

# Terms and Acronyms in Privacy in Telecommunications

Acronym /Term	Definition	Explanation	Web-resources
2G	Second Generation mobile technology	Refers to the family of digital cellular telephone systems standardised in the 1980s and introduced in the 1990s. They introduced digital technology and carry both voice and data conversation. CDMA, TDMA and GSM are examples of 2G mobile networks.	
3G	Third Generation mobile technology	The generic term for the next generation of wireless mobile communications networks supporting enhanced services like multimedia and video. Most commonly, 3G networks are discussed as graceful enhancements of 2G cellular standards, like e.g. GSM. The enhancements include larger bandwidth, more sophisticated compression techniques, and the inclusion of in-building systems. 3G networks will carry data at 144 kb/s, or up to 2 Mb/s from fixed locations. 3G comprises mutually incompatible standards: UMTS FDD and TDD, CDMA2000, TD-CDMA.	
3GPP	Third Generation Partnership Project	Group of the standards bodies ARIB and TTC (Japan), CCSA (People's Republic of China), ETSI (Europe), T1 (USA) and TTA (Korea). Established in 1999 with the aim to produce and maintain the specifications for a third generation mobile communications system called UMTS. Note that 3GPP is not itself a standardisation organisation and that all produced standards must be ratified by a standardisation organisation. A permanent project support group called the Mobile Competence Centre (MCC) is in charge of the day-to-day running of 3GPP. The MCC is based at the ETSI headquarters in Sophia Antipolis, France.	<a href="http://www.3gpp.org">http://www.3gpp.org</a>
3GPP2	Third Generation Partnership Project 2	A collaborative third generation (3G) telecommunications specifications-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotelecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. 3GPP2 was initiated as a result of the International Telecommunication Union's (ITU) International Mobile Telecommunications IMT-2000 initiative, covering high speed, broadband, and Internet Protocol (IP)-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming and seamless services independent of location. 3GPP2 is a collaborative effort between five officially recognised Standards Development organisations (SDO): ARIB – Association of Radio Industries and Businesses (Japan), CCSA – China Communications Standards Association (China), TIA – Telecommunications Industry Association (North America), TTA – Telecommunications Technology Association (Korea), and TTC – Telecommunications Technology Committee (Japan).	<a href="http://www.3gpp2.org">http://www.3gpp2.org</a>
AAA	Authentication, Authorization and Accounting	Key functions to intelligently controlling access, enforcing policies, auditing usage, and providing the information necessary to do billing for services available on the Internet. The term AAA is used to denote an internet security service architecture that provides the AAA services. The architecture includes AAA servers and AAA protocols. The AAA protocols include RADIUS and DIAMETER. Defined in IETF RFC 2903.	<a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/html/rfc2903">http://tools.ietf.org/html/rfc2903</a>
ADSL	Asymmetric Digital Subscriber Line	A data communications technology that enables faster data transmission over copper telephone lines than a conventional modem can provide. The access utilises the 1.1 MHz band and has the possibility to offer, dependent on subscriber line length, downstream rates of up to 8 Mb/s. Upstream rates start at 64 kb/s and typically reach 256 kb/s but can go as high as 768 kb/s. Specified by ANSI T1.413 and by ITU-T recommendation G.992.1. A version called ADSL Lite providing up to 1.5 Mb/s downstream rates is specified as G.992.2.	<a href="http://www.itu.int">http://www.itu.int</a>
AES	Advanced Encryption Standard	Also known as Rijndael. In cryptography, it is a block cipher adopted as an encryption standard by the US government. It is expected to be used worldwide and is analysed extensively, as was the case with its predecessor, the Data Encryption Standard (DES). AES was adopted by the National Institute of Standards and Technology (NIST) in November 2001 after a 5-year standardisation process. The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES selection process under the name 'Rijndael', a blend comprising the names of the inventors.	<a href="http://www.nist.gov">http://www.nist.gov</a>
AH	Authentication Header	AH is an IPsec protocol. This protocol is no longer needed in IPsec, but is retained for backward compatibility reasons. Defined in IETF RFC 4302.	<a href="http://www.ietf.org/">http://www.ietf.org/</a> , <a href="http://tools.ietf.org/html/rfc4302">http://tools.ietf.org/html/rfc4302</a>
AKA	Authentication and Key Agreement	A challenge-response based authentication cryptographic protocol that additionally also includes agreement on session key material. In the 3GPP sphere there exists several variants, including GSM AKA, UMTS AKA, IMS AKA etc. Note that the 3GPP2 CDMA2000 system uses an AKA protocol almost identical to the UMTS AKA protocol. Specified in 3GPP TS 33.102.	<a href="http://www.3gpp.org/ftp/Specs/html-info/33102.htm">http://www.3gpp.org/ftp/Specs/html-info/33102.htm</a>

Acronym /Term	Definition	Explanation	Web-resources
AN	Access Network	An access network is that part of a communications network which connects subscribers to their immediate service provider.	
AODV	Ad-hoc On-demand Distance Vector	The AODV routing algorithm is for routing data across Wireless Mesh Networks. It is capable of both unicast and multicast routing. It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. It is defined in IETF RFC 3561.	<a href="http://www.ietf.org/html/rfc3561">http://www.ietf.org/html/rfc3561</a>
AP	Access Point	A point where users access the system/network, e.g. a base station in a wireless network.	
ARAN	Authenticated Routing for Ad-hoc Networks	A secure routing protocol, ARAN detects and protects against malicious actions by third parties and peers. ARAN introduces authentication, message integrity, and non-repudiation to routing in an ad hoc environment as part of a minimal security policy.	
AsiaCrypt		AsiaCrypt is an IACR conference. The topic is cryptography and cryptographic protocols. IACR also holds the EuroCrypt and Crypto conferences.	<a href="http://www.iacr.org/">http://www.iacr.org/</a>
AuC	Authentication Centre	The AuC is the authentication centre in 2G and 3G cellular networks. The AuC is co-located with a HLR.	
