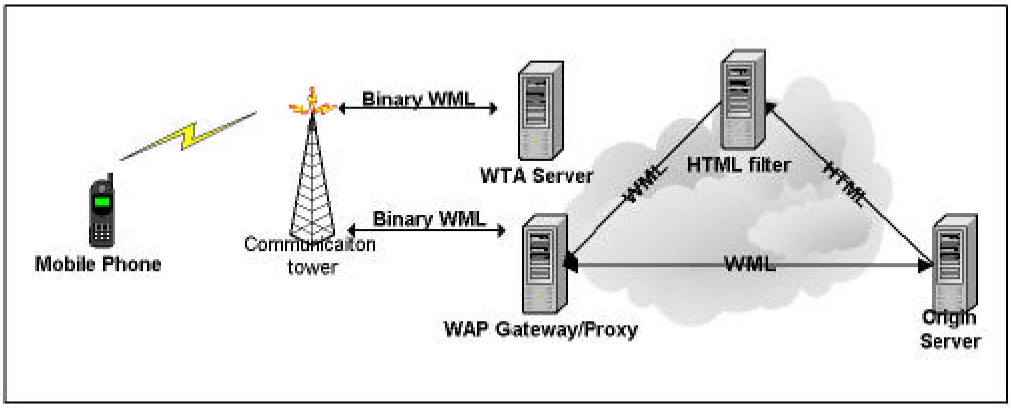


Figure 3 Example illustrating the work of WAP.

The HTML filter converts www-content (HTML) from the web-server into WAP-content (WML). This is sent to the WAP-proxy, that transports it binary to the client. The WTA-server is an example of an origin- or gateway server that responds to requests from the WAP client directly. It is used to provide access to features of the network provider’s telecommunications infrastructure.

In the example on figure 3 the client (mobile phone) communicates with two servers in the wireless network. When the client requests for a page on the origin server, the WAP-proxy translates WAP-requests, thereby allowing the WAP client to submit requests to the origin server. The origin server looks at the request and if the requested page is WAP-content it sends it directly to the WAP-proxy. When the requested page is an HTML-page the origin server sends it to the HTML filter machine that will process it into WAP-content and send it to the WAP-proxy. When the response comes back to the WAP-proxy it encodes the response into the compact binary format understood by the client.

WAP is designed in a layered fashion. The layers are shown in Figure 4. This is done in order to be extensible, flexible and scaleable. The session, transaction, security and transport layer is accessible directly for the many services and applications. Each layer makes the layer below invisible for the layer above.

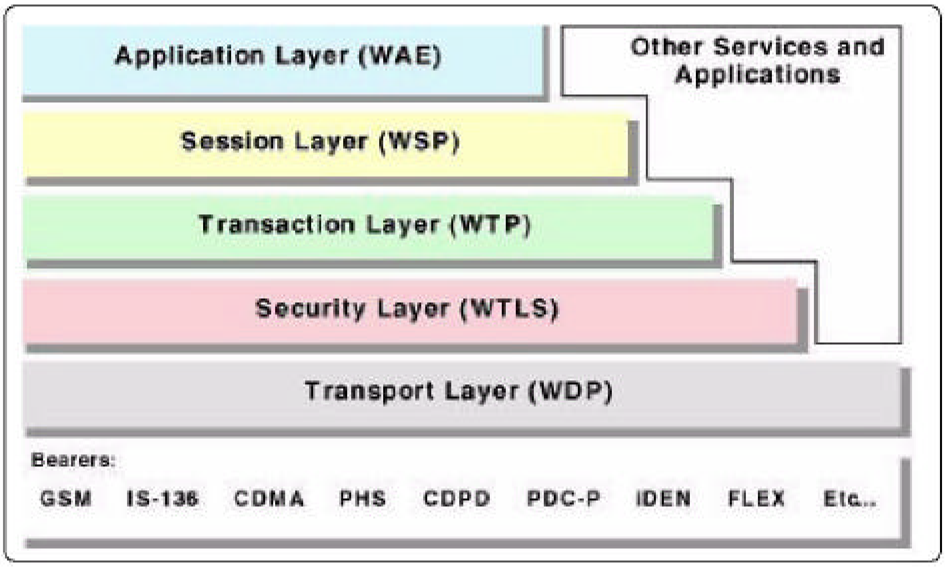


Figure 4 The layered fashion of the WAP protocol.

This picture is the official picture that WAPForum uses when showing pictures of the layers in the WAP architecture. Each layer is optional and other services and application can lay upon every layers as shown in the picture.

Wireless Application Environment (WAE)

This layer is a mixture of WWW and Mobile Telephony technologies. It includes a micro browser environment containing functionality like WML, WMLScript and WTA.

WAE includes different user agents that each has it own purpose. A user agent is the user interface attached to the current service in use on the wireless device. The user agents can in the wired world be compared to Microsoft Internet Explorer and Netscape Navigator. WML and WTA are examples of these. The WTA (WTAI) function allows the user to interact with mobile-phone features and other user agents not specified by WAE, like the calendar and phonebook.

Wireless Session Protocol (WSP)

The main task of the WSP is to set up a session between a client and the WAP Proxy/Gateway. This session handles session establishment and communication interrupt. Communication interrupt will for instance happen with the change of a bearer. The session has the ability to go into suspend mode if no communication is needed for some time, and later resumed.

The WSP consists of two configurations of the stack (services), a connection-oriented and a connectionless. The connection-oriented service operates above the transaction layer, Wireless Transaction Protocol (WTP). The WTP provide a reliable transmission. This means acknowledge of each package sent, and retransmission if not. The connectionless configuration offers a datagram service. This means that sent packages is not acknowledged when they arrive at the receiver, hence no guarantee of delivery is offered.

This security support (WTLS) is not provided by the WSP protocols directly. In this regard, the Security layer is modular. WSP itself does not require a Security layer; however, applications that use WSP may require it.

Wireless Transaction Protocol (WTP)

This is a light transaction protocol that is appropriate on cellular phone. It is responsible for control of transmitted and received messages. Messages that are sent gets a unique identifier, this obstruct the opportunity that the message is received twice. WTP has three different message classes.

1. Unreliable with no result message. No retransmission if the message is lost.
2. Reliable with no result message. The receiver sends acknowledge. Otherwise the message is resent.
3. Reliable with reliable result message. When the result package is received at the sender, the sender sends a acknowledge communication party.

The WTP can be extended with the functionality of segmentation and reassembling messages. Because of the constraint of the wireless bearers these functionalities have not been implemented in the standard configuration.

Wireless Transport Layer Security (WTLS)

This is the security layer in the WAP architecture and is comparable to the Transport Layer Security (TLS) used on Internet. WTLS has been optimized for use over the narrow-banded communication channels. In chapter four and Appendix A there will be more information regarding this layer.

Wireless Datagram Protocol (WDP)

This is the transport layer in the WAP architecture. WDP offers a consistent service to the upper layers of WAP and communicate transparent over the different bearer services.

The WDP specification lists all the bearers that are supported and the techniques used to allow WAP protocols to run over each of them. If WDP is used on a bearer supporting User Datagram Protocol (UDP), the WDP is not needed. On other bearers like GSM the datagram functionality is provided by WDP. This layer can be extended with features like reassembling and error reporting.

2.1.4 WAP version 1.2

WAP 1.2 will support Push services (proactive delivery of information from a WAP Gateway to a WAP terminal), User Profiles, WDP Tunneling, WMLscript, CryptoLibrary, Wireless Telephony Application, Wireless Application Environment enhancements and other features.

2.2 Security on the bearers GSM and GPRS

2.2.1 GSM

Two aspects of wireless communication do not provide the same level of protection as a fixed network:

- ?? Radio Path: Interception of data on the air interface
    - Loss of confidentiality of user data
    - Loss of confidentiality of user signaling information
    - Loss of confidentiality of user identity information
- ?? Access to mobile services: Illegitimate access to services which needs to be prevented

This can be prevented if features like subscriber identity confidentiality, subscriber identity authentication, user data confidentiality and signaling information confidentiality is implemented.

These features are:

- ?? International Mobile Subscriber Identity (IMSI), uniquely identifies the subscriber
- ?? Temporary Mobile Subscriber Identity (TIMSI), is sent in most instances to prevent an intruder to gain information on the resources the user is using, tracing the location of the user and matching the user and the transmitted signal.
- ?? Individual Subscriber Authentication Key (Ki)
- ?? Challenge-Response mechanism
- ?? Temporary randomly generated ciphering key (Kc)
- ?? Subscriber Identity Module (SIM)

Different algorithms are used to make the GSM-system even more secure:

- ?? A3 – used for authentication purposes
- ?? A8 – key generator algorithm, commonly similar to A3
- ?? A5 – used to encrypt voice and signaling data

This information is gathered from reference number 14 regarding the security in GSM.

2.2.2 GPRS

GPRS can be seen as an access networks to other network, which offer mobility as a value added service. It offers possibility that traveling employees can communicate with corporate LAN very easily even from abroad. To be able to use GPRS for transmitting confidential or private data the system must offer authentication and security functions. GPRS offers ciphering function over the radio network as well as authentication to the GPRS network.

The authentication inside the GPRS network is pretty good. If the algorithm used by a single operator is compromised the effect is not global. However, the operator must be very careful with its A3 algorithm, because if the authentication is not trustful lots of damage may be caused. However, authentication does not work against copying of SIM. If it can be copied then unauthorized user may use the identity of the authorized user until the subscription is invalidated.

The security of the transmitted data cannot be kept cryptographically excellent. Because the GEA is secret it cannot be well evaluated. Most probably, if the algorithm is compromised, the transferred data can be deciphered relatively easily. Also the key length, 64 bits, is too short nowadays. Another thing is that transmission is ciphered only between the SGSN and the MS. This makes lawful interception very easy which can be seen to hurt user's privacy.

GPRS does not offer ready security solutions for interworking between different GPRS networks nor interworking between GPRS network and intranet. Merely, possibilities are created as well as suggestions are given but they are left on responsibility of the GPRS operators and intranet administrators.

Because data between the MS and corporate LAN is almost always transmitted over insecure networks, the GPRS security functions are not enough. To make transmission secure an external intranet protocol is needed. One solution is to use IPSec. It fits well to the IP world and can be seen safe enough. Most probably it will become de-facto standard and companies can take advantage from IPSec development. IPSec restricts lawful interception a little bit because contents of the packets are relatively difficult to extract. However, user's location can be still tracked easily.

To gather this information the online web address in reference 18 was used.

2.3 Security issues in WAP

Commonly known on Internet is that the more levels of security, the more difficult is it to break through to a system. The WAP architecture got different bearers to carry the signal on the wireless network. The most commonly used today is GSM. Chapter 2.2.1 has some information on the security features in this system.

As shown in Figure 5 the WAP Gateway uses SSL to communicate securely with the web server. This ensures privacy, integrity and server authenticity. Towards the wireless network the WAP Gateway uses the security layer in the WAP protocol, WTLS.

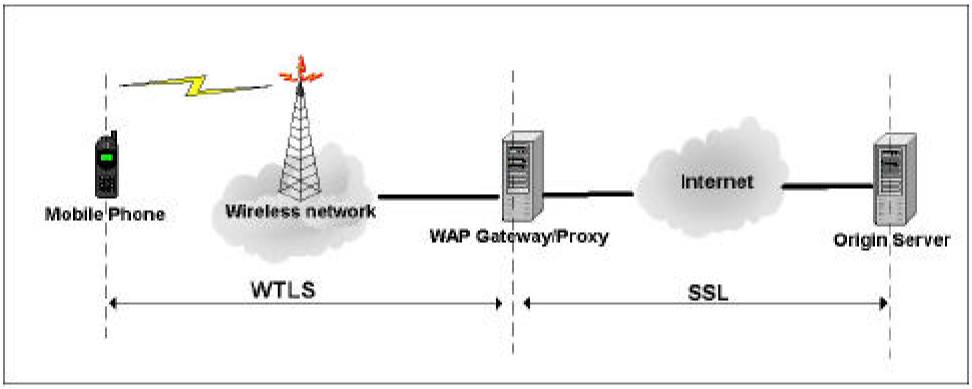


Figure 5 Security protocols in the WAP architecture.

From the mobile phone to the WAP Gateway the WAP architecture will use WTLS. In the WAP Gateway there will be a transition from WTLS to SSL. SSL is the most common security protocol used on Internet, and it is the most likely one to exist in the WAP architecture.

In essence, the WAP gateway is a bridge between the WTLS and SSL security protocols. WTLS processes security algorithms faster by minimizing protocol overhead and enable more data compression than traditional SSL solutions. As a result, WTLS can perform security well within the constraints of a wireless network. These optimizations mean that smaller, portable consumer devices can now communicate securely over the Internet.

The translation between SSL and WTLS takes milliseconds and occurs in the memory of the WAP gateway, allowing for a virtual secure connection between the two protocols.

This information was gathered from white paper “Understanding Security on the Wireless Internet” written by phone.com [10].

2.3.1 Terminal

As you could see on Figure 5 the terminal uses WTLS to provide privacy, integrity and authentication between itself and the WAP Gateway. [10:Understanding security on Internet]

Phone.com incorporates RSA Security encryption technology into the WAP-compliant UP.Browser? terminal and Up.Link? Server Suite products. Embedded into numerous mobile phones, UP.Browser utilizes RSA Security technology to provide secure wireless information access from wherever a consumer may be. In accordance to a company press release from Phone.com on 1'st of February UP.Browser v4.1 was designed as a WAP 1.1 Class C device includes all required layers of the WAP stack. Phone.com anticipates that the UP.Browser v4.1 will ship with 128-bit encryption for US and international markets, based on recent US government policy decisions and phone.com's receipt of US exports authorization. [16]

Ranging from smart phones like the Nokia Communicator 9000 to large, enterprise WAP servers, Nokia incorporates RSA BSAFE security components into its products to enable them to offer e-business services for the mobile Internet market. Nokia relies on RSA Security encryption technology to bridge the wired and wireless Internet worlds and provide a seamless user experience. [17: RSA BSafe]

2.3.2 WAP Gateway

At the Gateway the Adaptation layer terminates and passes the WDP packets on to a WAP Proxy/Server via a protocol, which is the interface between the Gateway that supports the bearer service and the WAP Proxy/Server (Figure 6).

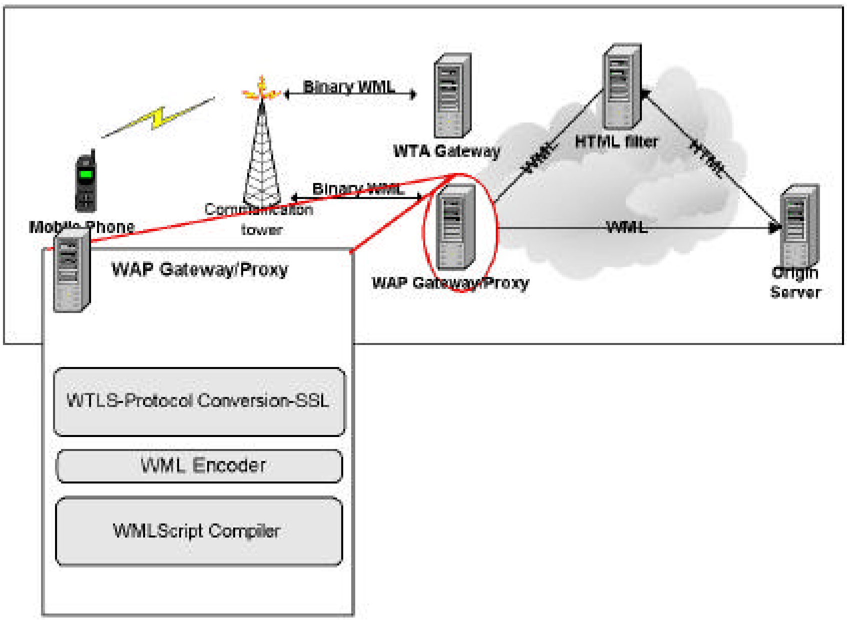


Figure 6 The features of the WAP Gateway.

