

---

# MUSE White Paper

## AAA Framework and Solutions for Broadband Access

---

Identifier: White Paper AAA  
Class: Report  
Version: 1  
Version Date: 7th January 2008  
Distribution: Public

## EXECUTIVE SUMMARY

MUSE has revisited the concept of AAA, and authentication in particular, in the context of a multi-service, multi-provider Broadband Access network. With the current approach taken to authentication, subscriber management is based on static line recognition or on PPP-based authentication. This becomes too limited for this new context, where multiple subscribers and providers can share a line, and at the same time a migration from PPP-based connectivity is under way while configuration is changing to a DHCP-based approach. Hence new solutions are required.

The first part of this white paper presents a framework for AAA with emphasis on the requirements and the possible authentication scenarios. An important distinction must be made between cases with support of nomadism and those without. In the second part, possible solutions are evaluated and compared based on how they respond to the requirements of the different scenarios and their intrinsic qualities. The solutions reviewed are 802.1X, CAPWAP, 802.1AE + 802.1af, PANA, and EAP-DHCP. Note that most are not finalized yet in standardisation. At the time of writing, EAP-DHCP looks like a suitable candidate for addressing the authentication needs, provided that it will comply with the identified protocol requirements.

## LIST OF CONTRIBUTORS

François Fredricx (editor)	Alcatel-Lucent
Arjan Van Ewijk	Alcatel-Lucent
Xavier Pougard	France Telecom R&D
Gilles Bourdon	France Telecom R&D
Roberta Maglione	Telecom Italia
Jaume Rius i Riu	Ericsson
Bob Melander	Ericsson
David Thorne	British Telecommunications
Mohit Thakur	Nokia Siemens Networks
Johannes Bergmann	Nokia Siemens Networks
Alex De Smedt	Thomson
Anna Olszewska-Olbryś	Telecom Poland
Arnoud Van Neerbos	Netherlands Organisation for Applied Scientific Research (TNO)
Miroslav Zivkovic	Alcatel-Lucent
Iñigo Pinilla	Robotiker

## TABLE OF CONTENTS

EXECUTIVE SUMMARY.....	2
TABLE OF CONTENTS.....	3
ABBREVIATIONS.....	4
REFERENCES.....	6
INTRODUCTION.....	7
<b>1 FRAMEWORK FOR AAA IN BROADBAND ACCESS.....</b>	<b>8</b>
2.1 Introduction to AAA.....	8
2.1.1 Authentication, the first A in AAA.....	8
2.1.2 Authorization, the middle A in AAA.....	8
2.1.3 Accounting, or the last A of AAA.....	8
2.2 Authentication: description and purpose.....	8
2.2.1 Enforcement of policies.....	9
2.2.2 Accounting purposes.....	10
2.2.3 Traceability purposes.....	10
2.2.4 Parental control for individual users.....	10
2.2.5 Distinguishing user types.....	10
2.2.5 Determining if a device is trusted.....	10
2.2 Problem statement.....	10
2.3 Functional Requirements.....	11
2.3.1 Basic requirements.....	11
2.3.2 Additional generic requirements.....	12
2.3.3 Additional requirements for nomadic users.....	12
2.3.4 Overview of possible usages.....	13
2.4 Authentication framework; general considerations.....	14
2.4.1 Types of authentication.....	14
2.4.2 Functional break-down of authentication.....	15
2.4.3 Business roles involved.....	16
<b>2 SOLUTIONS FOR AAA IN BROADBAND ACCESS.....</b>	<b>19</b>
3.1 Considered protocols.....	19
3.2 Authentication without nomadism.....	20
3.2.1 Technical Requirements.....	20
3.2.2 Assessment of authentication methods and protocols.....	21
3.3 Authentication in the context of nomadism.....	23
3.3.1 Nomadic context.....	23
3.3.2 Aim of authentication in the context of nomadism.....	24
3.3.3 Translation into Technical Requirements.....	25
3.3.4 Assessment of methods.....	26
<b>3 CONCLUSIONS.....</b>	<b>30</b>

## ABBREVIATIONS

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ALG	Application Layer Gateway
AN	Access Node
ARP	Address Resolution Protocol
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
AVP	Attribute Value Pair
BB	Broadband
BNG	Broadband Network Gateway
BRAS	Broadband Remote Access Server
CAPWAP	Control And Provisioning of Wireless Access Points
CHADDR	Customer Hardware Address
CIADDR	Customer Internet address
CP	Connectivity Provider
CPE	Customer Premises Equipment
CPN	Customer Premise Network
C-VLAN	Customer Virtual Local Area Network
DDoS	Distributed Denial of Service (attack)
DHCP	Dynamic Host Configuration Protocol
DIAMETER	Successor of RAIDUS (not an acronym)
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DSL	Digital Subscriber Line
DSLAM	DSL Access Multiplexer
DSLIF	DSL Forum
EAP	Extensible Authentication Protocol
EN	Edge Node
FMC	Fixed-Mobile Convergence
GSB	Global System for Broadband communications
HGI	Home Gateway Initiative
HSI	High Speed Internet
HW	Hardware
IMS	IP Multimedia Subsystem
IKEv2	Internet Key Exchange v2
IP	Internet Protocol
IPsec	Internet Protocol Security
ISP	Internet Service Provider
LAN	Local Area Network

MAC	Media Access Control
MCP	Media Content Provider
MPLS	Multi Protocol Label Switching
NA(P)T	Network Address (Port) Translation
NAP	Network Access Provider
NASS	Network Attachment SubSystem
NAT	Network Address Translation
NSP	Network Service Provider
OAM	Operations, Administration and Maintenance
PANA	Protocol carrying Authentication for Network Access
PAA	PANA Authenticator
PAC	PANA Client
PEP	Policy Enforcement Point
PON	Passive Optical Network
POPA	Post-PANA Address
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PRPA	Pre-PANA address
PVC	Permanent Virtual Connection
RADIUS	Remote Authentication Dial-In User Service
RFC	Request For Comments
RGW	Residential Gateway
RNP	Regional Network Provider
SBC	Session Border Controller
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
STB	Set Top Box
S-VLAN	Service Virtual Local Area Network
TR	Technical Report
UE	User Equipment
VID	VLAN Identifier
VLAN	Virtual Local Area Network
WT	Working Text

---

## REFERENCES

- [1] MUSE DTF1.8 – FMC Support in Fixed Access Architecture – June 2007
- [2] MUSE DTF1.9 Part B – GSB Access Network Architecture, Additional Network Architecture Topics – December 2007
- [3] MUSE DTF3.3 – Specifications of an advanced, flexible, multiservice residential gateway / Part 2; Solutions and enabler descriptions - October 2007
- [4] MUSE White Paper “MUSE Business Model in BB Access”, April 2007
- [5] MUSE White Paper “FMC support in Fixed Access Architecture”, December 2007
- [6] W. Dec et al, “Subscriber Sessions v2.5”, DSL Forum WT-146, July 2007
- [7] A. Cui, “Broadband Multi-Service Architecture & Framework Requirements”, DSL Forum TR-144, August 2007
- [8] B. Aboba et al, “Extensible Authentication Protocol (EAP)”, RFC 3748, June 2004.
- [9] L. Yang et al, “Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)”, RFC 4118, June 2005.
- [10] P. Calhoun et al, “CAPWAP Protocol Specification”, draft-ietf-capwap-protocol-specification-07 (work in progress), June 2007.
- [11] P. Calhoun et al, “CAPWAP Protocol Binding for IEEE 802.11”, draft-ietf-capwap-protocol-binding-ieee80211-04 (work in progress), June 2007.
- [12] Y. Ohba et al, “Protocol for Carrying Authentication for Network (PANA)”, draft-ietf-pana-pana-18 (work in progress), September 2007
- [13] Y. Ohba et al, “Protocol for Carrying Authentication for Network Access (PANA)” draft-ietf-pana-framework-10 (work in progress), September 2007
- [14] M. Parthasarathy, “PANA Enabling IPsec based Access Control”, draft-ietf-pana-ipsec-07, July 2005.
- [15] R. Pruss et al, “Authentication Extensions for the Dynamic Host Configuration Protocol” IETF draft-pruss-dhcp-auth-dsl-02, November 2007
- [16] S. Kent et al, “Security Architecture for the Internet Protocol”, RFC 4301, December 2005.
- [17] IEEE Std 802.1X – 2004, “LAN IEEE Standard for Local and Metropolitan Area Networks - Standard for Port based Network Access Control
- [18] IEEE Std 802.1AE-2006, “IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security.”
- [19] IEEE draft 802.1af, IEEE Draft Standard for Local and Metropolitan Area Networks — Port-Based Network Access Control — Amendment 1:Authenticated Key Agreement for Media Access Control (MAC) Security.