AV	Authentication Vector	The AV is the security credential basis for one challenge-response run in 3GPP and 3GPP2 systems. 3GPP TS 33.102 defines the AV as the following: AV := RAND    XRES    CK    IK    AUTN. '  ' is a symbol for bitstring concatenation.	<a href="http://www.3gpp.org/ftp/Specs/html-info/33102.htm">http://www.3gpp.org/ftp/Specs/html-info/33102.htm</a>
Bluetooth		A short-range wireless specification that allows radio connection between devices within a 10-metre range of each other. Bluetooth is designed as a Personal Area Network (PAN) technology with a wide variety of theoretical uses. Bluetooth is a short-range radio standard and communications protocol primarily designed for low power consumption. Bluetooth, which is a replacement technology for IrDA, provides a unified way to connect devices such as mobile phones, laptops, PCs, printers, digital cameras etc. Bluetooth was named after king Harald Bluetooth, King of Denmark and Norway (born in 910 and died in 985 or 986). The Bluetooth logo is a combination of the Nordic runes Berkanan and Haglaz forming a combined letter/symbol (a bind rune).	<a href="https://www.bluetooth.org/">https://www.bluetooth.org/</a>
BTS	Base Transceiver Station	The radio base station of a GSM network. It consists of one or more transmitter-receiver unit, each serving one carrier frequency.	<a href="http://www.etsi.org">http://www.etsi.org</a>
CDMA 2000	Code Division Multiple Access 2000	A family of third-generation (3G) mobile telecommunications standards that use CDMA, a multiple access scheme for digital radio, to send voice, data, and signalling data (such as a dialled telephone number) between mobile phones and cell sites. It is the second generation of CDMA digital cellular. The CDMA2000 standards CDMA2000 1x, CDMA2000 1xEV-DO, and CDMA2000 1xEV-DV are approved radio interfaces for the ITU's IMT-2000 standard and a direct successor to 2G CDMA, IS-95 (cdmaOne). CDMA2000 is standardized by 3GPP2. CDMA2000 is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States, not a generic term like CDMA.	<a href="http://www.3gpp2.org">http://www.3gpp2.org</a>
Challenge-Response Protocol		Challenge-Response protocols are entity authentication protocols. A principal entity Alice challenges the corresponding principal entity Bob. In order for Bob to respond correctly Bob must compute a reply using a cryptographic function and a personal, secret security credential. There are several distinct types of Challenge-Response protocols, depending on factors such as the type of cryptographic transform used, type of security credential used etc. Challenge-Response protocols can also be classified as unidirectional or mutual (they almost always take place between two principal entities).	
CN	Core Network	Term used for core network nodes in cellular systems. CN nodes include HLR/AuC, VLR/MS, VLR/SGSN, SMSC, EIR and GGSN.	
COMP 128		An infamous authentication and key agreement algorithm. The original COMP128 is an example implementation for the GSM A3 and A8 cryptographic functions. The COMP128 algorithm is fundamentally flawed and has been known to be so for more than a decade. The algorithm, which is an operator-specific algorithm (contained in the SIM card), is completely unsuitable for its designated tasks, yet it is still in use in several GSM/GPRS networks today.	
Cookie (HTTP cookie)		HTTP cookies (or just cookies) are small text objects sent by a server to a web browser. The cookie is returned to the server by the browser upon subsequent visits to the server site. The cookies are used for authenticating, tracking, and maintaining state information about user activities etc. The state information may include user identity, time of last visit, site preferences, the contents of electronic shopping carts etc. The cookies are stored on the client computer and may be a privacy liability. The lifetime of cookies can be set, but the expired cookies may remain on your computer.	
CS	Circuit Switched	A network that establishes a circuit (or channel) between nodes before they may communicate. This circuit is dedicated and cannot be used for other means until the circuit is cancelled/closed and a new one created. If no actual communication is taking place in this circuit then the channel remains idle.	

Acronym /Term	Definition	Explanation	Web-resources
Data Confidentiality (Confidentiality)		The property that information is not made available or disclosed to unauthorised individuals, entities or processes. This property is very closely related to provision of Data Privacy. Defined in 3GPP TS 33.102.	<a href="http://www.3gpp.org/ftp/Specs/html-info/33102.htm">http://www.3gpp.org/ftp/Specs/html-info/33102.htm</a>
Data integrity		The property that data have not been altered in an unauthorised manner. Note that this is a security definition. It differs from the communications definition of data integrity in that the security definition captures the possibility of malicious intent. Defined in 3GPP TS 33.102.	<a href="http://www.3gpp.org/ftp/Specs/html-info/33102.htm">http://www.3gpp.org/ftp/Specs/html-info/33102.htm</a>
Data Mining		Data mining is the process searching large volumes of data for patterns using various tools to categorize and correlate data into usable information. Data mining can also be defined as "the nontrivial extraction of implicit, previously unknown, and potentially useful information from data".	
Data obfuscation		In security terminology obfuscation is used in the context of concealing the meaning of information or communication by making it more confusing and harder to interpret. Data obfuscation is achieved by applying a transformation function to the data. Data obfuscation transforms may or may not be bijective functions.	
Data origin authentication		Enables the recipient to verify that messages have not been tampered with in transit (data integrity) and that they originate from the expected sender (authenticity). Defined in 3GPP TS 33.102.	<a href="http://www.3gpp.org/ftp/Specs/html-info/33102.htm">http://www.3gpp.org/ftp/Specs/html-info/33102.htm</a>
DDoS	Distributed Denial-of-Service	A distributed and coordinated DoS attack. Usually executed against internet homepages with thousands of (hijacked) computers involved.	
DH	Diffie-Hellman	The Diffie-Hellman key exchange is a cryptographic protocol that allows two parties to establish a shared secret key over an insecure communications channel. The basic DH exchange is unauthenticated and is thus susceptible to MitM attacks.	
DHS	Department of Homeland Security	A US federal state department responsible for coordinating all aspects of homeland security. DHS was created subsequent to the 9/11 terrorist attack.	<a href="http://www.dhs.gov/index.shtml">http://www.dhs.gov/index.shtml</a>
DIAMETER		An AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended as the successor of RADIUS. The basic concept is to provide a base protocol that can be extended in order to provide AAA services to new access technologies. Diameter is intended to work in both local and roaming AAA situations. Defined in IETF RFC 3588.	<a href="http://www.ietf.org/html/rfc3588">http://www.ietf.org/html/rfc3588</a>
DoS	Denial-of-Service	A denial-of-service attack (DoS attack) is an attack targeted at the availability of some resource. The attack usually tries to exhaust the capacity of the target in one way or another. Examples include attacks against internet infrastructures like DNS servers, but the most common example would be attacks against high-profile (corporate) homepages. Defined in IETF RFC 4732.	<a href="http://www.ietf.org/html/rfc4732">http://www.ietf.org/html/rfc4732</a>
DRD	Data Retention Directive	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006.	<a href="http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/L105/L10520060413en00540063.pdf">http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2006/L105/L10520060413en00540063.pdf</a>
DRM	Digital Rights Management	Any of several technologies used by publishers (or copyright owners) to control access to and usage of digital data (such as software, music, movies) and hardware, handling usage restrictions associated with a specific instance of a digital work.	
DTA	Data Transmission Algebra		
DYI	Dolev-Yao Intruder	The Dolev-Yao Intruder is an exceptionally capable Intruder. It can (and by definition will) capture all messages ever exchanged over any (entity external) interface. It can delete, insert and modify any message at will. Only appropriate and correct use of cryptographic protection can stop the DYI. The DYI will not corrupt the principal entities, but may try to masquerade as a principal entity.	
