Ensuring Wireless Security with 3G

Deliver secure mobile services

UMTS delivers the highly secure services that mobile data customers demand, helping to ensure maximum revenue generation for network operators.

This white paper addresses:

- Inherent UMTS security
- Implementing application-level security
- Mobile virtual private networks

Lucent Technologies
Bell Labs Innovations



CONTENTS

1 **Introduction** 3

2 **Security Architecture**

2.1 3GPP security 4

2.2 Application security

2.3 Summary 6

3 **Implementation**

3.1 3GPP implementation 6

3.1.1 Network access security 6

3.1.2 Network Domain Security 7

3.1.3 User Domain Security 8

3.1.4 Application Security 8

3.2 IPSEC 9

3.2.1 Security Association 11

3.2.2 Authentication 12

3.2.3 Lucent Technologies IPSec Client 12

3.3 Summary 13

4 **VPN types**

4.1 End-to-end IP with virtual circuits 14

4.2 End-to-end IPSEC 15

4.3 PPP-based non-transparent access 16

4.4 Summary 17

5 **Back office security**

5.1 Firewalls 17

5.1.1 Stateful Firewall 17

5.2 Summary 19

6 **Conclusion** **19**

7 **Appendix: acronyms and abbreviations** 20

Copyright © 2002 by Lucent Technologies. All Rights Reserved.

This material is protected by the copyright and trade secret laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts or licensing, without the express written consent of Lucent Technologies.

Notice

At the time of publication, this document accurately reflects the Lucent Technologies UMTS solution. However, as we are continually enhancing our products, we recommend that 6 months after May 2002 you obtain the latest version of this document from your Lucent representative.

1 Introduction

Security is a serious concern for mobile network operators and their customers alike. Indeed, the true potential for generating revenue from mobile data services will only be realized if network operators can guarantee delivery of the level of security their customers demand.

The requirement for wireless security is shared by both the business, and consumer markets. For example, security is a pre-requisite to remote, mobile access to confidential personal or corporate data. Similarly business transactions, online payments and m-commerce can only take place in a highly secure environment.

"the financial losses attributed to IT security breaches at US businesses and government departments grew by 42% between 1999 and 2000, to nearly $380 million." - Mobilizing the Enterprise", 2001

Focusing on the business market, independent research conducted by Total Research Corporation during October 2001 revealed that lack of security is a major roadblock preventing Telecoms & IT managers from implementing wireless data solutions. The importance of security was further highlighted in a recent report from Deloitte Consulting ("Mobilizing the Enterprise", 2001). According to this report, the financial losses attributed to IT security breaches at US businesses and government departments grew by 42% between 1999 and 2000, to nearly $380 million.

UMTS networks support the use of rigorous security techniques that were impractical with previous wireless technologies. In addition to the more robust network access security mechanisms built into the UMTS standards, data rates of up to 384kbps ensure that rigorous encryption can be implemented without compromizing the end users' perceived performance.

UMTS networks can support network-based VPN services, which are heavily reliant on the use of tunnelling technologies. Tunnelling effectively creates secure data paths through a shared network and helps to ensure privacy of information. UMTS-based VPNs use a combination of GPRS Tunnelling Protocol (GTP) through the UMTS packet-switched core network and Internet Engineering Task Force (IETF)-defined tunnelling protocols (such as IPSec (IP Security Protocol)) on the "fixed" side, towards the enterprize networks (IPsec tunnels can also be created end to end).

The Lucent Technologies UMTS solution supports several different IP (Internet Protocol) tunnelling techniques to deliver Mobile VPN (MVPN) services, providing operators with the flexibility to provide multiple VPN service deployment options to their customers.

In addition, 3GPP-defined security further enhances the network access security provided by GSM, ensuring UMTS users benefit from a cohesive, protected, secure environment.