The WAP Gateway contains transition features from WTLS to SSL and vice versa. It also contains a WML encoder that makes the information that goes over the wireless net into byte-code. The WMLScript Compiler takes the script as input and compiles it into byte-code.

For example, if the bearer is GSM SMS, the Gateway would be a GSM SMSC and would support a specific protocol (the Tunneling protocol) to interface the SMSC to other servers.

The sub-network is any common networking technology that can be used to connect two communicating devices; some examples are wide area networks based on TCP/IP or X.25, or LANs operating TCP/IP over Ethernet. The WAP Proxy/Server may offer application content or may act as a gateway between the wireless WTP protocol suites and the wired Internet.

This information is collected from reference 15 from phone.com and the official book on the complete standard in WAP [15: Official WAP].

WAP Gateway security considerations

Suppliers of the WAP gateway and network operators take every possible measure to keep the WAP gateway secure itself by:

1. Ensuring that the WAP gateway never stores decrypted content on secondary media.
2. Ensuring the removing of unencrypted content from the memory in the WAP gateway as fast as possible.
3. Securing the WAP gateway physically so only authorized administrators have access to the system console.
4. Limiting the access to the WAP gateway so that it is not accessible from a remote site outside the carrier firewall.
5. Applying all other security precautions used to protect billing systems and the Home Location Register to the WAP gateway.

As mentioned the WAP gateway uses WTLS to provide privacy, integrity and authentication between itself and the WAP browser client. It is based on TLS 1.0, and goes beyond TLS 1.0 by incorporating new features such as datagram support, optimizes handshake and dynamic key refreshing.

The Nokia Solution

The company policy in Nokia is to sell the WAP-gateway to ensure maximum security.

“In principle, the WAP gateway functionality can be located in e.g. teleoperator's domain in a way that only the company hosts the application server. Having the Nokia WAP Server in the company's own control provides clear benefits compared to the use of external WAP gateway.”

In accordance to Nokia if the companies own their own Gateway the following benefits will occur: security, independence, control, access to Intra- and Extranet and Quality of Service (QoS).

Security

The company running the Nokia WAP Server can have end-to-end secure WAP service from the WAP terminal to the Nokia WAP Server. If the company did not control the WAP Gateway functionality, there would be risk for man-in-the-middle attack at the point where the WAP gateway is located.

Independence

A company is able to provide WAP services to all its customers or employees independently from operators. This is possible because access to the WAP service can be implemented via Circuit Switched Data. A company can own, or outsource necessary infrastructure, such as a modem pool for that purpose.

Control

Through control over the Nokia WAP Server, the company has control over their own service implementation and changes are easily implemented when required. Also, through control over the Nokia WAP Server, the company can control who is accessing the services and use powerful security tools to restrict access to services.

Access to Intra- and Extranet

Through control over the Nokia WAP Server in the company network, company can let employees' access internal services and provide customers access to extranet type of services more easily and with less concerns on the security of business critical data.

Quality of service

By owning and controlling the WAP service implementation, the company can ensure the quality of the service. If the operator's WAP gateway was used for accessing all companies' internal information systems, the operator's gateway could become a bottleneck: the situation would be similar as if all web servers would be hosted by operators.

The information regarding the Nokia server is gathered online [7: Main benefits]

2.3.3 Digital Signature and Client certificate

Our current focus is, broadly, on establishing trust in the new medium of the Web. This is a difficult problem, involving both social and technical issues. Trust is established through a complex and ill-understood social mechanism including relationships, social norms, laws, regulations, traditions, and track records. Our activities are chosen to focus on specific areas that are both important and tractable. [11: WAPForum–W3C Cooperation]

This is regarding general rules regarding the protection of confidential documents at a site.

Restriction by user name and password:
Restriction by user name and password also has its problems. A password is only good if it's chosen carefully. Too often users choose obvious passwords like middle names, their birthday, their office phone number, or the name of a favorite pet goldfish. These passwords can be guessed at, and WWW servers, unlike Unix login programs, don't complain after repeated unsuccessful guesses. A determined hacker can employ a password-guessing program to break in by brute force. You also should be alert to the possibility of remote users sharing their user names and passwords.

Another problem is that the password is vulnerable to interception as it is transmitted from browser to server. It is not encrypted in any meaningful way, so a hacker with the right hardware and software can pull it off the Internet as it passes through. Furthermore, unlike a login session, in which the password is passed over the Internet just once, a browser sends the password each and every time it fetches a protected document. This makes it easier for a hacker to intercept the transmitted data as it flows across the Internet. To avoid this, you have to encrypt the data. [12: WWW Security FAQ].

Client/User authentication:
User verification a procedure for determining, and verifying, the identity of a remote user. User name and password is a simple form of user authentication. Public key cryptographic systems, described below, provide a more sophisticated form authentication that uses an un-forgeable electronic signature. [10: WWW Security FAQ].

Public Key Infrastructure (PKI):
Public key cryptography is a relatively recent development compared to symmetric key cryptography. In public key operations, two separate keys, one distributed publicly and one held privately, is used for each secure transaction. A secure operation is done with one key and undone with another. In other words, a pair of keys is required for a single transaction. The two principal operations in public key cryptography are encryption and digital signatures.

Through encryption and digital signatures, public key cryptography provides the five elements of network security: confidentiality, access control, authentication, integrity and non-repudiation.

Public key cryptography is computationally intensive, and therefore slow. It is impractical to use public key cryptography to protect all data. Instead a combination of symmetric key and public key techniques provide the best security for real-life use. Data is encrypted once for all recipients using a symmetric key. The symmetric key is, in -turn, encrypted for all recipients using each recipient’s public key.

At the heart of the PKI is the management of trust. The concepts of third-party trust and direct trusts are fundamental to the implementation of any network security product. Two strangers can trust each other if they each have a relationship with a common third party, and that third party vouches for the trustworthiness of the two people.

A Certificate Authority (CA) is a trusted entity whose central responsibility is certifying the authenticity of users. A network user's electronic identity issued by a CA is much like a passport in that it is the user's proof of being trusted by the CA. Anyone who trusts the CA should, through third-party trust, also trusts the user. [13: Entrust Tech., All about…PKI].

2.3.4 Origin Server

The origin server contains the WML-pages that the clients are able to browse.

It is possible to create an origin server with the WAP proxy/gateway functionality. This can be used to support end-to-end security solutions, or applications that require better access control or a guarantee of responsiveness, for instance WTA

2.3.5 Wireless Transport Layer of Security (WTLS)

This chapter will be used to enlighten the reader about the main features in WTLS. The reader should not put an effort into understand this information entirely.

The WTLS layer is modular, and it depends on the required security level of the given application whether it will be used or not. The WTLS technology is derived from the Transport Layer Security (TLS) used on Internet, which again is based on Secure Sockets Layer (SSL). The difference is that the WTLS protocol is optimized for low-bandwidth bearer networks with relatively long latency. It can be used on both connectionless and connection-oriented mode. If it is used, it is always placed on top of WDP.

WTLS provides the upper-level layer of WAP with a secure transport service interface that preserves the transport service interface below it. In addition, WTLS provides an interface for managing (e.g., creating and terminating) secure connections.

The primary goal of the WTLS layer is to provide *privacy, data integrity, authentication* and *Denial-of-service* protection between the client and the application server.

Privacy/Confidentiality:

Facilities in WTLS that hinders malicious nodes to intercept the data stream. This is done with the help of encryption of the data stream.

***Data integrity**:*

To ensure uncorrupted and unchanged data between the client and application server. To do this Message Authentication Code (MAC) is used.

***Authentication**:*

Facilities to authenticate the terminal and application server using digital certificates.

***Denial of Service**:*

Rejecting and detecting data that are not successfully verified. WTLS makes *denial-of-service* harder to accomplish.

Applications are able to disable or enable WTLS features depending on their security requirements. For instance if privacy is implemented on a lower level this can be disabled.

As you can see on Figure 7 the WTLS is a layered. The four protocols that are above the record layer are called clients.

This information is not easy to comprehend and if more information is needed it can be gathered from the specification documents on the WAP Architecture (30.april 1998) [4], the official book on WAP [15] and the white paper concerning security from AU System [10].

Record Protocol

When the record protocol receives a record from the layer above that is going to be transmitted, it optionally compresses the data, applies a MAC to it and encrypts it, before the package is sent. When the record protocol receives a record it decrypt it, verifies and decompress it before sending it to higher-level clients.

To optimize the transport of records, several of them can be transported in one Service Data Unit (SDU). This is normal to do with records that have a logic connection like the handshake records.

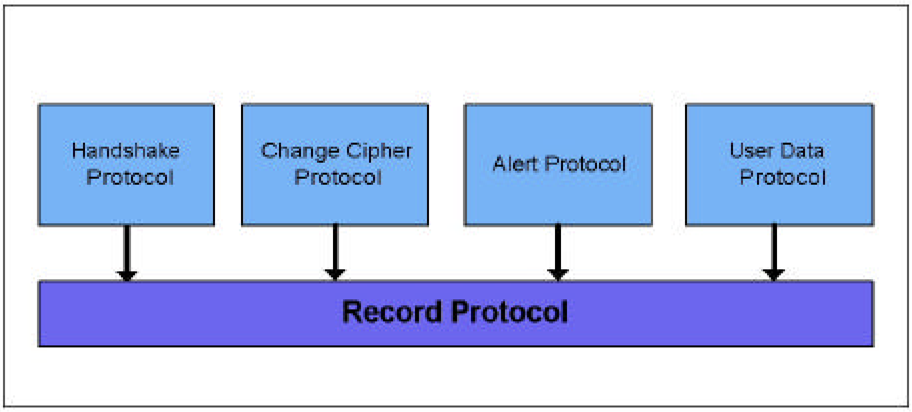


Figure 7 The record protocol and its clients

This figure shows that the four protocols handshake, change cipher, alert and user data will send the information to the record protocol. The record protocol will then again send this to the receiver.

Handshake

The handshake protocol is responsible for negotiation a secure session. In the connection phase all of the necessary security parameters are agreed upon. This can include cryptographic algorithms, key lengths, key exchange, and authentication. When a secure connection is established the client has the possibility to send secure data over the net.

Cipher Spec Protocol

This protocol implements to signal transitions in the ciphering strategies. It consists of a single message, which is encrypted and compressed under the current connection state. The message consists of a single byte of value 1. The reason to send this protocol is to notify the other party that subsequent records will be protected under the newly negotiated Cipher Spec and keys. If the cipher spec is NULL, all security in WTLS is “turned off”.

Alert Protocol

Alert messages transport how critical the messages are and a description of the alert. Alerts use a four-byte checksum that are calculated from the last record received from the other party. The receiver of the alert should verify that the checksum matches with the message earlier sent.

User Data Protocol

Consists of the payload that the terminal wishes to send.

WTLS Classes

Table 1 shows that the WTLS implementations may have support for various features. The specification sets different classes to make it easier to select these features. A class may have mandatory (M) or optionally (O) support for the various features. Certain features are not yet defined in the current version of the specification. The current version of the WTLS specification covers all the features in Class 1 (WTLS 1.2).

Table 1 WTLS Classes

FEATURE	CLASS 1	CLASS 2	CLASS 3
Public-key exchange	M	M	M
Server certificate	O	M	M
Client certificate	O	O	M
Shared-secret handshake	O	O	O
Compression	-	O	O
Encryption	M	M	M
MAC	M	M	M
Smart Card Interface	-	O	O

NOTE: If the Cipher Spec is NULL it is important to know that WAP offers no security.

Anonymous Handshake

This can be established using RSA or Diffie-Hellman for key-exchange. With RSA, the client generates a secret value and encrypts it with the server's uncertified public key extracted from the server key exchange message. With Deffie-Hellman the server's public value is contained in the server key exchange message and the client's is sent in the client key exchange message.

Completely anonymous handshake do not protect against active man-in-the-middle attackers. With the help of server authentication or tamper-proof channel to verify that an attacker did not replace the finished messages this can be avoided. [13: Official WAP, p. 616]

Key Refresh

The passive key refresh mechanism of WTLS makes it possible to update keys in a secure connection without handshaking. Key refresh makes crypto-analysis less attractive for an attacker because keys will be invalidated regularly and the material that can be gained is limited. This is particular useful in environments, where export-restricted encryption is used and handshaking is expensive. [13: Official WAP, p. 616]

Denial-of-Service Attacks

Since WTLS operates on top of datagrams, the implementation should pay special attention to preventing denial-of-service attacks. It should take into account that some networks transport addresses may be forged relatively easy. To avoid this it is not possible for an attacker to break up an existing connection/session by sending a single message in plaintext from a forged address. [13: Official WAP p. 616]

2.3.6 Security package from Baltimore Technologies

Baltimore Technologies

The software package, Telepathy WST that comes from Baltimore Technologies allows the developer to build in wireless e-security. To be more specific the developers will be able to integrate confidentiality, integrity and authentication. With the help of Public key Infrastructure it is also possible to implement authorization, integrity and non-repudiation.

When configuring a support service, for either a client or a server, you need to construct a list of cipher suites. There are four different strengths of cipher suites:

Export strength:
These suites contain 40-bit symmetric algorithms (RC5-40, DES-40) and either the SHA-1 or MD5 hash algorithm.

Non-export strength:
These are symmetric algorithms of at least 56 bits (DES, Triple DES, RC4-128) and either SHA-1or MD5.

Strong:
These are 1024-bit or higher asymmetric algorithms (RSA or Diffie-Hellman) combined with 128-bit or higher symmetric algorithms (Triple DES, RC4-128) and either SHA-1or MD5.

Mixed strength:
These cipher suites contain a full combination of all the above. Export 1024-strength: These cipher suites are experimental suites supporting recently exportable 1024-bit asymmetric and 56-bit symmetric algorithms.

If the cooperation's have very strong requirements and do not trust the RC5 or MD5 it is possible to create cipher-suites that suit the requirements of the cooperation. Baltimore Technologies recommend using Triple DES for maximum security for cooperation's. [6: WSecure White Paper]

2.4 Theory on the evaluation of a new system in NIS

The Headquarter of Defense in Norway has a department (FO/S) that takes care of the evaluation of all new communication systems. FO/S is a service-provider for the diplomatic-services, the military and the communication that civil government administration or other department must have with the military when consideration stand-by.

If the reader wishers to read more on this issue more information regarding this lie online in accordance to reference 32.

