Appendix

List of Abbreviations

136HS	136 High Speed
1xRTT	First phase of CDMA2000 (next phase is 3xRTT)
2G/2.5G	2nd Generation (Cellular System), General term for digital wireless networks using IP
3G	3rd Generation (Cellular System)
3GPP/3GPP2	3G Project Partnership (3GPP – UMTS/WCDMA and 3GPP – CDMA2000)
4G RAC	Radio Access Controller of 4G network
5GPP	5 GHz Partnership Project
5GSG	5 GHz Service Group
802.11	Original IEEE standard for “Wireless Ethernet ” at 2.4Ghz (FHSS or DSSS)
802.11a	IEEE standard for “Wireless Ethernet ”at 5.2GHz (OFDM)
802.11b	IEEE standard for High Rate “Wireless Ethernet ” at 2.4Ghz (DSSS)
802.11g	IEEE (proposed) standard combining 802.11a and 802.11b
AA	Authenticator Address
AAA	Authentication, Authorisation, and Accounting

AAAH	Home AAA
AAAL	Local AAA
AAL	ATM Adaptation Layer
ACELP	Algebraic Code Excited Linear Predictive
AES	Advanced Encryption Standard
AF	Assured Forwarding
AMPS	Advanced Mobile Phone System
Anonce	Authenticator Nonce
AP	Access Point – the end network equipment providing network access to the end users.
ARIB	Association for Radio Industry and Business
ARPU	Average Revenue Per User
AS	Authentication Server
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
AuC	Authentication Controller
B-ISDN	Broadband – Integrated Services Data Network
BPSK	Binary Phase Shift Keying
BRAIN	Broadband Radio Access for IP based Networks (IST-1999-10050)
BRAN	Broadband Radio Access Networks
BSC	Base Station Controller
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
BTS	Base Transceiver Station
CA	Certificate Authority
CBC	Cipher-Block Chaining
CBC-MAC	CBC Message Authentication Code
CCK	Complementary Code keying
CCM Mode	Counter Mode with CBC-MAC
CCMP	CCM Protocol
CDMA	Code Division Multiple Access
CDMA2000	Code Division Multiple Access 2000
CDPCISCO	Discovery Protocol

CDPD	Cellular Digital Packet Data
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CL	Convergence Layer
CN	Core Network
COPS	Common Open Policy Service
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CS	Circuit Switched
CSMA	Carrier Sense Multiple Access
CTR	Counter Mode
DAMPS	Digital Advanced Mobile Phone System
DBPSK	Differential Binary Phase Shift Keying
DCCH	Digital Control Channel
DCS	Dynamic Channel Selection
DECT	Digital Enhanced Cordless Telephone
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DLEN	MPDU Data Length
DoS	Denial of Dervice
DPSK	Differential Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DRNC	Drift Radio Network Controller
DSCP	Differentiated Services Code Point
DSSS	Direct Sequence Spread Spectrum
DTCH	Digital Traffic Channel
DWDM	Dense Wavelength Division Multiplexing
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security

ECC	Elliptic Curve Cryptography
(E)DCF	(Enhanced) Distributed Coordination Function (IEEE802.11e)
EDGE	Enhanced Data Rates for GSM Evolution
EF	Expedited Forwarding
EFR	Enhanced Full Rate
EK	Encryption Key
EPOC	New operating system for mobile devices (Symbian)
ESN	Enhanced Security Network (WEP2 (=TKIP) and AES devel opment)
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FA	Foreign Agent
FDD	Frequency Division Duplexing
FHSS	Frequency Hopping Spread Spectrum
FINEID	Finnish Electronic Identity
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMK	Group Master Key
GMSK	Gaussian Minimum Shift Keying
Gnonce	Group Nonce
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GTK	Group Transient Key
GTP	GPRS Tunnelling Protocol
GTP-U	GPRS Tunnelling Protocol-User plane HA Home Agent
HCF	Hybrid Coordination Function (IEEE 802.11e)
HDML	Handheld Devices Markup Language (now called WML)
HiperLAN	High Performance Wireless LAN - Versions 1 and 2 (European Standard)
HiperLAN/2	High Performance Radio Local Area Network 2 (ETSI/BRAN standard at 5.2GHz using OFDM)
HIRAN	HiperLAN /2 Radio Access Network
HLR	Home Location Register