2 Security Architecture

The following subsections discuss the main two aspects of UMTS security:

- Security defined within the 3GPP standards
- Application security

2.1 3GPP Security

The security mechanisms defined within the 3G Partnership Project (3GPP) standards are based on GSM security, with the following important changes:

- A change was made to defeat the "false base station" attack. The security mechanisms include a sequence number that ensures that the mobile can identify the network
- Key lengths were increased to allow for the possibility of stronger algorithms for encryption and integrity
- Mechanisms were included to support security within and between networks
- Security is based within the switch rather than the base station as in GSM. Therefore links are protected between the base station and switch
- Integrity mechanisms for the terminal identity (IMEI) have been inherently designed into the protocol, rather than as a late adder as in GSM

Integrity protection is one of the two most important security measures, allowing both the UTRAN and the User Equipment (UE) to check each other's validity. This excludes the possibility of a UE talking to a rogue UTRAN or the UTRAN talking to a rogue UE for a signalling connection. This is vital to WCDMA technology-based UMTS whereby each UE uses a common frequency band for communication.

Integrity and ciphering involve both the UE and network agreeing a set of keys, this occurs during the authentication and key agreement procedure. Authentication and key setting are triggered by the authentication procedure. The network may initiate authentication and key setting as often as the operator wishes. Key setting can occur as soon as the identity of the mobile subscriber is known by the VLR/SGSN.

The Cipher Key (CK) and Integrity Key (IK) are stored in the VLR/SGSN and transferred to the RNC when needed. The CK and IK for the Circuit Switched (CS) domain are stored on the USIM and updated at the next authentication from this domain. The CK and IK for the Packet Switched (PS) domain are stored on the USIM and updated at the next authentication from this domain.

If an authentication procedure is performed during a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the ME as part of the security mode set-up procedure that follows the authentication procedure.

Another important security measure is: "UTRAN Local Authentication". This is done via (packet) counter verification checks at the UE side, as requested by the UTRAN, whereby inconsistent counter checks highlight intrusion attacks ('man in the middle').

2.2 Application Security

Application security is not standardized by 3GPP, hence security solutions at this layer are dependent on the network operator's implementation.

The Lucent Technologies UMTS solution utilises IPSec (IP Security) as the fundamental mechanism for providing security features for applications. IPSec provides a standard, robust and extensible mechanism to provide security to IP and upper layer protocols. The IPSec working group of the IETF has published RFCs for the various aspects of IPSec including architecture, key management, base protocols and mandatory transforms.

IPSec combines several different security technologies into a complete system to provide confidentiality, integrity and authenticity. In particular, IPSec uses:

- Diffie-Hellman key exchange for deriving key material between peers on a public network
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid "man-in-the-middle" attacks
- Bulk encryption algorithms (such as 3DES) for encrypting the data
- Keyed hash algorithms (such as HMAC), combined with traditional hash algorithms (such as MD5 or SHA) for providing packet authentication
- Digital certificates signed by a certificate authority to act as digital ID cards

The Lucent Technologies IPSec products and clients provide Authentication Header (AH) using SHA-1and MD5, and Encapsulating Security Payload (ESP) using DES and 3DES. AH provides authentication of sender, integrity of message, and anti re-play protection for the whole IP packet, while ESP provides authentication of sender, integrity of message, confidentiality, and anti-replay protection on the IP packet payload. AH and ESP can be used together and/or layered to achieve additional protection and flexibility. The decision to use one, the other, or a combination will be driven by Enterprise security needs. In general, where publicly routable IP addresses are assigned to the subscriber and Network Address Translation (NAT) is not used, IPSec AH may be used separately or together with ESP. In cases where NAT is used between the security gateway and the security client, IPSec ESP is generally recommended.

It should be noted that any application security measure will not compromise network security specified by 3GPP Standards. This requirement (TS33.102) states that, although customer-based security measure at application level are applied to some applications (e-commerce, etc), integrity protection, ciphering, and local authentication must be included.

2.3 Summary

UMTS Security can be divided into two main aspects: 3GPP security and security at the application layer. 3GPP security provides secure access to the UMTS network and secure communications between the 3GPP elements. Application security provides protection between endpoints (which are dependent on configuration) utilizing IPsec.

Please see http://www.lucent.com/security for more information on Lucent Technologies security products.