2.4.1 Preface

This directive became active 1.martz-1998. The directive with appendix will secure that: the system have function and protection so that:

- The information not will be known to intruders (confidentiality)
- The information is not being altered by persons not authorized (integrity)
- The information is accessible for authorized users (availability)

This directive contains rules for electronic computations of information that, in accordance to the security-instruction, got the classification restricted, confidential or secret.

Electronic computation of information classified top secret or cosmic top secret is generally not allowed. The needs for computations of information with this classification will have to go through FO/S.

These directives apply classified computer systems, both stationary and mobile, this includes local and extern communication-systems.

The security-demands here are minimum. They are based on risk-evaluation related to classification and the way of operation. Each owner of the computer-system must take into consideration if the system needs protection beyond the demands in this directive.

The goal for security data processing is to attend to confidentiality, integrity and availability. The primary goal is the protection of confidentiality, but protection for integrity and availability is also necessary. [34: DSD – Formål]

2.4.2 Responsibility for computation of information on a external system

The owner of the system where the task is preformed has the responsibility for the security in the computation of the information. The employee has the responsibility to make a correct classification of the material, and must ensure if the system is approved when it comes to security concerning the classification and professional secrecy.

2.4.3 External communication

Secure Confidentiality

Classified computer communication between controlled environments must be protected with crypto-devices and a method to administrate the keys that are approved by the FO/S.

Secure Integrity

If the information is in danger of being altered on the way to destination, or fake information can be introduced, extra security-initiative must be taken. This can be to include secure integrity, check the users, digital signature and file-encryption. If more severe damage can occur the integrity of the information should be protected by the means of encryption method, for instance check-sums or digital signatures.

Crypto-algorithms

Crypto-algorithms to secure confidentiality must be implemented in the hardware. It must be NATO standard or an algorithm approved and controlled by FO/S. [35: Ekstern kommunikasjon].

2.4.4 Security evaluation

Security approval is a decision that a computer system is allowed to use classified computer processing in its operational environment.

The following computer systems must have an evaluation on the security.

- ?? Computer systems that will be processing classified information by the means of dedicated or multilevel method of operation.
- ?? Computer systems that will be processing classified information by means of multilevel method of operation
- ?? Crypto-equipment and methods to do the key-management.

The basis to get approved is an evaluation, control and possible a security-evaluation of all the security-initiatives and security-mechanism, and all the other conditions that can have significant on the security. This means that the following factors must be described in the basis-document:

- ?? Classification and the type of information
- ?? Users and organization
- ?? Physical security-attempt
- ?? The menace of tempest
- ?? Technical security-attempt of the system
- ?? Computer-communication
- ?? Connection to other computer-system
- ?? Procedure and instructions

An evaluation based on the basis-document will reveal possible holes in the security-attempt and will prevent that the development of the system continues before these holes is corrected. [33:DSD – Organisering].

2.5 Demo Application

This chapter will include an explanation on the two tools that I have used in the development of the application. First there will be an explanation on the connection between WML and XML.

2.5.1 XML and WML

Extended Markup Language (XML) is used to describe the actually content and structure of a document, and individual applications interpret how the document is to be viewed.

In accordance to an article written by WAP Forum on April of '99 [21: WAP] the use of eXtended Style Language (XSL) will automatically translate the content in xml-documents into content suitable for HTML (HyperText Markup Language) or WML (Wireless Markup Language). Likewise, content written in well-formed WML can also be translated to other XML-based markup languages using different XSL style sheet.

The article also describes the future of WML; "While the technology for universal content is still being developed, WML has been designed to be an integral part of this technology. Application developers can feel secure using WML today, knowing that there will be a migration path to the future.

2.5.2 Application

In accordance to the problem description in 3.2.3 there will be a theoretical description on the connection between XML and WML. This is based on the use of XML in a new system called *i*Portal in NIS.

A short description on *i*Portal

The purpose of *i*Portal is to integrate the different databases in NIS. The system will establish a information-portal that will function like a common entrance to all the databases in NIS. The meaning of the portal is to get an easier and faster access to the data, and also processes to be able administrate the access to the databases based on characters and digital certificate.

Document Type Definitions (DTD) is used to ensure that all documents are on an unambiguous format, in such a way that both the sender and receiver can read it. The DTD's contains specifications on how an XML-document must be build up. The document will be evaluated against a DTD when accessed. [30: Document Type Definitions].

The main function in *i*Portal

Totally there are three different XML-documents used in *i*Portal. These are search, answer and abort search. Each of these has a DTD. The DTD's in on the application-server and is accessible through a url.

The search routine will put together by metadata-conditions asked by the user, and will contain both sub-system specific conditions and general conditions. If the sub-systems notice that the condition mentioned is not relevant, the sub-system should ignore these conditions.

A sub-system will answer a search with one or more hits that will be showed to the user. A system can choose to compose one XML-document with all the hits and make a summary on the hits or to split up the answers in more XML-files. [31: *i*Portal Forstudie]

Abort a search. The metadata-conditions contained in an XML-document to abort a search is search id, user id, password and system name. [30: Document Type Definitions].

3 Method

This chapter consists of information regarding the collection of literature on the various issues in the report. The information collected is in chapter two and appendix A.

3.1 Literature

The information regarding the security layer is taken from various places. Because the information about WTLS in the specification was rather difficult to understand, I put an effort in collection the information from various places on Internet. Since the information became a little bit particulars I made the whole information about the security layer into Appendix A. The information in chapter four regarding WTLS is an overview over the main features that WTLS support regarding security.

The application got a solution when a project group at the Agder University College got the connection between XML and WML at a discussion board at Ericsson.

3.2 Tools

3.2.1 Professional HTML editor HomeSite

The intuitive WYSIWYN (what you see is what you need) interface gives you all the necessary site-building tools right at your fingertips. Increased productivity, enhanced project management, extended site deployment, and support for the latest Web technologies make the new HomeSite 4.5 release the obvious choice for quickly building great Web sites.

This was used to write asp, xml, xsl and wml files.

3.2.2 Nokia Toolkit

The phone simulations used in the Nokia WAP Toolkit are to show how applications may appear on a WAP-enabled mobile phone. Models 6110 and 6150 do not depict actual WAP-phones, whereas model 7110 does.

The Nokia WAP Toolkit gives owners of small handheld devices such as mobile phones access to a wide variety of wireless services over the Internet. It offers developers an environment for creating, testing and demonstrating WAP applications, allowing service providers to evaluate the usability of wireless applications and services with their end user organizations.

3.2.3 Visio 2000

The design of the entire picture is done in Visio. The ideas to the pictures is taken from various sources, among these WAPFourm.

4 Results on security issues in WAP, best infrastructure and the demo application

4.1 Security leaks in WTLS

In the WAP architecture it is important to take into consideration the fact that the security layer, Wireless Transport Layer of Security (WTLS) is mandatory. To ensure the existence of WTLS in a system it is important to ensure the existence of WTLS in both the terminal and WAP Gateway.

In accordance to the research study done by Saarinen at the University at Jyväskylä the security leaks in WTLS can be narrowed down to problems in the following fields:

?? Unauthenticated alert messages
?? Plaintext leaks
?? XOR MAC and Stream ciphers
?? RSA PKCS #1 attacks
?? DES encryption

In chapter 5.1.2 these problems will be discussed with a proposed solution at the end of each problem.

4.2 Potential solutions on the infrastructure

Based on chapter two, the results can be narrowed down to two main solutions. The solutions will be based on the use of a mobile operator or not.

4.2.1 Mobile operator solution

In this proposal of a solution the WAP Gateway will be at the operator. The operator will connect the mobile world and the Internet world by putting a WAP Gateway in as a node into the GSM system. The origin server will be at the costumer that will have to take the necessary security action to secure the environment.

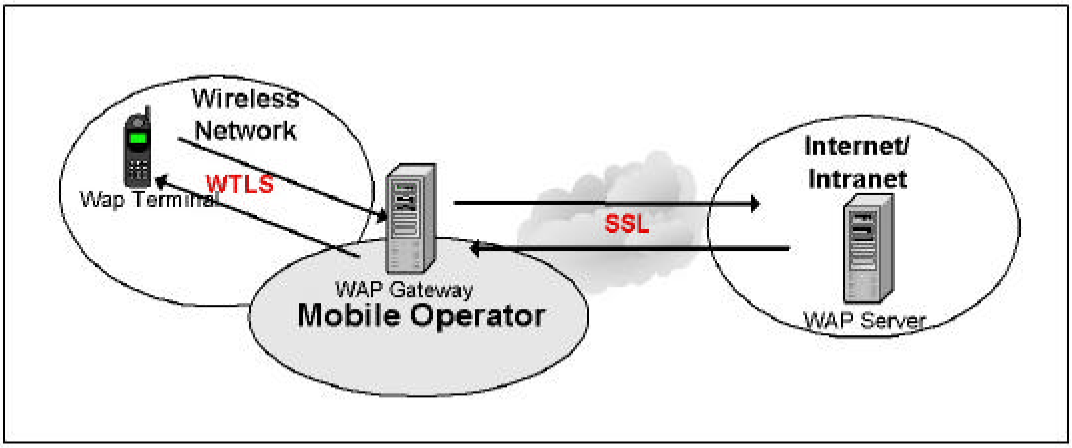


Figure 8 WAP Gateway controlled by the mobile operator.

The configured solution can be as showed on Figure 7 where the terminal will be operated by a user and the only task for the WAP Gateway will be to make a transition from WTLS to the security layer on Internet (in this case SSL).

4.2.2 Company solution

Based on the theory in chapter two the infrastructure is narrowed down to two possible infrastructures. This is based on the use of a WAP Server or a WAP Gateway.

Implementing a WAP infrastructure with the use of a WAP Gateway

One way in building an infrastructure is to invest in a WAP Gateway (Figure 9). This means that the company also must have a web-server that is configured for WAP.

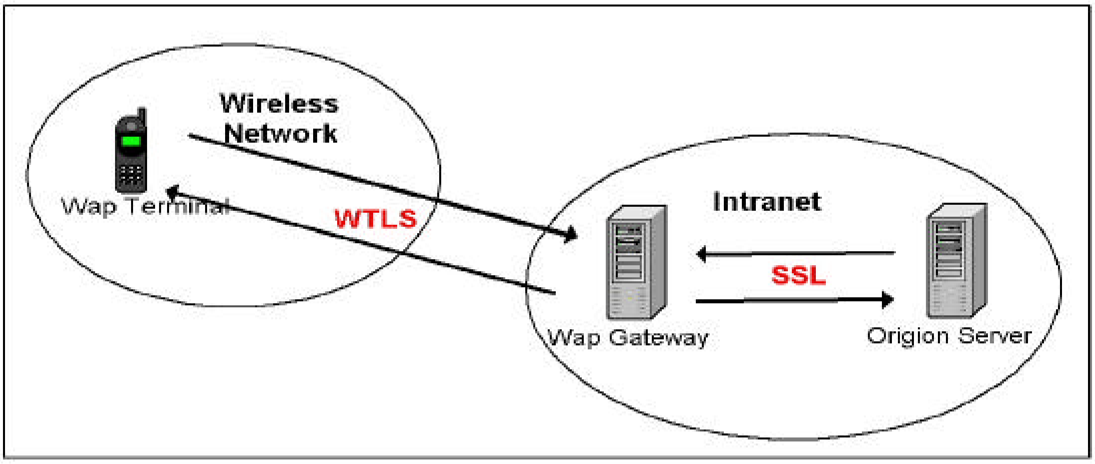


Figure 9 WAP Gateway controlled by the company.

As mentioned in chapter 4.3.2 Nokia offers this solution to their costumer. A company with this solution can have a modem pool inside to entirely operate on it's own.

Implementing a WAP infrastructure with a the user of a WAP server

This solution is based on the fact that the WAP architecture provides end-to-end security between the endpoints in the protocol (Figure 10). This can be done with a WAP Application Server. A WAP application server is a WWW-server with the WAP Gateway features implemented.

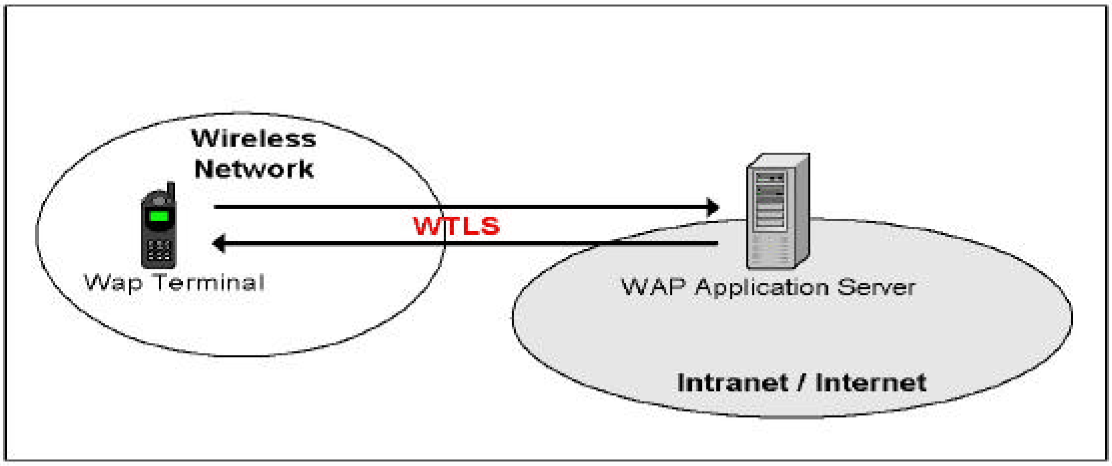


Figure 10 Solution with a WAP Application inside the company.

The WAP Application Server consists of a WML encoder, WMLScript compiler, protocol adapters, application logic, content database and WML decks with WML scripts.

This way the company can set up the WAP architecture with only one internal machine.

4.3 The result of the demo application

In accordance to the original problem description on 1.2.3 the implementation concerning the connection between XML and WML would only be solved on paper. Because of some help with the description in the WML file when implementing XML-related code, the solution is implemented in practice as a part of the demo application.

With the use of XSL witch is a powerful style sheet language, the connection between the XML-document and WML could be made. XSL is used to access data in between the tags in the XML-document.

The documentation received from NIS on the *i*Portal system was used to design the demo application. In 2.5.2 there is a short description on *i*Portal.

The solution implemented in this solution will contain an answer routine. The only security routine implemented is a login-procedure.

4.3.1 Scenario of a search with a WAP-phone

In this scenario a user will perform a search with the WAP-phone. The search is concerning some information regarding incident in a location on a specific time.

The answer will come to the phone in the form of multiple cards. The amount of card is based on the number of hits. If the search have 3 different hits the number of card will be 3 * (the number of information cards). The cards will contain information on where the location on the hit and the time of the incident.

When the user gets the information to the mobile phone he can click through the information. The answer will always lie on the WAP server for him to check the information a multiple periods of time.

4.3.2 Flow diagram

These Flow diagrams shows how the application works to day. The dotted line in Figure 12 shows implementations that are, as of now, not implemented. The features not implemented will be further discussed in chapter five.

