

# Wireless Security Primer

(Technology Security CIO Office TELUS Mobility)



# Wireless Security Primer

## (Technology Security CIO Office TELUS Mobility)

### Contents

1. Introduction .....	3
2. Business Drivers .....	4
2.1 Mobile Enterprise Computing .....	4
2.1.1 Horizontal Applications .....	5
2.1.2 Vertical Applications .....	5
2.2 Mobile Commerce .....	5
2.3 Mobile Services .....	5
2.4 Why Security is so important .....	6
3. Information Security Overview .....	6
3.1 Privacy and Confidentiality .....	6
3.2 Data Security .....	6
3.2.1 Identification, Authentication and Authorization .....	6
3.2.2 Encryption .....	6
3.2.3 Digital Signature .....	7
3.2.4 Public Key Infrastructure (PKI) .....	8
3.2.5 Integrity and Message Authentication .....	8
3.2.6 Non-repudiation .....	9
3.3 Network Security .....	9
3.3.1 Firewall .....	9
3.3.2 Virtual Private Network (VPN) .....	9
3.4 Application Security .....	10
3.4.1 Secure Socket Layer .....	10
3.4.2 Http Authentication .....	11
4. Wireless Security .....	11
4.1 Airlink Security .....	11
4.1.1 CDMA and 1X .....	11
4.2 Wireless Application Protocol (WAP) Security .....	12
4.2.1 Wap Architecture .....	12
4.2.2 WTLS .....	13
4.2.3 WAP Gap .....	14
4.2.4 WAP 2.0 .....	14
4.3 Mobile Device Security .....	15

4.3.1 Security Risks .....15  
4.3.2 Security Measures .....15  
5. Conclusion .....16  
6. Glossary .....17

©TELUS Mobility August, 2002. This document contains forward-looking statements about products, services, and technologies that are subject to certain risks and uncertainties and may change without notice. TELUS Mobility disclaims any intention or obligation to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise. For current information on TELUS Mobility product offerings please refer to [www.telusmobility.com](http://www.telusmobility.com).

# 1. introduction

The arrival of Third Generation (3G) wireless networking technologies has opened up a new horizon for the provision of timely and effective mobile wireless data services. They offer a substantial performance and cost advantage over Second Generation (2G) technologies and provide users with a much more fulfilling anytime, anywhere multimedia connection experience.

The increased intensity of business competition has driven enterprises of all sizes to find ways to improve productivity, increase speed to market, and introduce competitive differentiation by adding content and value adds to their products and services. Secure, high-speed wireless connectivity coupled with advanced mobile wireless devices such as smart phones, personal digital assistants (PDAs), and wireless modem cards, will enable businesses to operate faster, better, more cost-effectively, and more profitably through the use of always available content and feature-rich applications.

The number of digital wireless phones in use is expected to reach one billion worldwide by 2005 with the number of wireless Internet users predicted to exceed the number of wired PC Internet users by 2004. The use of wireless devices to access commercial applications such as mobile banking, brokerage and retailing will soon become a fundamental part of modern business. A new generation of consumers will start buying groceries, paying bills, purchasing clothes, playing games, and seeking expert advice over the wireless Internet. Mobile business-to-business (B2B) and business-to-consumer (B2C) transactions will prosper only if the industry succeeds in fostering a reliable and trusted global Mobile-Commerce (M-Commerce) environment.

In the traditional wired environment, security is a well-established discipline as we can always use a physical boundary to limit the scope of one's access so that the proper security controls can be put in place. However, in a wireless environment, the boundary is in the air making it much harder to monitor unauthorized access, especially in an always on scenario. Furthermore, mobile devices are getting smaller and smaller so that their chance of being lost is significantly higher. Therefore, the success of 3G wireless enterprise computing will depend upon an enterprise's capability to provide end to end security for both its wired and wireless computing environments.

## 2. Business Drivers

A recent Meta Group study has indicated that mobile wireless transactions will account for nearly 20% of all B2B transaction volume and 25% of all B2C transaction volume by 2003. Qualcomm has predicted that increasing data rates and a substantial improvement in usability will drive data traffic demand to over 200 megabytes per user, per month by 2006.

Recent trends also indicate a push of mobile computing into the business-to-employee (B2E) space so that enterprises can collect and share more information, their workers become more skillful and knowledgeable, and the quality of their products and services is improved significantly over time.