# 1 INTRODUCTION

Authentication, Authorisation, and Accounting (**AAA**) are important functions accompanying the autoconfiguration process that establishes a service in a multi-service access network. **Authentication** is the process of determining whether someone or something is, in fact, who or what it declares to be. Authentication is based on identifiers and security attributes, or so-called credentials. **Authorization** is the process of giving individuals or devices access to resources, guarantees or applications based on their identity. **Accounting** is the recording, classifying, summarizing, and interpreting of events for charging purposes.

It was important for MUSE to revisit the authentication process, for several reasons:

- In a conventional broadband access network, the Point-to-Point Protocol (PPP) has mostly been used so far for autoconfiguration. PPP is a tunnel based connectivity protocol suite with in-built authentication and autoconfiguration functionality, but has some disadvantages when deploying multiple services. A tunnel needs to be set-up for every path between a user-device in the home and an Edge point. For every layer 2 QoS class supported between the edge and the user, an extra tunnel is required. This is because of the fact that once packets enter a PPP tunnel, it is not possible anymore to reshuffle them based on e.g. IP QoS parameters. On top of that, a PPP based connectivity model cannot take advantage of multicast streams.
- The Dynamic Host Configuration Protocol (DHCP) was therefore introduced in the access network for the configuration and control of the link and network layer of a connection, as an alternative to PPP. DHCP however did not support two essential functions provided by PPP: authentication and session management. The MUSE project hence paid a lot of attention to solutions for authentication and management of IP sessions [6], as described in deliverable [2].
- Apart from the change of autoconfiguration protocol, MUSE is also aiming at solutions in multi-provider and multi-services environments. In terms of autoconfiguration this means that a single subscriber could have multiple simultaneous application sessions from different providers, each requiring an authentication.
- An additional new requirement is the support of nomadic users, which implies that users or devices need to be easily authenticated from different places in a network, and even from different networks (roaming situations). The consequence for the authentication process is that multiple subscribers can now be located behind a single line, and all need to be authenticated with their corresponding profile. This also implies interaction between different providers when roaming is involved, which is described in the MUSE White Paper on FMC [5].

Chapter 2 in this white paper presents the analysis of a new framework for AAA (authentication) in the light of requirements in multi-service, multi-provider broadband access networks supporting nomadism.

Chapter 3 investigates and compares existing protocols and protocols under definition for providing a technical solution to the identified requirements.

## 2 FRAMEWORK FOR AAA IN BROADBAND ACCESS

### 2.1 Introduction to AAA

#### 2.1.1 Authentication, the first A in AAA

The present-day telecommunication networks represent huge investments and aim at serving as wide an audience as possible. It is in the best interest of both users (paying for a service) and providers (selling access or applications at a guaranteed quality) to preserve these investments and avoid abuse of the resources. Authentication of the end-user is therefore a logical - but not obvious to realize - step in gaining connectivity to an application. But authentication does not only have a restrictive role, it also plays a supportive role to allow end-users to retrieve their privileges by recognizing them (and retrieving their profile) when they connect to the network or ask for an application.

Multiple possible levels of authentication can be applied. In order to determine which ones should be supported, it is important to clearly define the functional requirements to which authentication must provide an answer. A distinction should be made between scenarios with and without nomadicity. The technical aspect of a solution is then determined by the way authentication credentials are stored in the end-user's device, and the choice of the appropriate protocol to carry the credentials between that device and the network.

#### 2.1.2 Authorization, the middle A in AAA

The corollary of authentication is determining to which resources the end-user is authorized. The authorizations can be carried back to the respective network nodes during the authentication process, together with the authentication result.

#### 2.1.3 Accounting, or the last A of AAA

Accounting is also a necessary corollary. Authentication guarantees that the charges are billed to the right person. As it is specific from operator to operator depending on their wishes, and fits with any AA solution as soon as RADIUS or DIAMETER is used, it is not detailed further in this white paper.

### 2.2 Authentication: description and purpose

Authentication as such boils down to recognizing the identity of a user with a sufficiently high level of confidence. This recognition is either based on interpreting credentials sent by the end-user side (e.g. username@domain:pwd), or on a line/node/circuit-based tagging by the network (e.g. line-ID (DSL), port-ID or LLID (PON), PVC (ATM), ...).

Optionally, during the authentication process, additional information can be gathered about:

- the device type (STB with capabilities such-and-such, retail RGW, ...),
- the location in the access network (access line, access node, serving SBC, ...),

- and the type of access technology (eg xDSL flavour, Wimax, ...).

The purpose is to link a subscriber and his/her profile (profile describes authorizations and guarantees/limitations) to a request issued by the user (e.g. for an IP address, for a particular service), and to traffic to/from the subscriber and apply (subscriber-specific) policies to this traffic.

A fundamental difference should be noted between network-based and application-based authentication. **Network-based authentication** uses network mechanisms, and can be application-independent (does not involve an application platform). On the other hand, **application-based authentication** involves an application platform and is hence application-specific. It can be done independently from and in addition to network-based authentication.

Authentication is all about control from the perspective of providers (control of user requests, of resource consumption, of access to applications), and about assurance from the perspective of the end-user (of the privacy, of the network attachment point, of retrieving its own profile).

As mentioned in the introduction, there are several reasons for applying authentication. This merits a closer look.

### 2.2.1 Enforcement of policies

One of the basic applications of authentication is for setting and enforcing policies, which must be applied on requests and traffic associated with a subscriber, depending on the subscriber identity and his/her profile.

The policies can be of various types:

- policies on the traffic in terms of guarantees and restrictions (e.g. bandwidth per traffic class)
- controlling the access to resources (e.g. synchronisation rates, IP address allocation)
- controlling the access to applications (e.g. setting IGMP filters, IP destination address filters). Note that access control to some applications could also be done purely at application-layer (e.g. via login on a portal), transparently for the NAP.

Setting of policies can be done either statically or dynamically:

- Statically: a subscriber is associated with a fixed line, his/her parameters and policies are pre-configured in the corresponding nodes (e.g. Access Nodes)
- Dynamically: a subscriber is recognized at authentication, and policies are retrieved to the appropriate enforcement point, and applied there (for fixed and nomadic subscribers).

Configuration of network nodes:

- A very similar usage of authentication is to set per-user parameters and configuration options. Examples are the selection of a forwarding mode, VC activation, and choice of an S-VLAN for the uplink. Whereas these are not policies in the sense that it is something completely transparent for the end-user, authentication-based configuration follows the same methods as policy setting.