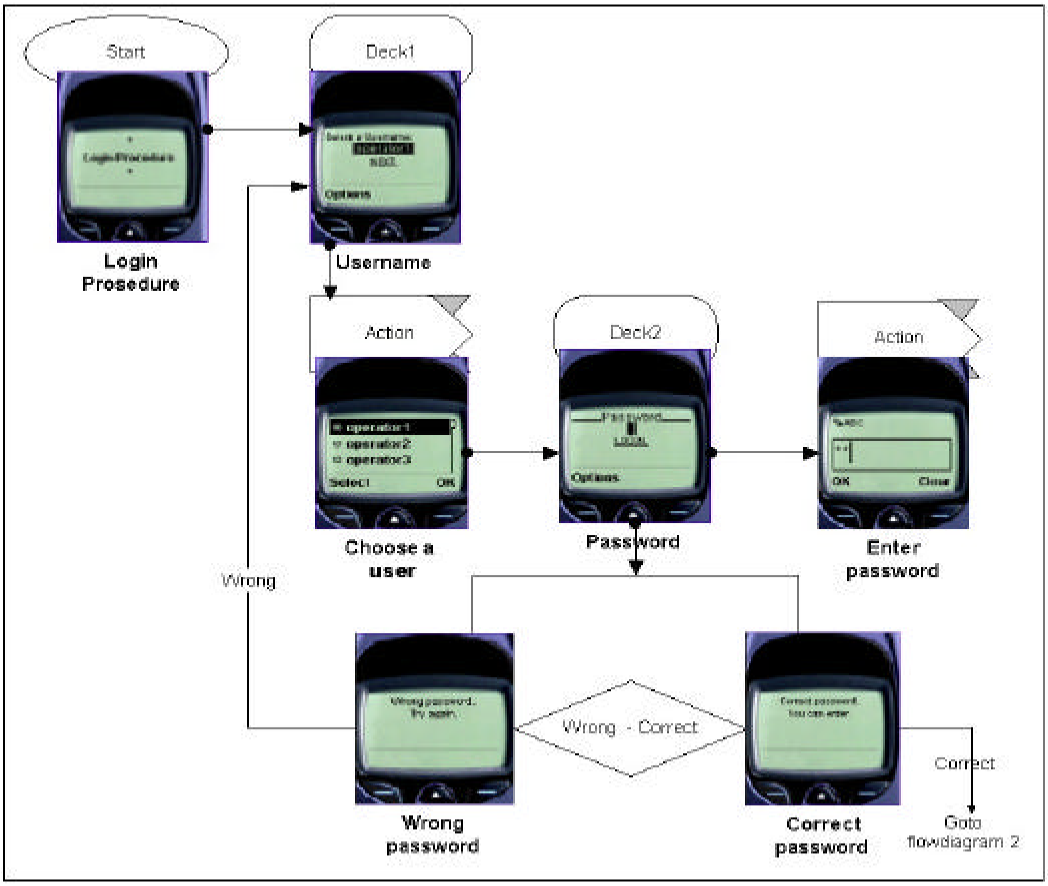


Figure 11 Flow diagram 1. This shows the ranking between the different cards and decks.

As you can see on the Figure 11 first thing shown is an introduction card. This card will be shown for three seconds before the program goes to the second card. This card allows the user of the terminal to choose a username. There are four usernames submitted into the database as of now. To make it easier the user will have the ability to choose from an option lists.

When the username is chosen the user must activate the hyperlink next in the terminal screen. This will lead the user to the entering of the password. When this is done the hyperlink login must be activated. If the password is wrong the user must start again by entering the username and password. Based on the right combination on username and password the user will be able to continue to the introduction page on Figure 12.

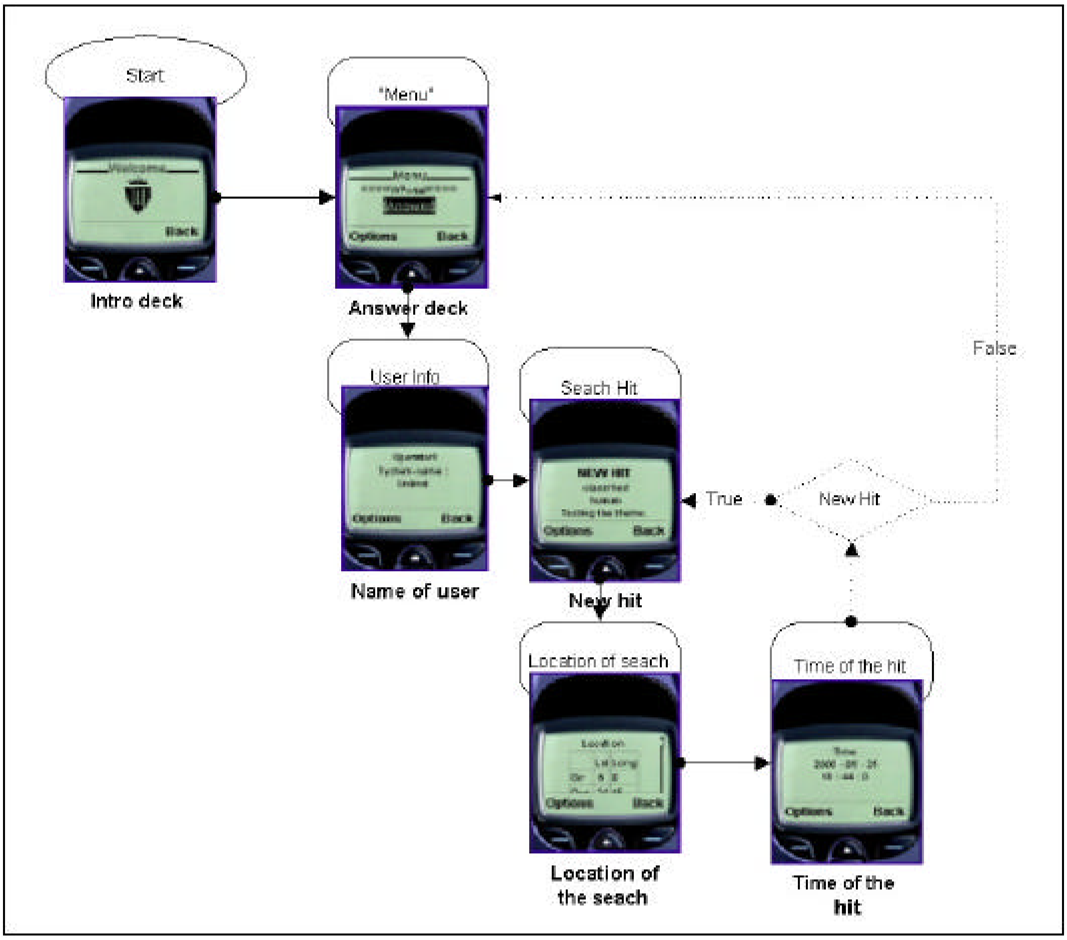


Figure 12 Flow diagram 2. This shows the implementation of the answer.xml document.

The introduction card consists of a picture that represents the Headquarter of Defense in Norway. When the first card has been shown for three second the application will go over to the menu card. The only menu choice implemented in this version of the application will to show the result of a search. When entering the result of the search called answer, the user will get some information on username, system-name and the theme-name. The next card will be the location of the hit and the last card will consist of the time at witch the hit occurred.

4.3.3 Connection between XML and WML in the application

In reality WML is only a Document Type Definition (DTD). A DTD provides a list of the elements, attributes, notations, and entities contained in a document as well as their relationship to one another. In each WML file there will be a document type declaration. This is a pointer to the DTD

The solution on the demo application

This is the code in the top of the XSL-file that generates the WML-output to a user of a WAP-browser.

Table 2 The code of the XSL-file.

Start Code	End Code
<?xml version="1.0"?> <xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl" xmlns="http://www.w3.org/TR/wbxml"> <xsl:template> <xsl:apply-templates/> </xsl:template> <xsl:template match="text()"> <xsl:value-of/> </xsl:template> <xsl:template match="/"> <xsl:pi name="xml">version='1.0'</xsl:pi> <xsl:eval no-entities="true">'<![CDATA[<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN" "http://www.wapforum.org/DTD/wml_1.1.xml">]]>'</xsl:eval>	</xsl:template> <xsl:template match="CONTENT"> <xsl:apply-templates/> </xsl:template> <xsl:template match="p"> <xsl:apply-templates/> <br/> </xsl:template> </xsl:stylesheet>

In between these lines the WML related code came. When accessing the information in the XML-document [Answer.xml] the XSL-code is used.

For instance when collecting the information regarding the user and systemname in answe.xml;

```
<SearchID>1</SearchID>
<UserID>Operator1</UserID>
<System Name="Unlimit"></System>
```

It was done in the following way [Answerwml.xsl];

Table 3 The description on the XSL-code that accesses the XML-document.

Code	Description
<xsl:value-of select="Answer/System/@Name"/>	The output of this is the name “unlimit”.
<xsl:value-of select="Answer/UserID"/>	The output of this is the username “Operator 1”. This username is as of now not dynamic. No matter witch operator is logged in the username will always be Operator 1

Using the <xsl:value-of-select=”tag-name”> gives the opportunity to get any of the information in the XML-document.

This is done all the way throughout the WML-file. All the tags in the XML-document are used. The user is entering the different card as shown in the flow diagram in [Figure 13].

4.3.4 Interfaces of the demo application

As mentioned in the above chapters the implementation of the solution consists only of a demonstration on the answer routine.

The introduction page contains the official logo to the Headquarter of Defense and NIS (Figure 13).

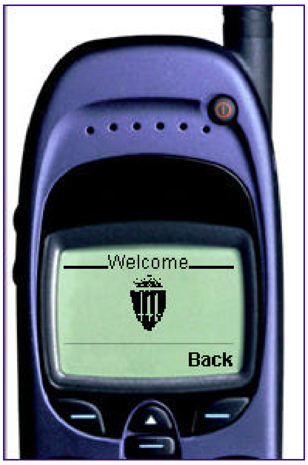


Figure 13 Introduction page to the answer application.

From this screen the application will enter the menu that as of know only consists of one choice (Figure 14).

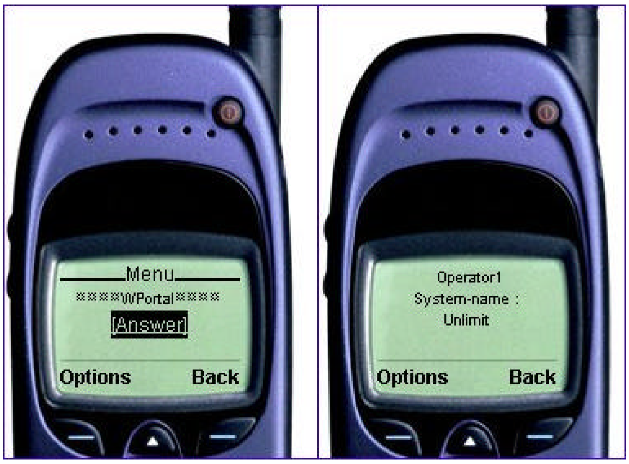


Figure 14 The user-interfaces of the answer-routine.

As you can see on figure 14 when entering the Answer menu the information regarding the user and the system-name will appear.

4.3.4 Login routine

The flow diagram of this routine is mentioned in Figure 11.

When generating WML out of an asp file it is important to send the right MIME type to the browser. This is done in the code on the following way; Response.ContentType = "text/vnd.wap.wml"

In this way the terminal will know that it is WML in the asp file. The output to the terminal will be pure WML. This is done in all the asp-files that want to show WML to the terminal.

The file conndb.asp contains a dynamic connection to the database. With the sentence <!--#include file=”conndb.asp” --> the connection will be opened dynamically.

Figure 15 shows the different interfaces that represent the login-procedure.

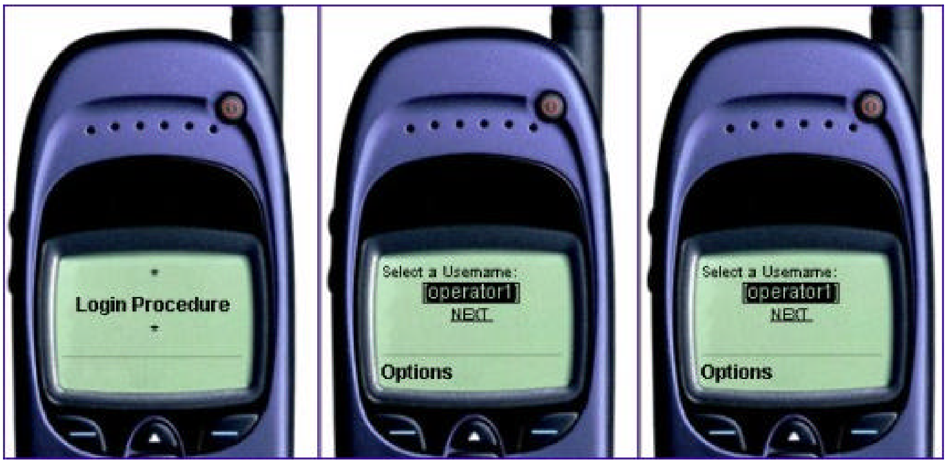


Figure 15 Start page when entering the Login routine.

In this part the user will be checked against an access-database. The database consists of a user-table that got three attributes; id, username and password as shown in Table 2. The primary key for the table is id.

Table 4 Attributes in the User table

Fieldname	Data type
Id	Autonumber
Username	Text
Password	Text

The code of the login routine is shown in Appendix B login.asp and login2.asp. When the user has entered the username and password, the application will take the two variables to login2.asp to be checked. If it is a match the application will load the answerwml.xsl file.

5 A discussion on the security issues, NIS vs. WAP and the application

This chapter consists of the discussion of the results in chapter four, the theory in chapter two and personal experience and knowledge on security.

5.1 Security in WAP

5.1.1 Levels of security

When thinking of security in a system it is important not just to take into consideration the security mechanism implemented into the system, but also the infrastructure. One rule as I see it, effectively secure your network, is to implement layers of security, the more layers you put in place the more effective will your security be. In the WAP infrastructure it is important to think of the layers of security when it comes to the WAP Gateway and WAP Server.

One layer can be ongoing training to the network administrators. This must also include some time for the administrators to focus on new exploits and bugs. This is one way of staying ahead of possible intruders and hackers.

A second layer may be physical security. This includes policies and restricted access to the servers and remote administration-tools. This will prevent incidents like giving the password of a system to persons not authorized to get that information. Intruders can come from the inside of a company and the term “need-to-know” is important to attend to.

Another thing is monitoring of system-logs. This monitoring can be done with the help of software or the administrator can start each day to look into the logs to see if there is something unusual. After a while an administrator will be able to see a structure and notice if there are some structure that should not be there.

The last layer is to have knowledge on the software on the systems. This includes known bugs. An evaluation process of the software that is bought in to the company should be mandatory.

5.1.2 Wireless Transport Layer of Security (WTLS)

Security Features

When implementing security into the applications the designer must take into consideration the functionality of the application compared to the level of security. In the WAP-technology some of the security features may be mandatory, optional or not there at all. The none existence of security occurs when the cipher-suite is assigned to the value NULL.

When designing an application there must be a decision on witch class in WTLS that will be implemented and witch key-exchange suite that will be used.

As you can see from Table 2 there are some features that are optional in WTLS. The current version of the WTLS specification covers all the features in Class 1 (WAP 1.2).