HR/DSSS	High Rate Direct Sequence Spread Spectrum
HSCSD	High-Speed Circuit-Switched Data
HSS	Home Subscriber Server
i-mode	See PHS
IAPP	Inter-Access Point Protocol (transfers client's state between APs)
IAS	Internet Authentication Server (Microsoft's Radius)
IBSS	Independent Basic Service Set
ICV	Integrity Check Value
ID	IDentifier
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IIS	Internet Information Server
IMEI	International Mobile Equipment Identity
IMSI	International Mobile subscriber Identity
IMT-2000	International Mobile Telecommunications for year 2000 and beyond
IP	Internet Protocol
IPPM	IP Performance Metrics
IPSec	IP Security Protocol
IrDA	Infra-red Data Association
ISDN	Integrated Services Data Network
ISM	Industrial, Scientific and Medical
ISP	Internet Service Provider – see also WISP
ITU	International Telecommunications Union
IV	Initialization Vector
IWU	InterWorking Unit
J2ME	Java 2 Micro Edition (Java enabled browsers in the handset)
L2CAP	Logical Link Control and Adaptation Protocol (Bluetooth)
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LED	Light Emitting Diode
LMP	Link Manager Protocol (Bluetooth)

MAC	Medium Access Control protocol
MAN	Metropolitan Area Network
MAP	(GSM) Mobile Application Protocol
MCC	Mobile Country Code
MD4	Message Digest 4
MD5	Message Digest 5
MGW	Media Gateway
MH	Mobile Host
MIC	Message Integrity Check
MIP	Mobile IP
MK	EAPol-Key MIC Key
MM	Mobility Management
MMAC	Multimedia Mobile Access Communication Systems (Japan)
MNC	Mobile Network Code
MPDUs	MAC Protocol Data Units
MPLS	Multi-Protocol Label Switching
MS	Mobile Station
MSC	Mobile Switching Centre
MS-CHAPv2	Cryptanalysis of Microsoft's PPTP Authentication Extensions
MSDU	MAC Service Data Unit
MT	Mobile Terminal
NAI	Network Access Identifier
NAS	Non Access Stratum
NIC	Network Interface Card
NIST	National Institute of Standards and Technologies
NMT	Nordic Mobile Telephone
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open System Interconnect
PBCC	Packet Binary Convolution Coding (Texas Instruments)
PBCCH	Packet Broadcast Control Channel
PCCCH	Packet Common Control Channel
PCF	Physical Control Field
PCMCIA	Personal Computer Memory Card International Association

PCN	Personal Communication Network (Equivalent to GSM 1800 MHz)
PCS	Personal Communications Service
PDA	Personal Digital Assistant
PDC	Personal Digital Cellular
PDCH	Packet Data Channel
PDH	Plesiochronous Digital Hierarchy
PDP	Packet Data Protocol
PDTCH	Packet Data Traffic Channel
PDU	Packet Data Unit
PEAP	Protected EAP
PHB	Per Hop Behaviour
PHY	Physical Layer
PHS	Personal Handyphone System (i-Mode/DoCoMo)
PKI	Public Key Infrastructure
PLCP	Physical Layer Convergence Protocol
PLMN	Public Land Mobile Network
PLP	Packet Loss Probability
PMK	Pairwise Master Key
PN	Packet Number
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
PRF	Pseudo Random Function
PRNG	Pseudo Random Number Generator
PS	Packet Switched
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network, the local telephone operator
PTK	Pairwise Transient Key
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RAC	Routing Area Code
RADIUS	Remote Authentication Dial-in User Service

RAN	Radio Access Network
RANAP	Radio Access Network Application Port
RC4	A variable key-size stream cipher with byte oriented operations
RC-LED	Resonant Cavity - Light Emitting Diode
RF	Radio Frequency
RFCxxx	Request for Comments xxx
RLC	Radio Link Control
RNAS	RAN Access Server
RNC	Radio Network Controller, 3G switch controlling the radio part.
RNSAP	Radio Network Subsystem Application Port
RNTI	Radio Network Temporary Identifier
ROSE	Radionet Open Source Environment
RrK	Rapid reKeying (IEEE Submission, August 2001)
RSN	Robust Security Network
RSN IE	RSN Information Element
RSVP	Resource reSerVation Protocol
SAC	Service Area Code
SACCH	Slow Associated Control Channel
SAI	Service Area Identifier
SAP	Service Access Point
SCAM	Supplemental Channel Assignment Message
SCRM	Supplemental Channel Request Message
SDH	Synchronous Digital Hierarchy
SDP	Service Discovery Protocol (Bluetooth)
SDU	Service Data Unit
SGSN	Serving GPRS Support Node
SIM	Subscriber Identification Module – see also (U)SIM
SIP	Session Initiation Protocol
SIR	Signal-to-Interference Ratio
SLA	Service Level Agreement
SLP	Service Locator Protocol
SM	Session Management
SMG	Special Mobile Group