EAP	Extensible Authentication Protocol	An authentication framework that enables clients to authenticate with a central server. EAP can be used with several authentication mechanisms (EAP methods), such as EAP-AKA, EAP-SIM, EAP-MD-5, etc. Defined in IETF RFC 3748.	<a href="http://tools.ietf.org/html/rfc3748">http://tools.ietf.org/html/rfc3748</a>
Eaves-dropping		The act of listening in on a conversation (or communication). Eavesdropping is a threat to the privacy of the conversation. Eavesdropping can be prevented in various ways, including the use of the security service Data Confidentiality.	
ECC	Elliptic Curve Cryptography	ECC is a type of public-key cryptography based on the algebraic structure of elliptic curves over finite fields.	

Acronym /Term	Definition	Explanation	Web-resources
EEA	European Economic Area	The agreement creating the European Economic Area (EEA Agreement) was negotiated between the Community, the then Member States, and seven member countries of EFTA. It was signed in May 1992 and came into force 1 January 1994. It was designed to allow EFTA countries to participate in the European Single Market without having to join the EU. The current members (contracting parties) are three of the four EFTA states – Iceland, Lichtenstein and Norway (without Switzerland) – the European Union and the 25 EU Member States.	<a href="http://ec.europa.eu/external_relations/eea/index.htm">http://ec.europa.eu/external_relations/eea/index.htm</a>
Entity Authentication (Authentication)		The provision of assurance of the claimed identity of an entity. Defined in 3GPP TS 33.102.	<a href="http://www.3gpp.org/ftp/Specs/html-info/33102.htm">http://www.3gpp.org/ftp/Specs/html-info/33102.htm</a>
EPC	Electronic Product Code	EPC is a standard for how to tag products electronically.	<a href="http://www.epcglobalinc.org/home">http://www.epcglobalinc.org/home</a>
ESP	Encapsulating Security Payload	A part of the IPsec framework for Internet security. The ESP extension header provides origin authenticity, integrity, and confidentiality of a packet. It is the preferred IPsec protocol and can provide all the security services IPsec provides. Defined in IETF RFC 4303.	<a href="http://www.ietf.org/html/rfc4303">http://www.ietf.org/html/rfc4303</a>
ETSI	European Telecommunication Standards Institute	A non-profit membership organisation founded in 1988. The aim is to produce tele-communications standards to be used throughout Europe. The efforts are coordinated with ITU. Membership is open to any European organisation proving an interest in promoting European standards. It was e.g. responsible for the making of the GSM standard. The headquarters are situated in Sophia Antipolis, France.	<a href="http://www.etsi.org">http://www.etsi.org</a>
GGSN	Gateway GPRS Support Node	Interface between the GPRS wireless data network and other networks such as the Internet or private networks. It supports the edge routing function of the GPRS network. To external packet data networks the GGSN performs the task of an IP router. Firewall and filtering functionality, to protect the integrity of the GPRS core network, are also associated with the GGSN along with a billing function.	<a href="http://www.etsi.org">http://www.etsi.org</a> , <a href="http://www.3gpp.org">http://www.3gpp.org</a>
GPRS	General Packet Radio Service	An enhancement to the GSM mobile communication system that supports data packets. GPRS enables continuous flows of IP data packets over the system for such applications as web browsing and file transfer. Supports up to 160 kb/s gross transfer rate. Practical rates are from 12 to 48 kb/s.	<a href="http://www.etsi.org">http://www.etsi.org</a> , <a href="http://www.3gpp.org">http://www.3gpp.org</a>
GPS	Global Positioning System	The Global Positioning System (GPS) is a worldwide radio-navigation system formed from a constellation of 24 satellites and their ground stations. GPS uses these 'man-made stars' as reference points to calculate positions accurate to a matter of metres.	<a href="http://www.gps.gov/">http://www.gps.gov/</a> , <a href="http://www.navcen.uscg.gov/gps/default.htm">http://www.navcen.uscg.gov/gps/default.htm</a>
GSM	Global System for Mobile communications	A digital cellular phone technology system that is the predominant system in Europe, but is also used around the world. Development started in 1982 by CEPT and was transferred to the new organisation ETSI in 1988. Originally, the acronym was the group in charge, Group Special Mobile, but later the group changed name to SMG. GSM was first deployed in seven countries in Europe in 1992. It operates in the 900 MHz and 1.8 GHz band in Europe and 1.9 GHz band in North America. GSM defines the entire cellular system, from the air interface to the network nodes and protocols. As of October 2006, there were more than 2.1 billion GSM users in more than 200 countries worldwide. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators and enables phone users to access their services in many other parts of the world as well as their own country. GSM differs significantly from its predecessors in that both signalling and speech channels are digital, which means that it is seen as a second generation (2G) mobile phone system. This fact has also meant that data communication was built into the system from very early on. GSM is an open standard which is currently developed by the 3GPP.	<a href="http://www.gsmworld.com/">http://www.gsmworld.com/</a> , <a href="http://www.etsi.org">http://www.etsi.org</a> , <a href="http://www.3gpp.org">http://www.3gpp.org</a>
Hash / Hash function		A hash function takes an arbitrary length string (the message) and computes a fixed length output string. The output is called the hash, the digest or the checksum. Cryptographic hash functions are different from ordinary hash functions. In the context of this edition of <i>Teletronikk</i> we shall only refer to cryptographic hash functions.	<a href="http://en.wikipedia.org/wiki/Cryptographic_hash_function">http://en.wikipedia.org/wiki/Cryptographic_hash_function</a>
HE	Home Entity	Non-3GPP acronym. Home server. Roughly equivalent to the 3GPP HSS.	
HE	Home Environment	Home Environment: responsible for overall provision and control of the Personal Service Environment of its subscribers.	
HHD	Hand Held Device	A generic name for a pocket-sized computing device, typically utilising a small visual display screen for user output and a miniaturised keyboard for user input (for example, PDA, smartphones etc.).	
HI	Handover Interface		

Acronym /Term	Definition	Explanation	Web-resources
HLR	Home Location Register	The Home Location Register or HLR is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network. More precisely, the HLR stores details of every SIM card issued by the mobile phone operator. Each SIM has a unique identifier called an IMSI which is one of the primary keys to each HLR record. The next important items of data associated with the SIM are the telephone numbers used to make and receive calls to the mobile phone, known as MSISDNs. The main MSISDN is the number used for making and receiving voice calls and SMS, but it is possible for a SIM to have other secondary MSISDNs associated with it for fax and data calls. Each MSISDN is also a primary key to the HLR record.	<a href="http://www.etsi.org">http://www.etsi.org</a>
Homo-morphic crypto-system		Homomorphic crypto-systems have the property that one specific algebraic operation on the plaintext is equivalent to another (possibly different) algebraic operation on the ciphertext. As an example, one can imagine a crypto-system in which addition on ciphertext element is equivalent to multiplication on plaintext elements. This would permit a user, which does not have access to the plaintext, to perform multiplication on the plaintext by executing multiplication operations on the ciphertext. This property is useful in developing Secure Multi-party Computation protocols.	
