AAA Authentication: New Use Cases

An AdvOSS Solution White Paper

Authors: Farhan Zaidi and Fawad Pasha

Contact: {farhan.zaidi, fawadpasha}@advoss.com

Whitepaper URL
www.advoss.com/resources/whitepapers/aaa-authentication-new-usecases.pdf

For more information, contact sales@AdvOSS.com

AAA Authentication: New Use Cases

Overview:

Authentication is the first and foremost function of a AAA Solution in any Service Provider's network. Originally the function was restricted to matching a username with its password or other identification key. Modern AAA solutions have seen the scope of Authentication broadened into many dimensions serving multiple other business interests. In this whitepaper, we will explore the new and emerging use cases for Authentication that are becoming critical business requirements in next generation telecommunication networks. We will use the term Service Provider to refer to providers of multiple service networks without distinguishing between operators and service providers. For each business use case, we will provide an overview of technical requirements needed to realize the use case.

The discussion that follows is applicable to a wide variety of access networks including wireless broadband e.g. WiMAX, DSL, fiber, mobile etc. It should be noted that although the discussion does not specifically mention Long Term Evolution (LTE) and Evolved Packet Core (EPC) networks that are usually coined as 4G, the use cases equally apply to these networks as well because the issues are applicable to new generation of telecommunication business scenarios and requirements.

Configurable Authentication Policy

An Authentication Policy Server allows authentication to be performed on different keys based on the settings for that service. It is possible for a network to be authenticating users based on their device MAC addresses for regular subscribers, based on their PIN numbers for unsubscribed pre-paid users and based on their username/password for Subscribers visiting other networks.

Technical Requirements:

A modern AAA solution should provide support for multiple authentication criteria used concurrently and policies for using those criteria for authentication. AAA should therefore, be aware of multiple types of user identities, their relations to subscriber accounts, and policies on which identity to authenticate in which conditions i.e. a Rule Based Engine to enforce policies.

Automatic Authentication

Automatic Authentication involves authentication without any action done on part of the user. It is usually done on MAC addresses of Customer Premises Equipment (CPE) or other identities hard coded in the CPEs or devices held by users.

Technical Requirements:

It requires the support of a Subscriber Manager like the Home Subscriber Server (HSS) that is capable of storing user's identities and also work flow support in the AAA Server to be able to perform different types of lease and lookup queries from different network elements based on network configuration. For example, when a user enters the network, the AAA client may only provide IP address as the user's identity in authentication request. AAA server may have to query the DHCP server to retrieve the actual MAC address this IP address was leased to. The workflow in AAA would then subsequently perform lookup in the HSS or Subscriber Manager to verify the MAC address.

Multiple successive authentications

In today's networks, Service Providers have multiple types of network elements acting as Service delivery and policy enforcement points within their networks. For example, in a wireless network such as WiMAX, some elements may be handling network access and initial over-the-air bandwidth allocation to wireless users, others may be providing IP based services for Internet access, yet others may be providing advanced classification of IP services by enforcing different policies to different types of IP traffic e.g. Voice Over IP, browsing, torrents etc. All these network elements require their own subscriber profiles to be provided to them when the user enters the network and starts to access their services. This provisioning of profiles of different network elements usually require multiple successive authentications where each network element in the user's service access path performs its own authentication based on one of the user identities relevant to that element.

Technical Requirements:

To realize this use case, a modern AAA solution must be able to support multiple successive authentication requests arriving back to back for the same user session, and send different subscriber profiles to different network element during its authentication. Each authentication request in this case may require a different authentication scheme for example, first authentication from a network access server may require EAP-TLS authentication, where as a second authentication from an IP Services policy enforcer may require basic username/password authentication, or basic MAC based authentication after performing a DHCP lease query.

This clearly requires support in the AAA solution for programmability and capability to realize different workflows in different environments.

Exclusivity of Devices:

Exclusivity of devices is a very important use case for new generation of Service Providers. A Service Provider may want to restrict the devices that can be used to access it network. Some of the reasons that may apply for such a policy are:

- Service Provider has contractual requirements or has financial reasons to force users to exclusively use the devices supplied by the Service Provider.
- Device interoperability is an issue and the Service Provider wants to make sure that users can only connect through tested and approved devices.
- Service Provider has some policies enforced in the devices that cannot otherwise be imposed on the network and wants to make sure that the users abide by those policies.

