

04.01.07

# Milestone MJ5.1.5: JRA5 Glossary of Terms - Second Edition - update of DJ5.1.1



## Milestone MJ5.1.5

Contractual Date:	31/12/2006
Actual Date:	04/01/07
Contract Number:	511082
Instrument type:	Integrated Infrastructure Initiative (I3)
Activity:	JRA5
Work Item:	I (One)
Nature of Deliverable:	O (Other)
Dissemination Level	PU (Public)
Lead Partner	SURFnet
Document Code	GN2-07-004

**Authors:** Manuela Stanica (DFN), Torbjörn Wiberg (Umeå universitet), Klaas Wierenga (SURFnet), Stefan Winter (RESTENA), Juergen Rauschenbach (DFN)

## Abstract

This document provides a glossary of terms to be used within the realm of Joint Research Activity 5 – Roaming and Authorisation

# Table of Contents

0	Executive Summary	iii
1	Introduction	1
2	Glossary	1

## 0 **Executive Summary**

The document was written to provide a common terminology for the GN2 Joint Research Activity 5, covering Roaming, Authentication and Authorisation areas. The glossary will be helpful for the internal work of the project activity, but should also enable non-specialists to become more familiar with the terminology used.

Project:	GN2
Milestone Number:	MJ5.1.5
Date of Issue:	04/01/07
EC Contract No.:	511082
Document Code:	GN2-07-004

# 1 Introduction

This document was written to provide a common terminology for the GN2 Joint Research Activity 5 covering Roaming, Authentication and Authorisation areas. The terms, as defined here, will be used in discussions and in the planned deliverables. It is expected that, as new terms emerge and become of relevance during the project work, they will be added in subsequent versions. The document should be seen as a living document with extensions and improvements provided at different project stages (cross check when writing new deliverables). The most recent version will be kept at the JRA5 home page.

The terms marked with ‘\*’ are specific to the JRA5 project (introduced or redefined in JRA5). The relevant standards body is sometimes indicated by ‘StB’ for instance “(StB IETF)”.

Project:	GN2
Milestone Number:	MJ5.1.5
Date of Issue:	04/01/07
EC Contract No.:	511082
Document Code:	GN2-07-004

## 2 Glossary

Term	Description
<b>3DES</b>	Triple <b>DES</b> or 3DES is three-pass Data Encryption Standard (168 bit key encryption)
<b>3G</b>	<b>3G</b> 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 relates to the Universal Mobile Telecommunications System (UMTS) and associated technologies.
<b>3GPP</b>	A 3G Partnership Project run by ETSI to develop a single standard for third generation mobile wireless systems, network architecture and protocols.
<b>802.11</b>	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 MAC (Media Access Control) and PHY (PHYSical) layers of the wireless LAN. 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. (St. IEEE)
<b>802.11a</b>	<b>802.11a</b> 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. (StB IEEE)
<b>802.11b</b>	<b>802.11b</b> 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. (StB IEEE)
<b>802.11g</b>	<b>802.11g</b> specifies a wireless access protocol operating in the 2.4GHz band using orthogonal frequency division multiplexing (OFDM). 802.11g supports data rates ranging from 6 to 54Mbps 802.11g provides backward compatibility with 802.11b. (StB IEEE)
<b>802.11h</b>	<b>802.11h</b> 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 Wireless LANs for "secondary use" only. (StB IEEE)
<b>802.11i</b>	<b>802.11i</b> defines enhancements to the 802.11 MAC Layer to increase security. 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 a WLAN. 802.11i will incorporate 802.1X and stronger encryption techniques, such as AES (Advanced Encryption Standard). (StB IEEE)

Term	Description
<b>802.16</b>	The <b>802.16</b> standard set, the "Air Interface for Fixed Broadband Wireless Access Systems," is also known as the IEEE WirelessMAN air interface. It focuses on the efficient use of bandwidth between 10 and 66 GHz (the 2 to 11 GHz is covered by the 802.16a standard published in 2003) and defines a medium access control (MAC) layer that supports multiple physical layer specifications customised for the frequency band of use. Max bandwidth is 280 Mbps per base station. (StB IEEE)
<b>802.1Q</b>	IEEE specification of Virtual LANs. This standard enables multiple independent logical networks within one physical network switching device (Access Point or switch).
<b>802.1X</b>	<b>802.1X</b> is a standard for port based authentication for access to (W)LANs, originally intended for use in fixed networks. It is a layer 2 solution between client and wireless access point or switch. (StB IEEE)
<b>A-SELECT</b>	An authentication solution developed by SURFnet, providing single sign on for web applications. <b>A-SELECT</b> can offer the use of multiple authentication mechanisms and uses SAML for communication.
<b>AA</b>	Authentication and Authorisation
<b>AA Middleware</b>	Infrastructural Network Services to carry out Authentication and Authorisation. (New)
<b>AAA</b>	<b>A</b> uthentication, <b>A</b> uthorisation and <b>A</b> ccounting
<b>AAI</b>	Authentication and Authorisation Infrastructure
<b>AAI Federation</b>	See Federated AAI.
<b>AAu</b>	Attribute Authority
<b>Acceptable Use Policy (AUP)</b>	A policy that users of the network must adhere to.
<b>Access Control</b>	The process of controlling access to a resource.
<b>Access Control Device</b>	A device that enforces an access control policy, typically by letting packets pass only under certain conditions. Access control devices can also divert packets (e.g., to a login page) when conditions for granting access are not fulfilled.
<b>Access Control List (ACL)</b>	An <b>Access Control List</b> is a means of determining the appropriate access rights to a given object depending on certain aspects of the process that is making the request (e.g. to prevent packets with a certain IP address from leaving a particular interface on the network element).
<b>Access Point (AP)</b>	<b>Access Point</b> - a hardware device or an application that acts as a communication hub for users of wireless LAN devices that wish to be granted access to a wired LAN / Internet connection. An AP can simply act as a communication point to an Authentication Server or can provide heightened wireless security itself by restricting unauthenticated access to specific protocols for example (e.g. EAP access for 802.1X authentication). An AP primarily provides the connectivity.
<b>Accounting</b>	The process of collecting information about a user's activity on the network, in order to make it possible to hold him accountable for his actions. It may collect information about the amount of time spent on the network, the services accessed while there and the amount of data transferred during the session. The collected data may be used for trend analysis, capacity planning, billing, auditing and cost allocation.
<b>ACL</b>	See <b>Access Control List</b> .