HSS	Home Subscriber Server	The home subscriber server contains all operative subscriber data, including information on subscribed services, location/roaming information and security credentials. Includes HLR/AuC and AAA services.	<a href="http://www.3gpp.org">http://www.3gpp.org</a>
HUB		A common connection point for devices in a network.	
IACR	International Association for Cryptologic Research	IACR is a non-profit scientific organisation whose purpose it is to further research in cryptology and related fields.	<a href="http://www.iacr.org/">http://www.iacr.org/</a>
Identity Privacy		A privacy service that ensures that the permanent identity of the principal entity is only disclosed to authorized entities. For the case when the entity has multiple identities the service must extend to cover all but anonymous/transient identities.	
Identity Theft		Identity theft can be divided into four categories: A) Financial Identity Theft (using another's name and social security number (or similar) to obtain goods and services, B) Criminal Identity Theft (posing as another when apprehended for a crime), C) Identity Cloning (using another's information to assume his or her identity in daily life), and D) Business/Commercial Identity Theft (using another's business name to obtain credit). An excellent source on identity theft is the Identity Theft Resource Center ( <a href="http://www.idtheftcenter.org/">http://www.idtheftcenter.org/</a> ).	<a href="http://www.idtheftcenter.org/">http://www.idtheftcenter.org/</a>
IDS	Intrusion Detection System	A software/hardware tool used to detect unauthorised access to a computer system or network. This may take the form of attacks by skilled malicious hackers, or Script kiddies using automated tools. An IDS is required to detect all types of malicious network traffic and computer usage. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorised logins and access to sensitive files, and malware (viruses, Trojan horses, and worms).	
IEEE	The Institute of Electrical and Electronics Engineers	USA based organisation open to engineers and researchers in the fields of electricity, electronics, computer science and telecommunications. Established in 1884. The aim is to promote research through journals and conferences and to produce standards in telecommunications and computer science. IEEE has produced more than 900 active standards and has more than 700 standards under development. Divided into different branches, or 'Societies'. Has daughter organisations, or 'chapters' in more than 175 countries worldwide. Headquarters in Piscataway, New Jersey, USA.	<a href="http://www.ieee.org">http://www.ieee.org</a>
IEEE 802.11	The IEEE 802 LAN/MAN Standards Committee Working Group for WLAN	Refers to a family of specifications developed by the IEEE for wireless local area networks. It also refers to the Wireless LAN Working Group of the IEEE 802 project. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. The IEEE accepted the specification in 1997. There are several specifications in the 802.11 family, including i) 802.11 – provides 1 or 2 Mbit/s transmission in the 2.4 GHz band; ii) 802.11a – an extension that provides up to 54 Mbit/s in the 5 GHz band. It uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS, iii) 802.11b provides 11 Mbit/s transmission in the 2.4 GHz band and was ratified in 1999 allowing wireless functionality comparable to Ethernet; iv) 802.11g provides 20+ Mbit/s in the 2.4 GHz band; v) 802.11z is a method for transporting an authentication protocol between the client and access point, and the Transport Layer Security (TLS) protocol. More variants are also under preparation, including support of 100 Mbit/s traffic flows.	<a href="http://www.ieee802.org/11">http://www.ieee802.org/11</a>
IEEE 802.11i		IEEE 802.11i is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. Its architecture contains the following components: 802.1X for authentication (entailing the use of EAP and an authentication server), RSN for keeping track of associations, and AES-based CCMP to provide confidentiality, integrity and origin authentication.	<a href="http://www.ieee802.org/11">http://www.ieee802.org/11</a>

Acronym /Term	Definition	Explanation	Web-resources
IEEE 802.16	The IEEE 802 LAN/MAN Standards Committee Working Group on Broadband Wireless Access Standards	A specification for fixed broadband wireless metropolitan access networks (MANs) that uses a point-to-multipoint architecture. Published on 8 April 2002, the standard defines the use of bandwidth between the licensed 10 GHz and 66 GHz and between the 2 GHz and 11 GHz (licensed and unlicensed) frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 30 miles to handle such services as VoIP, IP connectivity and TDM voice and data.	<a href="http://www.ieee802.org/16/">http://www.ieee802.org/16/</a> , <a href="http://www.wimaxforum.org/">http://www.wimaxforum.org/</a>
IEEE 802.1X	IEEE Standards for Local and metropolitan area networks – Port-Based Network Access Control	An IEEE standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. It is used for certain closed wireless access points, and is based on the EAP, Extensible Authentication Protocol.	<a href="http://www.ieee802.org/1/pages/802.1x.html">http://www.ieee802.org/1/pages/802.1x.html</a>
IETF	Internet Engineering Task Force	A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The technical work of the IETF is done in its working groups, which are organised by topic into several areas (e.g. routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year. The IETF working groups are grouped into areas and managed by Area Directors (AD). The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB. The Internet Assigned Numbers Authority (IANA) is the central coordinator for the assignment of unique parameter values for Internet protocols. The IANA is chartered by the Internet Society (ISOC) to act as the clearinghouse to assign and coordinate the use of numerous Internet protocol parameters. IETF's mission statement is given in IETF RFC 3935.	<a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/html/rfc3935">http://tools.ietf.org/html/rfc3935</a>
IH	Information Hiding	Information hiding addresses two areas of concern: privacy of information from surveillance (steganography) and protection of intellectual property (digital watermarking).	
IIF	Internal Interception Function		
IKE/IKEv2	Internet Key Exchange	IKE is the key exchange protocol for IPsec. It performs entity authentication and key exchange. Defined in IETF RFC 4306.	<a href="http://tools.ietf.org/html/rfc4306">http://tools.ietf.org/html/rfc4306</a>
IMS	IP Multimedia Subsystem	A standardised Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3GPP standardised implementation of SIP, and runs over the standard Internet Protocol (IP). Existing phone systems (both packet-switched and circuit-switched) are supported. IMS was originally defined by an industry forum called 3G.IP ( <a href="http://www.3gip.org">www.3gip.org</a> ) formed in 1999. 3G.IP developed the initial IMS architecture, which was brought to 3GPP for industry standardisation as part of their standardisation work for 3G mobile phone systems in UMTS networks. It first appeared in release 5 (evolution from 2G to 3G networks), when SIP-based multimedia was added. Support for the older GSM and GPRS networks was also provided. 'Early IMS' was defined to allow for IMS implementations that do not yet support all 'Full IMS' requirements. 3GPP2 (a different organisation) based their CDMA2000 Multimedia Domain (MMD) on 3GPP IMS, adding support for CDMA2000.	<a href="http://www.3gpp.org">http://www.3gpp.org</a> , <a href="http://www.ietf.org">http://www.ietf.org</a>
IMSI	International Mobile Subscriber Identity	The principal subscriber identity in 2G/3G systems. Structure and definition of IMSI is given both in ITU-T recommendations (E.212) and in 3GPP specifications (TS 23.003). Note that in ITU-T E.212 the acronym is defined as 'International Mobile Station Identity', but the structure is otherwise identical.	<a href="http://www.itu.int">http://www.itu.int</a> , <a href="http://www.3gpp.org/ftp/Specs/html-info/23003.htm">http://www.3gpp.org/ftp/Specs/html-info/23003.htm</a>
INI	Internal Network Interface		
Internet		From the commissioning of ARPANET by the US DoD in 1969 the packet switched Internet has gained acceptance and users all over the world. The release of WWW at the end of the 1990s and the browsing possibilities (see WWW) increased the demand for Internet. The interconnection of heterogeneous sub networks of different bandwidths, the best-effort service model and the global end-to-end logical addressing of the internet protocol (IP) has arranged for Internet to be the common information network multiplexing text, pictures, and video as well as packet switched telephony.	