### **2.2.2 Accounting purposes**

Authentication is obviously indispensable in order to perform per-subscriber statistics collection and when applying payment plans other than just flat-fee subscription.

### **2.2.3 Traceability purposes**

Traceability aims at answering the questions: “who uses a given IP address” and “which IP address does a subscriber use”. These answers help at troubleshooting, legal interception and localisation of emergency calls.

### **2.2.4 Parental control for individual users**

The purpose is to assign individual authorization profiles per user, to be managed by the subscriber to which these users relate. The typical example is parental control of children’s access rights.

Note that there are reasons for handling parental control locally in the RGW itself or at the application level instead of involving the network.

### **2.2.5 Distinguishing user types**

In the previous paragraph, it is mentioned how a user under parental control can be identified. In the same way it is possible to locally (i.e. in the RGW) identify visitors in the home, or hotspot users using the co-located hotspot in the home, on the basis of authentication between terminal and RGW. For a detailed description, please see [3].

### **2.2.6 Determining if a device is trusted**

This is more about checking the type of a device rather than checking subscriber authentication, the purpose being to determine if the device can be considered as trusted (i.e. of a certain type and un-tampered). A simple approach could use credentials (hard-coded in the device), a more comprehensive approach could require certificates (checking integrity of the device). If used, it should be a first step before authenticating the subscriber/user.

## **2.3 Problem statement**

The problem statement is decomposed into a series of questions, which are analysed below.

### ***Which authentication scenarios should be supported?***

Which of the previously listed usages should authentication enable? Furthermore the authentication context depends on whether nomadism is supported or not, and on whether a user is handled as a retail user or a wholesale user by the provider performing authentication. In the retail case the provider has a direct relationship with the user and has direct access to his/her profile. In the wholesale case, the user is managed by a third-party provider, which must be contacted in order to perform the authentication.

***Depending on the scenario, which level of authentication is required?***

The person to be recognized is in most cases the subscriber (the user who has subscribed for a service and who receives the bill for the service).

A subscriber can be identified as a member of a community (by using a generic credential) or as an individual (by using a personal credential). In identifying the individual subscriber, there are different levels:

- Subscriber per-line/per-circuit,
- Subscriber per RGW,
- Subscriber per-device,
- User per-device (finer level than subscriber; not who to bill (e.g. one parent of the household) but who is using the service right now (e.g. a child of a household)).

In parallel to subscriber authentication, two further questions arise: whether extra information (about location, access technology, device type) is required, and whether mutual authentication is required between client and network.

***Which technical solutions are suitable?***

Depending on the levels of authentication, how are they translated into technical requirements, and how suitable are possible solutions for these requirements.

## **2.4 Functional Requirements**

### **2.4.1 Basic requirements**

For any level of authentication and any context, some basic requirements must be respected:

- The credentials must be inserted, typed or hard-coded on the end-user device.
- The credentials, challenges and authorization results must be exchanged between the end-user device and the authentication server of the appropriate provider.
- As result of authentication, policies must be applied. This means that the authentication result must be bound to the “session” being set-up (session based on line/circuit or on IP address(es) or IP subnet) in order to associate the session with its policies, and that the policies to be applied on that session must be transmitted to the enforcement point (see the principle of IP sessions as defined in [6] and described in [2]). Note the difference between flow classification and flow identification.

## 2.4.2 Additional generic requirements

The context in which authentication will take place will create additional requirements, irrespective of whether the user is nomadic or not (specific requirements for nomadic users are mentioned in the next subchapter).

- First, the access network must be selected. In the context of multiple available networks (e.g. WiMAX + residential WiFi, or e.g. multiple WiMAX providers), the device needs to select the appropriate network.
- Multi-services and multiple-providers per subscriber (wholesale and retail) must be supported. Multiple authentications are needed for the same subscriber per RGW or per device behind the RGW. The correct provider must be selected and reached.
- In the context of non-PPP cases, a credential-based authentication method needs to be selected, both in terms of the authentication protocol to be used, and (when multiple authentications are needed), of doing them in a single step (single-sign on) or in multiple separate authentications.
- Context of multiple BNGs (e.g. one per service provider).

When multiple authenticators are present in the network, the right one must be reached.

- In the context of nomadism, it must be determined whether the user is at home or is being nomadic.
- Type of RGW

The RGW can be bridged, or hybrid L2/L3, or routed without/with NAPT. Depending on the RGW type and network topology there can be a need to cross IP nodes with NAPT between the supplicant and the authenticator.

- Access technology

Multiple access technologies are possible (xDSL, xPON, WiMAX). When there is a shared medium, a mapping on technology-specific identifiers is needed.

- Wireless access technology

Whenever a wireless access technology is involved, the security and confidentiality over the public part of the link must be addressed. This leads to the respective requirements of mutual authentication and encryption.

## 2.4.3 Additional requirements for nomadic users

The context of nomadism brings specific requirements, due to the fact that both visitors and hosts must be accommodated at the same time, possibly by different providers.

- One non-nomadic subscriber and multiple nomadic subscribers can be connected on the same line. Hence, multiple authentications for different subscribers must be performed on the same line.
- The terminal should be smart enough to select the right authentication method on the user's behalf depending on the technology of the network it is connecting to.

- Nomadic users can connect from their home access network or from a visited access network (roaming). The relevant providers must be reached during the authentication process.
- Both the host and the visitor count on security and confidentiality.
- Finally, if mobility must be supported, roaming must again be considered. And depending on the type of mobility, the handovers can cause interruptions or not in the application session, so there is a need to avoid or reduce delays due to re-authentication. Note that the mobility aspect is not elaborated here.

### 2.4.4 Overview of possible usages

Table 1 provides an overview of the necessary levels of network-based authentication for achieving the different authentication usages.

	<i>Setting and enforcing policies Configuration of nw nodes</i>	<i>Checking device is "trusted"</i>	<i>Parental control</i>	<i>Statistics, Subscriber or provider charging</i>	<i>Subscriber tracability for legal intercept</i>	<i>Subscriber tracability for emergency</i>
<i>Subscriber per-line/circuit</i>	<b>Sufficient when no nomadism and no wholesale.</b>			<b>Sufficient when no nomadism and no wholesale</b>	<b>Sufficient when no nomadism</b>	<b>Sufficient</b>
<i>Subscriber per RGW</i>	<b>Sufficient when no nomadism. Required when wholesale.</b>			<b>Sufficient when no nomadism Required when wholesale.</b>	<b>Sufficient when no nomadism</b>	
<i>Subscriber per device (device = terminal)</i>	<b>Required when nomadism.</b>			<b>Required when nomadism</b>	<b>Required when nomadism</b>	
<i>User per device (device = terminal)</i>			<b>Required</b>			
<i>Optional extra info; device type (device = RGW)</i>	<b>Useful</b>	<b>Required</b>				
<i>Optional extra info; location indication</i>						<b>Sufficient</b>
<i>Optional extra info; Access technology</i>	<b>Useful</b>					

**Table 1: Overview of authentication usages and respective needed authentication levels**

The most relevant usages for the MUSE partners are the setting of per-subscriber policies, the configuration of network nodes, statistics and charging, and subscriber traceability.

Parental control is not considered at network-level (should better be handled at application level or locally).

It is not obvious how to reach a high level of confidence in trusting a RGW, so it is better to avoid where possible to depend on a trusted RGW. However it can be interesting to check the device type (e.g. in order to know its capabilities and for a retailer to know whether the RGW is one of his devices).