Table 2 WTLS Classes

FEATURE	CLASS 1	CLASS 2	CLASS 3
Public-key exchange	M	M	M
Server certificate	O	M	M
Client certificate	O	O	M
Shared-secret handshake	O	O	O
Compression	-	O	O
Encryption	M	M	M
MAC	M	M	M
Smart Card Interface	-	O	O

The security leaks of the WTLS protocol have been discussed in the research study of Saarinen M.J. at the University of Jyväskylä. This is a official document that differs from those found by preliminary evaluation of a confidential draft of the WAP WTLS protocol.

The problem mentioned in the research study can be mentioned in some items. [1: Attacks against the WAP WTLS protocol]

Unauthenticated alert messages

Some of the alert messages sent in the protocol is sent in cleartext and is not properly authenticated.

An active attacker may replace an encrypted datagram with an unauthenticated plaintext alert message with the same sequence number without being detected. This lead to a truncation attack, that allows arbitrary packets to be removed from the data stream.

The alert messages that can be sent in clear text are mentioned in table 3 in Appendix A. When sending the alert messages are sent in cleartext no compression, MAC protection or encryption is used [15: Official WAP p. 569]. As mentioned under Security Features this means that the cipher-suite is assigned to NULL.

This can be solved by authenticate all the messages affecting the protocol state.

Plaintext leaks

Under exportable keys the initial IV of each packet can be determined by an eavesdropper from the Hello messages and the sequence number alone.

The exportable keys mentioned in Appendix A Table 3, have a minimal key-length and as mentioned in Appendix A under General understanding of ciphers forty bits is considered week. Thus an intruder can easily get the initial IV just by looking at the Hello messages. Also; Hello Request messages are omitted from handshake hashes. [15: Official WAP p. 13]

An eavesdropper can determine the change of keys because the record_type field is sent unencrypted. This field determines the type of the message; one type being the Change Cipher Spec type. Also the existence of error messages can be determined from the record_type field .The exact nature of the encrypted error messages cannot be determined.

The record_type field will be sent in a WTLSPlaintext structure as described in the Official book in page 569. For exportable keys, the IV of any block is known exactly.

A chosen plaintext attack against low-entropy blocks can occur using the fact that the Initialization Vector, IV is known or predictable. Thus the way in assigning a value to the IV should be more complicated and encryption on the record_field should be carried out.

XOR MAC and Stream ciphers

The MAC is an algorithm to be used for message authentication. This specification includes the size of the key used for MAC calculation and the size of the hash that is returned by the MAC algorithm. The explanation on how the XOR MAC is done is explained in Appendix A under the chapter Cryptographic Computation.

In the Appendix A it was mentioned that “exportable grade of encryption (e.g., RC5_40), XOR cannot provide as strong message integrity protection as SHA can.”

In accordance to Saarinen the 40-bit XOR MAC does not provide any message integrity protection if stream chippers is being used, regardless of the key length.

If inverting a bit in position n in the ciphertext, the MAC can be made to match by inverting the bit (n mod 40) in the MAC. This can be repeated arbitrary number of times. Thus, when stream ciphers are used, the XOR MAC does not provide any integrity protection.

The use of 40-bit MAC on stream ciphers should be avoided in a high-level security system.

RSA PKCS #1 attacks

In accordance to RSA Security [1],if the application can employs a server who can act as an *oracle* for a client in the following manner: a client can send chosen ciphertexts to the server and determine from the client's subsequent behavior (e.g., from an error message) whether or not the corresponding plaintext conforms with PKCS #1 v1.5.

This is used on the RSA encryption and signatures and performed according to PKCS #1, version 1.5. If the protocol includes an oracle that tells weather a given packet has a correct PKCS #1 v 1.5 padding, RSA can be decrypted with approximately 2^20 chosen ciphertext queries.

In some implementations the WTLS error messages bad_certificate and dedode_error may provide such an oracle to the attacker.

The recommendation is to use PKCS #1 version 2.0.

DES encryption

The 40-bit DES encryption uses five bytes of keying material. Because of the parity bit in each byte of a DES key, there are only 5 * 7 = 35 effective key bits in five bytes.

In accordance to “General understanding of cipher” in Appendix A 40 bit in a symmetric algorithm like DES is considered week. The protocol clearly does not meet its requirement of reaching the best possible security in export-weakened encryption modes.

5.1.3 Infrastructure

Mobile operator

The general security information regarding the levels mentioned in the beginning of this chapter must be taken into consideration. Optimized securities on all levels are very important. Also the security consideration regarding the WAP gateway in chapter 2.3.2 must be looked upon.

No control over the optional security in WAP

When the WAP Gateway is at the mobile operator, the mobile operator gets control over the security features. Some of the security features in WTLS are optional and the mobile operator can lower the security level in the WAP gateway as he find fit. Some mobile operator can even choose to not even include the WTLS layer. This is a risk for the costumer of the operator. It dose not matter how much security that are implemented into the application, if the WAP gateway don't have the security layer, the security will be non-existent.

Every situation has different security criteria, but a costumer would not be pleased to hear that intruders can attack the messages that are sent between the costumers towards the client. Especially if the reason for the intrusion is that the WAP gateway don't have the security layer implemented.

No end-to-end security

The costumer will not have end-to-end security because of the transition from WTLS to SSL. When this happen the information will occur in clear-text in the memory of the WAP gateway, witch is dangerous when considering man-in-the-middle attack.

Company solution

In this solution end-to-end security can be achieved. When the company invests in a WAP Server the end-point of the WAP protocol will be at the costumer. In this way the WTLS security protocol will be used from the user to the server. (Figure 10) This solution will decrease the possibility of a man-in-the-middle attack at the environment at witch the WAP Gateway is located.

It will also be considered an end-to-end security solution when the WAP Gateway is within the four walls of the company. If this happen the WAP Gateway is said to be trusted. (Figure 9)

When using the WAP Gateway approach inside a company a possible intruder will have to get through the security infrastructure between the WAP Gateway and WAP Server to get to the information. When it is a WAP Server the intruder can bypass the security features to the WAP Server and then get hold on the information on the same machine. Based on this the WAP Gateway solution will uphold more security than a WAP Server.

Also, a company is able to provide WAP services to all its customers or employees independently from operators. This is possible because access to the WAP service can be implemented via Circuit Switched Data. A company can own or outsource necessary infrastructure, such as a modem pool for that.

One can say that independence is the key to maximum security.

Certificate Authority (CA)

When security features like server certificate and client certificate are implemented into the application the delivery of these will often be carried out from a certificate authority.

When collaboration with a CA each client will receive a digital certificate, that uniquely identifies him. This will ensure the WAP Gateway, up to a certain point, that he is communication with the right client. The certificate will also be given to the server so the client knows that it is communicating with the right server and not a malicious one.

If a server gets a handshake message from a terminal with a relationship to a common CA (Figure 16) it checks to see if the certificate is valid. If the CA in the certificate could not be located, or the certificate couldn't be matched with a known, trusted CA the message will be discarded. To optimize the traffic and client processing, the certificate-chain should have minimal length. For server certificates, it is possible to have only one certificate: the server certificate certified by a CA public key of which is distributed independently.

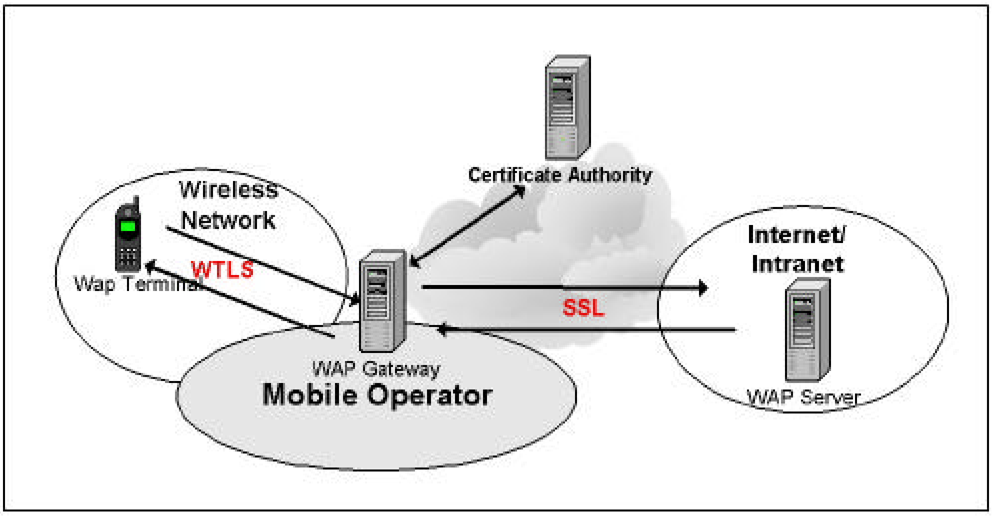


Figure 16 Solution with a certificate authority.

Client certificate chain is likely to contain several certificates. However, this is acceptable because the server processes this chain. Also, the server may get the client certificate from a certificate distribution service.

With a CA another trust relationship must exist. Everyone trusting the CA must, through third party trust, also trust the user. Definition on what CA is can be found in chapter 2.3.3 , regarding the digital signature and client certificate.

5.2 Discussion on the implementation of WAP in NIS

5.2.1 A short mention on the demands in NIS

The evaluation on an external system must follow the rules in the Directive of Computer Security. This is a major job that consists of making several documents ready for a committee. The committee makes a decision on the new system to see if it meets the demands required to be an operational system. If it is holes in the system they makes a list of the problems so that the project group can improve the system.

The evaluation is a comprehensive task that takes lots of effort and time to accomplish. In this thesis the significance will be put on the general rules of the evaluation.

This directive became active 1.martz-1998. The directive with appendix will secure that: the system have function and protection so that:

?? *The information not will be known to intruders (confidentiality)*
?? *The information is not being altered by persons not authorized (integrity)*
?? *The information is accessible for authorized users (availability)*

When concerning the **confidentiality** of WAP this is done with the help of encryption in WAP (2.3.5). As mentioned in the theory, functions like privacy (confidentiality) can be turned off if it is implemented at a lower level.

The **integrity** of WAP is taken care of with the help of a Message of Authentication Code. This will do it harder to intruders to alter the information between the client and server.

In using the WAP technology, **availability** is the foremost benefit. The technology is simple to implement and the equipment to use in order to take advantage of the information will be inexpensive.

5.3 A discussion of the Demo Application

5.3.1 Future improvements on the application

Implementation of multiple hits

In the solution of to day the implementation does not support multiple hits in the answer routine. This can easily be implemented with the help of the xsl-code <xsl:for-each select="Answer/Hit">”code concerning the information on one hit”</xsl:for-each>.

The number of card that must be shown to the user will be in a number of N*3, where N is the number of hits and three is number of cards containing information on each hit in this case.

The name of the information card must be a concatenation between a number and an informative name in accordance to the information shown in the card.

The dotted line in the flow diagram on figure 11 show the sequence of the card if implementation of multiple cards is implemented.

Dynamically generation of the XML-document

To make the search-criteria useful the XML-document must be generated dynamically by the means of the DTD-document or by coding it in asp or java.

The new versions on the program-language asp contain code that goes specific on these issues. It is possible to make an XML-document dynamically with these functions in asp. This makes the use of XML in a WML environment very powerful and lots of possibilities opens. The company can for instance take into consideration the making of an XML-generator on top of a company database. When implementing WML into this solution all the employers in the company will be able to access all a number of documents on the road. This will be an improvement considering the efficiency in a work process.

.

6 Conclusion

The **WTLS** protocol as it is today got several security problems. To summarize these problems are unauthenticated alert messages, possible plaintext attacks, loss of integrity in XOR MAC when using stream ciphers, RSA PKSC #1 attacks and low security in DES using 40 bit.

Unauthenticated alert messages can be avoided by authenticate all the messages concerning the protocol. Plaintext alerts can be avoided by encryption the record_type field in all the different types of cipher suite and design less predictable Initialization Vectors in cipher suite of 40 bits. The loss of integrity and low security in DES can be avoided by using more than 40 bits in the cipher suite. The problem with RSA PKSC#1 can be avoided by using RSA PKSC#1 v.2.0

More or less all of the security problems can probably be avoided using more than 40 bit cipher suites. It is important to keep in mind that in accordance to new encryption regulation announced by the Clinton administration on the 14.January 2000, the export of strong encryption is regardless of their strength or type of technology. [19: New U.S. Encryption Regulations a Major Step Forward for Online Privacy]. This means that the all the export cipher-suites in Appendix A [Table 3] are true. It is recommended that the designer choose a cipher-suite that is on a minimum bigger than 56 bits.

This doesn’t mean that the problem concerning clear-text and unauthorized error alert goes away. The recommendation that future version of WTLS should implement authentication on all messages concerning the protocol, implement PKCS #1 version 2.0 and encryption of record_type is still standing.

Based on the information gathered and the discussion in 5.1.3 maximum security in the **infrastructure** will be reach when implementing the company solution. When investing in a WAP server or WAP Proxy/Gateway the company will not have to worry about man-in-the-middle attack at the mobile operator. As mentioned this can happen because the information will occur as clear text in the memory of the WAP Gateway.

Also, a company is able to provide WAP services to all its customers or employees independently from operators. This is possible because access to the WAP service can be implemented via Circuit Switched Data. A company can own or outsource necessary infrastructure, such as a modem pool for that.

When it comes to client- and server certificate, government with high level of security should be able to control this, and not use an external Certificate Authority. In my opinion independence is the key to maximum security.

Another thing that must come into consideration is the knowledge of the employees responsible for the system. To be able to implement maximum security it is important to have an ambulatory employer in charge of the system. All the levels of security (5.1.1) concerning the infrastructure should be looked at when implementing any kind of system in a company.

The use of **XML**-document as a base for the interfaces shown for the user is fully supported by the means of **WML** and XSL. The style language makes it possible to implement more powerful features.

The demo application is a valid demonstration on the connection between WML and XML-documents. If implementing future features as described in 5.3.1 the application will be a fully functionally application against a database-XML-WML environment.

The making of an XML-generator on top of a company database and implementing WML into this solution, will do that all the employers in the company will be able to access all a number of documents regardless of where they are. This will be an improvement considering the efficiency in a work process.

Based on the information in 5.1 and the security criteria in **NIS**, the security as of now is not strong enough for NIS even thinks of implementing the technology. In future versions of WAP, the security leaks in WTLS will probably be fixed. Even then NIS must have a more secure bearer then GSM.

If implementing the WAP technology in the future it is recommended to go for the company solution, this will make the trust relationship to others companies unnecessary witch will make possible information stealing less possible.

The most secure bearer will have to be TETRA system. This would be a preferable solution, since it is a system that are separated physically to any public net, supported by WAP and run by government official.