### 2.1 mobile enterprise computing

Most mobile enterprise computing applications fall into one of two categories: horizontal or vertical applications. Notebooks are the most widely used mobile devices. Other devices include e-mail pagers, PalmOS and

PocketPC devices, cellular phones with microbrowsers (Wireless Application Protocol, WAP), and smart phones.

### 2.1.1 horizontal application

Horizontal applications are applications that are generic enough to be used across industries, such as e-mail, instant messaging (text, SMS), web browsing, calendaring and other collaboration tools, which are mostly productivity applications. Most horizontal applications are already pervasive throughout the mobile community, with e-mail being the most popular.

### 2.1.2 vertical application

Vertical applications are applications that are tailored to a specific industry with customized functionality, such as:

- Enterprise Resource Planning (ERP) tools such as PeopleSoft and SAP),
- Customer Relationship Management) (CRM),
- Sales Force Automation) (SFA),
- Customer Information System) (CIS)
- Inventory Control System (ICS)
- Automatic Vehicle Tracking (AVL).

These applications more difficult and expensive to move to the mobile environment.

## 2.2 mobile commerce

International Data Corporation (IDC) forecasts that \$21 billion worth of M-Commerce will take place in 2004, while Gartner Group predicts that 40% of B2C E-commerce in that same year will occur over wireless connections.

Early wireless applications such as field service and dispatch facilitate commerce but do not involve financial transactions.

Recent M-Commerce applications focus on transactions in which a user securely purchases or sells goods or services, involving a combination of location technology, financial settlement systems, devices and networks. Examples are financial trading, buying tickets, ordering from restaurants, updating financial portfolios, conducting banking transactions and comparison shopping.

- electronic wallets, which will be hosted by portals, application service providers (ASPs), banks or carriers to facilitate transactions by providing a centralized way for users to maintain account and shipping information;
- new location technologies, which will enable M-Commerce applications to take a user's location into account for access to localized and personalized information;
- electronic cash (Ecash) technologies, which will use new financial settlement systems to allow secure transmission of electronic cash on a wide-area or local-area basis, thus replacing the use of cash, checks and credit cards.

## 2.3 mobile services

The advent of mobile wireless technologies has given service industries new avenues to provide cost-effective, always there, right-at-your-finger-tip, customer-centred services. Service providers can now use various wireless Internet and wireless techniques (such as paging, one and two way short messaging) to manage customer relationships partners in order to provide more timely and responsive customer services.

High speed mobile wireless data services will provide businesses with new abilities to create services and products for their customers.

## 2.4 why security is so important

As businesses move towards the use of mobile devices over the wireless Internet and wireless WAN/LANs to access company and customer information systems, more stringent security measures will need to be put in place to ensure that such information is protected against the additional risks introduced by the more vulnerable wireless environment.

Wireless applications can succeed only if all the players are confident that transactions cannot be fraudulently generated or altered, that transactions are legally binding, and that the confidentiality of private information is adequately protected.

## 3. Information Security Overview

This section will introduce some basic security concepts and terminology that will be used in later sections when security mechanisms are discussed.

### 3.1 privacy and confidentiality

Communication is considered private when only the communicating parties are able to understand the contents of the transferred information. Privacy can be achieved by using cryptographic algorithms that encrypt the transferred information in a form that is too expensive or time consuming for outsiders to break.

Proper authentication, authorization and access control techniques can be used to protect the confidentiality of information so that only authorized parties are allowed to access such information.

### 3.2 data security

#### 3.2.1 identification, authentication and authorization

Identification is the process used to establish the identity of a communicating party that can be trusted.

Authentication is the process with which the communicating parties can be sure that the other party is who it claims to be. Authentication mechanisms can be based on a challenge-response protocol such as username/password prompt or a digital signature as described below in section 3.2.3.

Authorization is the process to ensure that only particular parties have the privilege to access particular information. Various access control techniques can be used to allow only authorized parties to access sensitive and confidential information.

#### 3.2.2 encryption

Encryption is the transformation of plain text into an unintelligible form called ciphertext through a mathematical process (cryptographic algorithm). The ciphertext may only be understood by someone who has the key that can be used to decrypt the cipher text.