## 2.5 Authentication framework; general considerations

### 2.5.1 Types of authentication

There can be three types of authentication involving the providers, plus a special case, which is purely local. For a description of the different business roles that can be played by providers, please consult the MUSE White Paper on Business Roles [4].

#### **Network-based: connectivity authentication**

Authentication to control access to the network resources and QoS, based on network mechanisms. For non-nomadic users, the exchange is happening between the user device and the NAP. For nomadic users in the public access network, the exchange is also between the user device and an authentication server in the NAP network, via an authenticator in the NAP network (see 2.4.3).

#### **Network-based: network service authentication**

Authentication to control access to IP configuration, based on network mechanisms. The exchange is between the user device and an authentication server in the NSP network, via an authenticator in the NAP network (see 2.4.3).

The way to combine the two network-based authentication types depends on the protocol used. A protocol like 802.1X is used for connectivity authentication (giving access to the network), after which the line-ID is used as network service authentication (giving IP configuration). With a protocol like PANA, the sequence starts with a temporary IP configuration giving only limited access, followed by a combination of the connectivity authentication and network service authentication (giving wider access, and after which a new IP configuration can take place via DHCP).

Please note that in fixed networks it is usual to combine both types of authentication (see 2.4.3).

#### **Application-based: Application service authentication**

Authentication to control access to the application itself (policies, policy decision and policy enforcement point in the application infrastructure), based on the application server (e.g. via HTTPS to a capture portal on the application server). The exchange is between the user terminal and the application server of the ASP, transparently for the NAP.

Application-based authentication requires a preceding IP configuration and connectivity, and can be done independently from network-based authentication.

The trigger for application-based authentication is given by the user's device (from the power-on if it is a dedicated device for an application, or at the time of request for the application by the user if the device could be used for multiple applications).

**Special case: local authentication**

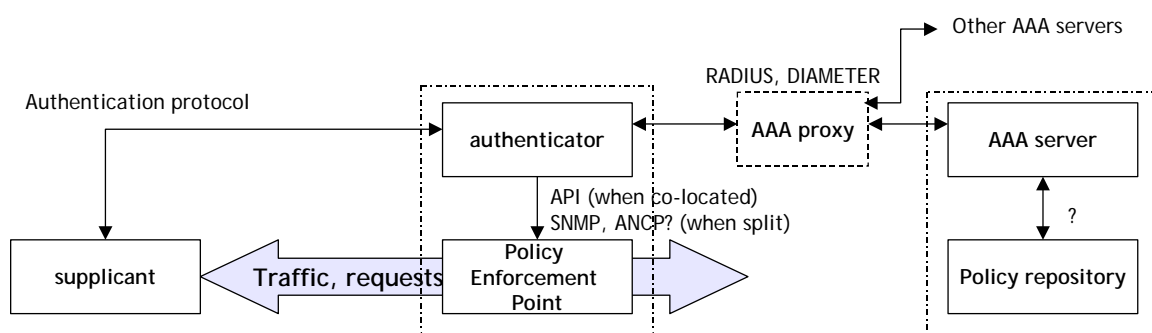
Local authentication in the private network is completely independent from the providers. It runs between a user device and the host's access point in the private network, without intervention of any provider. Examples are captive portals in a hotel, parental control at home, etc... Local authentication is for connectivity to the private network (e.g. WPA key), and possibly for network service in the private network (e.g. autoconfiguration in hotel).

This type of authentication as such is not detailed further, but is required for dealing with nomadic users. For a detailed description please refer to DTF3.3 Part 2 [3].

**2.5.2 Functional break-down of authentication**

The functional blocks for **network-based authentication** are composed of:

- (end-user side) the supplicant: holding the credentials and exchanging them with the authenticator,
- (network side) the authenticator: exchanging authentication messages between the user side and the AAA server, and transmitting the policies to the enforcement point,
- (network side) the AAA server; keeping the user credentials and related profiles,
- (network side) (optionally) AAA proxy: forwarding authentication messages between the authenticator and one of multiple AAA servers,
- (network side) Policy repository: definition of the policies,
- (network side) PEP: enforcement point for end-user traffic and requests.

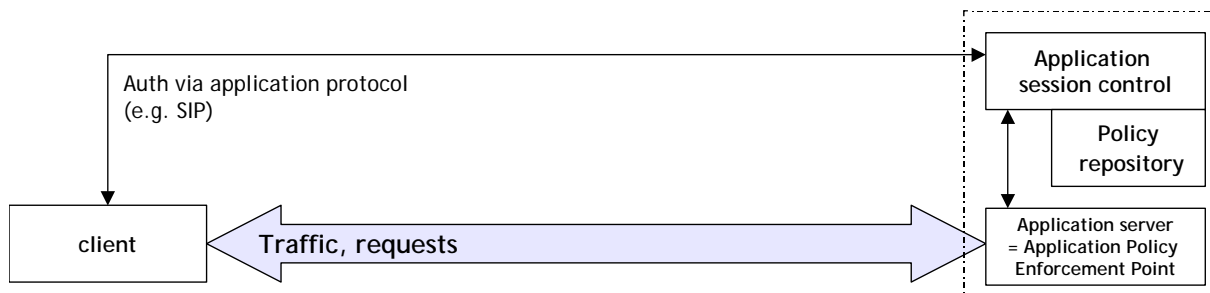


**Figure 1: Network-based authentication**

The functional blocks for **application-based authentication** are composed of:

- (end-user side) the client: holding the credentials and exchanging them with the network.

- (network side) the application session control: exchanging authentication messages between the user side and the application server.
- (network side) the application server, keeping the user credentials and related profiles, and applying the related application policies.
- (network side) Policy repository; definition of the policies.



**Figure 2: application-based authentication**

Finally, for local authentication, only the private network is concerned, with a supplicant communicating with an access point playing the role of authenticator and authentication server which is also the policy enforcer.

### 2.5.3 Business roles involved

Multiple providers can be involved as parties in the different kinds of authentication. Each provider can play one or multiple roles in the process; carrying out the authentication decision, keeping subscriber policies, or enforcing these authorization policies. Note that the description given here is based on the business roles as defined in MUSE [4].

- Providers that carry the authentication decision.  
These providers host the AAA server and use authentication to protect their resources.
  - Connectivity Provider (CP) (or Network Access Provider (NAP)) for granting access to the network, for allocating (private) IP addresses and for configuration of the access nodes,
  - Network Service Provider (NSP)/Internet Service Provider (ISP) for allocating public IP addresses,
  - Application Service Provider (ASP) for granting access to an application,
  - Note that the packager centralizes the subscriber's credentials and notifies the CP, NSP, ASP about them. This allows the packager to perform customer support and (pre)configuration of customer devices.
- Providers that forward the authentication message further to the right provider.

- (connectivity authentication) As multiple CPs can be supported by a NAP, the NAP is responsible for forwarding the authentications to the correct CP based on a RADIUS proxy inspecting the credentials.
  - (network service authentication) The CP in turn has to proxy the authentication requests (and responses) to the appropriate NSP (which can be the CP itself - also acting as an NSP - for supporting retail applications of an ASP), by hosting a RADIUS proxy.
- Providers that keep the subscriber policies to be applied.  
These providers host a policy server and are responsible for keeping per-subscriber profiles and policies.
    - NAP for connectivity guarantees,
    - NSP/ISP for IP configuration of the host and determining ACL,
    - ASP for application-related profiles.Note that the packager keeps the subscriber policies of the different providers.
  - Providers that support authentication in their network and enforce the policies  
The provider offering connectivity also has to host the authenticator for allowing the retrieval of the credentials, and has to ensure enforcement of the policies in the relevant nodes.
    - CP (or NAP) for connectivity authentication and possibly also for network service authentication (retail users, or trust relationship with NSP).Note that the ASP is a special case; for application service authentication the ASP must host the authenticator (on its application platform) and apply the policies.