7 Literature references

[1] Saarinen M.J. *Attacks Against the WAP WTLS Protocol* [Online], Web address: http://www.cc.jyu.fi/~mjos/ [29.mai-2000]

[2] RSA Security. *Diagnostic Test for Vulnerability to the Adaptive Chosen Ciphertext Attack on PKCS #1 v1.5*. [Online] Web address: http://www.rsasecurity.co.uk/rsalabs/pkcs1/diagnostic.html

[3] Baltimore Technologies, *WSecure Developers Guide*

[4] WAPForum (30-Apr-1998) *WAP Architecture Specifications*

[5] WAPForum (15-July-1999) *WAP over GSM USSD Specifications*

[6] WAPForum (05-Nov-1999) *WAP WTLS, WAP Wireless Transport Layer Security Specification*

[7] WAPForum (05-Nov-1999) *WAP WIM, WAP Wireless Identity Module Specification, Part: Security*

[8] Baltimore Technologies (07-Mar-2000), *WSecure White Paper* [Online]. Web address: http://www.baltimore.com/library/whitepapers/wsecure.html

[9] Nokia WAP Server, *Main Benefits* [Online]. Web address: http://www.nokia.com/corporate/wap/gateway_case1.html

[10] Phone.com (January-2000), *Understanding Security on the Wireless Internet* [Online]. Web address: http://www.phone.com/products/publications.html

[11] Johan Hjelm, Bruce Martin, Peter King (29-Sep-1998), *WAPForum - W3C Cooperation* [Online]. Web address: http://www.wapforum.com/what/docs/WAP-W3C-white-paper_v1.2.htm

[12] Lincoln Stein W3C (24-Mar-2000). *World Wide Web Security FAQ* [Online]. Web address: http://www.w3.org/Security/Faq/wwwsf3.html

[13] Entrust Technologies, *All about…PKI* [Online]. Web address: http://www.entrust.com/products/pki/cryptography.htm

[14] Berk Sunar & Can K. Sandalci, *GSM Security and Encryption* [Online]. Web address: http://security.ece.orst.edu/seminars/sunar1/

[15] Wiley Computer Publishing (1999), *Official Wireless Application Protocol – The complete standard*

[16] Phone.com (01-Feb-2000), *Phone.com Announces Version 4.1 of Its WAP Microbrowser for Wireless Phones With Full 128 Bit Encryption* [Online] Web address: http://au.us.biz.yahoo.com/prnews/000201/ca_phone_c_3.html

[17] Brochure. *RSA BSAFE? in the Wireless and Embedded Worlds*

[18] Lasse Huovinen, *Authentication and Security in GPRS environment: An overview* [Online]. Webadress: http://www.hut.fi/~lhuovine/netsec98/gprs_access.html

[19] Center for Democracy and Technology *New U.S. Encryption Regulations a Major Step Forward for Online Privacy* (13-Jan-2000) [Online]. Web address: http://www.cdt.org/press/000113press.shtml

[20] http://www.wirelessdevnet.com/training/WAP/WML.html

[21] WAPForum (04-Nov-1999) *WAP WML*

[22] WAPForum (04-Nov-1999) *WMLScript Specification, Approved*

[23] WAPForum (05-Nov-1999) *WMLScript Crypto Library Specification*

[24] NOKIA (09-1999, *Developers Guide. Nokia WAP Toolkit Version 1.2*

[25] Allaire Corp. *HomeSite HTML editing tool* [Online]. Web-address: http://www.allaire.com/products/homesite/index.cfm (28-05-2000)

[26] WAPForum (04-Nov-1999) WMLScript Standard Libraries Specification Approved ver.

[27] NOKIA (Sep-1999) *WMLScript Reference ver.1.1*[Online]. Web address: http://wap.grm.hia.no/prosjekt/Wap-Docs/Nokia_wml-script-reference.pdf

[28] NOKIA (Sep-1999) *WML Referance ver.1.1* [Online]. Web address: http://wap.grm.hia.no/prosjekt/Wap-Docs/Nokia_wml-reference.pdf

[29] Article, WapForum (09-04-2000), *Wireless Application Protocol* [Online]. Web address: http://www.openwirelessdata.org/wap.htm

[30] Forsvarets Overkommando Prosjekt *i*Portal (23-Des-99*), Document Type Definitions*

[31] Bjørn Hjelle, Robert Herland, Peter Ehrstedt, (02-Feb-99). *Forsvarets Overkommando, iPortal forstudie*

[32] Forsvarets Overkommando/Sikkerhetsstaben, *Datasikkerhetsdirektivet,*[Online] http://www.mil.no/fo/sikkerhetsstab/dsd/

[33] Forsvarets Overkommando/Sikkerhetsstaben**,** *DSD – Organisering* [Online], Web address: http://www.mil.no/fo/sikkerhetsstab/dsd/dsd-vedlegg13.html - 2 Organisering

[34] Forsvarets Overkommando/Sikkerhetsstaben**,** *DSD – Formål* [Online]. Web address: http://www.mil.no/fo/sikkerhetsstab/dsd/datasikkerhetsdirektivet.html - 1 Formål

[35] Forsvarets Overkommando/Sikkerhetsstaben**,** *DSD – Ekstern kommunikasjon* [Online]. Web address: http://www.mil.no/fo/sikkerhetsstab/dsd/datasikkerhetsdirektivet.html - 7.1.2 Ekstern kommunikasjon

[36] Michael Vernetti (Feb-2000), *WAP Deployment Fact Sheet* [Online]. Web address: http://www.wapforum.org/new/WAP_Deployment_Fact_Sheet_022000.doc

Abbreviations

CA	-	Certification Authority
DH	-	Diffie-Hellman
DSE	-	Data Encryption Standard
EC	-	Elliptic Curve
ECDH	-	Elliptic Curve Diffie-Hellman
FO/S	-	Forsvarets Overkommando / Sikkerhetsstaben
GPRS	-	General Packet Radio Service
IV	-	Initialization Vector
MAC	-	Message Authentication Code
NIS	-	Norwegian Intelligence Service
PDU	-	Protocol Data Unit
PKCS	-	Public Key Cryptosystem-Signing
SDU	-	Service Data Unit
SMS	-	Short Message Service
SSL	-	Secure Sockets Layer
TETRA	-	Terrestrial Trunked Radio
TLS	-	Transport Layer Security
WAP	-	Wireless Application Protocol
WAP	-	Wireless Application Protocol
WDP	-	Wireless Datagram Protocol
WML	-	Wireless Markup Language
WSP	-	Wireless Session Protocol
WTA	-	Wireless Telephony Application
WTLS	-	Wireless Transport Layer Security
WTP	-	Wireless Transaction Protocol

Glossary

Authentication
The process whereby a card, terminal or person proves who they are. A fundamental part of many cryptography systems.

Diffie-Hellman
It is used to create a shared secret random number, which can then be used as a symmetric algorithm's session key.

Digest
The result of passing a file through a hashing algorithm.

Digital Signature
A block of data created by hashing a file and encrypting the resulting digest using the sender's private key.

Hash Algorithm
An algorithm used to create a digest of the data.

Integrity
Proof that the message contents have not been altered, deliberately or accidentally, during transmission.

Non-repudiation
Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender’s identity, so that neither can deny having processed the data.

Private Key
A cryptographic key kept secret, which enables you to decrypt files that have been encrypted using your public key.

Public-key Certificate
A packet of data consisting of your public key and your basic identification details, all signed with the Certification Authority's public key to verify that it is authentic.

record_type
Defines the higher level protocol used to process the enclosed fragment. Contains also information about the existence of optional fields in the record and an indication about ciphering state.

Secure Socket Layer (SSL)
This is the scheme proposed by Netscape Communications Corporation. It is a low-level encryption scheme used to encrypt transactions in higher-level protocols such as HTTP, NNTP and FTP. The SSL protocol includes provisions for server authentication (verifying the server's identity to the client), encryption of data in transit, and optional client authentication (verifying the client's identity to the server).

Appendix A: Wireless Transport Layer of Security (WTLS)

This appendix is a collection of information, mostly from the WTLS specification, slightly modified, but also from the WSecure Developers Guide from Baltimore Technologies.

With the help of service primitives' communication between neighboring layers in the WAP architecture are accomplished. Service primitives consist of commands and responses associated with service requested of another layer. Service primitives are an abstract way of illustrating the services provided by one protocol layer to the layer above.

The general syntax of the primitive on the security layer is SEC-Service.type (Parameters). The type function in the syntax can be one of four abbreviations;

1. req – Request: requesting a service at a lower layer
2. ind – Indication: notify the higher layer of parameter related to a requested service
3. res – Response: acknowledge to the lower layer that the indication is received
4. cnf – Confirm: report to the layer requesting the service that everything went well

The parameter in the syntax is set using a table. The table indicates which parameters that are possible, and how they are used.

The secure connection is done by the means of the **Connection Manager** also called the connection management. Then the **Transport Service** takes over to transfer the user data to the receiver. This is done in the security primitive SEC-Unitdata.

Transport Service

The parameters used in this service are the source address, source port, destination address, destination port and the user data. All of these are mandatory when requesting a service. When an indication is sent, the address and port of the destination is optional. As mentioned above these parameters are sent using the primitive SEC-Unitdata.

Connection Manager

WAP operates in a connectionless environment. A server will receive datagrams from various clients at different times. The task of the connection manager is to create, maintain and destroy sessions from these clients. Another task is to initiate the handshake messages if necessary.

In the connection phase all of the necessary security parameters are agreed upon. This can include cryptographic algorithms, key lengths, key exchange, and authentication.

The connection management consists of several primitives. These are used to set up and maintain a secure connection between a client and server.

SEC-Create - Initiates a secure connection.
SEC-Exchange - Server can perform public-key auth. or key-exchange with client.
SEC-Commit - Indicates the end of handshake
SEC-Terminate - This primitive is used to terminate the connection.
SEC-Exception - Inform the other end about warning level alerts.
SEC-Create-Request - Sent from the server to the client to initiate a new handshake.

When a secure connection is established the client has the possibility to send secure data over the net.

Record Protocol

The WTLS Record Protocol is a layered protocol. When it receives a record from the layer above that is going to be transmitted, it optionally compresses the data, applies a MAC to it and encrypts it, before the package is sent. When the record protocol receives a record it decrypt it, verifies and decompress it before sending it to higher-level clients.

As shown in Figure 17 there are four protocols that sends their messages to the record protocol.

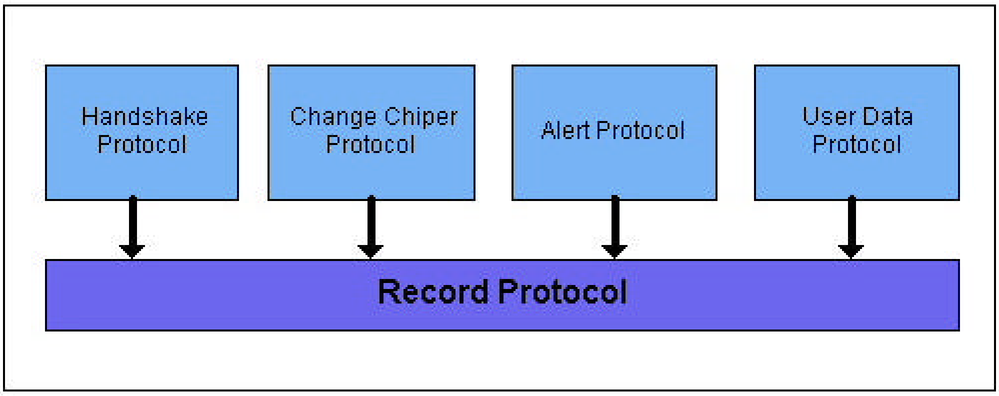


Figure 17 The record protocol and its clients.

The clients send records to the record protocol that will process- and transmit the records. To optimize the transport of records, several of them can be transported in one Service Data Unit (SDU). This is normal to do with records that have a logic connection like the handshake records.

The record protocol operates in the connection state along with the handshake protocol. It specifies a compression algorithm, encryption algorithm and MAC algorithm.

Once the security parameters have been set and the keys have been generated in what is called the pending state (Figure 18), the connection can then be initiated by making them the current states. These current states must be updated for each record processed.

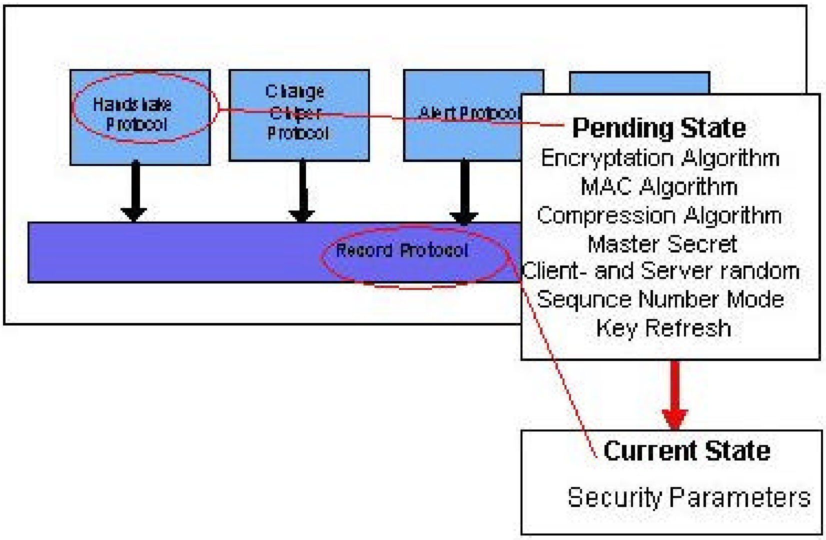


Figure 18 The current and pending state

The security parameters are set in the handshake protocol. It is the handshake protocol that makes the pending state over to the current during the connection of the session. Then the pending state is reinitialized to an empty state.

Before sending the records, the encryption and MAC function converts them into a cipher-text. The decryption functions reverse the process.

When using datagram-transport, explicit sequence numbering must be used because records can be lost, duplicated or received out of order.

Stream-ciphers convert compressed records to and from stream chipper-text records. For block-ciphers (RC5 and DES) the encryption and MAC functions convert compressed records to and from block chipper-text records.

Handshake Protocol

As mentioned by Baltimore Technologies the transformation from TLS to WTLS is based upon the need to support datagrams in a high latency, low bandwidth environment. To operate within this environment WTLS provides an optimized **handshake** through dynamic key refreshing. Dynamic key refreshing allows encryption keys to be updated on a regular and configurable basis during a secure session. This leads to a higher level of security and a considerable bandwidth saving on the relatively costly handshake procedure.

This protocol operates above the record layer. Here the cryptographic parameters of a secure connection are produced. The handshake messages are sent to the record layer where they are encapsulated within one or more WTLSPlaintext structures and sent as specified by the current connection. A client and server become united upon parameters like a protocol version, cryptographic algorithms, and authentication if they choose to do that and the public-key encryption techniques to generate a shared secret.

This protocol consist of three sub-protocols which are used to allow peers to agree upon security parameters for the record layer, authenticate themselves, instantiate negotiated security parameters and report error conditions to each other.

In the next figure there will be an overview over the messages sent between client and server when doing a handshake.