Cryptographic algorithms fall into three main categories:

- Symmetric Cryptography is based on the use of a secret key that is shared between the communicating parties, i.e., the same key is used to encrypt and decrypt the data. Typical algorithms used are DES, RC4 and RC5.
- Asymmetric Cryptography or Public Key Cryptography is based on the use of a pair of public and private keys associated with each party. Messages encrypted using the public key can only be decrypted using the corresponding private key, and messages digitally signed using the private key can be verified using the corresponding public key. Typical algorithms used include RSA and ECC (Elliptic Curve Cryptography).
- Message Digest Algorithms or Hash Algorithms are used to calculate a message digest, which is a value computed by a one-way function (hash function) from some data. A one-way function means that it is impossible to construct the original piece of information from the digest and that it is extremely difficult to construct another piece of information that has the same digest. Typical algorithms used include MD5 and SHA-1.

### 3.2.3 digital signature

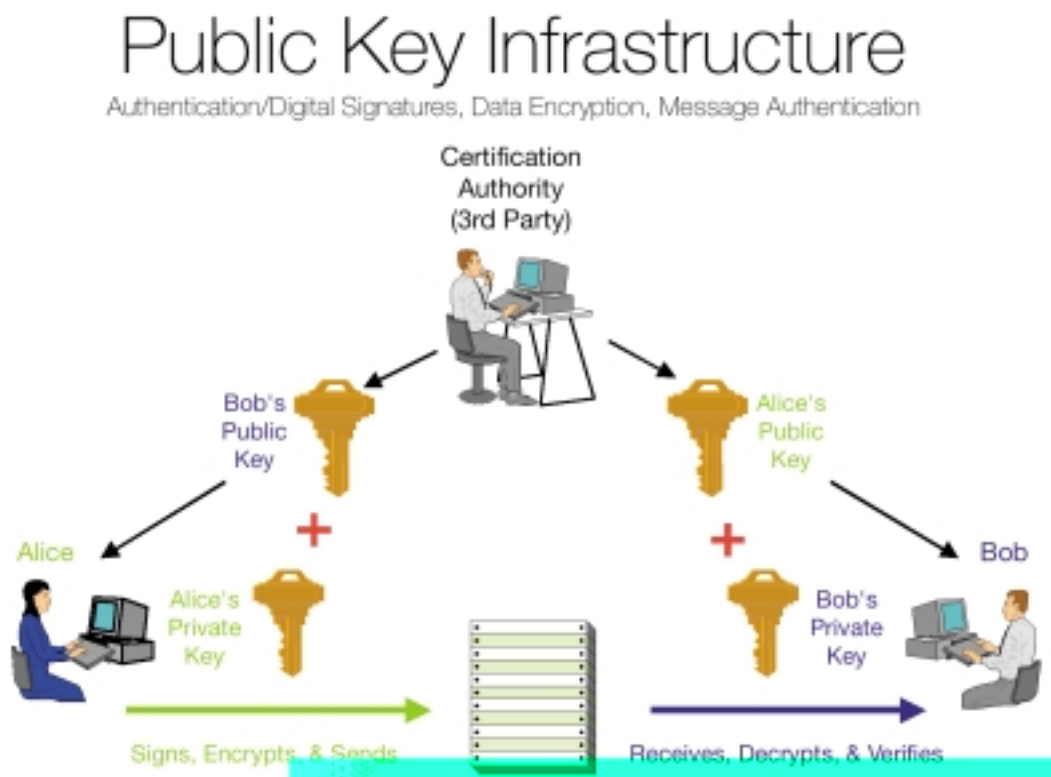
A digital signature is a technique used to prove that a piece of information has been created by a communicating party, and that it has not been tampered with during transmission. A message is signed digitally by first calculating its message digest and then encrypting the message digest with the originating party's private key. If the recipient is able to decrypt the digest using the originating party's public key, then it is sure that the message comes from the originating party. By re-computing the digest, the recipient can ensure the integrity of the message.

### 3.2.4 public key infrastructure (PKI)

A Public Key Infrastructure (PKI) is a system that uses asymmetric key (or public key) encryption to provide security services such as proof of identity, data privacy, non-repudiation and data integrity.

A digital or public key certificate is an electronic document binding together a communicating party's identity and his/her public and private key pair. Digital certificates and digital signatures are elements of PKI.

In order to ensure that a communicating party's public key used for encryption or digital signature verification purposes really belongs to that party, it has to be obtained from a trusted source, the Certification Authority (CA) who issued the original digital certificate to that party. A digital certificate is issued to a person or a party for a specific period of time after the CA has verified his/her identity, and the CA has the ability to revoke the certificate upon its expiry.