SMS	Simple Messaging Service (~ 100 characters)
Snonce	Supplicant Nonce
SONET	Synchronous Optical NETwork (network with SDH over fiber optical link)
SRNC	Serving RNC
SRP	Secure Remote Password
SSCS	Service Specific Convergence Sublayer
SSH	Secure Shell
SSID	Service Set Identifier
STA	Wireless Station – Any 802.11 device other than an AP.
SWAP	Shared Wireless Access Protocol
TA	Transmitter Address
TACS	Total Access Communications System
TDMA	Time Division Multiple Access
TEID	Tunnel Endpoint Identifier
TIA	Telecommunications Industry Association
TK	Temporal Key
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TOS	Type of Service
TPC	Transmit Power Control
TSC	TKIP Sequence Counter
TTA	Telecommunications Technology Association
TTAK	TKIP mixed Transmit Address and Key
UNII	Unlicensed National Information Infrastructure
UMTS	Universal Mobile Telecommunications System
URA	UTRAN Registration Area
USB	Universal Serial Bus
USF	Uplink Status Flag
(U)SIM	User Subscriber Identification Module – see also SIM
USSD	Unstructured Supplementary Services Data (<182 characters)
UTRAN	Universal Terrestrial Radio Access Network

UWCC	Universal Wireless Communications Consortium
VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Network
VSELP	Vector Sum Excitation Linear Predictive
WAE	Wireless Application Environment
WAMN	Wide Area Mobile Network
WAN	Wide Area Network
WAP	Wireless Application Protocol
WAP-NG	WAP Next Generation (WAP 2.0) based upon XHTML
WASP	Wireless Access Service Provider
WCDMA	Wideband Code Division Multiple Access
WCMP	Wireless Control Message Protocol
WDP	Wireless Datagram Protocol
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WEP IV	WEP Initialization Vector
Wi-Fi	Wireless Fidelity
WIM	Wireless Identity Module
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WML	Wireless Markup Language
WPA	Wi-Fi Protected Access Version 1
WPA2	Wi-Fi Protected Access Version 2
WPA IE	WPA Information Element
WPAN	Wireless Personal Area Network
WPKI	Wireless Public Key Infrastructure
WRAN	Wireless Radio Area Network
WRR	Weighted round robin (scheduler)
WSG	Wireless Second Generation
WSL	Wireless Session Layer
WSN	Wireless Support Node
WSP	Wireless Session Protocol

WTA	Wireless Telephony Application
WTAI	Wireless Telephony Application Interface
WTL	Wireless Transport Layer
WTLS	Wireless Transport Layer Security
WTP	Wireless (Transaction, Transport) Protocol
WWAN	Wireless Wide Area Network
X.509	ITU standard specifying contents of a digital certificate
XHTML	Extensible Hypertext Markup Language
XML	Extensible Markup Language

Glossary

1G: First Generation systems, which are analog and were designed for voice communications.

2G: Second-generation systems, which are digital and capable of providing voice/dat/fax transfer as well as a range of other value-added services, including SMS.

2.5G: Evolving second-generation systems that are intermediary options before the introduction of multimedia cellular.

3G: Third-Generation systems, which enable multimedia and are standardized under 3GPP.

3GPP: Third Generation Partnership Protocol.

4G: Fourth-generation systems. In early 2001, Alcatel, Ericsson, Motorola, Nokia and Siemens founded the Wireless World Research Forum (WWRF), whose "vision of the wireless world" was identified as that of 4G systems.

4-Way Handshake: The final procedure in the authentication protocol defined by the IEEE 802.1X standard.

802.1p: IEEE standard that defines techniques for supporting dynamic group multicast filtering and traffic prioritization in 802 LANs. The latter is accomplished by the use of a 3-bit user priority field contained in the 802.1q VLAN tag.

802.1q: IEEE standard that defines the method for supporting virtual LANs (VLANs) across 802 LANs, It works by inserting a 4- or 10-byte VLAN tag in each frame as it traverses one or more VLAN-capable bridges (switches).