3 Implementation

3.1 3GPP Implementation

3.1.1 Network access security

Lucent Technologies has implemented a fully 3GPP compliant security architecture. 3GPP does not define a standard authentication algorithm, allowing operators to choose their own versions, which comply with the published standards. The Lucent Technologies Cryptographer Team provide default algorithms or work in conjunction with operators to provide be-spoke algorithms.

Lucent Technologies implements ciphering and integrity according to the standardized methods described in 3GPP TS 33.102 assuring confidentiality and integrity on the air interface. Cipher and integrity keys are agreed during the authentication and key agreement procedure.

3.1.2 Network Domain Security

3GPP network domain security is based on a subset of the IPsec IKE (Internet Key Exchange) protocol. The 3GPP network domain security architecture provides hop-by-hop security.

Security Gateways (SEGs) are defined, which engage in direct communication with entities in other security domains. The SEGs then establish and maintain IPsec secured ESP Security Association in tunnel mode between security domains.

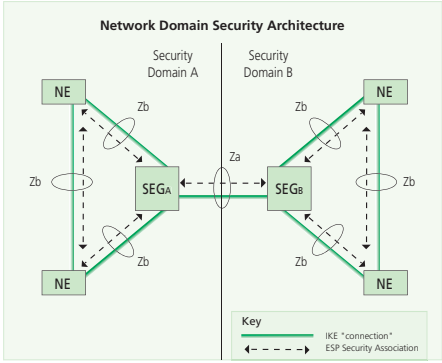
The Security Gateway is defined as a security entity located at the network border with the task to enforce the security policies, defined by the operator, concerning the packet flows between the own network and other networks. It can also be used to apply protection to packets exchanged directly with an external host, server or terminal if this is allowed by the policies.

Sensitive application level data - be it authentication data sent between the user and a service domain, a banking transaction, or any other sensitive data – will, and should, be protected using application level security mechanisms, since the trust relation in action is between the user and the application provider.

This means that data belonging to the user plane, i.e. packet flows over the Gi interface, will not be protected by the SEG, while all data belonging to the control plane will be protected by the SEG according to the relevant policies.

It is recommended that the SEG is placed in a network, a so called Extranet, which is separated from the internal network by a Firewall, FW. Typically also other network elements, like e.g. DNS servers and different types of proxies, could be located in such an Extranet. It is therefore also recommended to protect the Extranet itself by placing a second, outer Firewall between the Extranet and an external, shared transport network.

The diagram on the next page depicts the relationship between NEs (Network Elements) in the Network Domain Security architecture both for intra and inter domain security.



The Za-interface covers traffic between security domains. The SEGs use IKE to negotiate, establish and maintain a secure ESP tunnel between them.

The Zb-interface is located between SEGs and network elements and between network elements and also utilizes ESP+IKE.

3.1.3 User Domain Security

User Domain Security consists of two aspects:

- User to USIM security
- USIM to terminal security

User to USIM security is achieved through the use of a Personal Identification Number (PIN), whilst USIM to terminal security is achieved through showing knowledge of a secret key.

3.1.4 Application Security

VPN security is addressed in Section 4; in general, application security can be achieved using a server-authenticated WTLS or SL/TLS session. Servers can support a number of algorithms for authentication and encryption, including 1024-bit RSA and 163-bit ECC, and encryption including DES,

triple DES, RC4 and AES. A variety of password request-response mechanisms can be used including sending a 'password request' message along with a random challenge to which the client responds with the hash of its password and the random challenge using MD5 or SHA-1.

Internet browsing security can be provided by the use of SSL/TLS. A network operator wishing to offer a purely HTML-based web server to act as a portal would secure the client-portal traffic using SSL.

3.2 IPSec

IPSec is utilized by Lucent Technologies in its application layer security solution - in addition it is also utilized for network domain security.

"The IPSec protocol is a set of security extensions providing privacy and authentication services by using modern cryptographic methods."

