Deliver. Manage. Charge.

AAA Authorization: New Use Cases

An AdvOSS Solution White Paper

Authors: Farhan Zaidi and Fawad Pasha

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

www.advoss.com/resources/whitepapers/aaa-authorization-new-usecases.pdf

For more information, contact sales@AdvOSS.com

Introduction

Authorization has been a key function of a typical AAA server since the early days of Internet Service Provider (ISP) networks and also in prepaid scenarios of voice service networks. Authorization was used after Authentication to authorize the use of service before service delivery started.

Authorization was typically integrated with a charging engine and was supposed to ascertain that enough credit was available to start the service delivery and to make sure that Service Delivery stopped when the Subscriber ran out of credit. In Post-Paid scenarios, it was usually possible to totally skip authorization all together.

In recent years, we have seen explosive growth of multi-service telecommunication scenarios where converged voice, video, text messaging, and data services are now offered in a variety of prepaid, postpaid, wired, wireless, mobile, fixed and nomadic scenarios. To complicate matters further, new applications have emerged which run inside the data pipes and require a minimum level of Quality of Service (QoS) and Quality of Experience (QoE) for the users to maintain a satisfactory level of service. These are so called Over-The-Top (OTT) applications. Examples include Skype, Youtube, googletalk to name a few.   These changes in the trends when coupled with smart-phones and other smart devices on the subscriber side have put complex requirements on Authorization feature in a modern AAA solution. New generation AAA Servers are now expected to do lot more than integrate with Charging Engine and authorize pre-paid credit. In this whitepaper, we present some new representative business use cases that require support via the Authorization feature in new generation AAA platforms. In fact, now Authorization is not merely a feature; it's a full-fledged application that needs to handle complex business logic for different use cases of multiple and converged service scenarios. In this paper we use the term Communication Service Provider (CSP) loosely in the sense that it covers both; network operators as well as providers of application and other services.

Re-Authorization and Quota Reservation

The most basic authorization scenario that the AAA now needs to support is prepaid charging. This scenario has changed in recent years due to the maturity and advancement of business models. Let's take the example of voice service. Previously, Authorization was performed only at the start of a voice call. The AAA client embedded in the Soft-switch would send a AAA request when the user dialed a number. The AAA server would check the caller's credit status in the subscriber database, divide the total credit (in monetary units) by the destination's per minute rate in a rate-sheet applicable to the subscriber, and return the number of time units available for which the call could go on. This scenario, although simple had some sever limitations. The customer would not be able to make another call from the same origin if one call was already in progress. This may be required in several enterprises PBX, customer call center, wholesale voice and other multi-tenant applications and even OTT applications scenarios where we are now talking about fixed mobile convergence and so on. This severe limitation hampered CSPs from offering prepaid services in many cases.

To overcome this limitation, AAA standard protocols like Diameter have emerged that require the AAA client to re-authorize the session when the granted units have expired. RADIUS protocol has also added support for such re-authorizations. In the first authorization, the client is given units which are equivalent of a small chunk of the total available monetary credit of the subscriber. These monetary units are reserved by the quota manager module in the subscriber's session. The quota manager and session manager modules are usually part of the Authorization application. When these units expire, the client sends a Re-authorization request. At this request, the previously reserved units are debited from the subscriber's balance according to the rate applied while reserving them and another chunk of units is reserved and stored in the session manager. When the call drops, any unused units from the last reservation are refunded or credited back to the subscriber's account. Complexities may arise in this scenario when the rates to e applied during each reservation cross off-peak/oon-peak hours, or some other rating charging policy needs to be dynamically applied mid-call that may affect the rate or the number of units to be reserved. All this complexity is handled by an advanced Authorization application in a modern AAA platform.

To realize this use case, the following are the technical requirements for a AAA solution.

Technical requirements:

- Unit Reservation Application
  - This application is integrated with the rating and charging engine. It performs API calls into the charging engine to arrive at the correct units to be reserved, stores the reserved units in the ongoing subscriber session, handles policy driven decisions if rates or number of units reserved need to be changed and so on.
- Real-Time charging
  - A sophisticated rating and charging engine that exposes modular APIs is an important requirement to realize this use case.
- Policy manager
  - On each authorization event, the AAA server may need to query the policy manager for any action related to a change in reserved units or rating/charging scenario driven by policy rules. If the policy manager replies with an action, for example, to update subscriber's reserved units, the AAA carries out that action. A sophisticated policy manager with a rule based engine to specify policy rules on subscriber related data e.g. subscription details, profiles, quotas and other parameters related to rating and charging control is an essential part of today's advanced AAA platforms.
- Session Manager
  - The AAA server needs to keep track of the reserved units; consumed units based on both time and volume provided by the network elements and maintain that

information in real-time user sessions. Therefore, session management with tracking of usage is a fundamental requirement of a modern AAA solution.

Concurrency Authorization

As we have already seen in the previous use case, CSPs may need to control concurrency of sessions for subscribers. As an example, in a data service, a CSP may want to restrict one subscriber account to use one simultaneous session. On the other hand, in some cases, they may want to allow multiple user sessions per account where user sessions may be sharing Customer Premises Equipment (CPE) or devices, such as in family plans, multi-tenant and corporate environments. However, in such cases as well, they may want to limit the number of simultaneous subscriber sessions to a certain maximum. Authorization application must be able to perform such concurrency checks and maintain the real-time information in a session manager.

To realize this use case, the following are the technical requirements for a AAA solution.