Term	Description
<b>AES or Rijndael</b>	Rijndael is a block cipher, designed by Joan Daemen and Vincent Rijmen. This algorithm was selected by US NIST as AES ( <b>A</b> dvanced <b>E</b> ncryption <b>S</b> tandard). The cipher was designed for both hardware and software implementations. It has variable block length and key length. BestCrypt implements Rijndael with 256-bit key and 128-bit block. (StB NIST)
<b>AP</b>	See <b>Access Point</b> .
<b>AR</b>	Attribute Requester
<b>ARP</b>	<b>A</b> ddress <b>R</b> esolution <b>P</b> rotocol – the method for finding a host’s hardware address when only its network layer address is known. Due to the overwhelming prevalence of IPv4 and Ethernet, ARP is primarily used to translate IP addresses to Ethernet MAC addresses. It is also used for IP over other LAN technologies, such as Token Ring, FDDI, or IEEE 802.11, and for IP over ATM.
<b>AS</b>	Authentication Server
<b>Assertion</b>	A positive statement or declaration (of a successful Authentication or approved Authority). (Merriam-Webster)
<b>Athens</b>	A UK academic community solution for authorising the access of staff and students to online content.
<b>AUP</b>	See <b>Acceptable Use Policy</b> .
<b>Authentication (AuthN)</b>	The process of verifying the identity of an entity, either in person or electronically, where credentials are requested and checked to verify or disprove an entity's claimed identity.
<b>Authentication and Authorisation Infrastructure (AAI)</b>	An infrastructure that provides Authentication and Authorisation Services. The minimum service components include Identity and Privilege Management with respect to users and resources.
<b>Authentication Assertion*</b>	A statement conveying information about a successful Authentication of an Electronic Identity.
<b>Authentication Mechanism*</b>	A mechanism that receives a user’s credentials (such as username and password) of a claimed Electronic Identity and processes it to verify or disprove the claimed identity
<b>Authentication Service</b>	An Infrastructural Network Service that authenticates registered Electronic Identities and provides Authentication Assertions.
<b>Authentication Service Provider</b>	A physical entity in an AAI that provides an Authentication Service.
<b>Authentication Strength</b>	The level of assurance any client can place in an Authentication Assertion it receives.
<b>Authenticator</b>	piece of network equipment in the same LAN as the supplicant that forwards authentication information between the supplicant and an AS
<b>AuthN</b>	See Authentication.
<b>Authorisation (AuthZ)*</b>	The assignment of rights and capabilities granted to a specific Principal (such as a person). Normally Authorisation takes place when a user has been authenticated. Given an Authentication Assertion for an Electronic Identity for the requesting Principal, Authorisation is the process of deciding if a request to perform an action on a resource shall be granted or not. N.B.: The abbreviation AuthZ stems from the US-English spelling of Authorisation: Authorization
<b>Authorisation Service Provider</b>	An entity in an AAI that provides an Authorisation Service.

