



Mobility Task Force

Deliverable B

Glossary of technical terms for mobile/roaming/authentication/authorization

+

Glossary of non technical terms used by this group

Version 1.3.5

Editors: Roland Staring, Carsten Bormann <cabo@tzi.de>, Licia Florio licia@terena.nl

Contributions: Jardar Leira, Juergen Rauschenbach, Erik Dobbeltstijn, Sami Keski-Kasari, Tim Chown, Niels Pollem

Introduction

This document contains two lists. The first one is a [technical glossary](#) to define terms related to mobility, roaming, authentication and authorisation and was agreed at the time the task force was created, thus it is listed in the deliverable list. This list defines all technical terms used in the deliverables so far and will expand as necessary during the lifetime of the task force.

The second list is a [glossary of non-technical terms](#) and aims at defining the no-technical terms used in the deliverable in order to have a common understanding of the meaning to ensure consistency. The list is not complete yet and some terms could be better named. All the different terms pointed out the necessity of defining a policy.

1. Glossary of Technical Terms

| Terms | Description |
|----------------|--|
| 3DES | Triple DES or 3DES is three-pass DES (168 bit keys) |
| 3G | 3G is an ITU term for the third generation of mobile communications technology. 3G promises increased bandwidth, up to 384 kbit/s when a device is stationary or moving at pedestrian speed, 128 kbit/s in a car, and 2 Mbit/s in fixed applications. Usage of the term 3G encompasses a variety of wireless air interfaces such as GSM and other forms of TDMA as well as various forms of CDMA. |
| 802.11 | This was the first of the IEEE 802.11 standards for wireless networks operating on the 2.4GHz ISM band (Industrial, Scientific and Medical). It defines the wireless LAN MAC and the PHY layer. There are three non-compatible and different physical layers: FHSS, DSSS and Infrared (IR). The data rates for all are 1 and 2Mbps. The standard also defines WEP encryption. |
| 802.11a | 802.11 specifies a wireless access protocol operating in the 5GHz band using orthogonal frequency division multiplexing (OFDM). 802.11a supports data rates ranging from 6 to 54Mbps |
| 802.11b | 802.11 specifies a wireless access protocol operating in the 2.4GHz band using CCK (Complementary Code Keying), a modulation technique that makes efficient use of the radio spectrum. 802.11b supports data rates ranging from 1 to 11Mbps. |
| 802.11g | The charter of the 802.11g task group is to develop a higher speed extension (up to 54Mbps) to the 802.11b PHY, while operating in the 2.4GHz band. 802.11g will implement all mandatory elements of the IEEE 802.11b PHY standard. For example, an 802.11b user will be able to associate with an 802.11b access point and operate at data rates up to 11Mbps. |
| 802.11h | 802.11h extends 802.11a to address the requirements of the European regulatory bodies. It provides dynamic channel selection (DCS) and transmit power control (TPC) for devices operating in the 5GHz band (802.11a). In Europe, there's a strong potential for 802.11a interfering with satellite communications, which have "primary use" designations. Most countries authorize WLANs for "secondary use" only. |
| 802.11i | 802.11i is actively defining enhancements to the MAC Layer to increase security. to the existing 802.11 standard provides security only in the form of wired equivalent privacy (WEP), which specifies the use of relatively weak, static encryption keys without any form of key distribution management. This makes it possible for attackers to access and decipher WEP-encrypted data on your WLAN. 802.11i will incorporate 802.1X and stronger encryption techniques, such as AES (Advanced Encryption Standard). |
| 802.1X | 802.1X is a standard for port based authentication for access to LANs that was originally meant for use in fixed networks. It is a layer 2 solution between client and wireless access point or switch. |