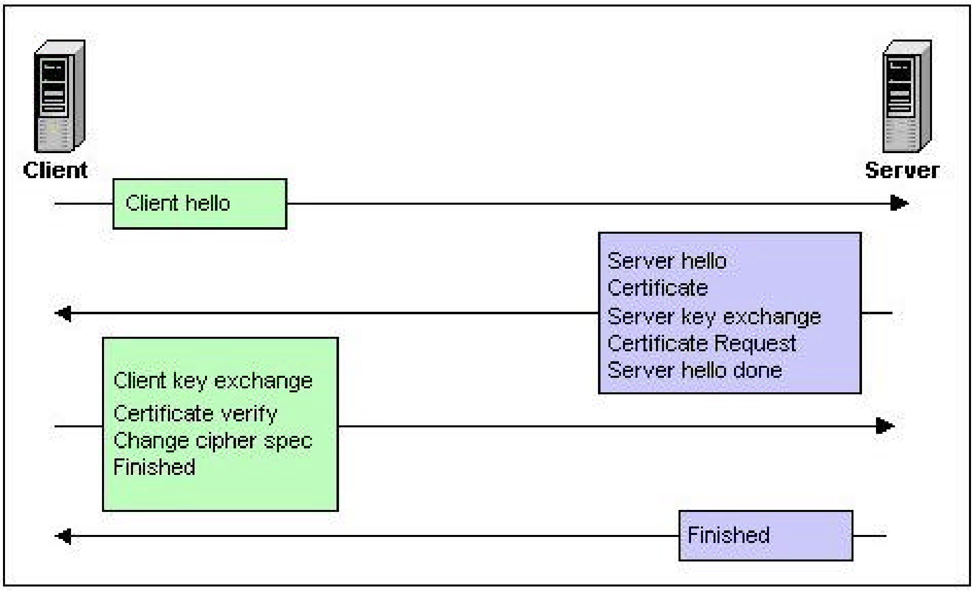


Figure 19 The sequence of messages in a full handshake.

The client and server must exchange hello messages to agree upon algorithms, and exchange random values. They must exchange certificate and cryptographic information to authenticate each other, and exchange cryptographic parameters to agree upon a shared secret. Then the secret is generated and random values are exchanged. At the end, the handshake parameters are checked to see if the peers has calculated the same security parameters, and that the handshake occurred without any tampering by an attacker.

The handshake messages must be sent in a specific order, if not, a fatal error will occur. One exception from this rule is the Hello Request message, which can be sent by the server at any time but which should be ignored by the client if it arrives in the middle of a handshake.

It is also possible for the client and server to resume a previous secure session (figure 19). This is done when the client sends a Client Hello using the Session ID of the secure session to be resumed. This is the start of a shorten- or abbreviated handshake. When a session continues after an interruption, the master-secret is not recalculated, the resumed session use the same master-secret as the previous one. New ClientHello.random and ServerHello.random values are exchanged in the shortened handshake.

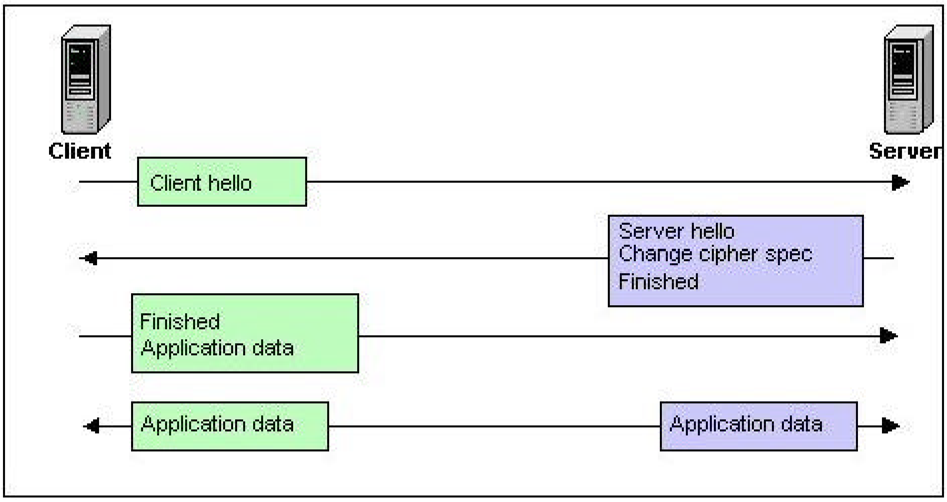


Figure 20 The sequence of messages in a shorten handshake.

If the server finds a match on the session id in the cache the connection will be reestablished, if not the server will initiate a full handshake. The server then sends a Server Hello using the same session id. Right after it sends a Change Cipher Spec followed by a finished message. When the client answer with the finished message the server may begin to exchange application data to the client.

The last method to do a handshake is to optimize the handshake (figure 20) using the client's certificate. The clients certificate can be stored in a certificate distribution service or from its own source.

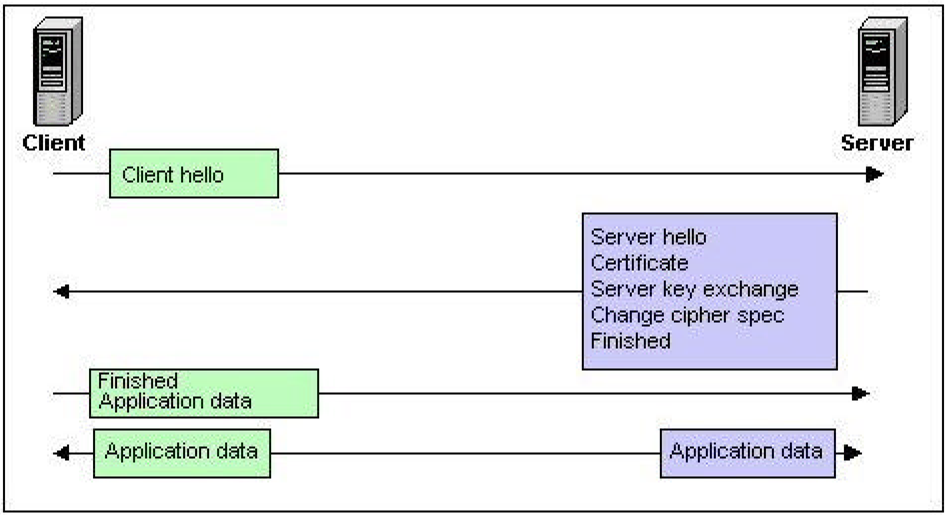


Figure 21 The sequence of messages in an optimized handshake.

If the Deffie-Hellman-type key exchange, assuming that those parameter type are used in the certificate, the server can calculate the pre-master secret and master secret at this point. In this case the server send the certificate, a change cipher spec and the finished message.

Handshake reliability over datagrams

In this environment handshake messages may be lost, come out of order or be duplicated. As mentioned before, a number of records may be concatenated in the same SDU. This is a way of making the handshake reliable over datagrams. It is also important that the client retransmits when necessary, and that the server responds to the retransmitted messages in the appropriate way.

When it is a full handshake the client must retransmit Client Hello and Finished Message after a predefined timeout. When the client has tried to retransmit a predefined number of times it muse terminate the handshake. The predefined numbers are written in the WTP, if present.

On the server side, the server must retransmit the SDU with the Server Hello until it receives a duplicated Client Hello message. When it receives a new Client Hello it must generate new security parameters. It must also retransmit the SDU that contains the Finished Message until it receives a “duplicated finished received” from the client.

When it is an optimized or shorten handshake, the Client Hello is retransmitted if necessary, and the FinishedMessage is attached at the tale of an application message. This is done until it receives the right respond or a “duplicated finished received” from the server.

The server in an optimized or shorten handshake will behave in the same matter as the full handshake when receiving a Client Hello. In the case of receiving duplicated finished massages the server must ignore them and keep the secure connection intact. If the server has no application data to send, it should send a “duplicate finished received” alert to the client.

Table 5 describes the right order of the handshake messages with no concern to which type of handshake it is.

Table 5 The handshake messages in the correct order

Message	Response message	Meaning
Hello message		Used to agree upon security parameters.
	Server Hello	Sent by the server when it is able to send an acceptable set of algorithms. If it can't find such a match it must respond with a handshake_failure alert.
	Client Hello	Can be sent in response to a hello request, or to renegotiate the security parameters in an existing connection.
	Hello request	Sent by the server several times. May be ignored by the client.
Server Certificate		Must always be followed by a server hello message if the server whishes to be authenticated. The certificate type must match the key exchange suite's algorithm. For server certification it is possible to have just on. In a client certificate chain there can be several. In a chain all the certification must use algorithms appropriate for the selected key exchange suit.
Server key exchange		Will be sent immediately after the server certificate message (or server hello). This message is only sent when Server Certificate does not contain enough data to exchange a pre-master secret.
Certificate Request		A server can request a certificate from a client. This message must follow the Server Certificate and Server key exchange (if sent).
Server Hello Done		Indicates the end of server hello and associated messages. After sending the "server hello done" the server awaits a client response. The client checks the certificate and other parameters.
	Client certificate	Sent after a Server Hello done. Sent If the server requests a client certificate.
Client key exchange		This message is sent after the client certificate. The pre-master key is sent.
Certificate verify		Explicit verification of a client certificate. Sent by the client following a client certificate. Used to check a client certificate with signing capabilities.
Change Cipher Spec		Sent by the client to the server. The client then copies the pending Cipher Spec into the current spec. Then the client sends the finished message under the new Cipher Spec. When the server receives the Change Cipher Spec it copies the pending cipher spec to the current. It then sends its own finished message.
Finished		Sent at the end of a handshake to verify success of the key exchange and authentication. Once one side has sent its finished message and received and validated the finished message from its peer it may begin to send and receive application data over the secure connection.

Change cipher specification protocol

This protocol exists to signal transitions in the ciphering strategies. It consists of a single message, which is encrypted and compressed under the current connection state. The message consists of a single byte of value 1. The reason to send this protocol is to notify the other party that subsequent records will be protected under the newly negotiated Cipher Spec and keys. The other party will then make the changes necessary and send a finished message back to its peer.

The Change Cipher Spec can be sent either by the server or client. The message is sent before the end of the handshake and after the agreeing of the security parameters. It must be checked that the Change Cipher Spec is received or sent before sending or receiving the finished message. This is an assurance that the messages are protected under the new Change Cipher Spec.

Available Bulk Encryption Algorithms [15 p. 611]

Table 3 The Available Bulk Encryption Algorithms

CIPHER	IS EXPORTABLE	EFFECTIVE KEY BITS
NULL	True	0
RC5_CBC_40	True	40
RC5_CBC_56	True	56
RC5_CBC	False	128
DES_CBC_40	True	40
DES_CBC	False	56
3DES_CBC_EDE	False	168
IDEA_CBC_40	True	40
IDEA_CBC_56	True	56
IDEA_CBC	False	128

Alert Protocol

Alert messages transport how critical the messages are and a description of the alert. Alerts use a four-byte checksum that are calculated from the last record received from the other party. The checksum is done in the following way:

1. Pad the record with zero bytes so that its length is modulo four
2. Divide the result into four-byte blocks
3. XOR these blocks together

The receiver of the alert should verify that the checksum matches with the message earlier sent by him.

There are two alert messages; these are the closure alerts and the error alerts. In the closure alert both the server and client must agree upon a closure of a connection. Any data received after this will be ignored. Concerning error alerts there are two possibilities, either a fatal error alert or a critical one. When one of the parties sends a fatal one, the communication peers must close the connection immediately and remove all of the information concerning the connection. When a critical is sent the connection must be closed, but they may keep the session identifiers and use it to establish a new secure connection.

Different error alert sent in clear text [15: p. 576 & p. 577]

Table 4 Alert messages

Alert name	Description
no_connection	A message was received while there is no secure connection with the sender. This message is fatal or critical. The message is sent in clear text.
bad_record_mac	This alert is returned if a record is received with an incorrect MAC. This message is generally a warning. The message is sent in clear text.
decryption_failed	A WTLSCiphertext decrypted in an invalid way; either it wasn't a multiple of the block length or its padding values, when checked, weren't correct. This message is generally a warning. The message is sent in cleartext.
record_overflow	A WTLSCiphertext record was received which had a length more than allowed bytes, or a record decrypted to a WTLSCompressed record with more than allowed bytes. This message is generally a warning. The message is sent in clear text.
decompression_failure	The decompression function received improper input (e.g., data that would expand to excessive length). This message is generally a warning. The message is sent in clear text.

General understanding of cipher

Ciphers are divided into symmetric or asymmetric ciphers. If sender and receiver have the same key encrypt and it is symmetric, if they have different keys it's asymmetric. PKI (Public key Infrastructure) is a term that comes from the asymmetric chipper technology.

This also provides a means of proving your identity. You encrypt a known message with your private key and send it to a friend. If your friend can decrypt the message correctly using the public key, he can be certain that the message must have come from you and not some impostor claiming to be you. This idea forms the basis of digital signatures.

Well-known asymmetric ciphers include RSA, Diffie-Hellman, DSA and Elliptic Curve

Symmetric ciphers have the advantage of speed. It is a proximally ten to a hundred times faster then asymmetric. Concerning the storage of local files this method will be the preferable. The strength of a symmetric cipher is up to the length of the key. Forty bits is considered weak, 128 and over are considered strong.

Different ciphers work in different ways, but all (good) ciphers have the some following things in common.

?? Their input and output are treated as byte streams.
?? To encrypt the data (to make it unreadable), we use the cipher with a key. The exact form of this key depends on the cipher. Frequently, it can be a simple random number.
?? To decrypt the data (to make it readable again), we use the cipher with a key.

Cryptographic Computations

The cryptographic computations are defined in the presentation language in WAP. The presentation language deals with the formatting of data and external representation similar to TLS.

In order to begin message protection, the WTLS requires specification to a suite of algorithms. These are the master secret, the random client value and the random server value.

A connection state is the operation environment of the Record Protocol. An algorithm is required to generate the connection state from the secure session parameters provided by the handshake protocol. The master secret is hashed into a sequence of secure bytes, which are assigned to the MAC secret, encryption keys and IVs. Encryption schemes is used to provide confidentiality it can also help to provide integrity- and authentication protection.

In WTLS many connection state parameters can be recalculated during a secure connection. This is called the key refresh.

The cipher-suite determines encryption and the MAC algorithms. The key-exchange suite determines key exchange and the authentication algorithms.

When doing a MAC the input data is first divided into the multiple blocks of 5 bytes. Then all blocks are XOR'ed one after another. If the last block is less than 5 bytes, it is padded with 0x00. SHA is much stronger than XOR for generating MACs, although there were no significant attacks reported on XOR MACs, which must be encrypted and is only used for CBC mode block ciphers. XOR is only intended for some devices with very limited CPU resources. Warning: With exportable grade of encryption (e.g., RC5_40), XOR cannot provide as strong message integrity protection as SHA can. It is recommended that the security consequence should be carefully evaluated before XOR MAC is adopted in those environments. In other than MAC operations for message integrity (e.g., PRF) the full-length SHA-1 is used. The cryptographic computations uses three different encryption scheme RSA, DH and ECDH. [15: p.613]

RSA (Rivest-Shamir-Adleman)

The RSA algorithm consists of a digital signatures and encryption. RSA is a public key encryption technique. This means that one key is needed for encryption and a different key is needed for decryption.

It is very difficult to determine the decryption key if you know the algorithm and the encryption key. An additional RSA characteristic is that either of the two keys can be used for encryption with the other used for decryption.

DH (Diffie-Hellman)

This is a key exchange algorithm. This is an algorithm that generates a session key for both parties during an attempt to establish a security association. The algorithm uses each party's unique private value, plus public values. DH allows two individuals to agree upon a shared secret key over an insecure medium, without any prior secret.