Term	Description
<b>Authorisation Service (AuthZS)*</b>	An Infrastructural Network Service that serves applications and content providers with Authorisation. The service replies with an Authorisation Assertion or a denial.
<b>AuthZ*</b>	See Authorisation
<b>AV-Pairs</b>	Attribute-Value pairs; information elements within RADIUS packets
<b>Bluetooth</b>	A short-range radio technology typically operating in the personal area network space. Tends to be aimed at simplifying communications and data synchronisation between devices.
<b>Bridge-CA</b>	A technology that joins Public Key Infrastructures (PKI) by creating trust links between them. Since different PKIs may have different architectures, security policies, and cryptographic suites, Bridge CAs must implement flexible mechanisms to link these PKIs.
<b>BE*</b>	Bridging Element (includes LFA and LA)
<b>Bridging Element*</b>	A software component in charge of mapping the eduGAIN protocols and profiles to those of the participating federations. Although the BE may be a centralised component in the local federation, it is however expected that federation software will be adapted to become eduGAIN aware by implementing a BE, thus enabling direct communication between identity and service providers belonging to different local federations.
<b>BVI</b>	<b>Bridge Virtual Interface</b> – a virtual interface within the campus switch router that acts like a normal routed interface. A BVI does not support bridging, but it actually represents the corresponding bridge group to routed interfaces within the switch router. The interface number is the link between the BVI and the bridge group.
<b>CA</b>	See <b>Certificate Authority</b> .
<b>CASG</b>	See <b>Controlled Address Space for Gateways</b>
<b>CCK</b>	<b>Complementary Code Keying</b> – Modulation schema that allows for multi-channel operation in the 2.4 GHz, using the existing IEEE 802.11 DSSS channel structure scheme.
<b>ccTLD</b>	<b>country-code Top Level Domain</b>
<b>CDMA</b>	<b>CDMA</b> can either refer to the general Code Division Multiple Access spread spectrum multiplexing technique, or the specific CDMA family of standards developed by Qualcomm, including cdmaOne (or IS-95) and CDMA2000 (or IS-2000). CDMA is the use of any form of spread spectrum by multiple transmitters to send to the same receiver on the same frequency channel at the same time without harmful interference.  Not to be confused with CDAM/CA (Collision Detection Multiple Access/Collision Avoidance) used in Ethernet!
<b>Certificate Authority (CA)</b>	An entity that is trusted to associate an entity identity with a public key. The CA links the key to the identity by issuing a certificate for the Subject containing the identity and the public key as data (signed with the private key of the CA). The validity of a certificate may be checked with the CA.
<b>CFI</b>	<b>Canonical Format Indicator</b>
<b>Credentials</b>	Evidence or testimonials concerning one's right to credit, confidence, or authority.
<b>CRL</b>	<b>Certificate Revocation List</b> – a list of certificates that have been revoked by the Certification Authority. The CRL can be compared to a blacklist containing the certificates which are no longer valid.

Term	Description
<b>CHAP</b>	<b>Challenge Handshake Authentication Protocol</b> – A PPP authentication protocol. CHAP does not exchange the password in clear text, but uses a challenge handshake.
<b>Confederation</b>	A co-operation of federations through means of legally binding arrangements.
<b>Controlled Address Space for Gateways (CASG)</b>	A collection of network addresses that are being assigned to trusted Virtual Private Networks (VPN) servers. The grouping of such network addresses into a (small number of) address spaces serves 1) to reduce the administrative overhead and 2) to tackle the issue of VPN scalability.
<b>DES</b>	<b>Data Encryption Standard</b> – Standard cryptographic algorithm developed by USA. DES uses 56-bit keys.
<b>DHCP</b>	<b>Dynamic Host Configuration Protocol</b> - a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device may get a different IP address every time it connects to the network.
<b>Diameter</b>	The Diameter base protocol is intended to provide an Authentication, Authorisation and Accounting (AAA) framework for applications such as network access or IP mobility. It evolved from the popular RADIUS protocol adding new features, such as the ability to ask for additional logon information beyond the basic authentication. Diameter supports user roaming. (StB IETF)
<b>DNS</b>	The Internet <b>Domain Name Service</b> is a distributed application for the provision of a mapping between names and IP addresses and vice versa.
<b>DNSsec</b>	An extension to the Domain Name Service that offers enhanced security features for the exchange of DNS records. (StB IETF)
<b>DNSRoam</b>	<b>Domain Name System Roaming</b> , name of the dynamic server discovery implementation in Radiator
<b>Docking Network</b>	A place where mobile devices can obtain network 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.
<b>DSSS</b>	<b>Direct Sequence Spread Spectrum</b> - The radio signals stay on their pre-set 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.
<b>EAP</b>	<b>Extensible Authentication Protocol</b> – a PPP authentication protocol that allows the plug-in of specific authentication mechanisms. EAP is a data link layer 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 Service, such as a Remote Authentication Dial-In User Service (RADIUS) server, to which the access point communicates over the wired network. There are a number of EAP types available today, examples are EAP-TTLS, EAP-TLS, PEAP and EAP-SIM. (StB IETF)
<b>EAP-FAST</b>	<b>Flexible Authentication via Secure Tunnelling</b> , a new IEEE 802.1X authentication type EAP-FAST offers flexible, easy deployment and management, supports several user and password database types, supports server-initiated password expiration and change, and does not require digital certificates.
<b>EAP-GTC</b>	<b>EAP with Generic Token Card</b> payload