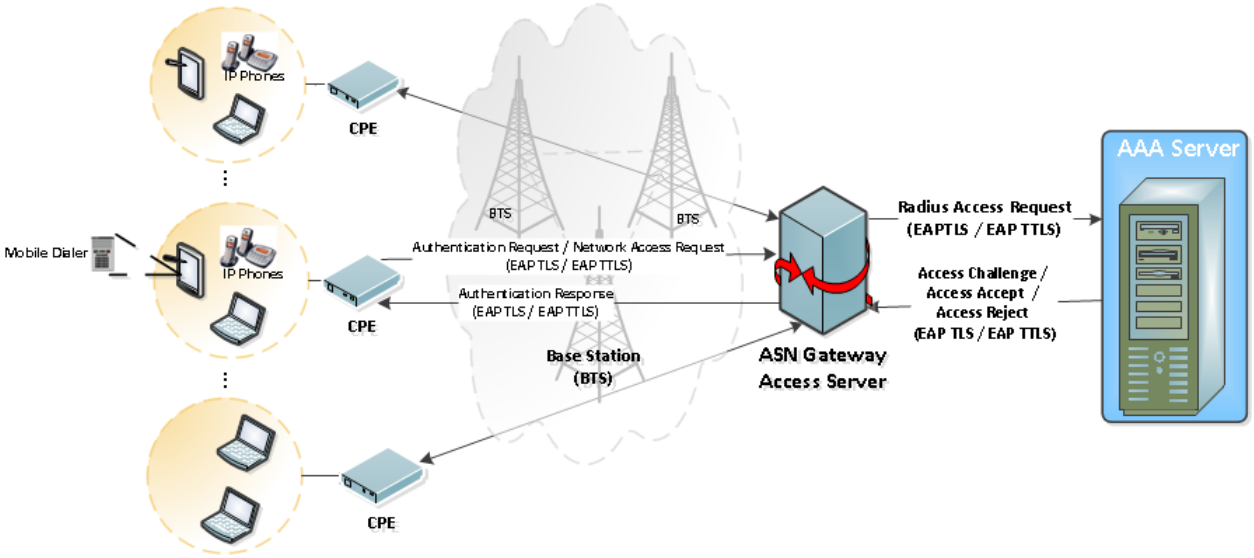
These and multiple other use cases may require the Service Provider to authenticate the devices used to access the Service.

Technical requirements:

To achieve this policy, the AAA solution needs to have:

- Certificate based authentication scheme e.g. EAP-TLS

In such a scheme the Service Provider provisions approved and signed certificates in the devices and then use mutual authentication where devices authenticate the network and the network authenticates the devices.



Control of Mobility:

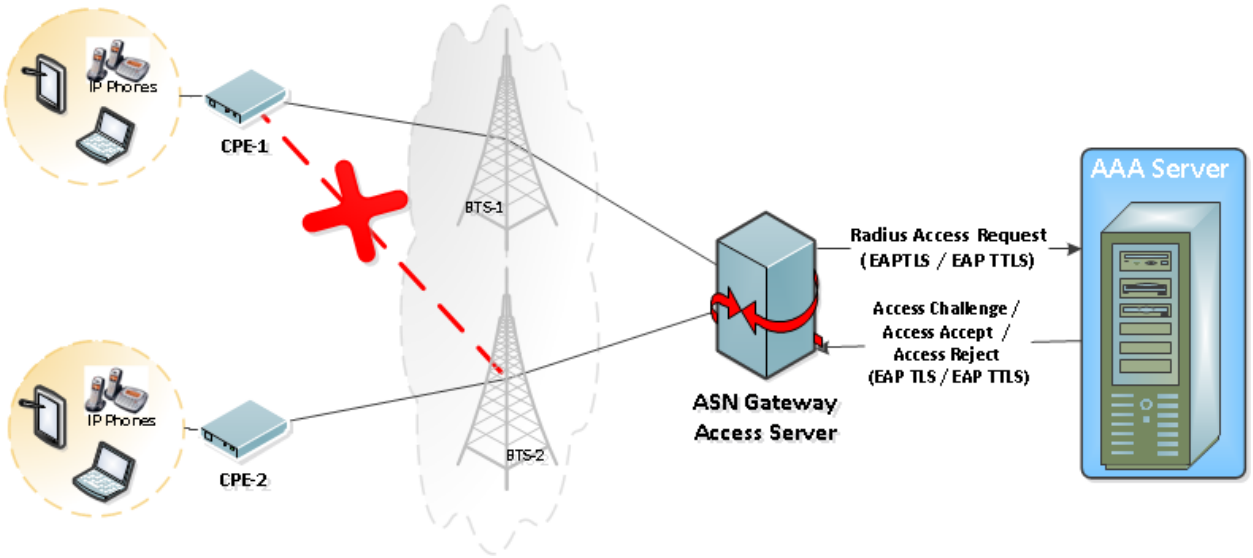
Control of Mobility applies when a Service Provider needs to restrict the geographical area from where a user can access the network. Usually it is for regulatory reasons where the license terms of the Service Provider do not allow its subscribers full mobility.