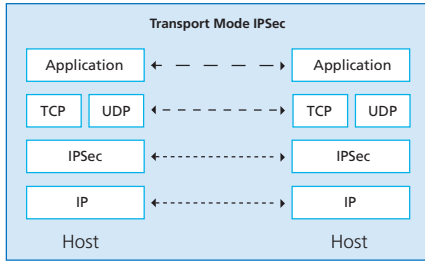
Lucent Technologies standards-based IPSec secured communications ensure highly sensitive information is not usable if intercepted over unsecured links in a communication path.

IPSec defines a new set of headers to be added to IP datagrams. These new headers are placed after the IP header and before the Layer 4 protocol (typically Transmission Control Protocol [TCP] or User Datagram Protocol [UDP]). The principal IPSec components are:

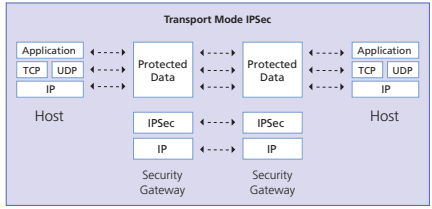
- IP Authentication Header (AH) - provides data origin authentication, data integrity and replay protection
- IP Encapsulating Security Payload (ESP) - provides data confidentiality, data origin authentication, data integrity and replay protection
- Internet Security Association and Key Management Protocol (ISAKMP) - provides a method for automatically setting up security associations and managing their cryptographic keys

The IPSec protocol suite provides a standard way for protecting all traffic on the Internet transparently, irrespective of the application. The IPSec protocol is a set of security extensions providing privacy and authentication services by using modern cryptographic methods. It can protect all traffic against unauthorized modification and eavesdropping and securely authenticate the parties that are communicating with each other. IPSec works in two ways:

1) The first, transport mode, is the native way. As shown below, it is the direct relaying of IPSec protected data from host to host, and is used in devices that incorporate IPSec into the way they stack TCP/IP data; for example, a laptop outfitted with client encryption (see figure on following page).



2) The second IPSec method is tunnel mode (see figure below). Here, IP traffic generated by hosts without IPSec support is captured from the wire by a security device, or gateway. As shown in the diagram below, the gateway encapsulates the entire IP packet with IPSec encryption, including the original IP header. It then adds a new IP header to the data packet and sends it across the public network to a second gateway, where the information is decrypted and sent in its original form to the designated recipient.



Tunnelling is performed by a VPN device residing at the entrance/exit points of a network. The device modifies (encrypts and authenticates) outgoing traffic and decrypts and authenticates incoming data according to the methods outlined by IPSec. Tunnelling is used to create secure VPNs. It enables distributed private networks to communicate securely over untrusted, public networks. When using tunnelling over the Internet, companies can build secure Wide Area Networks (WANs), intranets and extranets at a fraction of the cost associated with traditional methods. VPNs implemented in non-Internet environments, such as frame relay networks, provide comprehensive protection for mission critical applications. In all its configurations, tunnelling is a money-saving technology, both in terms of reduced communication costs and prevention of security breaches.

3.2.1 Security Association

IPSec provides many options for performing network encryption and authentication. Each IPSec connection can provide encryption or integrity or authenticity, or a combination of all three. When the security service is determined, the two communicating nodes must determine exactly which algorithms to use (for example, DES for encryption and MD5 or SHA for integrity). After deciding on the algorithms, the two devices must share session keys. The security association is the method that IPSec uses to track all the particulars concerning a given IPSec communication session. A Security Association (SA) is a relationship between two or more entities that describes how the entities will use security services to communicate securely. The nomenclature gets a little confusing at times, because SAs are used for more than just IPSec. For example, IKE SAs describe the security parameters between two IKE devices. Further references to security associations in the rest of this paper will specify whether they are IPSec or an IKE SA.

The security association is unidirectional, meaning that for each pair of communicating systems there are at least two security connections - one from A to B and one from B to A. The security association is uniquely identified by a randomly chosen number, called the security parameter index (SPI), and the destination IP address. When a system sends a packet requiring IPSec protection, it looks up the security association in its database, applies the specified processing and then inserts the SPI from the security association into the IPSec header. When the IPSec peer receives the packet, it looks up the security association in its database by destination address and SPI and then processes the packet as required. In summary, the security association is simply a statement of the negotiated security policy between two devices.