Term	Description
<b>EAP-MD5</b>	<b>EAP</b> with <b>Message Digest Nr. 5</b> payload This authentication method is unsuited for Wireless LAN scenarios as it does not provide mutual authentication of both user and network.
<b>EAP-OTP</b>	<b>EAP</b> with <b>One Time Password</b> payload
<b>EAP-SIM</b>	<b>EAP</b> with <b>Subscriber Identification Module</b> payload
<b>EAP-TLS</b>	<b>Transport Layer Security</b> (EAP Protocol), successor of SSL (StB IETF)
<b>EAP-TTLS</b>	<b>Tunnelled Transport Layer Security</b> (EAP protocol) (StB IETF)
<b>EAPoL</b>	<b>EAP over LAN</b>
<b>EDGE</b>	<b>Enhanced Data Rates for Global (or GSM) Evolution</b> , GPRS compatible, typically a connection that bonds 2-3 x GPRS connections together for a higher speed data connection.
<b>eduGAIN*</b>	AAI confederation created in GÉANT2-JRA5 in the purpose of interconnecting a set of national and community-wide AAI federations ( name composed of the “edu” prefix – commonly associated to academic and research environments in the Internet worldwide – and the GAIN acronym, standing for <i>GÉANT Authorisation Infrastructure</i> ).
<b>eduPerson</b>	An auxiliary object class (in LDAP terminology) for campus directories, designed to facilitate communication among higher education institutions. It consists of a set of data elements or attributes about individuals within higher education, along with recommendations on the syntax and semantics of the data that may be assigned to those attributes. (StB Internet2)
<b>eduroam*</b>	Roaming confederation aiming to provide mutual roaming network access to its members – European eduroam federations, their institutions and the end users.
<b>eduroam-ng*</b>	eduroam- <b>next generation</b> – the second iteration of eduroam, using a mixture of RADIUS and RadSec as authentication protocol
<b>eID</b>	See <b>electronic IDentity</b> .
<b>eIRG</b>	The mission of the <b>eInfrastructure Reflection Group</b> , whose members are appointed by the governments of the EU member states, is to identify the fundamental fabric, services and resources needed to enable pan-European e-Science.
<b>Electronic Identity (eID)*</b>	The information about a registered entity that the Identity Provider has chosen to represent the Identity of that entity. The eID includes a name or an identifier for the entity that is unique within the domain of the Identity Provider.
<b>ETSI</b>	<b>European Telecommunications Standards Institute</b> , a standardisation body for telecommunications standards and conformance test suites
<b>Federated AAI*</b>	An AAI that supports multiple Identity and Privilege Providers, trusted by the members of the federation.
<b>Federation</b>	A co-operation of organizations through legally binding arrangements, in the purpose of enhancing collaborations and transactions.
<b>FEIDE</b>	<b>Federated Electronic IDentity for Education</b> : An Authentication/Authorisation solution developed by UNINETT (Norway)
<b>FHSS</b>	<b>Frequency Hopping Spread Spectrum</b> . Radio technology in which the radio constantly hops between a range of channels. More energy-efficient than DSSS and survives narrow band interference better by hopping to the next channel.

Term	Description
<b>Firewall</b>	A computer that (a) acts as an interface between two networks (e.g., the Internet and an private network, and (b) regulates traffic between those networks for the purpose of protecting the internal network from electronic attacks originating from the external network and/or vice versa.
<b>FPP*</b>	<b>Federation Peering Point</b> – a centralised component in a local federation, currently in charge of publishing the metadata for the entire federation at the Metadata Server (MDS).
<b>Frequency re-use</b>	The partitioning of a Radio Frequency radiating area into cells so that each cell uses a frequency that is far enough away from a bordering cell using the same frequency so as not to cause interference problems.
<b>FQDN</b>	<b>Fully Qualified Domain Name</b> – an unambiguous domain name that specifies the node's position in the DNS tree hierarchy absolutely. To distinguish an FQDN from a regular domain name, a trailing period is added. Ex: somehost.example.com. An FQDN differs from a regular domain name by its absoluteness; a suffix will not be added.
<b>GGSN</b>	<b>Gateway GPRS Support Node</b> , a gateway that allows mobile cell phone users access to the Internet or specified private IP networks.
<b>GPRS</b>	<b>General Packet Radio Service</b> – an IP packet based service for a global system for mobile communication (GSM) networks. (StB ETSI/3GPP)
<b>GPS</b>	<b>Global Positioning System</b> . A US solution that uses satellite technology to determine a user's position on the earth for navigation or location based services. A European based system is under preparation.
<b>GRID</b>	The term Grid was coined in the mid 1990s to denote a proposed distributed computing infrastructure concept for advanced science and engineering. Actual implementations are providing support for the co-ordinated resource sharing and problem solving in multi-institutional Virtual Organisations (access to computers, software, data and other resources).
<b>GRE</b>	<b>Generic Routing Encapsulation</b> – a tunnelling protocol designed for encapsulation of arbitrary kinds of network layer packets inside arbitrary kinds of network layer packets.
<b>GSM</b>	<b>Global System for Mobile Communication</b> . A 2G mobile wireless networking standard GSM is deployed worldwide, it uses TDMA technology and operates in the 900, 1800 and 1900 MHz radio bands. (StB ETSI)
<b>gTLD</b>	<b>generic Top Level Domain</b>
<b>GTP</b>	<b>GPRS Tunnelling Protocol</b> that handles the flow of user packet data and signalling information between the SGSN and GGSN networks.
<b>GTP Tunnel</b>	A specific instance of the use of GTP.
<b>Guest User*</b>	A visiting user who expects to be able to use his/her credentials that are registered with his/her Home Institution authentication server in order to be granted access to resources at the visited network.
<b>GUI</b>	<b>Graphical User Interface</b> – a particular case of user interface for interacting with a computer which employs graphical images and widgets in addition to text to represent the information and actions to the user. Usually the actions are performed through direct manipulation of the graphical elements.
<b>Handover</b>	<b>Handover</b> , 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.