AAA: Authentication, Authorisation and Accounting: An AAA server performs these functions, processing requests using a AAA protocol such as RADIUS.

AAAH: Home AAA: Logical function within the loose coupling architecture that provides AAA functions to support subscribers who have a permanent relationship with that network.

AAAL: Local AAA: Logical function within the loose coupling architecture that enforces the AAA policy within the local HiperLAN /2 network.

Access Point: A device through which computer clients connect to a WLAN.

AES: Advanced Encryption System: An encryption method based on the Rijndael algorithm that will be the basis for future wireless encryption standards.

Agent advertisement: The procedure by which a mobility agent becomes known to the mobile node. An agent advertisement message is constructed by attaching a special extension to a router advertisement message.

Agent discovery: The process by which a mobile node can obtain the IP address of a home agent or foreign agent, depending upon whether the mobile node is home or away from home. Agent discovery occurs when a mobile node receives an agent advertisement, either as a result of periodic broadcast or in response to a solicitation.

AP: Access Point: A wireless station that also provides services such as association and distribution of frames to other station or a network.

AP: Access Point: Interface between the radio network part and the wired network part of a HiperLAN /2 network, offering wireless connectivity to MTs.

AS: Authentication Server: A network component that performs authentication. A RADIUS server is an example of an AS.

Association: A set of mutually agreed security parameters for protected communication.

Authentication: User identification or client computer identification for legitimate access to computing resources.

Authentication Protocol: Rules and procedures for authentication.

Authentication Server: A computer program dedicated to authentication of users and computer clients.

Authenticator: 802.1X term for an entity that facilitates authentication. Access points act as authenticators.

Beacon: A radio transmitter or the signal emitted by it when the emission is used as a directional guide, such as a homing beacon or a localizer beacon.

Binding: See Mobility binding.

Binding update: The message that supplies a new binding to an entity that needs to know the new care-of address for a mobile node. The binding update contains the mobile node's home address, new care-of address, and a new registration lifetime.

Bridge: A device connecting two or more network segments within the same logical local area network.

Broadcast Traffic: The same data packet is sent to all hosts in a network.

BSS: Basic Service Set: A set of 802.11 stations that communicate with each other.

BSSID: Basic Service Set Identifier: A unique identifier for a particular BSS. In infrastructure mode, the MAC address of an access point.

CA: Certificate Authority: An authority that issues and manages digital security credentials such as public-key certificates.

Certificate: A record, cryptographically signed by a CA, with a public key and identity information about the key owner.

CN: Correspondent Node: A peer with which a mobile node is communicating. A correspondent node may be either mobile or stationary.

COA: Care-of Address: An IP address which identifies the mobile node's current point of attachment to the Internet, when the mobile node is not attached to the home network. The protocol can use two different types of care-of address: a foreign agent care-of address is an address of a foreign agent with which the mobile node is registered; a colocated care-of address is an externally obtained local address which the mobile node has associated with one of its own network interfaces.

COPS: Common Open Policy Service: A protocol used for policy control and provisioning.

Credentials: Identity proof information.

CRL: Certificate Revocation List: A list of client certificates that were revoked by the authority before they expired.

Cryptographic key: A symmetric key or a public key or a private key.

Cryptographic Protocol: Rules and procedures for applying cryptographic algorithms.

Cryptographic Signature: A hash of a digital document or of a digital message encrypted with the private key of the signer.

DER format: A format for storing certificates in files.

Digital Certificate: Usually same as certificate.

Digital Signature: Usually same as cryptographic signature.

EAP: Extensible Authentication Protocol: A general protocol for authentication which support multiple authentication mechanisms.

EAPOL-Key Packet: Created and transmitted by the Authenticator in order to provide media specific key information in WPA key management.

Eavesdropping: Unauthorized read access to transmitted information.

Encapsulation: The process of incorporating an original IP packet (less any preceding fields such as a MAC header) inside another IP packet, making the fields within the original IP header temporarily lose their effect.

Encryption: The process of obscuring information to prevent it from being read by unauthorized parties.

Encryption Algorithm: A set of operations implementing encryption.

FA: Foreign Agent: A router on the foreign network that assists a locally reachable mobile node on that network. The foreign agent assists the mobile node in receiving datagrams delivered to the care-of address.

Firewall: A network traffic filter.

Foreign Network: The network to which the mobile node is attached when it is not attached to its home network. The mobile node's care-of address is local to the foreign network and is reachable from the rest of the Internet.

FreeBSD: An open source UNIX based operating system.