| | |
|------------------------|--|
| AAA | Authentication, Authorisation and Accounting |
| Access List | A list kept by network elements to control access to or from the element for a number of services (e.g. to prevent packets with certain IP address from leaving a particular interface on the network element) |
| Accounting | The process of keeping track of a user's activity while accessing the network resources, often including the amount of time spent in the network, the services accessed while there and the amount of data transferred during the session. Accounting data is used for trend analysis, capacity planning, billing, auditing and cost allocation. |
| AES or Rijndael | Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen. This very algorithm was selected by US NIST as AES (advanced encryption standard). The cipher was designed with both hardware and software implementation in mind. It has variable block length and key length. BestCrypt implements Rijndael with 256-bit key and 128-bit block. |
| AP | Access Point - a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing heightened wireless security and for extending the physical range of service a wireless user has access to. |
| Authentication | In security, the verification of the identity of the person or a process |
| Authorisation | In security, the assignment of rights and capabilities to a specific person or process |
| Bluetooth | A short-range radio technology aimed at simplifying communications and data synchronization between devices. |
| CHAP | Challenge Handshake Authentication Protocol – A PPP authentication protocol. CHAP does not exchange the password in clear text, but uses a challenge handshake. |
| CCK | Complementary Code Keying – Modulation schema that allows for multi-channel operation in the 2.4 GHz, using the existing IEEE 802.11 DSSS channel structure scheme. |
| DES | Data Encryption Standard – Standard cryptographic algorithm developed by the US. DES encrypts one block in 16 rounds. DES uses 56-bit keys. |
| DHCP | Dynamic Host Configuration Protocol - a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network |
| DSSS | Direct Sequence Spread Spectrum - The radio signals stay on its pre-set encrypted channel, but this channel covers a wide range of frequencies. It has a wider frequency range to select a channel than FHSS but is less efficient and will also suffer badly from narrow band interference that covers its selected channel. |
| Diameter | The Diameter protocol is a proposed protocol which can be used for policy, AAA (Authentication, Authorization and Accounting) and resource control. The protocol has been setup to coexist with RADIUS |
| EAP | Extensible Authentication Protocol – a PPP authentication protocol that allows the plug-in of specific authentication protocols. EAP is also the protocol for the optional IEEE 802.1X wireless LAN security feature. An access point that |

| | |
|----------------------------|--|
| | supports 802.1X and EAP acts as the interface between a wireless client and an authentication server, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network. |
| FHSS | F requency H opping S pread S pectrum. The radio constantly hops between channels. More energy efficient than DSSS and survives narrow band interference better by hopping to the next channel. |
| Firewall | A firewall is a set of related network elements that protects the resources of a private network from outside attacks. A firewall examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. |
| Frequency | Number of cycles per seconds, measured in Hertz (e.g., of an alternating current) |
| Frequency re-use | The partitioning of an RF radiating area into cells so that each cell uses a frequency that is far enough away in a bordering segment using the same frequency to not cause interference problems. |
| GGSN | G ateway G PRS s upport n ode, a gateway that allows mobile cell phone users access to the public network (PDN) or specified private IP networks. |
| GPRS | G eneral P acket R adio S ervice – defined and standardised by ETSI/3GPP, an IP packet based service for global system for mobile communication (GSM) networks. |
| GSM | G lobal S ystem for M obile C ommunication. A 2G mobile wireless networking standard originally defined by ETSI, GSM is deployed worldwide, it uses TDMA technology and operates in the 900, 1800 and 1900 MHz radio bands. |
| GTP | G PRS T unnelling P rotocol that handles the flow of user packet data and signalling information between the SGSN and GGSN network. |
| GTP Tunnel handover | A specific instance of the use of GTP Handover, or handoff as it is called in North America, is the switching of an on-going call (more generally, communication relationship) to a different channel or cell |
| Handshake | Sequence of messages exchanged between two or more network devices to ensure transmission synchronisation. |
| Infrared | Electromagnetic waves whose frequency range is above that of microwaves but below the visible spectrum. Requires Line of Sight. |
| IPSec | I P S ecurity framework that provides data confidentiality, data integrity, data authentication between peers. IPSec provides security services at the IP layer and uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encrypted and authentication keys to be used by IPSec. |
| IPv4 | I P v ersion 4 of the internet protocol, employing a 32 bit IP-address |
| IPv6 | I P v ersion 6 of the internet protocol; the successor to IPv4, employing a 128 bit IP-address |
| LEAP | LEAP , or EAP-Cisco Wireless, an early attempt at an EAP plug-in for WLANs. Generally believed to be supplanted by PEAP and/or EAP-TTLS. |