Intruder		In the security literature the term Intruder is reserved for a hostile malicious entity that will intently try to break one or more of the goals of a cryptographic protocol, a protected environment or similar. Sometimes the terms Adversary or Attacker is used for the same purpose.	

Acronym /Term	Definition	Explanation	Web-resources
IP	<b>Internet Protocol</b>	A protocol for communication between computers, used as a standard for transmitting data over networks and as the basis for standard Internet protocols. Originally defined in IETF RFC 791.	<a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/html/rfc791">http://tools.ietf.org/html/rfc791</a>
IPsec	<b>IP Security</b>	The IP security architecture consist of a base architcture and associated security protocols. This includes the ESP and AH security protocols as well as the IKE/IKEv2 key exchange protocols. IPsec is now in its third main revision. Defined in IETF RFC 4301.	<a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/html/rfc4301">http://tools.ietf.org/html/rfc4301</a>
IR	<b>Infrared</b>	In our context: A technology for short-range data transfer based on optical (infrared) communication. Used in laptops, mobile phones etc. See IrDA.	
IrDA	<b>Infrared Data Association</b>	IrDA is a nonprofit organization whose goal it is to develop globally adopted specifications for infrared wireless communication.	<a href="http://www.irda.org/">http://www.irda.org/</a>
ISDN	<b>Integrated Services Digital Network</b>	A digital telecommunications network that provides end-to-end digital connectivity to support a wide range of services, including voice and non-voice services, to which users have access by a limited set of standard multi-purpose user-network interfaces. The user is offered one or more 64 kb/s channels.	<a href="http://www.itu.int">http://www.itu.int</a>
ISO	<b>International Standardisation Organisation</b>	ISO is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a non-governmental organisation established in 1947. The mission of ISO is to promote the development of standardization and related activities in the world with a view to facilitating the international exchange of goods and services, and to developing cooperation in the spheres of intellectual, scientific, technological and economic activity.	<a href="http://www.iso.org">http://www.iso.org</a>
ITU	<b>International Telecommunication Union</b>	On 17 May 1865, the first International Telegraph Convention was signed in Paris by the 20 founding members, and the International Telegraph Union (ITU) was established to facilitate subsequent amendments to this initial agreement. It changed name to the International Telecommunications Union in 1934. From 1948 a UN body with approx. 200 member countries. It is the top forum for discussion and management of technical and administrative aspects of international telecommunications.	<a href="http://www.itu.int">http://www.itu.int</a>
ITU-T	<b>International Telecommunication Union – Standardization Sector</b>	A sector of the ITU whose mission it is to ensure an efficient and on-time production of standards (Recommendations) covering all fields of telecommunications. It was created on 1 March 1993, replacing the former International Telegraph and Telephone Consultative Committee (CCITT).	<a href="http://www.itu.int/ITU-T/">http://www.itu.int/ITU-T/</a>
k-anonymity		Data records adhere to k-anonymity if each released record has at least (k-1) other records in the release whose values are indistinct over those fields that appear in external data. k-anonymity provides privacy protection by guaranteeing that each released record will relate to at least k individuals even if the records are directly linked to external information.	
KDC	<b>Key Distribution Center</b>	The combination of Authentication Server and Ticket Granting Server of the Kerberos authentication protocol. It is defined in IETF RFC 4120.	<a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/html/rfc4120">http://tools.ietf.org/html/rfc4120</a>
Kerberos		Kerberos is a computer network authentication protocol which allows individuals communicating over an insecure network to prove their identity to one another in a secure manner. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. Kerberos prevents eavesdropping or replay attacks, and ensures the integrity of the data. Its designers aimed primarily at a client-server model, and it provides mutual authentication – both the user and the server verify each other's identity. Kerberos builds on symmetric key cryptography and requires a trusted third party. It was developed by The Masschusetts Institute of Technology (MIT) in the 1980s and is now maintained by IETF. It is defined in IETF RFC 4120.	<a href="http://www.ietf.org">http://www.ietf.org</a> , <a href="http://tools.ietf.org/html/rfc4120">http://tools.ietf.org/html/rfc4120</a>
LAN	<b>Local Area Network</b>	A network shared by communicating devices, usually in a small geographic area. A system that links together electronic office equipment, such as computers and word processors, and forms a network within an office or building.	
LBS	<b>Location Based Service</b>	LBS are services offered to subscribers based on their current location.	
LCS	<b>Location Services</b>		
LEA	<b>Law Enforcement Agency</b>	A Lawful Interception (LI) entity.	
LEMF	<b>Law Enforcement Monitoring Facility</b>	A Lawful Interception (LI) function.	
LI	<b>Lawful Interception</b>	Lawful interception plays a crucial role in helping law enforcement agencies combat criminal activity. Lawful interception of public telecommunications systems in each country is based on national legislation in that country.	<a href="http://portal.etsi.org/li/Summary.asp">http://portal.etsi.org/li/Summary.asp</a>

Acronym /Term	Definition	Explanation	Web-resources
Location Privacy		A privacy service that ensures that the location of the principal entity is only disclosed to authorised entities.	
LR	Local Registers		
MAC	Medium Access Control	The lower of the two sub layers of the Data Link Layer. In general terms, MAC handles access to a shared medium, and can be found within many different technologies. For example, MAC methodologies are employed within Ethernet, GPRS, and UMTS.	