FreeS/WAN: Open source VPN software for Linux computers.

Gateway: A device connecting a network to an internet.

Group Key: A symmetric key for protected communication between an AP and all client computers authenticated by this AP.

HA: Home Agent: A router on a mobile node's home network that tunnels datagrams for delivery to the mobile node when it is away from home.

Handover: To maintain a path between an MT and a correspondent node when the MT moves between cells of the same radio technology or between different radio technologies with a minimum of involvement from the user.

Hardware Token: A certified private key stored in a separate computer chip.

Hash: A fixed size, unique, cryptographic bit pattern derived from a document or from a message.

Header: The control information in a data packet before the payload.

HiperLAN/2 Network: Consists of a number of Access Points with continuous radio coverage and of associated mobile terminals.

HLR: Home Location Register: Centralized entity containing subscription data that is required for user authentication and encryption in a 2nd generation GSM network on a per user basis.

Home Address: A static IP address on the home network that is assigned for an extended period of time to a mobile node. The home address may be permanently assigned to the mobile node, or may be dynamically assigned for the duration of the mobile node's session.

Home Network: The network associated with the mobile node's home address. IP routing mechanisms will deliver datagrams destined to a mobile node's Home Address to the mobile node's Home Network.

HSS: Home Subscriber Server: A centralized entity containing subscription data that is required for user authentication and encryption in a 3rd generation mobile network (UMTS) on a per user basis.

IAPP: Inter-Access Point Protocol: A protocol for communicating information between access points in order to support roaming.

IEEE: Institute of Electrical and Electronics Engineers: A non-profit, technical professional association for electrical and electronics engineering.

IEEE 802.11i: A forthcoming standard for OSI layer 1 and 2 WLAN security

IEEE 802.1X: A standard for authentication of computers clients connected to a Local Area Network port or to a WLAN access point.

Internet: A network consisting of interconnected networks. An internet is any network, which has the same structure as Internet.

IETF: Internet Engineering Task Force: The principal body engaged in the development of new Internet standard specifications.

Key Hierarchy: Rules for deriving symmetric session keys from a symmetric master key.

Key Management: Rules and procedures for creation, distribution, storage, and use of cryptographic keys.

LEAP: Lightweight EAP: A Cisco vendor-specific authentication method that provides mutual authentication and dynamic WEP key generation.

Linux: An open source UNIX based operating system.

Macrocell: cell with coverage radius of many Km.

Microcell: cell with coverage radius of up to many hundreds of meters.

Master Key: The symmetric key used to generate symmetric session keys.

Multicast Traffic: The same data packet is sent a subset of all hosts in a network.

Minimal Encapsulation: An encapsulation technique which uses fewer header bytes for tunneling packets to the care-of address than the default IP-within-IP method uses.

MN: Mobile Node: A computing device that may change its point of attachment from one network or sub-network to another through the Internet. The mobile node is assigned a fixed home address on a home network, which correspondent nodes may use to address their packets to, regardless of its current point of attachment.

Mobility: Ability of an MT to be used in different network environments, within a single and in different administrative domains, with minimum user intervention.

Mobility Agent: A node (typically a router) that offers support services to mobile nodes. A mobility agent is either a home agent or a foreign agent.

Mobility between administrative domains: Ability for a MT to function in a serving network different from the originating network mobility between network environments: refers to the ability of an MT to be used in different network environments, such as home, corporate and public roaming: mobility between administrative domains.

Mobility Binding: The triplet of numbers that associates a mobile node's home address with its care-of address and registration lifetime.

MSC server: Switching Center for Circuit Switched traffic in 3G networks.

MT: Mobile Terminal: End system equipment providing the interface to people.

Nonce: A unique random value that is never reused.

OpenBSD: An open source UNIX based operating system.

Open Source Software: Software, which is available also as source code without a commercial software license.

OpenSSL: Open source software implementing the Secure Sockets Layer protocol.

Open1x Project: Open Source Implementation of the IEEE 802.1X standard.

Pairwise: Two entities associated with each other.

Pairwise Key: A symmetric session key used by two entities associated with each other.

Pass phrase: A sentence used as a password.

Payload: The information content of a data packet in data communication .

PEM Format: A format for storing certificates in files.

Per-Packet Key: Every data packet is encrypted with a different symmetric key.

Picocell: cell with coverage radius of many meters.

PKCS12: A format for storing a Public Key Cryptography key pair in a file.