### 3.2.5 integrity and message authentication

Content integrity means that the receiving party can be sure that the transferred information is exactly what the other party originally sent. Integrity can be established by computing a message digest and attaching it in every message before the message is sent. The receiving party can then re-compute the digest and compare it to the original digest.

### 3.2.6 non-repudiation

Non-repudiation means that once someone has received a message, the sender cannot deny having sent it. Non-repudiation can be implemented using digital signature, which in some countries is as legally binding as a hand-written signature.

## 3.3 network security

### 3.3.1 firewall

A firewall is a security mechanism used to protect a network from harmful attacks or intrusion from outside that network. It may be comprised of hardware and/or software.

- **Packet Filtering Firewall.** This type of firewall screens all packets passing through it. It may look at values such as the source IP address, the destination and some basic information contained in the packet. At a simple level, a network router can function as a packet screening firewall directing or deflecting packets based on source, destination and purpose.
- **Application Proxy Firewall.** This type of firewall acts as a broker between clients and services providing much more sophistication than packet screening firewalls. They operate at the application level and can make very detailed policy decisions about the traffic going through it. Proxy firewalls can also change the IP address of a client in order to hide the address from the outside service (referred to as Network Address Translation – NAT).

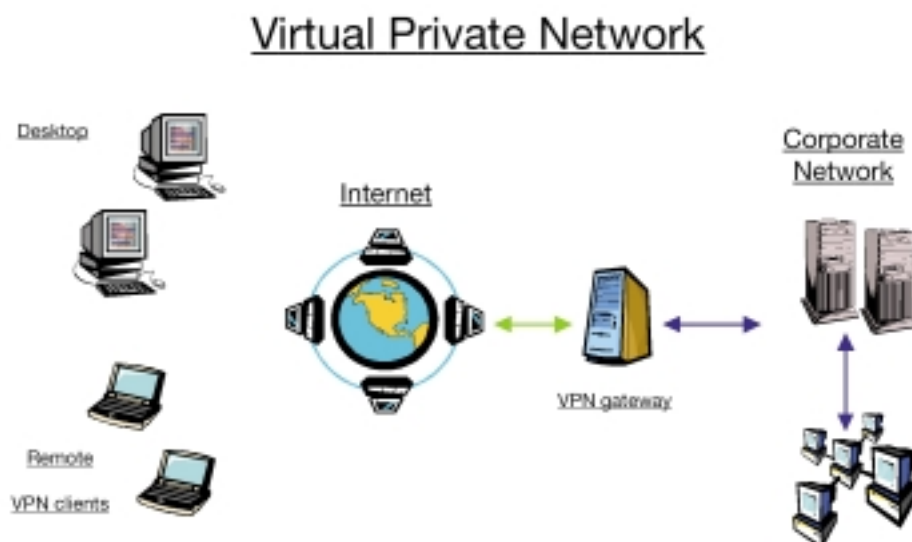
### 3.3.2 virtual private network (VPN)

A Virtual Private Network (VPN) is a private, encrypted, communication tunnel that connects a remote user or office to the enterprise network over the Internet instead of over a dedicated dial-up phone line.

A secure VPN is a VPN connection with strong authentication to ensure that the remote users tapping into the organization's network are really whom they say they are.

A typical VPN works like this:

- the remote user connects to the internet Point of Presence (POP) (dial-up, ADSL, or wireless); and the connection is then encrypted, and tunneled through the Internet, and established with the destination server located.



VPNs are typically used for the following scenarios:

- Remote user access which allows remote users to connect to the corporate LAN via the Internet;
- LAN-to-LAN connectivity which consolidates LAN traffic of remote offices onto a high-speed Internet connection;
- Extranets which provide LAN-to-LAN connectivity between the enterprise and its business partners, customers and even suppliers.

Internet Protocol Security (IPSec) is a standard developed by the Internet Engineering Task Force (IETF) for providing network-layer authentication, access control, encryption, message integrity and replay protection for securing communications between network devices and applications.

IPSec offers two modes of operation: transport and tunnel. With transport mode, the security endpoints correspond with the communication endpoints (i.e., sender and recipient), providing end-to-end security for traffic that passes across a multi-segment network, such as the Internet. In tunnel mode, security is applied on one or more network segments between the sender and recipient resulting in security that is transparent to the communication endpoints, i.e., neither the sender nor the recipient needs to be IPSec-aware.

In a typical VPN environment, device identification is performed through the exchange of a single, shared secret key. As IPSec supports the use of industry standard X.509 digital certificates, IPSec-compliant VPN is more appealing for enterprises that have already invested in Public Key Infrastructure (PKI).