IKE is based on two public key algorithms:

- The Diffie-Hellman key agreement protocol and
- The RSA digital signature/encryption algorithm

IPSec assumes that a security association is in place, but it does not have a mechanism for creating that association. The IETF chose to break the process into two parts: IPSec provides the packet-level processing, while the Internet Key Management Protocol (IKMP) negotiates security associations.

IKE creates an authenticated secure tunnel between two entities and then negotiates the security association for IPSec. This process requires that the two entities authenticate themselves to each other and establish shared keys.

"Security needs to be robust, but it should not impact productivity – 3G satisfies the requirements of both IT managers & users alike"

3.2.2 Authentication

IKE is very flexible and supports multiple authentication methods. The two entities must agree on a common authentication protocol through a negotiation process. At this time, the following mechanisms are implemented:

- Pre-shared keys - where the same key is pre-installed on each host. IKE peers authenticate each other by computing and sending a keyed hash of data that includes the preshared key. If the receiving peer is able to independently create the same hash using its preshared key, it knows that both parties must share the same secret, thus authenticating the other party.

- Public key cryptography - where each party generates a pseudo-random number and encrypts it in the other party's public key. The ability for each party to compute a keyed hash containing the other peer's pseudo-random number, decrypted with the local private key as well as other publicly and privately available information, authenticates the parties to each other. This system provides for deniable transactions. That is, either side of the exchange can plausibly deny that it took part in the exchange (which is not the case when using PKI in conjunction with a certification authority, i.e. a digital signature).

- Digital signature - where each device digitally signs a set of data and sends it to the other party. This method is similar to the previous one, except that it provides non-repudiation (i.e. either side cannot deny that they took part in the exchange). Both digital signature and public key cryptography require the use of digital certificates to validate public/private key mapping. IKE allows the certificate to be accessed independently (for example, through DNSSEC) or by having the two devices explicitly exchange certificates as part of IKE.

3.2.3 Lucent Technologies IPSec Client

The Lucent IPSec Client forms the remote access VPN component of Lucent's IP services portfolio. Purpose-built for carrier-managed services, this feature-rich software provides a complete remote access VPN solution for telecommuters and mobile workers with PCs running Microsoft's Windows® 95, Windows®98, Windows®2000, Windows NT® or Windows ME® operating systems. Standards-based IP Security (IPSec) features and centralized management options combine with matchless value-added capabilities to deliver a totally secure solution that is extremely easy to install and use.

A built-in "Personal Firewall" ensures protection even for always-on services. Users can surf the Web, log into an enterprise-wide intranet VPN, or connect to multi-party extranets safely and simply, regardless of the connection mode-dial-up modem, WAN router, DSL, cable, or wireless link. With smooth interoperability across Lucent's IP services portfolio, the Lucent IPSec Client ensures the right solution for a wide range of price and performance requirements.

Key Features and Benefits

- Integral ironclad security - built-in stateful firewall, strong packet encryption, choice of authentication methods
- Easy to install and use - intuitive graphical user interface (GUI), simple point-and-click installation, "near zero" configuration
- Centralized management - Lucent Security Management Server (LSMS) software, completely integrates provisioning and management of large scale remote access VPN services, supporting up to 20,000 simultaneous IPSec Client tunnels and hundreds of thousands of users
- Interoperability across the entire Lucent IP services portfolio - ensures all-in-one private intranet, semi-private extranet, and public Internet access for every site and user

3.3 Summary

Implementation of the 3GPP security protocol is largely constrained by the exact nature of the 3GPP specifications, however, algorithms can be tailored to operator needs. IPSec forms the major part of network domain security as defined by 3GPP, however, it can also be used both for operator specific protection of network interfaces and at the application layer.

