VIRTUAL EXPERIENCE
OCTOBER 11-14

2021 Fall Technical Forum
SCTE • NCTA • CABLELABS

Cable and Wireless Subscriber Management Convergence

A common approach to Identity Management

A Technical Paper prepared for SCTE by

Pablo Stalteri
Master Solution Architect
Hewlett Packard Enterprise
Mississauga ON, Canada, L4W 5G2
pablo.stalteri@hpe.com

Table of Contents

List of Figures

List of Tables

1. Introduction

Most operators offering Cable and Wireless services have been implementing their Operations Support System (OSS) platforms using a silo approach, where different access technologies and business units resulted in the deployment of dedicated systems. Thus, to support wireline, broadband, cable TV, IPTV or wireless services, for residential or enterprise customers, multiple Billing, CRM, subscriber and identity management systems are being deployed. Furthermore, technology evolution and tactical execution methodologies when launching new services have contributed to produce different subscriber identification flows for the authentication and authorization required to access each service, as well as a plethora of subscriber data bases and data sources focused on solving the associated entitlement problem. Then the Cable and Wireless operator end up managing and maintaining multiple systems performing similar functions, with increased OPEX, offering different experience to the end customer depending on the service to be used.

In the next paragraphs we will describe the Subscriber Management Convergence solution that has been implemented in North American Triple and Quad Play operators, offering a virtualized consolidated 360-degree view of the subscriber profile for any type of access technology, type of device or type of service offered, encompassing both enterprise and residential customers, making use of legacy data sources to avoid the need of costly migrations.

2. Subscriber Management Convergence Solution

In the telecommunications market every operator tries to differentiate from competition by offering new services to their customers in the hope that they will adopt them if there is a real benefit for the subscriber and user experience is consistent with services already purchased. Most of the times, the real benefit is measured in terms of cost, and for that purpose operators try to bundle the new service with others the subscriber already has, to offer a cross-product discount, but this bundling is sometimes difficult to do from the OSS systems perspective, as there may be a subscriber database for Wireless services, another for Cable and another for Wireline services, making impossible for the operator to link all services of the subscriber during purchasing time. We have seen time and again cases where the CSP has defined an Account for Wireless services, another for Cable and another for Wireless, joining all this information together only during invoicing time, so the end customer receives only one bill. Therefor cross-product discounts are generally limited to services within the same technology: Cable services only (if you have HBO and Netflix service, then bundle package includes x% discount), or Wireless services only, etc. This silo approach ends up penalizing the customer that uses different access technologies, and so the real benefit is not materialized.

With regards to the end user experience, this one is also difficult to implement when the operator has different subscriber databases for each technology and business unit (residential, enterprise), as query entitlements to indicate if a particular service can be used by the subscriber generally

provides specific information associated to the silo that has been reached, without a full view of all services the subscriber has, and the application receiving this data differs from one another depending on the type of device the subscriber is holding. Some of these device applications require user identification and passwords to grant access, which are difficult to remember and maintain by the end user.

Some operators have tried to overcome these issues by consolidating all subscriber profile data into one big database, taking months and years to migrate data from legacy systems to the new one, which added to their OPEX and slow down the speed to which new services can be launched to the market. In these cases, changes done on legacy systems, such as Product catalogue QoS upload/download bytes, service monthly usage limit, throttling, etc, must be replicated in the centralized DB in a timely fashion to ensure consistency, adding complexity to the solution.

These challenges can be summarized as follows:

1. Integrate Subscriber's Data and Entitlements of all users, from cable, wireline and wireless into a single platform. Store identifiers available in user devices
2. Changes done on legacy systems (such as Product catalogue QoS upload/download bytes, etc) must be immediately available to external applications

Subscriber Management Convergence solution provides an answer to each of these requirements, by increasing flexibility in the creation of new services and fast integration with legacy data sources, without the need for long migrations or data consolidation implementation. The concept is based on "use the data that you already have" from legacy applications, accessing subscriber information via user equipment identifications readily available, and presenting each external application the data they need so that end subscriber always has the same user experience. The main advantages of this approach are:

- Abstracts data models from external applications, offering dedicated views to each of them
- Supports entitlement queries for all type of subscribers: cable, wireline and wireless
- Flexible business logic enabling sequential and/or parallel requests to data sources
- Easy integration with legacy data bases and platforms, with more than 100 protocols available
- No need of data consolidation or data migration
- Adaptable to Operators ecosystem: no impact on existing applications or legacy systems

The solution is based on two products that are integrated using 3GPP protocols, deployed in a virtualized environment and benefits from a micro service architecture, to pave the way to 5G implementation.