MAC	Message Authentication Code	A MAC function computes a cryptographic signed integrity checksum over an arbitrary length input string under the control of a secret key. MAC functions are quite similar to hash functions, but the MAC function output can only be computed with knowledge of the secret key. MAC functions can be used to provide the message origin authentication and data integrity security services.	<a href="http://en.wikipedia.org/wiki/Message_authentication_code">http://en.wikipedia.org/wiki/Message_authentication_code</a>
MAP	Mobile Application Part	A protocol that enables real time communication between nodes in a mobile cellular network. A typical usage of the MAP protocol would be for the transfer of location information from the VLR (Visitor Location Register) to the HLR (Home Location Register). Defined in 3GPP TS 09.02 for GSM and in 3GPP TS 29.002 for UMTS.	<a href="http://www.3gpp.org/ftp/Specs/html-info/0902.htm">http://www.3gpp.org/ftp/Specs/html-info/0902.htm</a> , <a href="http://www.3gpp.org/ftp/Specs/html-info/29002.htm">http://www.3gpp.org/ftp/Specs/html-info/29002.htm</a>
MitM	Man-in-the-Middle	In security literature MitM attacks is a class of attacks where the Intruder is located between the legitimate entities. All communication passes through the Intruder, which may selectively delete, deflect, modify and insert messages.	
MIX		The MIX concept is often associated with onion routers, but a MIX can be local and need not route messages. The functionality of a MIX is to disassociate message addresses and message content while still being able to deliver the message to the intended recipient.	
MS	Mobile Station	An MS is the mobile phone. It corresponds to the UE (User equipment).	
MSC	Mobile services Switching Centre	The Mobile services Switching Centre or MSC is a sophisticated telephone exchange which provides circuit-switched calling, mobility management and GSM services to the mobile phones roaming within the area that it serves. This means voice, data and fax services, as well as SMS and call divert. It is located in the core network of a visited network and has an interface towards the radio access network. A Gateway MSC (GMSC) is the MSC that determines which visited MSC the subscriber who is being called is currently located. It also interfaces with the Public Switched Telephone Network. All mobile to mobile calls and PSTN to mobile calls are routed through a GMSC. The term is only valid in the context of one call since any MSC may provide both the gateway function and the Visited MSC function; however, some manufacturers design dedicated high capacity MSCs which do not have any BSCs connected to them. These MSCs will then be the GMSC for many of the calls they handle.	<a href="http://www.etsi.org">http://www.etsi.org</a>
MSISDN	Mobile Station Integrated Services Digital Network	MSISDN refers to the 15-digit number that is used to refer to a particular mobile station. It is the mobile equivalent of ISDN. The ITU-T recommendation E.164 defines the international numbering plan that MSISDN is based on.	<a href="http://www.itu.int">http://www.itu.int</a>
NFC	Near Field Communication Technology	NFC, jointly developed by Sony and Philips, was approved as an ISO/IEC standard on 8 Dec 2003. It was approved as an ECMA standard earlier on. On 18 March 2004 Nokia, Sony and Philips formed NFC-forum to advance NFC development. NFC is essentially about data sharing between devices using short-range radio technologies. NFC holds the promise of bringing true mobility to consumer electronics in an intuitive and psychologically comfortable way since the devices can hand-shake only when brought literally into touching distance.	<a href="http://www.nfc-forum.org/home">http://www.nfc-forum.org/home</a>
NGN	Next Generation Network	A network concept that aims at providing a framework to encompass the large variety of existing and emerging protocols and services, facilitate a further evolution of these, decouple the evolution from the underlying network infrastructure, and facilitate the interfacing of a plethora of available media. The rationale behind NGN lies founded in paradigm shifts that have been taking place within the technological solutions and the business models in the telecom industry as a whole. The concept is based on IP-technology and is being specified by ITU-T.	<a href="http://www.itu.int">www.itu.int</a>
Nonce	Number used once	A nonce is a cryptographic term used for an element that must provide uniqueness and that will only be used once. A nonce is normally either A) a sequence number, B) a time-stamp, or C) a pseudo-random number.	
P2P	Peer To Peer	A computer network that does not rely on dedicated servers for communication but instead mostly uses direct connections between clients (peers). A pure peer-to-peer network does not have the notion of clients or servers, but only equal peer nodes that simultaneously function as both 'clients' and 'servers' to the other nodes in the network.	

Acronym /Term	Definition	Explanation	Web-resources
Personal Privacy		Personal privacy is a surprisingly difficult term to pinpoint. One aspect is a person's ability to keep details of their daily lives and personal affairs out of public view. It should also include a measure of control over personal information collected by others about themselves. The control right should among other things include the right to restrict the usage and to ensure that the information is correct. Privacy is also sometimes related to a right to being anonymous. Privacy can be seen as an aspect of security and is often achieved by means of security techniques and methods.	
Phishing		Phishing is an activity where a fraudster tries to acquire sensitive/private information. They commonly use social engineering techniques. The most sought after information is usernames, passwords and credit card details etc. A well know phishing technique is to masquerade as a trustworthy website. This includes internet/online banks, auction companies like eBay and other trustworthy sites where you may be compelled to leave sensitive data. Phishing is typically carried out using email, and the users are conned to login or otherwise convey information at a website.	
PKI	Public Key Infrastructure	An arrangement which provides for third-party vetting of, and vouching for user identities. It also allows binding of public keys to users. This is usually carried by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates. The term is used to mean both the certificate authority and related arrangements as well as, more broadly and somewhat confusingly, to mean use of public key algorithms in electronic communications. The latter sense is erroneous since PKI methods are not required to use public key algorithms.	
POTS	Plain Old Telephone Service	A very general term used to describe an ordinary voice telephone service. See also PSTN.	
prf	pseudo-random function	A function that generates a stream of pseudo-random numbers.	
Privacy-Preserving		Techniques that ensure that the referred to privacy properties are an invariant property through the execution. Normally the privacy-preserving term is reserved for cryptographic algorithms and protocols that can be formally proven to preserve a given privacy characteristic throughout the execution of the algorithm/protocol.	
PS	Packet Switched	Communication switching method in which packets (units of information carriage) are individually routed between nodes over data links which might be shared by many other nodes. Packet switching is used to optimize the use of the bandwidth available in a network, to minimize the transmission latency (i.e. the time it takes for data to pass across the network), and to increase robustness of communication. The concept of packet switching was developed by Paul Baran in the early 1960s, and independently a few years later by Donald Davies, as described below. Leonard Kleinrock conducted early research and published a book in the related field of digital message switching (without the packets) in 1961, and also later played a leading role in building and management of the world's first packet switched network, the ARPANET.	
Pseudonym		A pseudonym is an alias, used by an individual as an alternative to a person's true name. Use of pseudonyms may provide a measure of identity anonymity.	
Pseudo-Random		Pseudo-randomness (in security) is a property that is normally associated with the characteristics non-predictability, uniqueness and non-repeatability. Statistically the pseudo-random number should (almost always) appear to be uniformly distributed.	
PSK	Pre-Shared Key	In communication security, a secret which was previously shared between the two (or more) parties using an external channel. The characteristics of this secret or key are determined by the system which uses it. It can be a password, a passphrase or a hexadecimal string. This secret is used by all systems involved in the cryptographic processes used to secure the traffic between the systems.	