## 3.4 application security

### 3.4.1 secure socket layer

Secure Socket Layer (SSL) is a transparent software layer that is located above TCP/IP and below the application protocols in the protocol stack to provide privacy between two communicating applications by performing the following functions:

- establishing a secure connection between two computers;
- transparently encrypting and decrypting information transferred over the secure connection; and
- ensuring message integrity using message digests.

As SSL is transparent and not sensitive to data content, it can be used to secure any kind of transaction. When establishing a secure connection, the communicating parties set up a normal HTTP connection plus:

- negotiate the cryptographic algorithms to be used;
- negotiate a secret key used in the communication; and
- optionally authenticate each other.

After executing this handshake protocol, SSL encrypts and decrypts transferred information transparently.

With SSL, privacy of communication is based on symmetric encryption (RC4). An asymmetric algorithm (RSA) is used during handshake to negotiate the secret key for symmetric encryption. Content integrity is implemented by digitally signing the transferred information using MD5 or SHA. Authentication takes place using X.509 certificates.

### 3.4.2 http authentication

There are three types of HTTP authentication:

- **HTTP Basic Authentication** which provides a simple challenge-response authentication mechanism that may be used by a server to challenge a client request and by a client to provide authentication information such as a username/password combination. One problem with this approach is that the username and password are passed over the network in clear text.
- **HTTP Digest Authentication** which uses hashing for the challenge-response authentication. When the client contacts the server, a challenge message is issued to the client. This is operated on using a hashing algorithm such as MD5 and the password. The corresponding hash is sent back to the client where it is compared to the server hash. Based on this comparison the client will gain access to the server or will be denied access.
- **HTTP Proxy Authentication** which acts between a proxy server and the client rather than the origin server. The client requests the protected resource through the proxy which sends a challenge. The client responds with a username/password combination. If this combination is acceptable to the proxy, then the client gains access to the resource through the proxy.

## 4. Wireless Security

This will provide an overview of current and future wireless technologies and appropriate security mechanisms used by TELUS Mobility in the provision of mobile wireless data services to its customers.

### 4.1 airlink security

#### 4.4.1 CDMA and 1X

Code Division Multiple Access (CDMA) technology was originally developed for U.S. military use over 50 years ago and was commercially introduced by QUALCOMM for cellular use in 1995. CDMA is a spread spectrum technology that splits sound into small segments that travel on a spread spectrum of frequencies.

Privacy is inherent in the way CDMA works. Each call is spread over a 1.25MHz carrier, which is much wider bandwidth than that which is required for a single call. Each segment of conversation (or data) is identified by a digital code known only to the CDMA phone and the base station. This means that virtually no other device can receive the call.

CDMA's digitally encoded transmissions are designed using over 4.4 trillion codes, which resists eavesdropping and virtually eliminates cloning and other types of fraud. As a result, CDMA is inherently secure, offering users a high degree of confidence that transmissions are not readily intercepted, and is quite unlike its analog predecessor.

CDMA IS-95 (or cdmaOne) networks are 2G CDMA networks with data rates that can reach a maximum of 144 kbps.

CDMA2000 1x technology is a 3G technology that offers both voice and data services. It provides up to twice the capacity of earlier CDMA systems with data rates that can reach a theoretical maximum of 144 kbps, without

sacrificing voice capacity for data capabilities. Furthermore, CDMA2000 1x technology is backward-compatible with earlier CDMA technology, providing an easy and affordable upgrade path for both wireless carriers and consumers.