- **Data Federation** allows applications to query account, subscriber, service and device information from a set of downstream data sources, being the main one Unified Identity Repository (UIR). It federates external data sources via different protocols, to build a **consolidated XML response** and supports AuthN and AuthZ to allows the subscriber to access premium content (Entitlements)
- **UIR** provides an LDAP database which stores identification values (keys), that are used to access legacy data sources to obtain detail information

The outcome can be summarized as follows:

- Rapid adaptation to new business cases
- The data federation **abstracts query requests** so that applications do not need to care about data models and/or where data is retrieved
- Reduce implementation and maintenance costs: single platform across all access types, business units and services
- When legacy IDs are maintained, service catalogue **changes** are **reflected immediately**

3. Solution Architecture

Figure 1 shows the generic LDAP subscriber profile data model that has been implemented in several Quad Play operators using UIR.

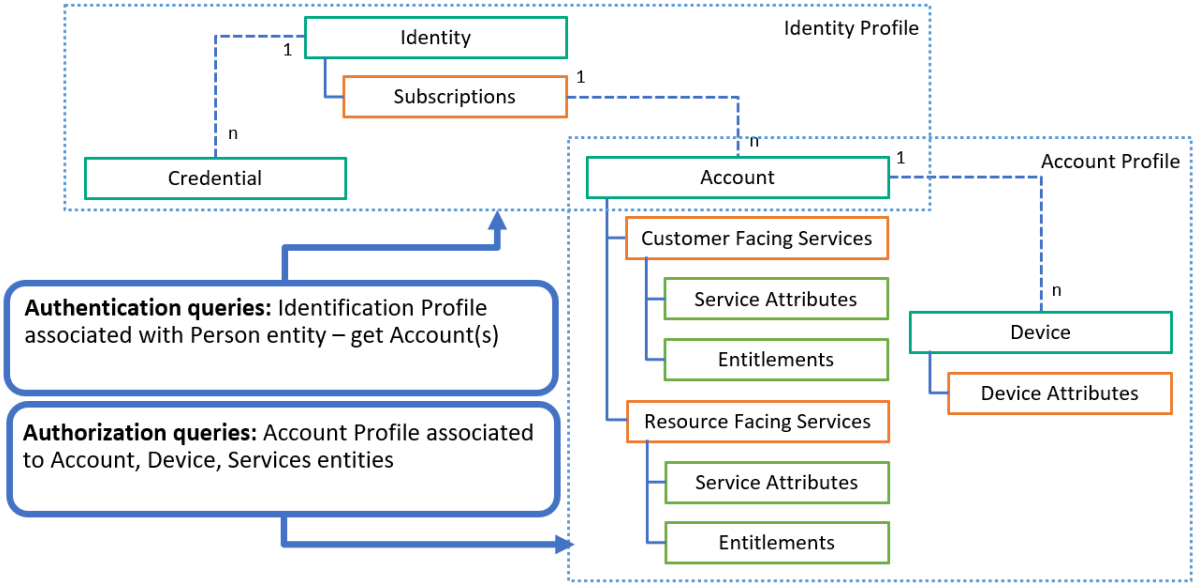


Figure 1 - UIR – Subscriber Profile Data Model

For every subscription, there is an Identity profile, storing different credentials, and an Account profile, which can be made up of multiples accounts (one for Cable, another for Wireless, another for Wireline, etc), which are keys to the corresponding legacy OSS systems the operator has. LDAP ensures the extensibility of the data model and we have found that it can adapt to the realities of any type of CSP.