It can also be based on specially discounted prices and packages only offered to rural or other less congested areas where the Service Provider does not want the users to be able to move to other congested areas and user Service in those areas while paying lower prices.

Technical Requirements:

Realizing this requires the following from a AAA Solution:

- Awareness of the geographical topology of the Service Provider network
- Option to classify users into different groups
- Create access control lists (ACLs) based on the groups of users which are enforced at the time of initial Authentication



In the figure above, CPE-2 is trying to access the network via the wireless Base Station 1 (BTS-1, and Access Server or an ASN-Gateway (WiMAX standard term for an aggregated Network Access and policy enforcement Point), while CPE-2 is accessing the same Access Server via Base Station 2(BTS-2). Since CPE-1 belongs to a group associated with the ACL of BTS-1, and CPE-2 belongs to a group associated with the ACL of BTS-2, they are allowed access by the AAA server. However, if CPE-1 tries to access the network via BTS-2, it will be denied since its group is not part of ACL associated with BTS-2.

Identity Theft Protection:

Identity theft happens when a user's account credentials are used by another user (hacker) without its consent. This is an act of fraud, can cause Service Provider lost revenues and also cause legal problems if the activity involved fraud with other institutions involving Service Provider's network.

Service Providers need to make sure that the identities of their users are protected and that they are not dependent on a mere UserName/Password pair.

Technical Requirements:

Effective identity theft protection requires a combination of user and device authentication. In the first stage, the device is authenticated to ensure that a certified device issued to a subscriber is accessing the network. This is followed immediately by a second stage of authentication using username/password. This ensures that a legitimate user is accessing via her own device. Even if a hacker steals the username/password, since she would be accessing from a different device, the request will be denied. On the other hand, if the hacker only manages to steal the device, she would additionally need username/password credentials to complete the authentication process.

A typical method to achieve the combined authentication in a modern AAA solution is to have support for a Tunneling protocol in addition to the basic certificate based scheme e.g. EAP-TLS. In the first stage, a tunnel is established using mutual authentication of EAP-TLS as described earlier. In the second stage, a username/password based protocol e.g. PAP/CHAP/MS-CHAP is run inside the secure tunnel to let the user verify her identity. This method is used in EAP-TTLS (EAP based Tunneled TLS)

Account Sharing Prevention:

Account sharing happens when a user willingly shares her credentials with another user. This is a different use case than the Identity Theft but has a similar nature.

The Service Provider may like to block account sharing because it may have devised unlimited plans assuming office hour or home hour usage and would like to avoid sharing of accounts between devices.