QoS	Quality of Service	The "degree of conformance of the service delivered to a user by a provider, with an agreement between them". The agreement is related to the provision/delivery of this service. Defined by EURESCOM project P806 in 1999 and adopted by ITU-T in recommendation E.860. [E.860].	<a href="http://www.itu.int">http://www.itu.int</a> , <a href="http://www.eurescom.de">http://www.eurescom.de</a>
RADIUS	Remote Authentication Dial-In User Service	An authentication and accounting system used by many (W)ISPs. Then logging into a public Internet service you must enter your username and password. This information is passed to a RADIUS service, which checks that the information is correct, and then authorizes access to the WISP. RADIUS is an AAA protocol. It is intended to work in both local and roaming situations. The RADIUS specification is maintained by a working group of the IETF. Defined in IETF RFC 2865.	<a href="http://www.ietf.org/">http://www.ietf.org/</a> , <a href="http://tools.ietf.org/html/rfc2865">http://tools.ietf.org/html/rfc2865</a>
RAN	Radio Access Network	A part of a mobile telecommunication system. It implements a radio access technology. Conceptually, it sits between the mobile phone and the core network (CN). Examples are GERAN (GSM RAN), UTRAN (UMTS RAN) and E-UTRAN (LTE RAN).	
Random		There are several definitions of what random is intended to mean; notably one has A) an information-theoretic definition; B) a definition for the statistics field; and C) a definition for security/cryptography. To distinguish from 'true' randomness one often refers to pseudo-random properties in security terminology.	

Acronym /Term	Definition	Explanation	Web-resources
RFC	Request For Comment	An RFC is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Changes can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.	<a href="http://www.whatis.com">http://www.whatis.com</a>
RFID	Radio Frequency Identification	RFID is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. An RFID tag is a small object that can be attached to or incorporated into a product, animal, or person. RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from an RFID transceiver. Passive tags require no internal power source, whereas active tags require a power source.	
RRM	Radio Resource Management		
SA	Security Associations		
SAODV	Secure Ad-hoc On-demand Distance Vector routing	SAODV is an extension of the AODV routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation.	
SGSN	Serving GPRS support node	SGSN is an exchange which performs packet switching functions for mobile stations located in a geographical area designated as the SGSN area. It is located in the core network of the visited network in 2G/3G systems. It has an interface towards the radio access network. The SGSN is the PS equivalent of the VLR/MSC for CS connections.	<a href="http://www.3gpp.org">http://www.3gpp.org</a> , <a href="http://www.etsi.org">http://www.etsi.org</a>
SHM	Structural Health Monitoring	Structural Health Monitoring is an activity where actual data related to civil structures is observed/measured and registered based on high performance sensors, precision signal conditioning units, broad band analogue-to-digital converters, optical or wireless networks, global positioning systems etc.	<a href="http://www.ishmii.org/">http://www.ishmii.org/</a>
SIM	Subscriber Identity Module	The SIM is a subscriber identity module for GSM/GPRS subscriptions. In 2G systems the term SIM is used for a dedicated smartcard with subscriber identity information (including security credentials and algorithms). In 3G systems a SIM is an application running on the UICC (smartcard). Although the terms UICC and SIM are often interchanged, UICC refers to the physical card, whereas SIM (in 3G) refers to a single application residing in the UICC that collects GSM/GPRS user subscription information. The corresponding UMTS subscriber application is the USIM (which is always present on a UICC). The SIM provides secure storing of the key identifying a mobile phone service subscriber but also subscription information, preferences and storage of text messages. The equivalent of a SIM in UMTS is a Universal Subscriber Identity Module (USIM). Defined in 3GPP specification series 31.	<a href="http://www.3gpp.org/ftp/Specs/html-info/31-series.htm">http://www.3gpp.org/ftp/Specs/html-info/31-series.htm</a>
SMC	Secure Multi-party Computation	The research in the field of SMC is often considered to be initiated by Andrew C. Yao in 1982. In short, Yao proposed the so-called millionaire problem in which Alice and Bob are two millionaires who want to find out which is the richer. However, they do not want to reveal how much money they have to each other or to other parties. Solutions to this and other SMC problems tend to rely on use of advanced and sophisticated public-key crypto-system primitives.	
SN	Serving Network	The SN consists of one or more access networks (AN) attached to a core network (CN).	<a href="http://www.3gpp.org">http://www.3gpp.org</a> , <a href="http://www.etsi.org">http://www.etsi.org</a>
Spyware		The term 'spyware' is used for software that collects personal information about users without their informed consent. The spyware often uses stealth techniques to hide its activity or posing as a legitimate application (which makes it a Trojan).	
SS7	Signalling System #7	A set of telephony signalling protocols which are used to set up the vast majority of the world's PSTN telephone calls.	<a href="http://www.itu.int">http://www.itu.int</a>
Steganography		Steganography (literally, covered writing) explores methods to hide the existence of hidden messages.	
TC	Technical Committee		
TETRA	TERrestrial TRunked RAdio	TETRA is a digital trunked mobile radio standard developed by the European Telecommunications Standards Institute (ETSI). The purpose of the TETRA standard was to meet the needs of traditional Professional Mobile Radio (PMR) user organisations, which include utilities, public safety (including the police, the fire brigade, the medical emergency services), government, military, border control, etc.	<a href="http://www.tetramou.com/">http://www.tetramou.com/</a>

Acronym /Term	Definition	Explanation	Web-resources
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking	The ETSI core competence centre for fixed networks and for migration from switched circuit networks to packet-based networks with an architecture that can serve in both. TISPAN is responsible for all aspects of standardisation for present and future converged networks including the NGN (Next Generation Network) and including service aspects, architectural aspects, protocol aspects, QoS studies, security related studies, mobility aspects within fixed networks, using existing and emerging technologies. To a large extent this work is centered around adapting the 3GPP IMS architecture to the TISPAN/NGN environment. TISPAN is structured as a single technical committee, with core competencies, under which there are Working Groups and Project Teams.	<a href="http://www.etsi.org">http://www.etsi.org</a> , <a href="http://portal.etsi.org/tispan">http://portal.etsi.org/tispan</a>
TLS	Transport Layer Security	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and a client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).	<a href="http://www.whatis.com">http://www.whatis.com</a>
TMSI	Temporary Mobile Subscriber Identity	TMSI is a 4-octet (byte) unstructured temporary subscriber identity used in the GSM/GPRS/UMTS systems. Subsequent to initial successful location updating and after encryption has commenced the VLR/SGSN may (should) assign a TMSI to the MS. The TMSI is subsequently to be used as replacement for IMSI. The TMSI is assigned in encrypted form and only used in cleartext, and thus there is no externally apparent binding between the IMSI and the TMSI. In effect this provides a (weak) measure of location- and identity privacy for the mobile subscriber. Defined in 3GPP TS 23.003.	<a href="http://www.3gpp.org/ftp/Specs/html-info/23003.htm">http://www.3gpp.org/ftp/Specs/html-info/23003.htm</a>
ToR	The onion Router	ToR is an anonymity network technology.	<a href="http://tor.eff.org/">http://tor.eff.org/</a>
Trojan		A Trojan is a deceptive program that contains or installs a malicious program (malware) while masquerading as a legitimate application. The term is derived from the classical myth of the Trojan Horse.	