The Identity profile is used in entitlement queries submitted by external applications, such as Video On Demand, wireless application or WiFi, to authenticate the physical subscriber (person) using a key that is provided by the device used. Thus, in the case of cable this can correspond to the MAC Address of the Set top box, IMSI for wireless, eSIM for Tablet, etc. In this way the subscriber does not need to memorize any userid / password to access the service: the device itself provides this key automatically when the service is selected. The result of the authentication query is the Account number.

The Account profile is accessed via the Account number previously retrieved for the authorization query, which with the input of type of service accessed and device used, allows to validate if the subscriber is entitled to use the service/device. Please note that in one account you may have multiple services (each one with several instances) and allow several types of devices/instances. Examples:

- A wireline Account may have Internet service, IPTV service, Digital TV service, Home Phone service, Home Alarm service, etc.
- A wireless Account may have Share data plan service made up of 2 smartphones (father-mother), each one with each own MSISDN, one Individual data plan service (son) with another MSISDN, etc

- Devices can be classified into access device (i.e GPON, FTTH, etc), consumer devices (set up box, smartphones, smartwatch, tablet, etc), each one with its own instance ID

The second component of the solution, Data Federation, is implemented in a layered architecture to provide flexibility in the northbound and southbound interfaces, as displayed in Figure 2. It consists of:

API Broker Layer

Logical component that hosts one or more API broker components. It provides HTTPS/REST based interfaces to which North Bound applications can authenticate, connect and query the system

Business Logic Layer

Based on API request type it triggers the flow selecting the Data Sources to consolidate the dedicated response:

1. Flow execution order in which each corresponding query needs to be executed according to business logic
2. Query in parallel and / or sequential order the different Data Sources using the appropriate protocol
3. Receive response from all Data Sources and keep them in memory
4. Compose all answers into a virtual data model to create the XML response (Payload)

Data Source Layer

Set of out of the box connectors to interface with each Southbound Data Source (ex. LDAP, JDBC, WebServices, HTTP/REST, SOAP/XML, etc) to acquire relevant information from keys retrieved from UIR and / or external data sources.