Technical Requirements:

AAA Solution needs to have the following support to prevent this

- Concurrency Checks: AAA should be able to limit user's session to the allowed number of concurrent sessions (usually one session only)
- Combined device and user authentication using EAP-TLS and EAP-TTLS

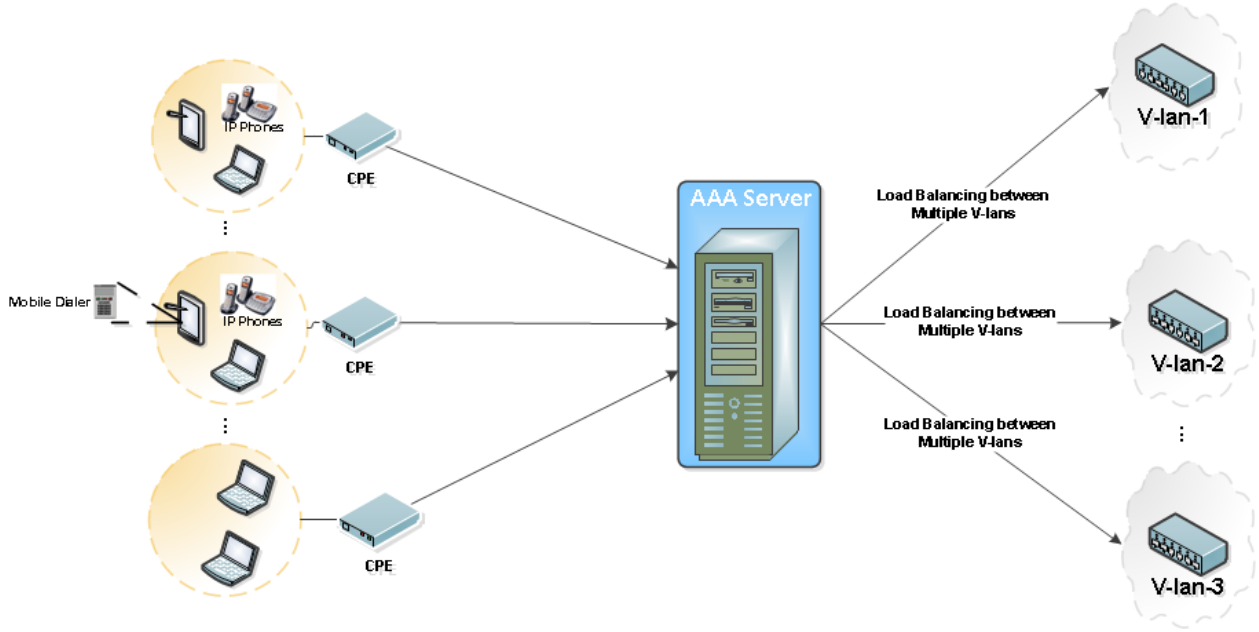
- Support in HSS or Subscriber Manager to allow Service Provider to be able to set the number of concurrent sessions for each user where account sharing is to be prevented

Load Sharing among VLANs

Authentication is the main entry point in the network. It is at this point that a Service Provider needs to make sure that her network is not overloaded at any point in time in order to avoid congestion. Service Providers usually want to distribute load among multiple Virtual LANS (VLANs) at this stage. A VLAN is usually assigned to an entering device at authentication time by providing the VLAN information to the network access server.

Technical Requirements:

- Awareness of available VLANs
- Support of Zoning of Subscribers into Groups
- Allocation and Retention Policy of Subscriber groups into VLANs



In the figure above, the CPEs entering the network are load balanced among multiple VLANs so that no one VLAN is overloaded. This is only made possible by making the AAA solution aware and responsible for VLANs and their assignment.

Lawful Intercept:

Lawful intercept involves informing an LEA (Law Enforcement Agency) about the activities of selected users on the network. Since Authentication is the first point of entry into the network, LI is best enforced at this layer. Depending on the nature of LI request, the AAA Solution may be required to:

- Only inform LEA about the start and stop of any session from selected users
- Send detailed statistics about ongoing session
- Route the media (voice, video etc) to the LEA as well

Technical Requirements:

AAA Solution needs to have support for the following:

- Support to store LI related rules for selected subscribers
- Rule based engine to process LI rules for each new session request
- If Media is involved, then ability to force Routing of sessions towards terminators
- Forking proxy to fork AAA activity towards multiple targets including the LEA Server
- Support for fulfilling specialized workflows and business logic in the AAA solution to be able to inter-operate with different requirements posed by LEAs