Term	Description
<b>Handshake</b>	Sequence of messages exchanged between two or more network devices to ensure transmission synchronisation.
<b>Harmonised Electronic Identity*</b>	A common user electronic identity (eID) model (eg. common choice of attributes) to be used by the Home Institutions participating in a Confederation Service, in order to enhance exchanges across different federations.
<b>H-BE*</b>	<b>Home Bridging Element</b>
<b>HI*</b>	see Home Institution
<b>HLS*</b>	see MDS
<b>HO*</b>	<b>Home Organisation</b>
<b>Home Institution* (of a user)</b>	The institution where the eID of the user is registered, and has established credentials that give the user access to local resources such as network access. The user normally resides at this institution.
<b>HTTP</b>	<b>Hyper Text Transfer Protocol</b>
<b>IANA</b>	<b>Internet Assigned Numbers Authority</b> – an organization broadly responsible for the allocation of globally-unique names and numbers that are used in Internet protocols that are published as RFC documents.
<b>Identity</b>	The essence of an entity and often described by its characteristics. ( Liberty Alliance)
<b>Identity Federation*</b>	A Federated AAI containing multiple Identity Providers, trusted by the members of the federation.
<b>Identity Management (IdM)</b>	The process of creating, maintaining, asserting and destroying Electronic Identities. Identity Management is managed by an Identity Provider.
<b>Identity Provider*</b>	An entity in an AAI that performs Identity Management.
<b>ID-WSF</b>	<b>Identity Web Services Federation</b> – a Liberty Alliance Project providing the framework for building interoperable identity-based Web Services.
<b>IDN</b>	<b>Internationalised Domain Name</b>
<b>IEEE</b>	Institute of <b>E</b> lectrical and <b>E</b> lectronics <b>E</b> ngineers, Inc., a non-profit, technical professional association
<b>IEEE 802.1Q</b>	see 802.1Q
<b>IEEE 802.1X</b>	see 802.1X
<b>IETF</b>	<b>Internet Engineering Task Force</b> - A standardisation body for Internet standards.
<b>IMAP</b>	<b>Internet Message Access Protocol</b> (commonly known as IMAP or IMAP4, and previously called Internet Mail Access Protocol) – an application layer Internet protocol that allows a local client to access e-mail on a remote server.
<b>IMAPS</b>	<b>Internet Message Access Protocol Secured</b> – an extension of the Internet Message Access Protocol (IMAP) to include encrypting through SSL/TLS.
<b>IMS</b>	The <b>Internet Multimedia Subsystem</b> provides a platform for information and communication services based on an all-IP network.

Term	Description
<b>Infrastructural Network Service*</b>	An Infrastructural Network Service, such as an Authentication or Authorisation Service, serves applications and content providers with common functionality that have been externalised from applications for efficiency and quality reasons. Infrastructural Network Services belong to a type of software called Middleware.
<b>Institutional RADIUS Proxy Server*</b>	An institutional RADIUS server that, if the guest user's Home Institution belongs to the same Identity Federation as the local institution, acts as a proxy server to forward the user's authentication request via the National RADIUS Proxy Server to the Authentication Service of the user's Home Institution. A successful authentication does not automatically authorize the user to roam and the RADIUS Server may pose an Authorisation query to an Authorisation Service or may itself perform an authorisation of the authenticated guest user.
<b>International RADIUS Proxy Server*</b>	A RADIUS Server that acts as a proxy server to forward authentication requests between National RADIUS Proxy Servers. See Institutional RADIUS Proxy Server for further details. (New)
<b>Internet Key Exchange (IKE)</b>	Internet <b>K</b> ey Exchange is a negotiation and key exchange protocol. (StB IETF)
<b>IPSec</b>	<b>IP Security</b> is a framework that provides data confidentiality, data integrity and data authentication between peers. IPSec provides security services at the IP layer and uses IKE (Internet Key Exchange) 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. (StB IETF)
<b>IPv4</b>	<b>IP version 4</b> of the internet protocol, employing a 32 bit IP-address. (StB IETF)
<b>IPv6</b>	<b>IP version 6</b> of the internet protocol; the successor to IPv4, employing a 128 bit IP-address. (StB IETF)
<b>JRA</b>	An EC term in FP6 for <b>J</b> oint <b>R</b> esearch <b>A</b> ctivity
<b>LA</b>	<b>L</b> ocal <b>A</b> daptor
<b>Layer2</b>	The OSI model: Layer 2 is the data link layer
<b>Layer3</b>	The OSI model: Layer 3 is the network layer
<b>LDAP</b>	<b>L</b> ightweight <b>D</b> irectory <b>A</b> ccess <b>P</b> rotocol, a directory service
<b>LEAP</b>	<b>L</b> ightweight <b>E</b> xtensible <b>A</b> uthentication <b>P</b> rotocol, 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.
<b>LFA</b>	Local Federation Adaptor (formerly known as LFC, Local Federation Connector)
<b>LFC</b>	See LFA
<b>LoA</b>	<b>L</b> evel of <b>A</b> ssurance - describes the degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity.
<b>Local User (network)*</b>	A user of a network of her/his Home Institution.