EC DH (Elliptic Curve DH)

EC uses mathematical trickery to speed up public-key operations.

Appendix B: Application Code

Answer.xml:

This is the XML document that is generated out of a search in a database.

```
<?xml version="1.0" standalone="yes" ?>
<!--<!DOCTYPE Answer SYSTEM "http://monica.grm.hia.no/secure/wportal/answer.dtd">-->
<Answer>
  <SearchID>1</SearchID>
  <UserID>Operator1</UserID>
  <System Name="Unlimit"></System>
  <Hit>
    <Summary>Dette er en test, Dato: 2000-25-05 17:57:03.0</Summary>
    <Link>http://monica.grm.hia.no/secure/wportal/info/unlimit.wml</Link>
    <Detail>Test detalj informasjon.</Detail>
    <MetadataElement Name="Styrke1" Value="345"></MetadataElement>
    <MetadataElement Name="Styrke2" Value="678"></MetadataElement>
    <Area>
      <Latlong>
        <Latitude>
          <Deg>34</Deg>
          <Min>45</Min>
          <Sec>3</Sec>
          <Dir>N</Dir>
        </Latitude>
        <Longitude>
          <Deg>45</Deg>
          <Min>45</Min>
          <Sec>7</Sec>
          <Dir>E</Dir>
        </Longitude>
      </Latlong>
    </Area>
    <Time>
      <Year>2000</Year>
      <Mon>05</Mon>
      <Day>25</Day>
      <Hour>18</Hour>
      <Min>44</Min>
      <Sec>0</Sec>
    </Time>
    <Source>human</Source>
    <Classification>classified</Classification>
    <Theme>Testing the theme.</Theme>
  </Hit>
  <!--<Hit>
```

```
   <Summary>xxxxx xxxxxxxxx, xxxxx: xx xxxx xxxx, xxxx: xxxxxxxxx, xxxx
                  (xxxxNxxxxxE), Dato: 1999-xx-xx xx:xx:xx.x
   </Summary>
   <Link> http://www.xxxxxx.xxxx.xxx/xxxxxxii.htm </Link>
   <Detail>Tag: xx xxxxx: xxxxxxxxx x xxxxxxxxxxxxx Dato: xxxxxx xxxxxx
             Tag: xx xxxxx: xxxxxxx xx xxxx xxxxxxxx xxx Dato: xxxxxx xxxxxx
   </Detail>
   <MetadataElement Name="Xxxxx" Value="xxxxxx"></MetadataElement>
   <MetadataElement Name="Regnr" Value="xxxxxx"></MetadataElement>
   <Area>
     <Latlong>
       <Latitude>
         <Deg>xx</Deg>
         <Min>xx</Min>
         <Sec>x</Sec>
         <Dir>N</Dir>
       </Latitude>
       <Longitude>
         <Deg>xx</Deg>
         <Min>xx</Min>
         <Sec>x</Sec>
         <Dir>E</Dir>
       </Longitude>
     </Latlong>
   </Area>
   <Time>
     <Year>1999</Year>
     <Mon>xx</Mon>
     <Day>xx</Day>
     <Hour>0</Hour>
     <Min>0</Min>
     <Sec>0</Sec>
   </Time>
   <Source>xxxx</Source>
   <Classification>xxxxxxx</Classification>
   <Theme> xxxxxxxxx xx xxxxxx </Theme>
 </Hit>-->
</Answer>
```

Answerhtml.xsl:

```
<?xml version="1.0" encoding="windows-1252"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl"
              xmlns:HTML="http://www.w3.org/Profiles/XHTML-transitional">

  <xsl:template><xsl:apply-templates/></xsl:template>
  <xsl:template match="text()"><xsl:value-of/></xsl:template>

<xsl:template match="/">
<html>
  <STYLE>
         BODY       { margin:0px; background-color: #FFFFDD; width: 30em;
                    font-family: Arial, Helvetica, sans-serif; font-size: small; }
         H1     { color: #888833;  margin-left: .40em}
         H2     { color: #888866;  margin-left: .60em}
         H3     { color: #888899;  margin-left: .80em}
         P          { margin-top: .5em; margin-bottom: 0.5em; margin-left: 1em}
  </STYLE>
 <body bgcolor="white">

<H1>Systemname : <xsl:value-of select="Answer/System/@Name"/></H1>
<table>
<tr>
 <td><b>User Information : </b> <xsl:value-of select="Answer/UserID"/></td>
</tr>
</table>

<table>
 <xsl:for-each select="Answer/Hit">
 <tr>
  <td>
          <table>
          <tr>
          <td>
                    <P>
                    <hr></hr>
                    Summary : <xsl:value-of select="Summary"/><br/>
          Link :    <xsl:value-of select="Link"/><br/>
                    Detail :  <xsl:value-of select="Detail"/> </P>
                    </td>
          </tr>
          <tr>
                    <td>
                    <b>Latitude</b><br/>
                    Deg : <xsl:value-of select="Area/Latlong/Latitude/Deg"/><br/>
                    Min : <xsl:value-of select="Area/Latlong/Latitude/Min"/><br/>
          Sec : <xsl:value-of select="Area/Latlong/Latitude/Sec"/><br/>
          Dir : <xsl:value-of select="Area/Latlong/Latitude/Dir"/>
                    </td>
                    <td>
                    <b>Longitue</b><br/>
                    Deg : <xsl:value-of select="Area/Latlong/Longitude/Deg"/><br/>
          Min : <xsl:value-of select="Area/Latlong/Longitude/Min"/><br/>
          Sec : <xsl:value-of select="Area/Latlong/Longitude/Sec"/><br/>
          Dir : <xsl:value-of select="Area/Latlong/Longitude/Dir"/>
              </td>
                    <td>
                    <b>Time</b><br/>
                    <xsl:value-of select="Time/Year"/>-
                    <xsl:value-of select="Time/Mon"/>-
                    <xsl:value-of select="Time/Day"/><br/>
                    <xsl:value-of select="Time/Hour"/>:
                    <xsl:value-of select="Time/Min"/>:
                    <xsl:value-of select="Time/Sec"/>
                    </td>
          <tr>
                    <td>

                    Source        : <xsl:value-of select="Source"/><br/>
                    Classification : <xsl:value-of select="Classification"/><br/>
                    Theme         : <xsl:value-of select="Theme"/>
                    <hr></hr>
                    </td>
          </tr>
          </tr>
    </table>
  </td>
          </tr></xsl:for-each>
</table>

 </body>
</html>

</xsl:template>
  <xsl:template match="p">
    <P><xsl:apply-templates/></P>

</xsl:template>
</xsl:stylesheet>
```

Answerwml.xsl:

When it is a WAP-compliant browser the Anserwml.xsl will generate WML and send it to the terminal.

```
<?xml version="1.0"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/TR/WD-xsl"
xmlns="http://www.w3.org/TR/wbxml">
<xsl:template>
<xsl:apply-templates/>
</xsl:template>
<xsl:template match="text()">
<xsl:value-of/>
</xsl:template>
<xsl:template match="/">
<xsl:pi name="xml">version='1.0'</xsl:pi>
<xsl:eval no-entities="true">'<![CDATA[<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD
WML 1.1//EN" "http://www.wapforum.org/DTD/wml_1.1.xml">]]>'</xsl:eval>

<wml>

<template>
        <do type="prev">
        <prev/>
        </do>
</template>

<card id="Answer">
        <do type="accept">
        <go href="#info"/>
        </do>
        <p align="center">
        <small>
        <xsl:value-of select="Answer/UserID"/><br/>
        System-name : <br/>
        <xsl:value-of select="Answer/System/@Name"/>
        </small>
        </p>
</card>

<xsl:for-each select="Answer/Hit">

        <card id="info">
                <do type="accept">
                <go href="#location"/>
                </do>
                <p align="center">
                <b>NEW HIT</b><br/>
                <small>
                <xsl:value-of select="Classification"/><br/>
                <xsl:value-of select="Source"/><br/>
                <xsl:value-of select="Theme"/>
                </small>
                </p>
        </card>

        <card id="location">
                <do type="accept">
                <go href="#time"/>
                </do>
                <p align="center">
                <small>
                <b>Location</b><br/>
                <table columns="3">
                <tr><td></td><td> <b>Lat</b> </td><td> <b>Long</b> </td></tr>
                        <tr><td>Dir </td><td> <xsl:value-of
select="Area/Latlong/Latitude/Dir"/></td><td><xsl:value-of
select="Area/Latlong/Longitude/Dir"/> </td></tr>
                        <tr><td>Deg </td><td> <xsl:value-of
select="Area/Latlong/Latitude/Deg"/></td><td><xsl:value-of
select="Area/Latlong/Longitude/Deg"/> </td></tr>
                        <tr><td>Min </td><td> <xsl:value-of
select="Area/Latlong/Latitude/Min"/></td><td><xsl:value-of
select="Area/Latlong/Longitude/Min"/> </td></tr>
                        <tr><td>Sec </td><td> <xsl:value-of
select="Area/Latlong/Latitude/Sec"/></td><td><xsl:value-of
select="Area/Latlong/Longitude/Sec"/> </td></tr>
                </table>
                </small>
                </p>
        </card>

        <card id="time">
                <do type="accept">
                <go href="#location"/>
                </do>
                <p align="center">
                <small>
                <br/>
                <b>Time</b><br/>
                <xsl:value-of select="Time/Year"/> -
                <xsl:value-of select="Time/Mon"/> -
                <xsl:value-of select="Time/Day"/><br/>
                <xsl:value-of select="Time/Hour"/> :
                <xsl:value-of select="Time/Min"/> :
                <xsl:value-of select="Time/Sec"/>
```

```
                    </small>
                    </p>
          </card>
</xsl:for-each>
</wml>

</xsl:template>

<xsl:template match="CONTENT">
          <xsl:apply-templates/>
</xsl:template>
<xsl:template match="p">
          <xsl:apply-templates/>
          <br/>
</xsl:template>
</xsl:stylesheet>
```

index.asp:

This file will check if it is an html-browser or a WAP-browser that are entering and open the corresponding file.

```
<%



  Set XMLDoc = Server.CreateObject("Microsoft.XMLDOM")
  Set XSLDoc = Server.CreateObject("Microsoft.XMLDOM")
  XMLDoc.Async = false    'don't do anything before XML is loaded
  XMLDoc.load(Server.MapPath("answer.xml"))

   if InStr(Request.ServerVariables("HTTP_USER_AGENT"), "Mozilla") then

    'we have a web browser

     xslfile = "answerhtml.xsl"
     XSLDoc.async = false
     XSLDoc.load(Server.MapPath(xslfile))
     Response.Write XMLDoc.transformNode(XSLDoc.documentElement)
     Response.End

  else

     'we have a WAP user agent

     Response.ContentType = "text/vnd.wap.wml"

     xslfile = "answerwml.xsl"
     XSLDoc.async = false
     XSLDoc.load(Server.MapPath(xslfile))
     Response.Write XMLDoc.transformNode(XSLDoc.documentElement)
     Response.End
  end if

%>
```

index.wml:

After the login, the terminal will enter the index start-page.

```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">
<!-- Source Generated by WML Deck Decoder -->
<wml>
        <!-- Back and home -->
        <template>
                <do type="accepet" name="exit" label="Back">
                        <prev/>
                </do>
        </template>

        <!-- Introduction card -->
        <card id="card1" title="Welcome" ontimer="#card2">
                <timer value="50"/>
                <p align="center">
                        <img src="image01.wbmp" alt="NIS"/><br/>
                </p>
        </card>

        <!-- Introduction -->
        <card id="card2" title="Menu" newcontext="true">
                <p align="center">¤¤¤¤<small>WPortal</small>¤¤¤¤
                <a href="index.asp">[Answer]</a>
                </p>
        </card>
</wml>
```

conndb.asp:

This file connects the application up to the user-database.

```
<%      option explicit

        Dim conn    'connection to a access datatbase

   Set conn = Server.CreateObject("ADODB.Connection")
        'DSN-less connection to access
conn.Open "DRIVER={Microsoft Access Driver (*.mdb)};DBQ=" &
Server.MapPath("user.mdb") & ";"

%>
```

login.asp:

Here the user has to enter its username and password.

```
<!--#include file="conndb.asp" --><%
   'send the right MIME type
   Response.ContentType = "text/vnd.wap.wml"

   Dim SQLquery
        Dim rsUser
%>
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">

<wml>
        <card id="card1" title="Username">
        <p align="center">
        <small>
        <%
                SQLQuery = "SELECT [username] FROM User"
                set rsUser = conn.Execute(SQLquery)

                if rsUser.eof then
         rsUser.close
         set rsUser = nothing
         Response.write("There are no users in the database")
         Response.write("</p></card></wml>")
         Response.end
                end if
        %>
                </small>
        <br /><br/>
                <select name='user'>
        <%
                Do while not rsUser.eof
                 response.write("<option value='" & rsUser("username") & "'>" &
rsUser("username") & "</option>" & vbcrlf)
         rsUser.MoveNext
                loop
        %>
                </select><br/>
                <small>
                <anchor title="Password">NEXT
                        <go href="#password">
                         <postfield name="user" value="$(user)" />
                        </go>
                </anchor>
                </small>
        </p>
        <%
                rsUser.close
                'conn.close
                set rsUser = nothing
        %>
        </card>

        <card id="password" title="Password">
                <p align="center">
                <br/>
                <input name="pword" type="password"/><br/>

                <small>
                <anchor title="Check">LOGIN
                        <go href="login2.asp">
                         <postfield name="user" value="$(user)" />
                         <postfield name="pword" value="$(pword)" />
                        </go>
                </anchor>
                </small>
                </p>
        </card>
</wml>
```

login2.asp:

This file checks to see if the user entered the correct password belonging to the username.

```
<!--#include file="conndb.asp" -->
<%
    'send the right MIME type
    Response.ContentType = "text/vnd.wap.wml"

    Dim SQLquery
    Dim rsCheck
    Dim check

    'user = Request("user")
    'pword = Request("pword")

    SQLquery = "SELECT * FROM user WHERE username = '" & Request("user") & "'
and password='" & Request("pword") & "'"
    set rsCheck = conn.Execute(sqlQuery)

    if rsCheck.eof then
        'rsCheck.close
    'set rsCheck = nothing
    'Response.end
        check = 0
    else
        check = 1
    end if

    rsCheck.close
    set rsCheck = nothing
%>

<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD WML 1.1//EN"
"http://www.wapforum.org/DTD/wml_1.1.xml">

<wml>
    <% if check = 1 then %>
        <card id="redirect" ontimer="http://localhost/secure/wportal/index.wml">
            <!--<do type="accept" label="OK">
                <go href="http://localhost/secure/wportal/index.wml"/>
            </do>-->
            <timer value="20"/>
            <p align="center">
            <small>
            Correct password. <br/>You can enter.<br/>
            </small>
            </p>
        </card>
    <% else %>
        <card id="redirect" ontimer="login.asp">
            <!--<do type="accept" label="Again">
                <go href="login.asp"/>
            </do>-->
            <timer value="20"/>
            <p align="center">
            <small>
            Wrong password. <br/>Try again.<br/>
            </small>
            </p>
        </card>
    <% end if %>
</wml>
```