| | |
|---|---|
| MAC address | Media Access Control address – also referred to as adapter address. A 48-bit interface address, often represented by a 12-digit alphanumeric string, separated by dashes into six sets of two digits, that uniquely identifies every hardware networking device on the planet. For example, 00-20-78-A3-49-5E is a valid MAC address. |
| Mobile IP | Mobile IP is a standard that allows users with mobile devices whose IP addresses are associated with one network to stay connected when moving to a network with a different IP address. |
| OFDM | Orthogonal Frequency Division Multiplexing . The data is split up among several closely spaced sub-carriers. It also has a shorter preamble than CCK. |
| PAP | Password Authentication Protocol – a username/password-based authentication protocol used in PPP |
| PEAP | Protected Extensible Authentication Protocol |
| PPP | Point-to-Point Protocol – provides router to router and host to network connections over synchronous and asynchronous point-to-point circuits. |
| Proxy | A Proxy Server sits in between a Client and the "real" Server that a Client is trying to use. Clients are sometimes configured to use a Proxy Server, usually an HTTP server. The clients makes all of its requests to the Proxy Server, which then makes requests to the "real" server and passes the result back to the Client. |
| RADIUS | Remote Authentication Dial In User Service - Transport protocol for AAA purposes |
| RAS | Remote Access Server . |
| Roaming: - WLAN Roaming - Wireless Roaming | Wireless Local Area Network Roaming refers to the ability to move from one administrative domain to another without interruption in service or loss in connectivity. Wireless Roaming - refers to the ability to gain as transparent as possible secure network access at a visited institution, to either (1) gain restricted access to the Internet or (2) be given a connection to the user's home institution network to authenticate and gain access to user resources or the internet via the home institution network thereafter. |
| SSID | Service Set Identifier . 1-32 octets that identifies the wireless network. The clients SSID must match the access points to associate. If the client sets an SSID of "Any" or _blank_ it will associate to the first active mode access point it finds regardless of its SSID. |
| TACACS | Terminal Access Controller Access Control System – Authentication protocol for remote access authentication and related services such as event logging. User passwords are administered centrally in a database than in individual routers. |
| TKIP | Temporal Key Integrity Protocol . An alternative to WEP that uses as 128-bit RC4 key for encryption. Hardware that encrypts WEP can be modified by software to encrypt TKIP. |
| TLS | Transport Layer Security |

| | |
|------------------------|--|
| TTLS | Tunneled Transport Layer Security |
| UMTS | Universal Mobile Telecommunications System - a third generation (3G) wireless standard widely embraced in Europe and other countries with GSM infrastructure. According to the GSM association, UMTS will offer a wide range of voice, data and multimedia services. Data rates will reach from 114 to 2000 kbit/s (or 2 Mbps) depending on whether the user is stationary or in motion. |
| UWB | Ultra Wide Band - a wireless communications technology that can currently transmit data at speeds between 40 to 60 megabits per second and eventually up to 1 gigabit per second. UWB transmits ultra-low power radio signals with very short electrical pulses, often in the picosecond (1/1000th of a nanosecond) range, across all frequencies at once. UWB receivers must translate these short bursts of noise into data by listening for a familiar pulse sequence sent by the transmitter. |
| VLAN | Virtual LAN - group of devices on one or more LANs configured using management software to a communicate as if attached to the same wire when in fact they are physically connected to different LAN segments. These logical connections are very flexible. |
| VPN | Virtual Private Network – Enables IP traffic to travel over a secure tunnel over a public TCP/IP network by encrypting all traffic from one network to another at the IP level. N.B.= Note that the definition of VPN in this deliverable is different from the one Cisco use. They regard a VPN as something that's protected against other customers but not against the operator, so it doesn't necessarily use encryption. I can see confusion coming out of this one, so it might be worth a note in the glossary: "Cisco's use of the term VPN does not require encryption" |
| Web based login | Access to the wireless network is granted at the border of the network where the session is intercepted. The user receives a web page where the credentials need to be entered to allow traffic to pass through. |
| WEP | Wired Equivalent Privacy - an optional security mechanism defined within the 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable (see also: 802.11i) N.B.= This definition is different from the one Cisco use. They regard a VPN as something that's protected against other customers but *not* against the operator, so it doesn't necessarily use encryption |
| WiFi | Wireless Fidelity - is meant to be used generically when referring to certain recent types of Wireless LAN standards created by IEEE 802.11. Any products tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers |
| Wireless | Equipment, service or technology for transporting data or information without wires but rather through air waves (frequencies) using radio or microwave technology |
| WLAN | Wireless Local-Area Network a type of local-area network that |