Term	Description
<b>MAC address</b>	<b>Media Access Control</b> address – also referred to as adapter or hardware address. A 48-bit or 64-bit interface address, often represented by a 12-digit (für 48-bit) or 16-digit (for 64-bit addresses) alphanumeric string, separated by dashes or colons into six (for 48-bit) or eight (for 64-bit) sets of two digits, that identifies every networking hardware device. For example, 00-20-78-A3-49-5E is a valid MAC address. Since network adapters exist that can be configured to change their MAC address to an arbitrary value, the identification provided by the MAC address cannot be considered globally unique and un-forgable.
<b>MDS*</b>	<b>Meta Data Service</b> (formerly known as HLS – Home Location Service) – provides centralised storage of metadata for eduGAIN and dynamic distribution upon request from the Bridging Elements
<b>Middleware</b>	The term has different meanings in different contexts but normally denotes specialised, rather high-level software that sits between applications or between the application layer and lower layers in the OSI reference model.
<b>MIPv6</b>	See <b>Mobile IPv6</b>
<b>Mobile Device</b>	A device that is intended to attach to networks at more than one physical location.
<b>Mobile IP</b>	<b>Mobile IP</b> is a standard that allows users with mobile devices to stay connected while moving to a network with a different IP address space.
<b>Mobile IPv6</b>	<b>Mobile IPv6</b> is an mobile IP protocol based on IPv6. It provides better and more effective support for mobile nodes (no triangular routing) then mobile IP(v4). (StB IETF)
<b>MPPE</b>	<b>Microsoft Point-to-Point Encryption</b> – a protocol for encrypting data across Point-to-Point Protocol and Virtual Private Network links.
<b>MS-IAS</b>	<b>Microsoft Internet Authentication Service</b> – the Microsoft Implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy.
<b>MS-CHAP</b>	<b>Microsoft Challenge/Handshake Authentication Protocol</b>
<b>NAPTR</b>	<b>Naming Authority PoinTeR</b> , a DNS resource record
<b>NAS</b>	<b>Network Access Server</b>
<b>NAT</b>	<b>Network Address Translation</b> – an Internet standard that enables a local-area network (LAN) to use one set of IP addresses for internal traffic and a second set of addresses for external traffic.
<b>National RADIUS Proxy Server*</b>	A RADIUS Server that acts as a proxy server to forward authentication requests to the user's home institution either via another Institutional (or Regional) RADIUS Proxy Server within an NREN or via the International RADIUS Proxy Server.
<b>.NET</b>	Microsoft .NET is an umbrella term that applies to a collection of products and technologies from Microsoft. Most have in common a dependence on the Microsoft .NET Framework, a component of the Windows operating system.
<b>NIST</b>	<b>National Institute for Standards and Technology</b> is an 1901 founded agency and USA's first federal physical science research lab.
<b>NMI</b>	<b>National Middleware Initiative</b> in USA, see also <a href="http://www.nsf-middleware.org/">http://www.nsf-middleware.org/</a>
<b>NREN</b>	<b>National Research and Education Network</b>
<b>OFDM</b>	<b>Orthogonal Frequency Division Multiplexing</b> . The data is split up among several closely spaced sub-carriers. It also has a shorter preamble than CCK (Complementary Code Keying).
<b>OID</b>	Object Identifier

Term	Description
<b>OpenSAML</b>	OpenSAML ( <a href="http://www.opensaml.org">http://www.opensaml.org</a> .) is a set of open-source libraries in Java and C++ which can be used to build, transport, and parse SAML messages. OpenSAML lets an application use SAML messages or SAML application profiles to express and carry security information between software components and systems.  OpenSAML has been produced by Internet2 members as part of their work on the Shibboleth project.
<b>PAP</b>	<b>P</b> assword <b>A</b> uthentication <b>P</b> rotocol – a username/password-based authentication protocol used in PPP, developed by Cisco and Microsoft
<b>PAPI</b>	Originally <b>P</b> oint of <b>A</b> ccess to <b>P</b> roviders of <b>I</b> nformation (not used today): An Authentication/Authorisation solution that has been developed by RedIRIS (Spain)
<b>PEAP</b>	<b>P</b> rotected <b>E</b> xtensible <b>A</b> uthentication <b>P</b> rotocol (EAP-Protocol)
<b>PERMIS</b>	<b>P</b> rivil <b>E</b> ge and <b>R</b> ole <b>M</b> anagement <b>I</b> nfrast <b>R</b> ucture <b>S</b> tandards <b>V</b> alidation: An Authorisation Policy engine that has been developed by the University of Salford.
<b>PFX</b>	<b>P</b> ersonal in <b>F</b> ormation e <b>X</b> change – a common file extension for X.509 certificates. A .pfx File may contain certificate(s) (public) and private keys (password protected).
<b>PKI</b>	See <b>P</b> ublic <b>K</b> ey <b>I</b> nfrast <b>R</b> ucture
<b>Policy CA</b>	The Root CA in a PKI where the CAs have a common Certificate Policy. (SwUPKI)
<b>POP</b>	<b>P</b> ost <b>O</b> ffice <b>P</b> rotocol – an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection.
<b>POP3S</b>	<b>P</b> ost <b>O</b> ffice <b>P</b> rotocol version <b>3</b> <b>S</b> ecured – an extension of the POP version 3 (POP3) protocol to include encryption via SSL/TLS.
<b>PPP</b>	<b>P</b> oint-to- <b>P</b> oint <b>P</b> rotocol – provides router-to-router and host-to-network connections over synchronous and asynchronous point-to-point circuits.
<b>PPTP</b>	<b>P</b> oint-to- <b>P</b> oint <b>T</b> unneling <b>P</b> rotocol – a method for implementing virtual private networks (VPN); it works by sending a regular PPP session to the peer with the Generic Routing Encapsulation (GRE) protocol.
<b>Principal</b>	An entity that belongs to the organisation and is capable of making decisions, and for which authenticated actions are done on its behalf. A Principal may acquire an eID.
<b>Private Key</b>	see Public Key
<b>Privilege Management</b>	The process of creating, maintaining and releasing information concerning the privileges and responsibilities a Principal has in an organisation.
<b>Privilege Provider</b>	An entity in an AAI that performs Privilege Management, and whence indirectly assigns authorities.
<b>Provisioning*</b>	In the context of roaming and AAI: The work done to provide the AAI and the applications with the identity and privilege information about principals and resources needed to perform authentication and Authorisation.
<b>Proxy*</b>	A Proxy is an agent that sits between a Client and a Server. Clients are sometimes configured to use a Proxy, usually when accessing an HTTP server. The Client makes all of its requests to the Proxy Server, which then makes requests to the HTTP server and passes the result back to the Client. In this context also RADIUS servers that forward requests and responses on behalf of a Client or another RADIUS server is a Proxy.