## 4.2 wireless application protocol (WAP) security

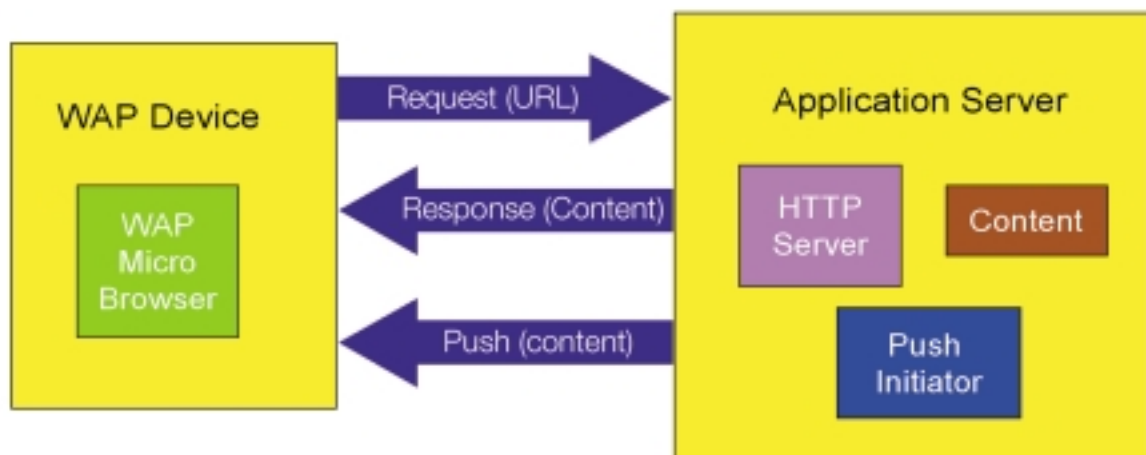
The Wireless Application Protocol (WAP) is a worldwide standard for providing Internet communications and advanced services on digital mobile phones, pagers, personal digital assistants and other wireless devices. The WAP Forum was formed in December 1997 to bring together service providers, device and infrastructure manufacturers, Internet content providers and application developers to develop and promote a set of communication protocols for wireless devices to ensure the interoperability and growth of the wireless Internet-based services.

### 4.2.1 WAP architecture

The WAP system architecture is based on the World Wide Web programming model. It is optimized to suit the characteristics of a mobile network and the limited form factors of the wireless devices (i.e., one-finger navigation, smaller screens, and limited RAM/ROM).

The Wireless Markup Language (WML), which is the core markup language of WAP, provides the foundation of a microbrowser specifically designed to support the unique characteristics of the wireless devices. While the content and applications are hosted on the Web servers, the microbrowser software within the wireless device interprets the byte code and displays the interactive WAP content (WML and WMLScript).

### WAP Programming Model



A facility, called the WAP gateway, is placed at an access point to the Internet between a WAP client and the supporting Web server. The gateway converts the protocols and data formats between the client (WAP-compliant protocol) and the server (Internet standard protocol).

WAP defines a Wireless Application Environment (WAE) to enable carriers, manufacturers and content developers to develop advanced differentiating services and applications including the microbrowser, scripting facilities, email,

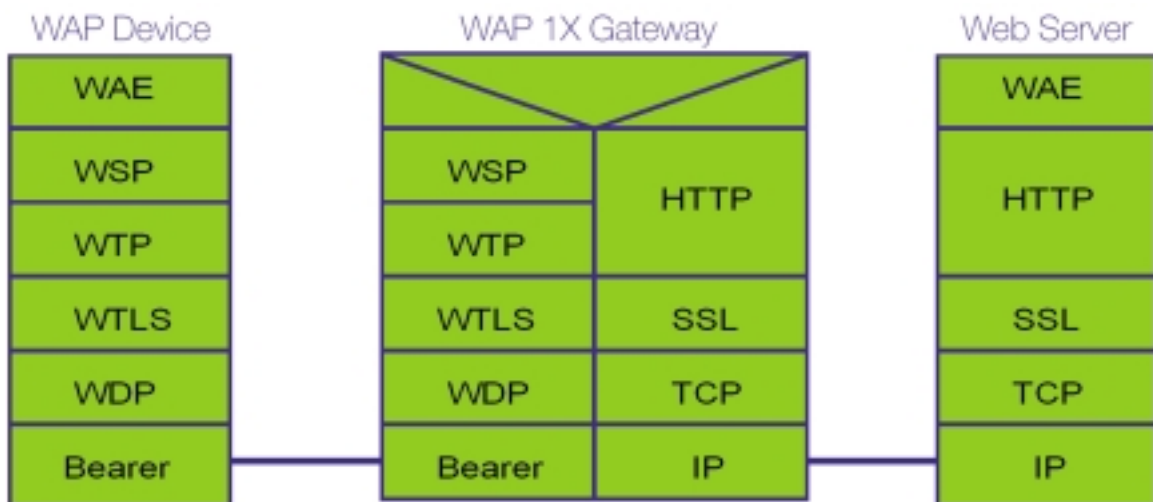
World Wide Web, mobile handset messaging and mobile to telefax access.

The Wireless Session Protocol (WSP) provides a lightweight session layer to allow sufficient exchange of data between applications.

The Wireless Transaction Protocol (WTP) provides transaction support, adding reliability to the datagram service provided by WDP.