4 VPN Types

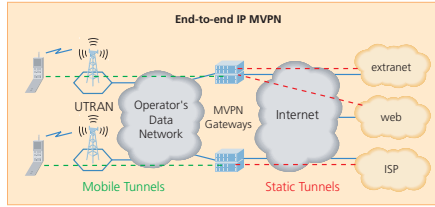
Lucent Technologies secured VPNs add strong IETF based security services such as IPSec. Access to and exchange of information in the VPN requires tunnelling, encryption, authentication, and access control technology. With the various forms of encryption and authentication, requirements for both access and end-to-end communications can be met. Three possible configurations that Lucent Technologies support are:

- End-to-end IP with Virtual Circuits
- End-to-end IPSec
- PPP-based non transparent access

The three types are discussed in more detail in the subsections below. Note: these three configurations are examples only – other configurations are possible.

4.1 End-to-end IP with virtual circuits

IP based non-transparent access is a basic service enabled by the UMTS network, in conjunction with the existing landline IP infrastructure. An end-to-end IP VPN service provides a mobile subscriber IP connectivity to a destination network, using virtual circuits between the GGSN and the target destination. Access control and QoS to the virtual circuits may be applied which are governed by the VPN policy associated with the target network stored in the GGSN, or centrally in an LDAP server in the Regional POP. This type of VPN service does not provide data privacy protection.



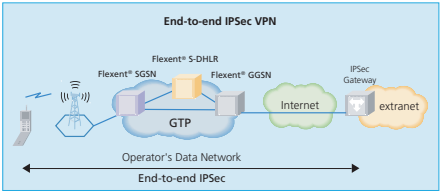
The application in the terminal forms the IP packet with the terminal IP address as the original IP address, and the destination server (or its proxy) address as the destination address. The packet is passed to the lower layers for transmitting to the UTRAN which relays it to the SGSN using the GTP

tunnel established previously. The SGSN recovers the GTP PDU and relays the packet to the GGSN by encapsulating it in another GTP tunnel established previously at the PDP context activation. The GGSN performs GTP processing, retrieves the connectivity information stored previously, processes the packet accordingly, and delivers the packet using the virtual circuit to the destination network. If NAT is used, it is performed before virtual circuit related processing. The access to the virtual circuit may be checked based on filtering selectors, such as destination IP address. After the NAT processing, the WSP private IP address for the terminal is translated to a public address. The source port number may also be changed so the IP session can be uniquely identified. When the destination network receives the packet at the other end of the virtual circuit, it routes the packet to its final destination based on the destination IP address.

4.2 End-to-end IPSec

End-to-end IPSec VPN services provide mobile subscribers with secure communications between IPSec end points. However, the IP packet format is much more complex than that of a non-IPSec protected IP packet. An IP packet generated by the application in the source system will have additional IP headers added by IPSec processing and possibly by UDP encapsulation.

Tunnel mode IPSec adds at least 16 bytes to the packet length. Encryption dependent padding for maintaining boundaries may add up to 255 bytes. In the end-to-end IPSec configuration, these overheads are carried in the air interface, reducing the user perceived data rate. Furthermore, since encryption renders plaintext into random ciphertext, any link layer compression is not only failing but is actually detriment to bandwidth because it will most likely increase the amount of data sent. To alleviate this problem, the payload is compressed before encryption. IP Payload Compression Protocol (IPCom) can be used to convey the compression algorithm to the peer. PCP can also be negotiated by IKE.



The end-to-end IPSec VPN session is initiated after the end-to-end IP connectivity is established as part of the PDP context activation procedure. The GGSN performs general IP connectivity establishment such as APN validation, GTP tunnel establishment, terminal IP address (used for outer IP header) assignment, etc. At the successful completion of the PDP context activation, MS invokes IPSec client and initiates the IKE procedures to establish an IPSec security association with the IPSec GW in the destination network for uplink packets. In response, the IPSec gateway in the destination network will initiate a security association with the client for downlink packets.

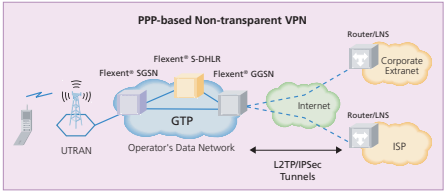
IKE includes mutual authentication of IPSec peers. For IPSec gateway authentication, the key used for authentication is shared between the gateway and all of its IPSec clients peers, if PKI is not employed.