Term	Description
<b>Public Key, Private Key</b>	<p>A <b>Public Key</b> encryption system that uses two keys - a Public Key that is known to everyone and a Private or secret Key that is known only to the Principal associated with the key.</p> <p>The keys make up a pair where what is encrypted by one can be decrypted by the other and vice versa, and knowing the Public Key it is virtually impossible to deduce the Private Key. Thus the Public Key can be used to encrypt a message to be sent and only the Private Key kept by the receiver can decrypt it. The Private Key of the sender can be used to digitally sign a message and the sender's Public Key can be used by the recipient to verify the authenticity of the message and the identity of the sender.</p>
<b>Public Key Infrastructure (PKI)</b>	The entire set of organisations, practices, processes, server platforms, software, and workstations used for the purpose of administering policies, certificates and public keys. (SwUPKI)
<b>QoS</b>	<b>Quality of Service</b> according to a service level agreement
<b>RADIUS</b>	<b>Remote Authentication Dial In User Service</b> - Transport protocol for AAA purposes. (StB IETF)
<b>RadSec</b>	modified RADIUS protocol
<b>RAS</b>	<b>Remote Access Server</b>
<b>R-BE*</b>	Remote Bridging Element
<b>RDP</b>	<b>Remote Desktop Protocol</b> – a multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services.
<b>Realm*</b>	an authoritative domain for user authentication; an AS which is authoritative for a realm is able to prove the identity of a supplicant that tries to authenticate. eduoam realms are in the form of DNS domain names, delimited from the local part of the user name with an @ symbol
<b>Resource</b>	Any information entity, application, IT-controlled physical equipment or service available through the Internet, whatever its nature and use.
<b>RI*</b>	Remote Institution
<b>Roaming: (WLAN Roaming / Wireless Roaming)*</b>	<p><b>Wireless Local Area Network Roaming (WLAN Roaming)</b> refers to the ability to move from one administrative domain to another without interruption in service or loss in connectivity.</p> <p><b>Wireless Roaming</b> - refers to the ability for a guest user to gain as transparent and secure network access as possible at the guest institution, to either</p> <ol style="list-style-type: none"> <li>(1) gain restricted access to the Internet or</li> <li>(2) be given a connection to the user's home institution network to authenticate and gain access to resources as authorized by the guest or home institution.</li> </ol>
<b>Root CA</b>	The top level Certification Authority in a hierarchy of such authorities. See also Policy CA.
<b>SAML</b>	<p>The <b>Security Assertion Mark-up Language</b> is an XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. Assertions are issued by SAML authorities, which can use various sources of information in creating their responses.</p> <p>SAML defines a protocol by which clients can request assertions from SAML authorities and get a response from them. This protocol, consisting of XML-based request and response message formats, can be bound to many different underlying communications and transport protocols; SAML currently defines one binding, to SOAP over HTTP. (StB OASIS, <a href="http://www.oasis-open.org">http://www.oasis-open.org</a>). (StB OASIS)</p>
<b>SAP</b>	<b>Service Access Point</b> (see Access Point)