Support for Virtual Operators

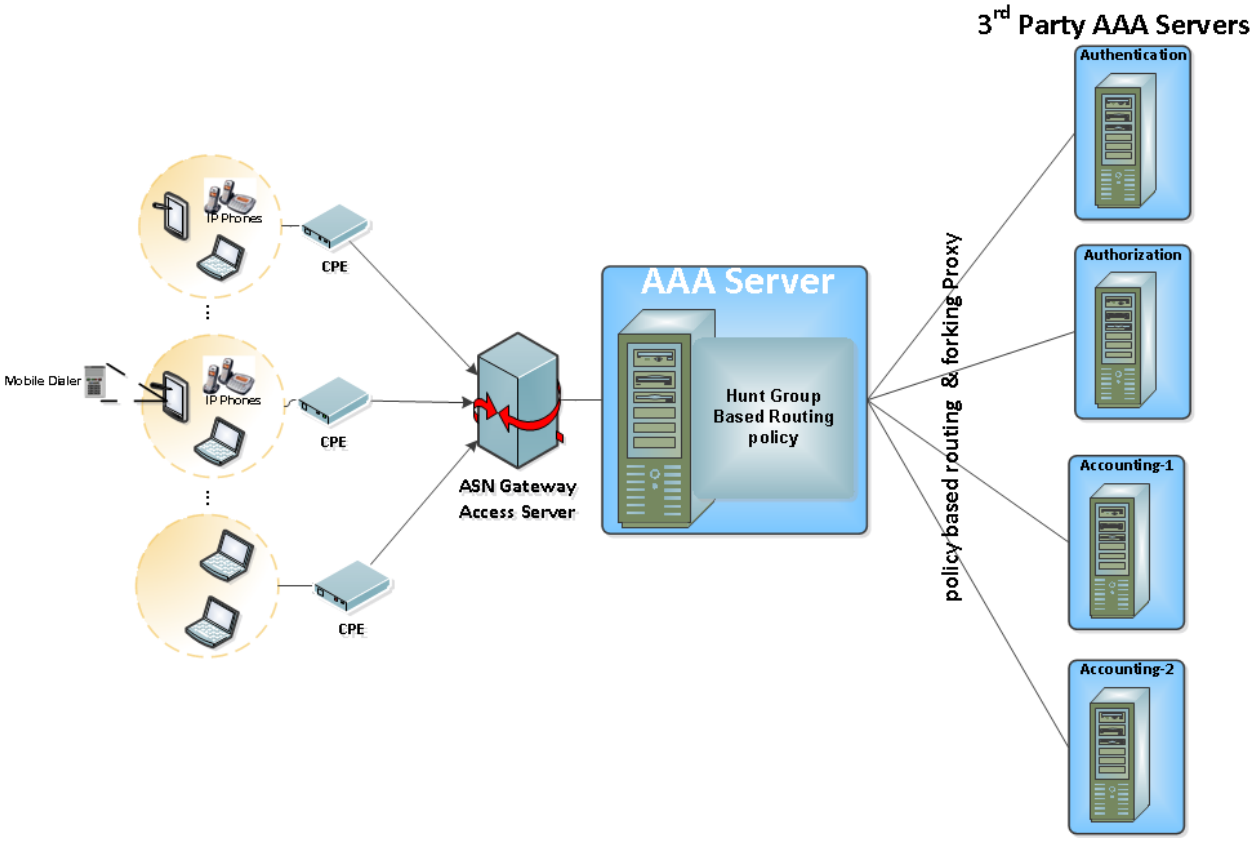
Virtual Operators ride on the existing networks of Service Providers. Different combinations are possible for the Virtual Operators to function. They may have their own Subscriber Managers or they may share the Subscriber Managers of the parent Service Provider. From a AAA perspective, specialized routing of authentication requests is required for multiple co-existing virtual operator domains and realms.