4.3 PPP-based non-transparent access

The VPN configuration leverages existing landline dialup infrastructure to supporting remote access VPN services for mobile subscribers. A mobile subscriber first gains access to the UMTS network and initiates a request to establish an IP connectivity between the user and the destination network. After the UMTS network establishes the IP connectivity with the destination network, the subscriber invokes a PPP session, the PPP traffic is relayed by the GGSN to the destination network by an L2TP tunnel. Destination networks participating in L2TP based VPN will retain full control over IP address assignments and AAA functions.

Other than PPP relay, and L2TP tunnelling, the services that may be provided by WSPs offering this configuration include QoS between GGSN and EBS, VPN management, and VPN traffic segregation.

The terminal will have a PPP client installed. PPP traffic is encapsulated in an L2TP tunnel from the GGSN to the destination network. The GGSN serves as a L2TP Access Concentrator (LAC). An L2TP peer in the destination network, an L2TP Network Server (LNS), terminates the L2TP tunnel. PPP traffic, retrieved from the L2TP tunnel, terminates at the Remote Access Server (RAS).



4.4 Summary

A variety of options exist for implementing VPNs. The option chosen will be highly dependent on the level of security and existing infrastructure of the VPN customer.

5 Back Office Security

The Lucent Technologies Flexent® GGSN, based on the Lucent SpringTide 7000 Wireless™ IP Services Switch, enables configuration of virtual routers that separate traffic generated by different user communities and customize the flows associated with each customer and provider network in the VPN configuration. Each customer or provider router can define its own interfaces to the associated networks, have its own user group, maintain and advertise its own routing information, and define its own address space.

The Flexent GGSN can support a variety of IP security options that can be used to protect the entire UMTS network, or individual network-based services emanating from the GGSN interfaces. Security features include such components as:

- Stateful and Stateless Firewalls
- Encryption (IPSec, DES/3DES)

Stateful and Stateless firewalls will be described in the following sub-section, details of encryption can be found in Section 3.2.

5.1 Firewalls

Firewalls are crucial to the security of the UMTS infrastructure. Firewalls block unauthorized traffic, thereby protecting the network configuration from various types of attacks. The Flexent GGSN supports both stateful and stateless firewalls, which permit or block traffic. Stateful firewalls are dynamic and more advanced than packet-filtering, or stateless firewalls. Packet filtering includes initially the "allow" and "deny" type of filtering based on source or destination addresses, protocols, and ports. In contrast, stateful firewalls can be configured using policies, with a set of rules that permit or block traffic based on the type of traffic.

5.1.1 Stateful Firewall

Stateful firewalls must be configured on a per-service basis and can either be a user-based or interface-based service. Firewall policies can never be router-based, since router service policies do not use packet information (such as incoming and outgoing interfaces).

A stateful Firewall understands the different protocols that pass through it, so it can securely allow or block traffic, as well as authenticate the use of related IP services.

Features:

- Enhanced Packet Filtering
- Stateful TCP and UDP filtering
- Dynamic State Aware Multi-port Application Support
- Multi-media applications with dynamic multi-porting
- Application aware firewalling supporting:
  - FTP
  - H.323
  - RealAudio
  - RealVideo
  - StreamWorks
  - VDOLive
  - Oracle SQL*Net
  - Sun RPC
  - UNIX R-commands (e.g. rlogin, rexec, and rsh)

The Lucent firewall platform provides protection against common intrusion and denial of service attacks. Enabling/disabling each protection function is selectable. The intrusion detection and prevention service is applied to the traffic entering inside the network via a subnet interface or a user session (user-based firewall service). For IP source address spoofing intrusion prevention, the traffic originating from inside the network will be inspected for source address validity. The following features are supported:

- IP Source Address Spoofing
- TCP SYN Attack
- LAND TCP and LAND UDP
- Ping Flooding
- Ping of Death
- Ping Scan or Sweep
- Port Scan

The firewall maintains a cache of information regarding connections that are initiated from the inside. By default, firewalls are designed to allow connections from the inside to the outside, as well as the return communications for a particular transaction. All other connections initiated from the outside are blocked, unless the firewall is configured to allow them through.