Term	Description
<b>Schema</b>	Definition of object classes and attributes, for example LDAP-schemas or XML-schemas.
<b>SDK</b>	<b>Software Development Kit</b> – a set of development tools that allows a software engineer to create applications for a certain software package, software framework, hardware platform, operating system or similar.
<b>Server</b>	A computer or an application that provides a service. In this context often an AAA server.
<b>Service Provider*</b>	An entity that provides access to a service based on federated authentication.
<b>Shibboleth</b>	An Internet2 project to investigate technology to support inter-institutional Authentication and Authorisation for access to (mainly) web content.
<b>SIM</b>	<b>Subscriber Identity Module</b> is a smart card, the size of a postage stamp used in mobile phones.
<b>SMS</b>	<b>Short Messaging Service</b> – Uses the mobile (GSM) network to send up to 160 characters as a text message to one or more mobile users.
<b>SNMP</b>	<b>Simple Network Management Protocol (SNMP)</b> – a Layer 7 or Application Layer protocol that is used by network management systems for monitoring network-attached devices for conditions that warrant administrative attention. It is part of the Internet protocol suite as defined by the Internet Engineering Task Force (IETF)
<b>SOA</b>	<b>Service Oriented Architecture</b>
<b>SOAP</b>	<b>Simple Object Access Protocol (StB W3C)</b>
<b>SP*</b>	<b>Service Provider</b>
<b>SPOCP</b>	SPOCP (pronounced as SPOC-P), that is short for <b>Simple Policy Control Project</b> , is a co-operative project whose task is to provide the partners with software for authentication and Authorisation services. It has been developed by 5 Swedish universities and UNINETT.
<b>SQL</b>	<b>Structured Query Language</b>
<b>SRV</b>	DNS resource record which specifies the location of the server(s) for a specific protocol and domain
<b>SSID</b>	<b>Service Set Identifier</b> . 1-32 octets that identifies the wireless network. The client's SSID must match the access point's to associate. If the client sets an SSID of "Any" or _blank_ it will associate to the first active mode access point it finds or in other implementations the AP with the best signal quality, regardless of its SSID.
<b>SSL</b>	<b>Secure Socket Layer</b> is an application level security protocol that allows secure communications between users, providing privacy, data integrity and optional authentication
<b>Supplicant</b>	piece of software that initiates and performs network authentication on the client side (term from the IEEE 802.1X standard)
<b>SwUPKI</b>	<b>PKI for Swedish Universities and University Colleges</b>
<b>TACACS</b>	<b>Terminal Access Controller Access Control System</b> – An authentication protocol for remote access authentication and related services such as event logging. User passwords are administered centrally in a database rather than in individual routers.
<b>TKIP</b>	<b>Temporal Key Integrity Protocol</b> . An alternative to WEP that uses as 128-bit RC4 key for encryption and that allows for per-packet encryption and key rotation. Hardware that encrypts WEP can be modified by software to encrypt TKIP.
<b>TLD</b>	Top Level Domain
<b>TLS</b>	Transport Layer Security – encrypts network packet payloads from end to end

Term	Description
<b>Trust Fabric*</b>	The trust structure (on a technical and organisational level) between the members of a (con)federated infrastructure, such as eduroam, eduGAIN or a Shibboleth federation.
<b>UMTS</b>	<b>Universal Mobile Telecommunications System</b> - 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.
<b>URI</b>	<b>Uniform Resource Identifier</b>
<b>URN</b>	<b>Uniform Resource Name</b>
<b>UWB</b>	<b>Ultra Wide Band</b> - 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.
<b>Virtual Organisation (VO)</b>	A group or association of users collaborating in a common experiment, project or other joint venture. A <b>VO</b> is formed as a selection of users belonging to different administrative domains. (eIRG)
<b>Visited Institution (Guest Institution)*</b>	An institution that a user is "visiting" (guest user). The user is normally registered at their Home Institution.
<b>Visitor User (Guest User)*</b>	A visitor user or guest user is a user that connects to a visited institution.
<b>VLAN</b>	<b>Virtual LAN</b> - A group of devices on one or more LANs configured, using management software, to 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.
<b>VOMS</b>	<b>Virtual Organisation Membership Service</b> - A service that provides information on the user's relationship with her Virtual Organisation: her groups, roles and capabilities.
<b>VPN*</b>	<b>Virtual Private Network</b> – 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.
<b>W3C</b>	<b>The World Wide Web Consortium</b> develops interoperable technologies (specifications, guidelines, software, and tools)
<b>WAYF</b>	<b>Where Are You From</b> – a Shibboleth-specific service which allows the user to choose the appropriate identity provider, when they attempt to access a resource protected by a service provider.
<b>WCDMA</b>	<b>Wideband Code Division Multiple Access</b> - A technology for wideband digital radio communication of Internet, multimedia, video and other capacity-demanding applications. WCDMA is the technology behind the third generation mobile telephone systems in Europe, Japan and the United States and provides an increase of data transmission rates in GSM systems by using CDMA multiplexing technique instead of TDMA.

Term	Description
<b>Web Based Network Login</b>	Access to the 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.
<b>WEP</b>	<b>Wired Equivalent Privacy</b> - 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 (unmatched goal, WEP provides a weak security only) (see also: 802.11i)
<b>Wi-Fi</b>	<b>Wireless Fidelity</b> - 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
<b>WiMAX</b>	WiMAX is another name (ETSI) for the 802.16 standards family
<b>Wireless</b>	Equipment, service or technology for transporting data or information without wires but rather through air waves (frequencies) using radio or microwave technology
<b>WLAN</b>	<b>Wireless Local-Area Network</b> a type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes.
<b>WPA</b>	<b>Wi-Fi Protected Access</b> . 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 802.11i with TKIP encryption or pre-shared secrets.
<b>WPA2</b>	<b>Wi-Fi Protected Access, version 2</b>
<b>WSDL</b>	<b>Web Services Definition Language</b>
<b>WSF</b>	<b>Web Services Framework</b> (see ID-WSF)
<b>XML</b>	<b>eXtensible Mark-Up Language</b>
<b>X.500</b>	Set of ITU-T computer networking standards covering electronic directory services, digital certificates (X.509) etc.