A further important question that may be raised in this context is the following: when is there a need to distinguish both types of authentication (connectivity / network service)?

- In typical current deployments (no nomadism) a single authentication step both grants access to the network (connectivity authentication), and to the IP configuration (network service authentication). It is performed by the NAP when there is a trust relationship NAP-NSP, or relayed to the NSP (the NAP can e.g. just look at the line to enforce access policies to its network).
- For nomadic users connecting from their home NAP, such a trust relationship can still occur, and a single authentication step can be arranged. Note that, if there is no such relationship anymore, there must be separate network service authentication (by the NSP) and credential-based connectivity authentication (by the CP), as the line-id is no longer sufficient.

- When introducing roaming for nomadic users, combining both types of authentication is not always an option. There can be no trust anymore between all visited NSPs and all home CPs, excepted for the case of fixed-mobile roaming, if the routing happens via the home NAP and the IP configuration is performed by the home NSP.

## 3 SOLUTIONS FOR AAA IN BROADBAND ACCESS

### 3.1 Considered protocols

The Extensible Authentication Protocol (**EAP**) [8] is the prevalent authentication protocol working with different types of credentials. Credentials can for example be certificates, one-time passwords, or smartcards. EAP is carried during the authentication phase of PPP, between the PPP client and the BRAS. But since it was an objective to find authentication solutions complementary to DHCP, other protocols to carry EAP must be investigated.

**IEEE802.1X** allows carrying EAP over Ethernet and is used to open a port to an Ethernet switch. The advantage is that it is a defined standard and available on products today. The limitations of the standard are that it cannot cross bridges or routers, it cannot be VLAN-tagged, and it is not conceived for multiple authentications on the same physical port for wired access (it allows MAC-binding authentication in IEEE802.11 WiFi).

Using IEEE802.1X in an architecture that supports Control and Provisioning of Wireless Access Points (**CAPWAP**) [9],[10],[11] is a possible solution to the mentioned problems. The CAPWAP architecture splits the access point into a wireless termination point on the residential gateway and an access controller, which performs authentication, on a trusted access node in the network. All control frames, including those for authentication, and data frames are carried over an encrypted tunnel that is terminated in the access controller. The advantage is that the terminals are not impacted (no new requirements). However CAPWAP is positioned for IEEE802.11 WiFi devices, and as such is not expected to be available on wired devices (e.g. for wired terminals behind a bridged RGW).

Another track investigated is the use of **802.1AE** [18] in combination with **802.1af** [19] allowing for a secure tunnel connection between the terminal itself and the AN across a bridged RGW (or bridged part of the RGW). The enforcement is based on the MAC address of the user which is integrity protected by the 802.1AE protocol. However as this protocol is not yet deployed on terminals, it fits more in a longer term timeframe.

The Protocol carrying Authentication for Network Access (**PANA**) [12],[13],[14] is a link-layer agnostic network access authentication protocol. It is conceived to transport EAP across layer 3 networks and PANA's multi-hop extension allows for crossing routers. It is possible to have multiple EAP sessions per line. In the assumption that the PANA exchange is initiated by the client, Network Address and Port Translation (NAPT) can be traversed between the supplicant and the authenticator (Network Address Translation (NAT) can be traversed irrespective of the initiating party). As PANA is not involved in the autoconfiguration process, it needs interaction with DHCP in the network node to enforce the authentication result at layer 3. This means that the two separate state machines must be coupled. PANA uses an unauthenticated IP address at the start of the PANA authentication process, which requires extra protection measures to address security concerns. The specification of PANA is in the process of being finalized in the pana WG of the Internet Area at IETF.

A more recent initiative in IETF is the extension of DHCP for carrying EAP over DHCP (see [15]). **EAPoDHCP** allows for crossing routers and handling multiple EAP sessions per client. Unlike PANA, EAPoDHCP is intended to become an integral part of the DHCP autoconfiguration process and avoids the need for an assignment of a temporary IP address prior to authentication. It will impact the DHCP state machine in client and proxy. A specific proxy function is needed in the RGW for allowing authentication of nomadic terminals when the RGW is of the routing type with NAPT. It otherwise has similar potential as PANA.

Finally, PANA or EAPoDHCP can be combined with **IPsec** [16] as tunneling method for providing confidentiality and distinction between host and visitor traffic in the context of nomadism.

## 3.2 Authentication without nomadism

### 3.2.1 Technical Requirements

Given the required levels of authentication described in Subchapter 2.3, the levels of authentication without nomadism for which a solution must be found are:

- subscriber per-line/circuit,
- subscriber per RGW,
- device type.

#### **Subscriber per line / circuit**

Recognition of the subscriber based on a **line-ID** allows performing a single authentication per line. Recognition of the subscriber based on a **circuit-ID** allows performing multiple authentications per line, though always of the same subscriber (multiple circuit-Ids could lead to different AN settings per PVC for one subscriber).

They are static in the sense that there is a fixed relationship line/circuit and subscriber-ID, which must be set and updated by management.

#### **Subscriber per RGW (per terminal)**

When the RGW is recognized by means of credentials, the authentication is the same as in the case of a subscriber per-line. The difference with per-line is that the credentials allow for easier management of subscriber modifications (physical address) and wholesale scenarios, as these are dynamically deduced from the credentials at each session set-up. The RGW can also support multiple authentications (this depends on the authentication protocol), which is useful for wholesale scenarios (simultaneous multi-provider case).

In the case where the RGW cannot be involved in the authentication (e.g. a bridged RGW will not participate in EAP over DHCP exchanges), one of the terminals needs to perform the authentication.

#### **Device type**

The purpose is to recognize the RGW as pertaining to a specific type, e.g. to check whether it is a retail RGW box sold by the provider.

Figure 3 shows the different functional blocks for subscriber authentication in a non-nomadic context. Depending on the RGW type and the authentication protocol, the supplicant can be located in the RGW or on a user device. The authenticator collects the credentials and sends them to an authentication server, and the Policy EP enforces the received policies. Note that there can be a local authentication between a wireless terminal and the RGW, totally unnoticed by the network.

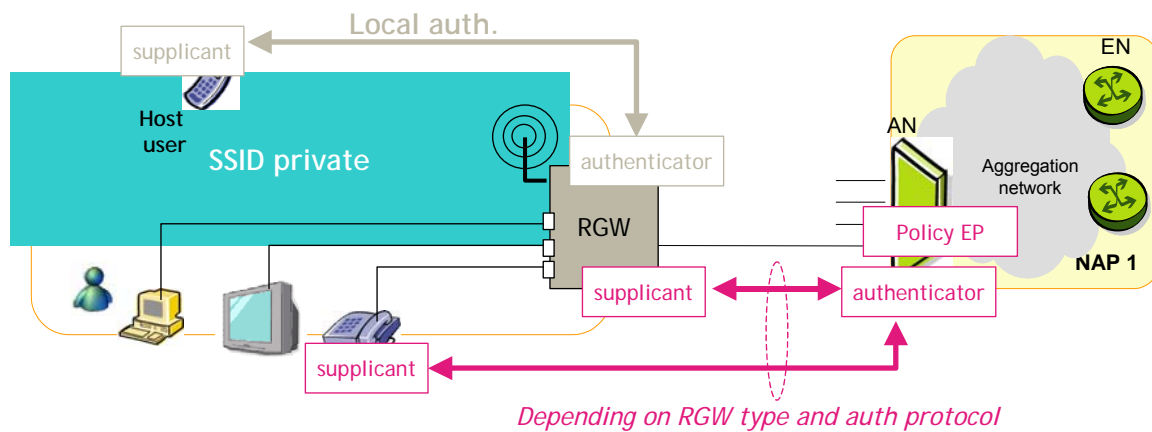


Figure 3: Functional blocks

### 3.2.2 Assessment of authentication methods and protocols

The protocols of interest are 802.1X, PANA, and EAPoDHCP. **Table 2** contains a summary of the pros and cons of each method.