| | |
|------------|--|
| | uses high-frequency radio waves rather than wires to communicate between nodes. |
| WPA | Wi-Fi Protected Access. An IEEE 802.11i "snapshot" promoted by the Wi-Fi Alliance and their members. It is a replacement for the weak WEP protection and uses IEEE 802.1x a with TKIP encryption. |

2. Glossary of No-Technical Terms

| Terms | Similarly used terms (including those identified in current drafts) | Description |
|---|---|---|
| ACCESS CONTROL DEVICE | Access device Access point Base station Access controller | A device that enforces an access control policy, typically by letting packets pass only in the presence of certain conditions. Access control devices can also divert packets (e.g., to a login page) as long as the conditions for enabling access are not fulfilled |
| ADMINISTRATOR | Administrators, Network Administrators, University administrators | The person who is responsible for administering network devices, AAA servers and user access in general. |
| "CASG" - CONTROLLED ADDRESS SPACE FOR GATEWAYS or RELAY NETWORKS | Relay network, forwarding network, trusted network, proxy network, trusted network address space, controlled gateway address space. | A collection of network addresses that are being assigned to trusted VPN servers. The grouping of such network addresses into a (small number of) address spaces serves to 1) reduce the administrative overhead and 2) tackle the issue of VPN scalability. |
| DOCKING NETWORK | | A place where mobile devices can obtain access. Typically packets from docking networks have to transit access control devices to leave the docking network. Access to the docking network could be wireless or wired. |
| HOME INSTUTION (of a user) | Local institution, home network, home campus, home network, | An Institution where a user is registered at, and has established credentials with to gain access to a local account for network access. The user normally resides at this institution. |

| | | |
|---|--|---|
| INTERNATIONAL RADIUS PROXY SERVER / | INTERNATIONAL ROAMING ROOT SERVER | A RADIUS Server that acts as a proxy server to forward requests from one NREN to another NREN. |
| INSTITUTIONAL RADIUS PROXY SERVER | | An institution RADIUS proxy server to communicate between the institutions existing RADIUS server and the national radius proxy server so that roaming related requests and translating the RADIUS roaming requests to LDAP for example, could be done in this network element. It could also limit which users are allowed to roam and what kind of access is allowed to their AAA server. |
| LOCAL USER (with respect to a network) | User, Person, workstation users, students, employees, end-user, per institution user, researchers, | A user of a network of her/his home institution. |
| MOBILE DEVICE | Fat clients, Thin clients, notebooks, laptops, PDAs, mobile devices, platforms, user terminal, | A device that is intended to attach to networks at more than one point to establish a network connection. A device that can wireless allow seamless mobility on behalf of a user, independently of the physical location of the device |
| NATIONAL RADIUS PROXY SERVER | NATIONAL ROAMING ROOT SERVER | A RADIUS Server that acts as a proxy server to forward requests from one institution or region to another within an NREN. |
| NREN | | National Research and Education Network |
| ROAMING | | See the definition of Roaming in the glossary of Technical Terms |
| SERVER: | Top level server, subordinate server, | A computer that provides a service. In this context often an AAA server. |
| VISITED INSTITUTION: | Visitor campus, guest campus, remote institution | An institution that a user is "visiting" and is defined at that institution as a visitor user / guest wants network access and is in fact registered in their home institution. |

Deliverable B: Glossary of technical terms for mobile/roaming/authentication/authorisation + no-technical terms used by the task force

| | | |
|-----------------------|--|--|
| VISITOR (USER) | User, Person, workstation users, students, guest, employees, end-user, per institution user, researchers, roaming users, unauthorised hosts, | A visitor user is a user that connects to a visited institution. |
|-----------------------|--|--|