Technical requirements:

- Home Subscriber Server (HSS) or Subscriber Manager (SuM)
  - This is the main data repository of the subscribers and subscriptions. It contains values of concurrency limits for subscriber sessions among many other attributes related to AAA applications.
- Session Manager

Request Authorization

When subscribers use a particular service such as voice, video, gaming, Internet access, messaging etc. they usually make a request to use the service. As examples, a voice caller would dial the desired destination, an Internet service user would type in a URL to access a web-site, an Instant messaging user would connect or send message to a target destination etc. Sometimes, CSPs may also like to control the points of origin of subscribers invoking a particular service. As a typical example, a subscriber may not be able to access Internet service from a particular area if CSP has placed restrictions on mobility of subscribers. Similarly, a voice caller may not be allowed to dial certain destinations if he is calling from a particular set of area codes. Furthermore, in next generation networks like IMS (IP Multimedia Subsystem), services will be addressed using URLs, for example, to invoke HD voice, a subscriber may type a specific URL.

In all these cases, CSPs may have plans, packages and service offerings in place that have associated lists of origins and destinations with them and that may allow/disallow and control access to target destinations, URLs, area codes, countries, points of origin etc.

To realize such use cases, the following are the technical requirements for the Authorization application of a modern AAA solution.

Technical requirements:

- HSS or SuM
- Zoning and group management of origins and destinations
- Policy manager having rules related to zones and groupings

Capability Authorization and multiple services

A subscriber may invoke multiple services during an ongoing session. Each subscription that a customer purchases may have multiple services as part of it and each service, or combination of services may have sets of capabilities with them. A subscriber may be allowed to change or add/remove services mid-sessions too. Examples include making a voice call during an ongoing data session; adding video to a voice only call, starting an interactive chat/collaboration session during a data or voice session etc. A subscriber must access and use services based on her subscribed service offerings and plans/packages. All of these service access scenarios require authorizations and re-authorizations of services and service flows both in the beginning and middle of a subscriber session.

To realize such use cases, the following are the technical requirements for the Authorization application of a modern AAA solution.

Technical requirements:

- HSS or SuM storing subscription information and profiles for different services
- Policy manager having rules related to capabilities and multiple service invocations

QoS and QoE Authorizations

CSPs may have service offerings based on different Quality of Experience (QoE) and Quality of Service (QoS) levels. QoE deals with end to end and overall service experience by a subscriber when using the service. Examples include the latency experienced when changing the channels quickly in an IPTV session, waiting time in a customer call center etc. QoS on the other hand deals with the provisioning of service parameters in different network elements that deliver the service so that they could discriminate between different types of services at different priorities. Examples include giving priority to voice and video traffic over normal Internet browsing, reserving bandwidth and other resources for delay and throughput sensitive applications etc.

Usually, QoS settings at various network elements combine together to give a desired QoE. Many networks elements provide capabilities for efficient traffic management and separation.

This allows CSPs to support prioritized traffic such as VoIP and Video calling, granular control over torrents and other specialized traffic while browsing. This type of granular control necessitates authorization of services based on desired and configured QoS for subscribers, thus enhancing the QoE and enabling the service provider ability to charge for premium services based on different QoE levels and their associated Service Level Agreements.

To realize such use cases, the following are the technical requirements for the Authorization application of a modern AAA solution.

Technical requirements:

- HSS or SuM storing subscription information and profiles for different QoE and QoS levels and the SLAs associated with service offerings
- Policy manager having rules related to QoS and QoE levels and associated SLAs

Terminating or vendor side capacity control

Many services by their nature require connecting or passing the traffic through to destinations or targets. Network elements act as intermediaries in this case and route the traffic through to other third party vendors that are supplying part of the service as a terminating end-point. The role of the CSP is usually that of a middle-man so to speak in such business models. Examples include routing voice traffic to destination switches, sending instant messages to destination messaging service providers, routing gaming traffic to suppliers of gaming service, content providers for video on demand services etc.

In all such cases, the destination vendor or the so called terminator of service may have certain capacity in its network, beyond which it may have problems handling the incoming traffic. The CSPs would therefore, like to control the traffic sent to their terminators or third party providers by sending only traffic within the limits of the service level agreement they have with the specific third party provider.

To realize such use cases, the following are the technical requirements for the Authorization application of a modern AAA solution.

Technical requirements:

- Third party service providers module that manages their SLA and capacity information
- Maintenance of real-time information about the terminating side current capacity for each vendor

Conclusions

Converged and multiple services coupled with OTT applications are opening new doors to service providers for creating innovative business models and revenue streams. They can now offer several differentiated service offerings and bundled service packages due to the enhancement in capabilities of network elements in terms of QoS levels and thus improve and differentiate between different QoE levels for the same service. However, these new dimensions to service offerings have posed new challenges for AAA platforms that sits at the core of the CSP domain today. AAA servers are not mere servers now, neither are Authentication, Authorization and Accounting merely features of a monolithic application as they used to be in traditional AAA servers. Now, AAA is a complete service management platform with separate applications for Authentication, Authorization and Accounting. These applications need to run complex business logic in collaboration with several other modules and subsystems of this platform. Authorization of services is a key component application of a modern AAA solution with has to deal with and realize several complex use cases for CSPs.

We have tried to cover some representative use cases in this whitepaper along with the identification of the modules required to realize those in a typical modern AAA platform. The cases covered are however, not exhausted by any margin. New and more advanced business cases are emerging as CSPs launch new services, mixing them with existing ones and creating even more differentiated and attractive service offerings and revenue streams. Authorization will definitely sit at the heart of all such scenarios in the emerging next generation all IP networks such as LTE and IMS.

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