TS	Technical Specification		
TST	Tamper-resistant pseudonym tester		
TTP	Trusted Third Party	In cryptography, an entity which facilitates interactions between two parties who both trust the third party; they use this trust to secure their own interactions. TTPs are common in cryptographic protocols, for example, a certificate authority (CA).	
UE	User Equipment	A UE is a mobile phone (terminal unit, radio unit and smartcard (SIM and/or UICC/USIM)).	
UE	User Entity		
UICC		A physically secure device, an IC card (or 'smart card'), that can be inserted and removed from the terminal equipment. It may contain one or more applications. One of the applications may be a USIM. Defined in 3GPP specification series 31.	<a href="http://www.3gpp.org/ftp/Specs/html-info/31-series.htm">http://www.3gpp.org/ftp/Specs/html-info/31-series.htm</a>
UMTS	Universal Mobile Telecommunication System	The European member of the IMT 2000 family of 3G wireless standards. UMTS supports data rates of 144 kb/s for vehicular traffic, 384 kb/s for pedestrian traffic and up to 2 Mb/s in support of in-building services. The standardisation work began in 1991 by ETSI but was transferred in 1998 to 3GPP as a corporation between Japanese, Chinese, Korean and American organisations. It is based on the use of WCDMA technology and is currently deployed in many European countries. As of October 2006 there are more than 90 million subscribers worldwide. The first European service opened in 2003. In Japan NTT DoCoMo opened its 'pre-UMTS' service FOMA (Freedom Of Mobile multimedia Access) in 2000. The system operates in the 2.1 GHz band and is capable of carrying multimedia traffic.	<a href="http://www.3gpp.org/">http://www.3gpp.org/</a> , <a href="http://www.umts-forum.org">http://www.umts-forum.org</a>
URL	Uniform Resource Locater	A subset of Uniform Resource Identifiers (URI) that identify resources via a representation of their primary access mechanism (e.g. their network 'location'), rather than identifying the resource by name or by some other attribute(s) of that resource. Originally defined by IETF in RFC 1738, later merged with RFC 1808 to RFC 2396 on URN.	<a href="http://www.ietf.org">http://www.ietf.org</a>
USIM	Universal Subscriber Identity Module	An application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security. Defined in 3GPP specification series 31.	<a href="http://www.3gpp.org/ftp/Specs/html-info/31-series.htm">http://www.3gpp.org/ftp/Specs/html-info/31-series.htm</a>
UTRAN	UMTS Radio Access Network	Part of the 3G standard UMTS. The UTRAN consists of a set of Radio Network Sub-systems (RNS) connected to the Core Network through the Iu-Interface. An RNS consists of a Radio Network Controller (RNC) and a number of base stations called Node Bs. They provide the radio interface Uu towards the User Equipment (UE). Specified by 3GPP. An overall description is found in 3GPP TS 25.401.	<a href="http://www.3gpp.org/ftp/Specs/html-info/25401.htm">http://www.3gpp.org/ftp/Specs/html-info/25401.htm</a>
VLR	Visitors Location Register	VLR is a temporary database of the subscribers who have roamed into the particular area which it serves. Each Base Station in the network is served by exactly one VLR, hence a subscriber cannot be present in more than one VLR at a time. The data stored in the VLR has either been received from the HLR, or collected from the MS. In practice, for performance reasons, most vendors integrate the VLR directly to the V-MSC and, where this is not done, the VLR is very tightly linked with the MSC via a proprietary interface.	

Acronym /Term	Definition	Explanation	Web-resources
WEP	<b>Wired Equivalent Privacy</b>	An implementation of RC4. It is part of the IEEE 802.11 standard (ratified in September 1999) and is a scheme used to secure wireless networks (WiFi). WEP was designed to provide comparable confidentiality to a traditional wired network, hence the name. However, the WEP security protocol is completely broken and attacks will now succeed within a couple of minutes. A new standard, IEEE 802.11i, provides improved security feature. See also WPA/WPA2.	<a href="http://www.ieee802.org">www.ieee802.org</a> , <a href="http://www.wifialliance.org">http://www.wifialliance.org</a>
<b>Wi-Fi Alliance</b>		A non-profit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. Currently the Wi-Fi Alliance has 207 member companies from around the world, and over 1000 products have received Wi-Fi® certification since certification began in March 2000.	<a href="http://www.wifialliance.org">http://www.wifialliance.org</a>
<b>WiMAX</b>	<b>Worldwide Interoperability for Microwave Access</b>	A specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. Based on the IEEE 802.16 WMAN. Published on 8 April 2002, the standard defines the use of bandwidth between the licensed 10 GHz and 66 GHz and between the 2 GHz and 11 GHz (licensed and unlicensed) frequency ranges and defines a MAC layer that supports multiple physical layer specifications customized for the frequency band of use and their associated regulations. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 50 km to handle such services as VoIP, IP connectivity and TDM voice and data.	<a href="http://www.ieee802.org/16/">http://www.ieee802.org/16/</a> , <a href="http://www.wimaxforum.org/">http://www.wimaxforum.org/</a>
<b>WLAN</b>	<b>Wireless Local Area Network</b>	This is a generic term covering a multitude of technologies providing local area networking via a radio link. Examples of WLAN technologies include Wi-Fi (Wireless Fidelity), 802.11b and 802.11a, HiperLAN, Bluetooth and IrDA (Infrared Data Association). A WLAN access point (AP) usually has a range of 20-300 m. A WLAN may consist of several APs and may or may not be connected to Internet.	
<b>WPA</b>	<b>Wi-Fi Protected Access</b>	An improved version of WEP (Wired Equivalent Privacy). It is a system to secure wireless (Wi-Fi) networks, created to patch the security of WEP. As a successor, WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared.	<a href="http://www.ieee802.org">http://www.ieee802.org</a> , <a href="http://www.wifialliance.org">http://www.wifialliance.org</a>
<b>WPA2</b>	<b>Wi-Fi Protected Access 2</b>	An extension to WPA that includes the remaining elements of IEEE 802.11i.	<a href="http://www.ieee802.org">http://www.ieee802.org</a> , <a href="http://www.wifialliance.org">http://www.wifialliance.org</a>
<b>WSN</b>	<b>Wireless Sensor Networks</b>	A WSN is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants.	