Method	Benefit	Drawback / limitation
Line-ID / circuit-ID	* available and simple to implement (DHCP option 82)	* No credentials => only one fixed identity per line (per circuit)
EAP over 802.1X (RGW is supplicant)	* Available in products today.	* Not conceived for multiple authentications on same port. (note that EAPOL frames are untagged => VLANs cannot be used for multiple auth)  * Requires Ethernet in the stack.
EAP over PANA (L3 RGW => RGW supplicant)  (L2 RGW => terminals supplicant)	* Based on IP SA => supports multiple authentications per line  * allows binding of IP session with subscriber ID  * same mechanism can be used with IPv4 and IPv6	* Uses unauthenticated temporary IP SA => requires binding method to be updated with permanent IP addr. => and requires security measures for PANA messages (possibly involves PANA snooping in AN)  * Requires binding of two protocol stacks (PANA and DHCP)

	<ul style="list-style-type: none"> <li>* PANA being finalized in IETF</li> </ul>	<ul style="list-style-type: none"> <li>* Version being standardized is less complete than the original.</li> <li>* Not available on current RGWs/terminals</li> <li>* Acceptance by industry is a question mark</li> </ul>
<p><b>EAP over DHCP</b></p> <p>(L3 RGW =&gt; RGW supplicant)</p> <p>(L2 RGW =&gt; terminals supplicant)</p>	<ul style="list-style-type: none"> <li>* Authentication is part of the DHCP exchange =&gt; supports multiple authentications per line (each IP client can have separate authentication)</li> <li>* allows binding of IP session with subscriber ID</li> </ul>	<ul style="list-style-type: none"> <li>* Requires modification of DHCP proxy (or server if no proxy)</li> <li>* Requires change of DHCP client stack</li> <li>* Not available on current RGWs/terminals</li> <li>* Recent work and acceptance by industry is a question mark</li> <li>* Solution does not yet consider IPv6</li> </ul>

**Table 2: Assessment of authentication protocols for the context without nomadism**

It may be stated that the line-ID is limited to a single authentication, but is extensively used today for subscriber recognition, and will continue to be used, at least for giving a location indication (and PVC-based circuit-ID is used in legacy ATM networks).

The use of standard 802.1X allows a limited authentication, with only one dynamic subscriber per-RGW authentication (all traffic on the same line is bound to the same authentication). Some operators currently use 802.1X for subscriber or mostly for device type identification. It is hence well suited for single authentication of a residential gateway on an Ethernet based access line and is, as such, a solution for simple immediate needs but without being future-proof.

It does not allow for multiple authentications on the same line, as needed in the context of multiple service providers. Note that it would be possible to circumvent this by designing an IEEE802.1X proxy on the residential gateway that authenticates the users or devices behind it, but this then requires a trusted residential gateway that directly connects the network's AAA infrastructure, which is not a secure option for many providers.

Two candidates, PANA and EAPoDHCP, are potential solutions for multiple authentications per line, although there is no guarantee of industry acceptance for either. Both allow performing subscriber per-RGW (if routed RGW) and subscriber per-device (if bridged RGW). The main difference in operation is that PANA is a separate protocol requiring a temporary IP address (Pre-PANA Address (PRPA)) to carry EAP, whereas EAPoDHCP is an extension of the existing DHCP exchange for autoconfiguration. This has some consequences in terms of security measures (extra measures may be needed in the AN to guard against DoS with PANA messages with unauthenticated PRPA) and complexity (binding of two separate state machines in the IP node). On the other hand, PANA is agnostic of IPv4 or IPv6, whereas the EAPoDHCP currently only considers IPv4.

Finally, some DHCP options (60, 77) may be suited for device type recognition but the integrity aspect requires further elaboration (possibly combining with option 90).

### 3.3 Authentication in the context of nomadism

#### 3.3.1 Nomadic context

A nomadic user is always considered as a subscriber as he/she has subscribed to a nomadic profile and gets billed for it.

The nomadicity of a user can be expressed in different ways, as illustrated in Figure 4:

- (1) the user reconnects between its home private network and a public wireless network
- (2) the user reconnects between its home private network and a visited private network
- (3) the user reconnects between different visited private networks
- (4) the user reconnects between a visited private network and a public wireless network
- the user connects to its profile via a terminal of the visited private network.

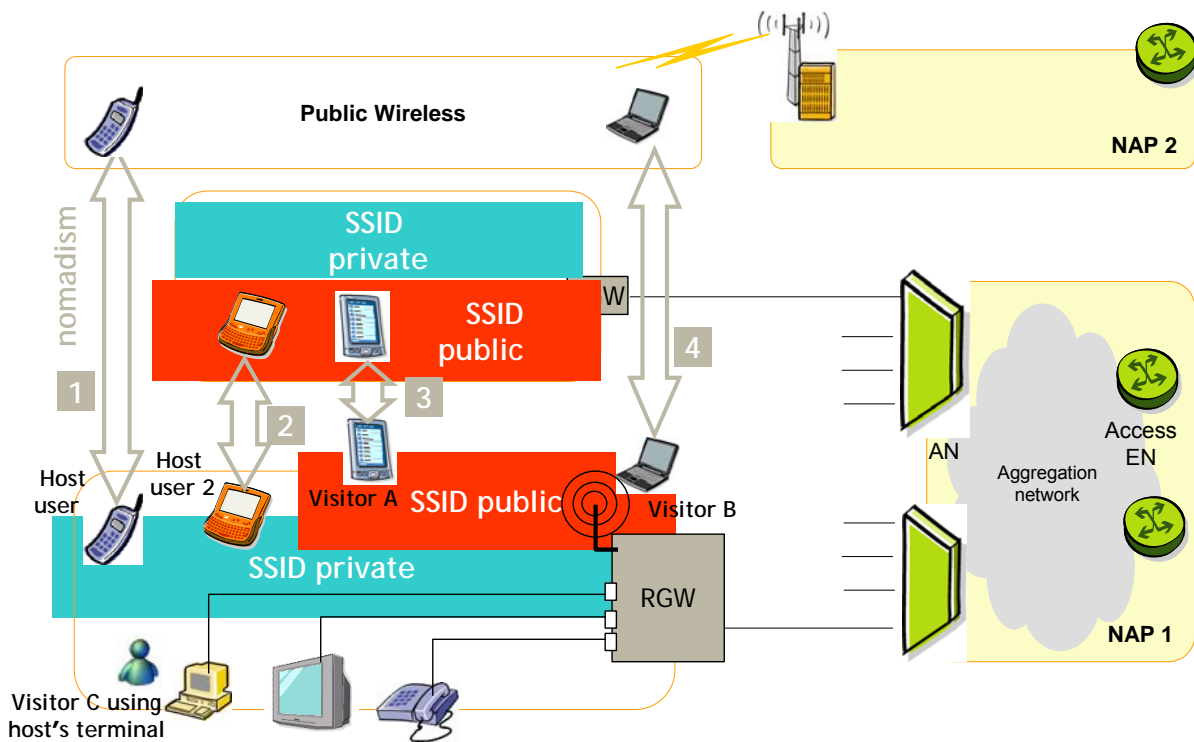


Figure 4: Possible changes of attachment point by a nomadic user

As a first step, prior to any nomadism-specific authentication, there will be a connectivity authentication to access network:

- Whenever a RGW is powered on, a connectivity authentication is first performed between the RGW and the NAP (identical to the case without nomadism, see section 3.2.7), before any nomadic user consideration.
- Whenever a wireless terminal connects to a public wireless network, a connectivity authentication (based on the terminal technology) is first performed between the terminal and the NAP.