The Wireless Transport Layer Security (WTLS) is an optional security layer providing encryption facilities at the Transport level for applications.

The Wireless Datagram Protocol (WDP) is the transport layer that sends and receives messages via any available bearer network, such as CDMA, GSM, TDMA, iDEN and CDPD.



#### 4.2.2 WTLS

The Wireless Transport Layer Security (WTLS), an optional security layer, provides transport level encryption facilities and transparently encrypts and decrypts information sent between a WAP client and a WAP gateway so that the communication between the two cannot be understood or altered by a third party.

There are 3 different versions of the WTLS protocol as defined by its authentication type:

- no security
- share secret-based authentication
- public key-based authentication

Furthermore, WTLS comes in 3 classes:

- Class 1 allows for an anonymous secured channel between the WAP client and the WAP gateway.
- Class 2 includes all the features of Class 1 plus server authentication.
- Class 3 includes all the features of Class 2 plus client authentication.

### 4.2.3 WAP gap

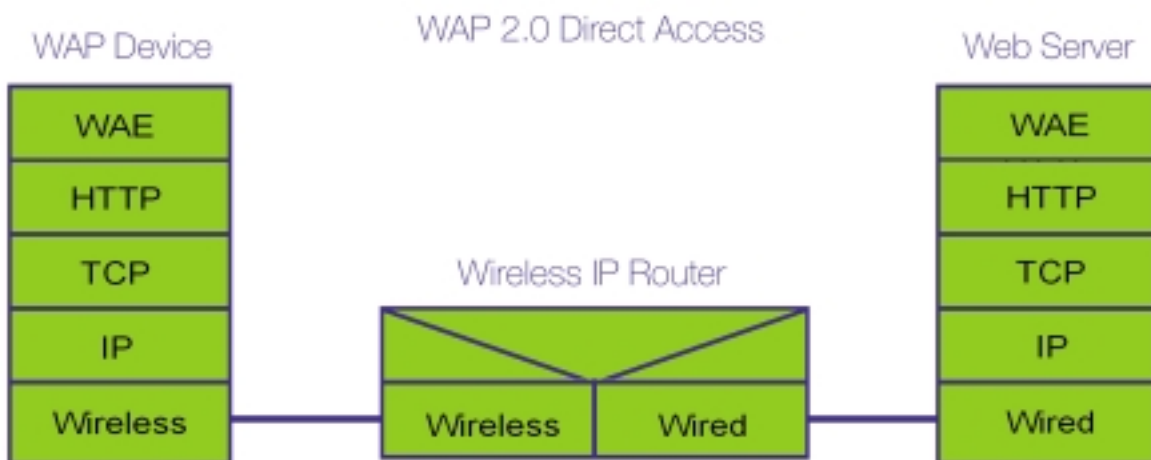
WAP defines the transfer of information between a WAP client and a Web server through a WAP gateway. However, the WAP protocol only covers the portion of the transmission between the WAP client and the WAP gateway. It relies on existing Internet protocols for the transmission between the WAP gateway and the Web server. If an application uses WTLS to encrypt and secure the link between the WAP client and the WAP gateway, the data will need to be decrypted at the WAP gateway and re-encrypted using SSL for the secure transmission between the WAP gateway and the Web server. The split second when such decryption and encryption occurs in the WAP gateway is known as the WAP gap.

WAP gateways use the following approaches to limit such exposure:

- Data is unencrypted only in the WAP gateway memory and is not written to any permanent storage medium.
- Data is only unencrypted for the shortest possible time (typically microseconds).
- Physical access to the WAP gateway host machine is restricted to a few authorized personnel.

### 4.2.4 WAP 2.0

The WAP Forum released version 2.0 of the WAP specifications in July 2001 in an effort to adopt the most recent Internet standards and protocols into the WAP standard, including the support for TCP, TLS and HTTP, and the elimination of the requirement of a WAP proxy (or gateway) and the WAP gap exposure.



## 4.3 mobile device security

This section will discuss the security threats that mobile devices such as laptops, digital phones or Personal Digital Assistants (PDAs) are susceptible to, especially under the always-connected scenario, and identify some of the security measures that can be taken to protect such devices.

### 4.3.1 security risks

As mobile business applications are bringing significant benefits to enterprises that need to operate close to their customers and business partners, they also introduce greater security risks to the corporate networks and enterprise computing environments. The access can be from anywhere, anytime so that the devices can no longer be protected by traditional security applications such as the corporate firewall or centralized anti-virus scanning. Furthermore, the mobile devices being used are getting smaller and smaller so that the chance of being stolen or lost is much higher, putting company confidential information stored on such devices at risk. As a result, protecting company mobile devices requires security applications on every device.