PKI: Public Key Infrastructure: A configuration of systems and components required to manage and administer a public key environment.

Pre-Shared Key: A pre-installed symmetric key.

Private Key: The key in a Public Key Cryptography key pair known exclusively by the key pair owner.

Probe Response: An action taken or an object used to learn something about the state of a network.

Public Key: The publicly known key in a Public Key Cryptography key pair.

Public Key Cryptography: Two different but interrelated keys are used for encryption and decryption. One key is public and the other key is private. The key interrelation is easily created but too complex to crack.

Radio AP: BTS's, Node B's, etc.

RADIUS: Remote Authentication Dial-in User Service: A protocol used to perform authentication, authorization and accounting (AAA).

RC4: A variable key-size stream cipher with byte oriented operations. A registered trademark of RSA.

Registration: The process by which the mobile node informs the home agent of its current care-of address.

Registration Lifetime: How long the mobility agents may use a mobility binding.

Replay Attacks: A security violation whereby a malicious third entity attempts to imitate a transaction recorded during a previous and valid transaction between two protocol entities. Both protocol entities have to be aware that the subsequent identical traffic streams may no longer be valid. Since the previous transaction was valid, the algorithms for detecting replay attacks need to incorporate data that can never be reproduced in any correct subsequent transaction.

Route Optimisation: A process that enables the delivery of packets directly to the care-of address from a correspondent node without unnecessarily detouring through the home network.

Secret Key: The same as a symmetric key.

Security Association: A collection of one or more security contexts, between a pair of nodes, which may be applied to Mobile IP protocol messages exchanged between them.

Security Context: A security context indicates an authentication algorithm, a secret (a shared key), and a style of replay protection in use.

Security Protocol: Rules and procedures to be applied in protected data communication.

SIM Card: The SIM (Subscriber Identification Module) card is a smart card that identifies a user to the network and contains a microprocessor chip, which stores unique information about an account, including phone numbers and security numbers (PIN and key). There are two different sizes of SIM cards used for GSM phones, one is the same size as a credit card and the other is about the size of a stamp. Both cards contain the same electrical circuits; only the plastic surrounding it different. Functions on the SIM card includes: memory space to save up to 100 names and phone numbers, in addition to as many as 15 SMS, short text messages.

SLP: Service Locator Protocol: A protocol which provides a method to discover and select network services.

Smart card: A computer chip embedded in a plastic card.

Soft Token: Same as software token.

Software Token: A certified private key stored in a file.

SPI: Security Parameter Index: An index identifying a security context between a pair of nodes among the contexts available in the Security Association.

SRP: Secure Remote Password: A cryptographically strong authentication mechanism suitable for negotiating secure connections and performing a secure key exchange using a user-supplied password.

SSID: Service Set Identifier: An arbitrary string naming an access point or set of access points for purposes of identifying the WLAN to clients.

STA: Wireless Station: Any 802.11 device other than an AP.

Supplicant: 802.1X term for an entity that is being authenticated. Often a synonym for client, workstation, or user.

Symbian: Company which develops operating system for hand-held devices. Most wireless manufacturers have adopted this OS.

Symmetric Key: The same key is used for encryption and decryption.

TLS: Transport Layer Security: A protocol designed to provide privacy and data integrity between two communicating applications. Specifically, EAP-TLS provides protected ciphersuite negotiation, mutual authentication, and key management. transactions are eventually handled by the AAAH, possibly via one or more intermediaries.

Tunnel: The path followed by a datagram while it is encapsulated. An encapsulated datagram is routed to a knowledgeable de-encapsulating agent, who de-encapsulates the datagram and delivers it to its ultimate destination.

Unicast Traffic: A data packet is sent to only one receiver.

USB Adapter: Provides connectivity through a computer's USB port.

Virtual Private Network: Software implementing IPSec.

Visited Network: A network other than a mobile node's home network, to which the mobile node is currently connected.

Visitor List: A list of mobile nodes visiting a foreign agent.

Visual Basic: A programming environment from Microsoft for graphical Windows applications.

VPN: Virtual Private Network: A method of using encryption and tunneling to securely connect users over a public network.

WEP: Wired Equivalent Privacy: An 802.11 privacy service – encrypts data over wireless medium.

Wi-Fi Alliance: The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification.

WLAN: Wireless Local Area Network: A network that provides the features of traditional LAN technologies such as Ethernet and Token Ring using wireless technology.

X.509: International Telecommunications Union standard specifying contents of digital certificate.