The second step will be the nomadism-related authentication itself. It basically consists of connectivity authentication by the home CP (via the visited CP if needed as in cases 4, 3) followed by network service authentication by the home NSP (via the visited NSP if needed as in cases 4, 3).

### 3.3.2 Aim of authentication in the context of nomadism

The aim is basically to differentiate requests and traffic between visitors and host users in order to apply different settings in the network elements, enforce different policies with given guarantees, and gather statistics for different charging. It is important to indicate what has to be authenticated and recognized, for the host and his/her related users (household members and restricted visitors), and the nomadic hot-spot users. For a description of the different types of users, please see [3].

The needs for authentication can be different between a host and its related users.

- Individual users pertaining to the host must not be recognized individually, and they can reuse the host's connectivity as such. For them local authentication is sufficient, no intervention from the network is needed.
- Restricted visitors are users who are explicitly allowed by the host to use his/her connectivity and profile. They don't have to be recognized.
- On the other hand, the host must be recognized in order to receive the associated profile on the line, also when he/she relocates to his/her home.

For nomadic visitors (connecting to the network either directly or via a host RGW), there are two possible options:

- In the most complete option, the individual nomadic subscriber is recognized by the network in order to apply to his/her traffic the policies pertaining to his particular profile. This means that credential-based authentication of the user per-device is needed.
- In a simplified option, the nomadic user is recognized not individually but as being nomadic, in other words as a community member with a fixed profile. In both cases, extra information about the device type and the access technology can be useful.

Note that when a nomadic user returns in his/her own private residential network, he/she wants to retrieve all his/her authorizations again and not be considered as a “visitor” anymore.

The simplest solution is to connect via his/her private SSID or via a cable to the RGW.

### 3.3.3 Translation into Technical Requirements

#### **Subscriber authentication per-device**

This level of authentication is needed to identify nomadic users behind a RGW. This means that multiple authentications have to run on the same line, for different subscribers (host + nomadic visitors), and possibly to multiple NSPs. It also means that the nomadic device must be authenticated even when behind a routed RGW with NAPT, see further.

#### **Security**

Given that the connectivity is now shared between host and visitors, the security aspect must be covered.

A first requirement is confidentiality for the host. The reach of visitors in the private network must be restricted (e.g. within a dedicated public SSID standing next to an encrypted private SSID).

A second requirement is confidentiality for the visitor for the case there is no trust relationship with the host. This requires tunnelling from the visitor's device (not the RGW) to the AN (or beyond). Application encryption is an alternative, albeit depending on the application.

A last requirement is the ability to trace IP addresses to their related subscribers (legal intercept). Anti-spoofing in wireless network requires a tunnel from the device to the network.

#### **Dealing with different kinds of RGW (supplicant on device behind RGW)**

As described in MUSE deliverable [3], it is recommended to partition the RGW in a part for visitors and a part for the host and his/her associated users. The preferred implementation for the visitor part is a bridged implementation. Layer 2 connectivity allows easy visitor per-device authentication without obstruction by NAPT; each visitor receives his/her IP address and authenticates, but a tunnelling protocol is still needed for the confidentiality.

If fully routed RGWs (with NAPT) have to be supported, the situation is more complex. NAPT causes all individual visitors to be aggregated as a single IP address (on a VR in the RGW dedicated for visitors), so it blocks visibility of individual visitors.

In order to retrieve full visibility, the RGW should either ask for a separate IP address per visitor (on its WAN side), or tunnelling should be used instead in order to directly reach the terminal through the RGW. As tunnelling is required anyhow for confidentiality, the tunnelling approach is retained.

An alternative for authenticating individual visitors is to entrust the enforcement of the authentication to the RGW, whereby the RGW directly contacts the provider's AAA infrastructure. However this last point raises severe security concerns and this alternative is better avoided.

### 3.3.4 Assessment of methods

Protocols considered for carrying EAP are 802.1X (also via CAPWAP), 802.1AE+802.1af, PANA, and EAPoDHCP. Additionally IPsec is considered as tunnelling protocol. Table 3 contains a summary of the pros and cons of each assessed method.

Method	Benefit	Drawback / limitation
<b>Line-ID / circuit-ID</b>	* available and simple to implement (DHCP option 82)	* No credentials => only one identity per line (per circuit) => <b>not suited for nomadism</b>
<b>EAP over 802.1X</b>	* Available, in products	* In principle cannot cross bridges (except if MAC@ of peers known in advance)  * Cannot cross routers  * Not conceived for multiple authentications on same port  * Doesn't offer confidentiality as such => <b>as such standard form not suited for nomadism</b> Note that non-standard implementations could be a stop-gap.
<b>CAPWAP</b>	* Overcomes 802.1X limitations; Tunnels auth (WPA over 802.1X) from terminal to the authenticator in the AN. Data is also tunneled and encrypted by WPA to the AN. => confidentiality included.  * No requirement on WiFi terminals	* Requires hybrid RGW with CAPWAP in the visitor's part.  * Not positioned for terminals wired to a bridged RGW  * Requires CAPWAP controller in AN.
<b>802.1AE (MACSec) + 802.1af</b>	* Overcomes 802.1X limitations; Similar approach to CAPWAP but encryption on layer 2, and authentication enforcement based on terminal's MAC address (integrity ensured by MACSec) => confidentiality and anti-spoofing (L2)	* Limited to visitors behind a bridged RGW (with VLAN tagging).  * Requires extra protocol stack in terminals (not available yet).  * Requires extra protocol stack in the AN.  * 802.1af still draft => not yet supported (but finalized soon)
<b>EAP over PANA</b>	* Based on IP SA => not limited to single auth per line.  * Can work with routers (if PRPA via DHCP) and NAT between PaC and PAA (but see drawback).  * can be used for IP session binding  * same mechanism can be used with IPv4 and IPv6  * PANA being finalized in IETF	* As a visible IP address is required, it cannot enforce multiple authentications with NAPT between the PaC and PAA  * Based on IP SA => requires to be updated with permanent IP addr and requires IP-awareness at enforcement point.  * no confidentiality nor anti-spoofing  * Not available on RGWs/terminals  * Acceptance by industry is a question mark

<p><b>EAP over DHCP</b></p>	<ul style="list-style-type: none"> <li>* Authentication is part of the DHCP exchange =&gt; each IP client can have separate authentication</li> <li>* can be used for all cases of RGWs (but see special functionality for authentication of a terminal behind routed RGW with NAPT)</li> <li>* can be used for IP session binding</li> </ul>	<ul style="list-style-type: none"> <li>* For the case of the authentication of a device behind a routed RGW with NAPT, requires a DHCP proxy function in the RGW</li> <li>* Requires modification of DHCP client and DHCP proxy (and server if no proxy)</li> <li>* Based on IP SA =&gt; requires IP-awareness at enforcement point.</li> <li>* no confidentiality nor anti-spoofing</li> <li>* Not available on RGWs/terminals</li> <li>* Recent work, acceptance by industry is a question mark</li> <li>* Solution does not consider yet IPv6</li> </ul>
<p><b>PANA or EAPoDHCP or non-std 802.1X</b>  <b>+ IPsec (started via authentication)</b></p>	<ul style="list-style-type: none"> <li>* See respective pro's</li> <li>* IPsec allows traffic differentiation across a routed RGW with NAPT, and confidentiality, and guarantee for anti-spoofing</li> </ul>	<ul style="list-style-type: none"> <li>* See respective con's</li> <li>* Higher processing load for IPsec at termination point</li> </ul>