### 4.3.2 security measures

Protection is always needed for both the communication channel and the data stored on the mobile devices.

It is important that the appropriate authentication and authorization mechanisms are in place to ensure that unauthorized users cannot use the devices to access the corporate networks or other services that he/she is not authorized to access. Furthermore, proper device authentication will also prevent unauthorized access of confidential or sensitive data stored on such devices. Content encryption can also be used to protect data stored on such devices.

In order to prevent the mobile devices from introducing harmful contents such as viruses to the corporate networks, anti-virus software should be installed on such devices and virus scanning should be performed on a regular basis. Currently a few security vendors provide anti-virus software that runs on the Palm, Windows CE (Pocket PC) or other handheld device operating systems.

For mobile devices with operating systems that provide VPN support such as Palm and Windows CE, VPN clients can be installed on such devices to ensure secure access to the corporate networks or other corporate services.

## 5. Conclusion

Wireless security is not much different from wired security. Organizations want several things from any secure network. The first is to identify, authenticate and authorize users. The second is to secure the data on the end user device, and as it travels from the end user device to the destination host. The third is to ensure that data integrity is intact, ie. that traffic has not be altered en route.

At TELUS Mobility, network reliability starts with designing our networks right, the first time. Carrier class security is deployed in our core network, with secure links between network elements and highly controlled access to network infrastructure. The inherent security associated with the CDMA airlink minimizes risks such as cloning, eavesdropping and transmission interception over the wireless network. 1X users will be required to enter user id and password in order to access the network, further securing the transmission by first authorizing the user.

Mobile devices extend the reach of the enterprise network, and therefore need to be considered when deploying enterprise-wide security. In the past, wireless has faced unique difficulties such as limited bandwidth, high latency and unstable connections. Now, the faster nature of TELUS Mobility's 1X network creates the opportunity for organizations to extend existing wireline security methods to mobile wireless devices.

In order to achieve secure end to end connections in the wired world, client/server VPN solutions and SSL connections have become increasingly popular. In the wireless world, any organization wishing to ensure end to end security may apply VPN solutions. This becomes more viable as PDAs increasingly have the computing power to support an IPSec VPN client and where enterprise network supports VPN gateways. Use of firewalls and SSL connections between network elements add additional elements of security. Further secure layers are possible with the addition of PKI authentication and encryption.

TELUS Mobility has been offering data solutions for almost ten years. We have the knowledge, the experience, the people, and a host of satisfied clients to back our claim. We're not too proud to admit that there are some things outside our areas of expertise. Often it is necessary to have inside industry knowledge to craft an appropriate wireless solution.

Extending the TELUS Mobility team through strategic partnerships with device manufacturers, system integrators, value-added resellers, and specialized consultants ensures that we fill in any gaps that might exist in our knowledge base. It also ensures that we have a network of solution partners to help meet your needs.

## 6. glossary

Term	Definition
Access Control	First generation of wireless networks. Analog.
Accountability	Security principle that an individual is entrusted to safeguard and control particular information and/or information technology resources and is answerable to proper authority for the loss or misuse of such resources.
Auditability	Assurance that sufficient logs or records of activities are maintained to assess the adequacy of security controls and to ensure compliance with established security policies and procedures.
Authentication	Security measure used to verify the identity of an entity.
Authorization	The granting or denying of access rights to an entity.
Availability	Timely and reliable access to information and/or information technology resources for authorized entities.
Confidentiality	Assurance that information is not disclosed to unauthorized entities.
Digital Signature	Cryptographic process used to assure the authenticity, integrity and non-repudiation of a message originator.
Encryption	The transformation of plaintext into an unintelligible form called ciphertext through a mathematical process. The ciphertext may only be read by someone who has the key that decrypts the ciphertext.
Entity	A user, program, process, system or device.
Identification	Security measure or process used to recognize an entity.
Integrity	Assurance that the information or information technology resources are reliable, correct or complete and that they have not been modified or destroyed in an unauthorized manner.
Non-Repudiation	The inability of an entity to deny actions.
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
Reliability	The assurance that a system maintains consistent, intended and trustworthy operation over a given period of time.
Vulnerability	A weakness in a system's security requirements, design, implementation or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.