Technical Requirements:

AAA solution needs to have support for the following to allow Virtual Operators to function

- Forking proxies to fork Authentication requests towards Subscriber Managers of virtual operators
- Support for multiple Realms of accounting

- Rule based engine to direct routing of AAA requests towards virtual operators



In the above figure, policy based routing capability is shown in the AAA server. The third party AAA servers or Subscriber Managers for that matter are given their own realms or domains. AAA server maintains policy rules associated with these realms. Each realm may have a group of target AAA servers or Subscriber Managers associated with it. AAA server should be able to fork requests to one or more target servers after applying the provisioned policy rules.

Policy based routing and realms management is a general technique used to realize several business use cases e.g. LI use case discussed earlier as well as the roaming use case discussed later in this document are also realized using this technique.

IP Address Allocation

IP Address allocation is done at the time of Authentication. Service Provider may want IP addresses to be allocated according to its IP Allocation Policy. The IP address could be used to determine many things about the users including:

- Geographical location
- Access methods towards the network (cable, wireless, fiber, copper etc)

Technical Requirements:

AAA solution needs to have the following

- An awareness of IP Addresses
- Support to classify IP addresses in IP Pools
- Assign individual IP Addresses or IP pools to subscribers
- Statically or dynamically assign IP addresses from the pools based on the output of a Rule Based engine are per Service Provider policy

Allowing CPE Sharing:

A Service Provider may want to allow sharing of CPEs among multiple users. This may be required for business reasons where one CPE in an enterprise location could be shared by many different people within the office, each of them having a separate account with Service Provider. This could also be required in a multi-tenant environment e.g. in a building where multiple tenants share a small number of CPEs provided by the building management.

It could also be required at public places where any user with an existing account could move to get access.

Technical Requirements:

Although this use case is realized by combined device and user authentication as described for identity theft case i.e. combined device and user authentication. The only difference here is that the device is authenticated only once when it powers up while user authentication goes on as users enter and leave the network and access services. Therefore, instead of running a tunneled protocol inside TLS as described earlier, username/password based authentication may happen separately from EAP-TLS. The only requirement at the time of username/password authentication would then be to verify the MAC address of the device from a device database, and then perform username/password authentication individually for the user.

Roaming:

Roaming support involves two different use cases. In first, the Service Provider may want to allow its subscribers to roam to other networks and still be able to use the service. In the second use case, the Service Provider may want to allow Subscribers from other networks to be able to roam to its coverage areas and have service. This requires Interconnect Service Level Agreements (SLAs) between Service Providers.

Technical Requirements:

From a AAA authentication perspective, the same technologies have to be used that are required to realize LI and virtual operator use cases. They are:

- support for Realms
- Support for forking proxy

Conclusions

Modern AAA systems are getting far more complex and advanced in functionality than the traditional ones used to access basic Internet access and voice services. Authentication once thought to be a mere username/password verification technique, is now considered a critical process that realizes several Service Provider policies in a variety of complex business use cases. This has posed several challenges to the AAA solution providers, some of which we have tried to capture in this whitepaper. Next generation AAA systems require extensibility, programmability, workflow support and multiple concurrent authentication techniques used simultaneously in the same user session. Policy definitions, Subscriber Managers like HSS, and Rule based engines to realize specific business logic are becoming increasingly important. Service Providers need to consider these features when evaluating AAA solutions in order to be able to remain competitive and future proof in this age of rapidly changing technological market-place. Furthermore, due to the complexity of Authentication techniques, meeting the scalability and performance requirements has also posed significant challenges. A good AAA solution must scale to large number of users and devices in a cost effective manner as the Service Provider's business grows in size. Meeting this requirement due to the increasingly complex use cases, some of which have been highlighted in this paper, is a tough technological challenge for AAA solution vendors.

About AdvOSS:

AdvOSS is an emerging B/OSS and Switching vendor that offers core-to-edge Billing, AAA & Call Control products to diverse range of Communication Service Providers (CSPs) across the globe. It provides customizable, scalable and cost effective solutions that add value and reduce overall operating expenses of Telecom Operators & CSPs.

More than 400 medium size customers and many Tier 1 telecoms in 40 countries rely on AdvOSS products for their business. This includes leading Operators like Wateen Telecom (Warid Telecom Group), Qatar Telecom, Orascom Telecom and many other CLECs and Carriers.

For more information, visit our website www.AdvOSS.com or contact us at sales@AdvOSS.com