**Table 3: Comparison of authentication methods**

As a conclusion, it may be stated that there are no “killing arguments” in favour of one particular protocol, but some relative differences;

- Line-identification and standard 802.1X are not suited for the job because the line-identification ties a user to a fixed line and they both do not allow for multiple authentications on the same line. Non-standard variants of 802.1X may be used but should only be considered as stop-gap solutions.
- CAPWAP is a method to push the 802.1X-based authenticator from the RGW to the AN. It requires an adapted RGW (split mode; CAPWAP for visitors and normal mode for home users) that performs the tunnelling of management and data frames between RGW and AN. Due to the compatibility of CAPWAP with existing terminals, CAPWAP is quite interesting in the shorter-term. For more details, please see [1].
- The combination 802.1AE+802.1af is another method to push the 802.1X-based authenticator to the AN. It requires an adapted RGW but also adapted terminals (must support the 802.1AE and 802.1af stacks). Hence this solution is more suited on the longer-term. For more details, please see [1].
- PANA and EAPoDHCP are quite equivalent in functionality and limitations:
  - They allow subscriber authentication per RGW (PANA or DHCP client on RGW) and subscriber authentication per device (PANA or DHCP on terminal behind RGW)

- For the case of authentication of a terminal behind a routed RGW with NAPT, EAPoDHCP requires a special DHCP proxy function in the RGW as normally no DHCP messages are exchanged between the terminal and the network in this case. PANA on the other hand would have no problem to run the authentication as such across a NAPT but would not be able to do policy enforcement as it is based only on the IP address and a same public IP address would be shared by multiple terminals. But this can be solved with IPsec (see further).
- EAPoDHCP is a somewhat lighter process than PANA. There is no need for a temporary IP@, no interaction between two different protocol state machines, and the process is totally transparent for the AN. However EAPoDHCP requires an update of the DHCP client and proxy (and server if no proxy). For the client side it is claimed to be easier to add a PANA stack than modifying the DHCP stack.
- PANA is agnostic on the use of IPv4 or IPv6, whereas EAPoDHCP currently only considers IPv4.
- Both can be used for binding of IP sessions to subscriber IDs (see [2]).

When PANA or EAPoDHCP are used, IPsec tunnelling is required in order to allow for confidentiality (encryption) and traffic differentiation (assignment of a public IP address to the visiting terminal even if behind a NAPT). The security association also prevents spoofing. For more details please see [2] and [3].

Support of nomadic users is the most straightforward if they can be connected via a bridged (part of the) RGW, because their terminals will be visible at layer 2 from the network side, allowing for direct authentication and traffic differentiation based on IP address. However a tunnelling method would still be required to guarantee confidentiality for the visitor. Hence the most versatile and generic solution is to combine PANA or EAP-DHCP with IPsec to cross any type of RGW (even routed RGWs with NAPT) and provide both confidentiality, traceability and traffic differentiation. More details are given in the next sub-chapter.

As for a choice between PANA and EAP-DHCP, MUSE expresses a preference for EAPoDHCP for its slightly lower impact and complexity, provided several requirements on the proper use of the protocol are met (see [2] for details).

### 3.3.5 EAPoDHCP in the case of nomadism

When using EAPoDHCP for supporting nomadic subscribers, it must be combined with IPsec, in the same way PANA must be combined with IPsec, as was described in [1] and [3]. The same reasoning can be applied for EAPoDHCP as for PANA.

#### **Bridged RGW**

The RGW is transparent for DHCP messages. There is direct exchange between the subscriber terminal and the DHCP proxy in the network. After authentication and IP address allocation, an IPsec tunnel can be started to provide confidentiality.

#### **Routed RGW without NAPT**

The local DHCP relay in the RGW must allow the DHCP messages to flow between the nomadic subscriber terminal and the access network. This local relay should not add option 82 or a giaddr.

After successful authentication, the terminal of the nomadic subscriber is allocated a public IP address. It then uses this public IP address to run IKEv2 and establish an IPsec tunnel.

### **Routed RGW with NAPT**

The RGW must allow the nomadic subscriber terminal to send and receive DHCP messages across the RGW for the purpose of authentication. When the nomadic subscribers are also connected to the NAPT part of the RGW, the RGW needs a DHCP proxy (acting like a server for the DHCP client and as a client for the DHCP server in the network). This is investigated next (Note that if the nomadic subscribers are connected to a non-NAPT part of the RGW, the solution is the same as for a bridged or routed RGW without NAPT).

The sequence is as follows. First of all, the RGW determines if the terminal that contacts it with DHCP belongs to a nomadic user (for which it must act as the local DHCP proxy) or is a terminal of a home user (for which it must act as a local DHCP server allocating a private IP address). When it has recognized it is a nomadic visitor, it must allow the DHCP exchange to cross the RGW by means of the local DHCP proxy. When the terminal of the nomadic subscriber has performed a successful authentication, it can request a private IP address from the local DHCP server in the RGW (note the RGW should not allocate a private IP address to a terminal that did not authenticate successfully). The IPsec tunnel is then set up by means of IKEv2, as described for PANA in [1] and [3]. Once the IPsec tunnel is established, the visitor has a guarantee of confidentiality, and the operator is able to distinguish the traffic from that specific authenticated nomadic subscriber.

## 4 CONCLUSIONS

Authentication is a cornerstone in the control of resource consumption, delivery of guaranteed services, and compliance to regulatory requirements on traceability and legal intercept.

The high-level requirements have been listed in this white paper, where it is important to differentiate between the context without nomadism and the (more complex) context with nomadism which brings additional requirements.

A list of possible usages of authentication is matched with associated required levels of authentications. The involvement of the different business roles is highlighted.

Finally, MUSE has analyzed and developed technical solutions for responding to these requirements. Although there is no simple “silver-bullet”, several possibilities (albeit still in the process of standardization) have been identified.

For non-nomadic users the line/circuit identification and standard 802.1X protocol are simple methods to achieve a limited level of authentication. A more complete response to the requirements of multi-provider multi-service environment (requiring multiple authentications per line) can be offered by non-standard 802.1X, PANA or EAPoDHCP.

For nomadic users the complexity increases in the interaction of the visited and home providers. The additional requirement of multiple subscriber per line obliges multiple authentications per line. The additional requirements of confidentiality and security require the use of tunneling and encryption. A possible short-term track is CAPWAP which imposes no requirements on the terminal, but is more oriented to wireless cases (wired terminals behind a bridged RGW requiring another authentication method). Longer-term tracks are 802.1AE+802.1af (for visitors behind a bridged RGW part) and PANA or EAPoDHCP (or a non-standard version of 802.1X). The latter two must be combined with IPsec tunneling for confidentiality and traffic differentiation.

After comparing PANA with EAPoDHCP in MUSE the choice is not clear-cut, as is also reflected by the current discussion inside the IETF WG. However given the extra requirements with PANA of binding two protocol state machines and the extra impact of PANA snooping for filtering purposes, MUSE favours the use of EAPoDHCP as the global authentication method to fit all authentication needs (applicable to both for nomadic and non-nomadic cases), provided the necessary requirements as indicated in this document and in [2] can be met.