When data streams interact with packet filtering firewalls, the firewall is configured with a set of rules that allow or block traffic based on IP addresses or port numbers. However, when data streams interact with Stateful firewalls, the firewall is configured with a set of rules that allow or block traffic based on the type of traffic (not specific IP addresses or port numbers).

5.2 Summary

A number of IP security methods need to be used to protect the entire UMTS network, or individual network-based services emanating from the GGSN interfaces. Features such as firewalling and encryption are essential to achieve this objective.

6 Conclusion

Security is critical to the success of mobile data services - business and consumer customers will only subscribe to mobile data services if the network operator delivers the level of security they demand.

The security mechanisms built into the 3GPP standards means that UMTS is inherently highly secure – more so than existing GSM systems. For example, the 3GPP standards have been designed to defeat "false base station" attacks and security has been extended into the core network, rather than terminating at the base station. The Lucent Technologies UMTS solution is built around a fully 3GPP-compliant security architecture.

In addition to the inherent standards-based security measures, UMTS delivers the high bandwidth required to support application-level security without compromizing the end-user experience. The Lucent Technologies solution utilizes IPSec to provide end-to-end security. The Lucent IPSec Client provides a complete remote access VPN solution for laptop PCs running the standard Microsoft operating systems. Furthermore, it is easy to install and easy to use.

VPN services are expected to be a valuable source of revenue for 3G network operators – providing mobile professionals with secure mobile access to business-critical data and applications. The Flexent GGSN, at the heart of Lucent's UMTS packet-switched core network, supports a number of different VPN configurations, providing operators with the flexibility to deliver the security solution their customers demand.

As well as delivering the highest capacity and throughput of all GGSNs on the market, the Lucent's Flexent GGSN supports additional functionality such as stateless and stateful firewalls, providing the operators and their customers with protection against intrusion and denial-of-service attacks.

"The security mechanisms built into the 3GPP standard means that UMTS is inherently highly secure – more so than existing GSM systems"

APPENDIX Acronyms and Abbreviations

3DES	Triple DES
3GPP	Third Generation Partnership Project
DES	Data Encryption Standard
FW	Firewall
GGSN	Gateway GPRS Support Node
GW	Gateway
IKE	Internet Key Exchange
L2TP	Layer 2 Tunnelling Protocol
LDAP	Lightweight Directory Access Protocol
ME	Mobile Equipment
MS	Mobile Station
MVPN	Mobile VPN
NE	Network Element
PKI	Public Key Infrastructure
POP	Point of Presence
PPP	Point to Point Protocol
QoS	Quality of Service
RFC	Request for Comment
SGSN	Serving GPRS Support Node
SHA	Secure Hash Algorithm
SPD	Security Profile Database
USIM	UMTS Subscriber Identification Module
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
VPN	Virtual Private Network
WSP	Wireless Service Provider

Lucent Technologies
Global Mobility Marketing
Lucent Technologies NS UK Ltd
The Quadrant
Stonehill Green
Westlea
Swindon
Wiltshire SN5 7DJ
UK

Response Centres:

EMEA Tel: +44 (0) 7000 582 368
Fax: +44 (0) 1344 488 045
Email: mobility@lucent.com

Asia Pacific Email: wirelessap@lucent.com

NAR/CALA Tel: +1 888 426 2252
Fax: +1 314 317 6480

Lucent is a world-class supplier of mobility solutions. Innovation is at the heart of our business. Our Centres of Excellence and the global facilities of Bell Labs, are shaping the way our world communicates. We offer unchallenged market leadership in CDMA radio access, the underlying technology for UMTS, ATM backbone networking technology, circuit and packet billing as well as the expertise to integrate and deploy complex networks. Call Lucent for complete end-to-end mobility solutions.

Visit our web site at www.lucent.com

Lucent Technologies
Bell Labs Innovations

This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties or tariffs relating to these products. Any technical specifications contained herein are approximate and subject to change without notice.

Brochure number: Ensuring Security W/P 07/2002.
Copyright 2002 Lucent Technologies