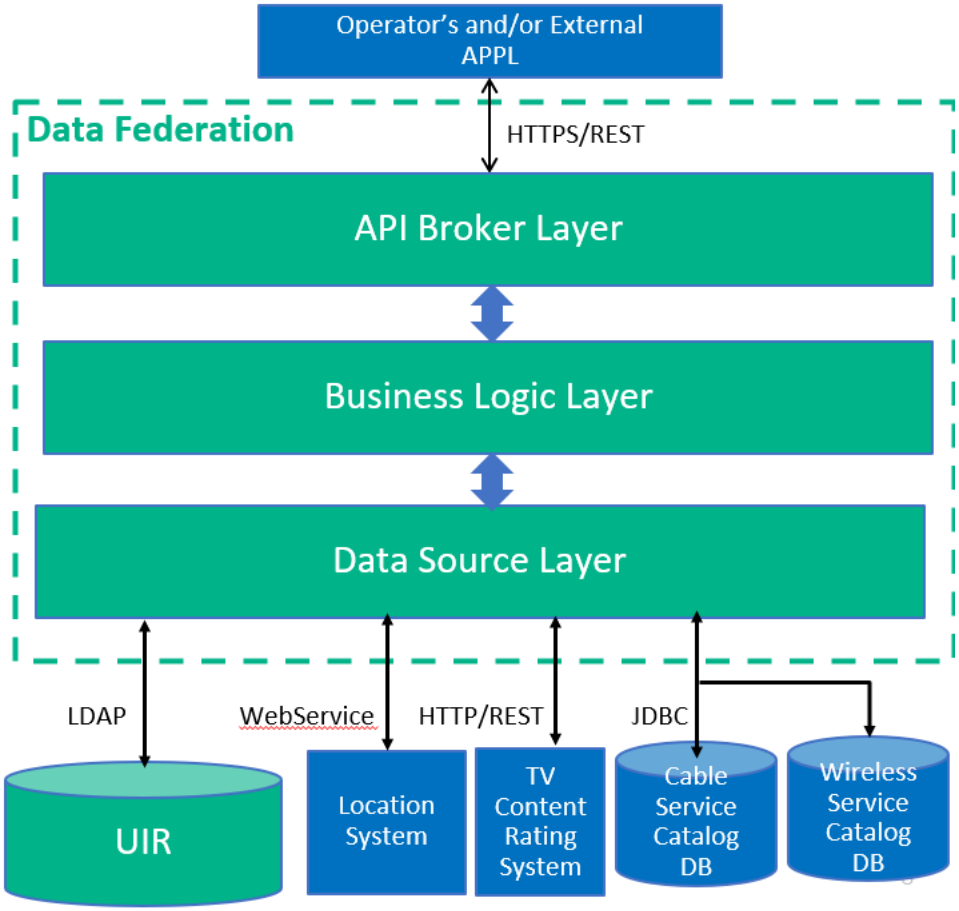


Figure 2 - Data Federation Architecture

It is important to mention that Data Federation is built using micro services technology provided by the enhanced Interactive Usage Manager (eIUM) platform. The rich set of out of the box connectors give the desired flexibility in both northbound and southbound interfaces, while its library of java classes provides the foundation for the business logic layer. Each of the layers are easily configurable, adapting to the realities of each operator in a matter of weeks. The Figure 3 presents an example of API implementation for Cable Enterprise application. Please note the sample list of external applications, some of them from the operator, some from partners (such as content partners), which make use of the authentication and authorization flows supported by the combination of Data Federation and UIR.

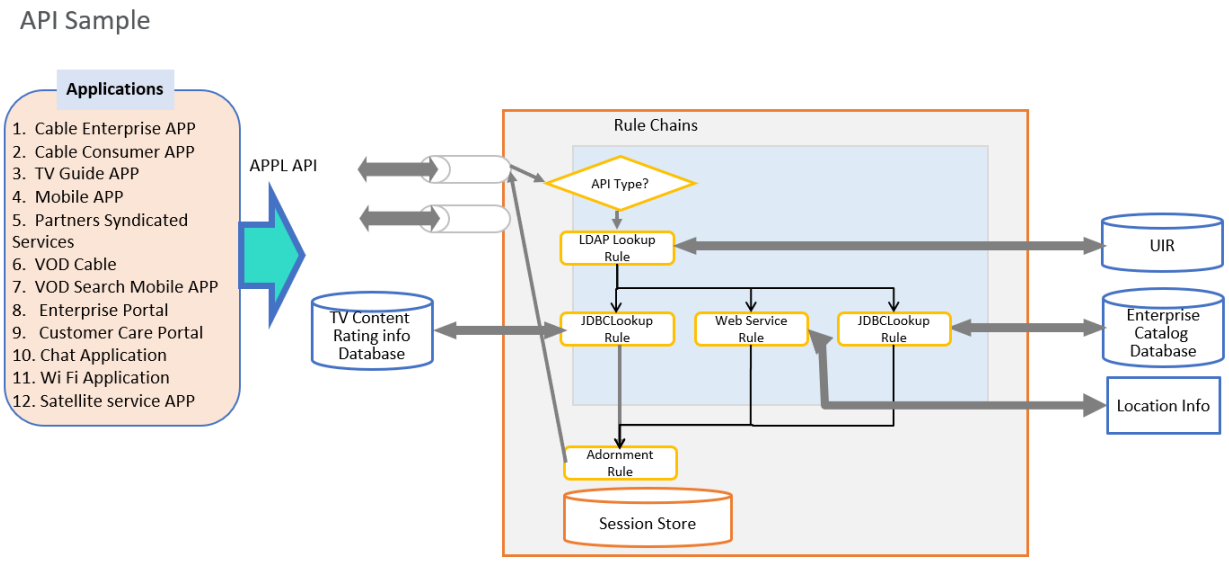


Figure 3 - Data Federation – API Sample

UIR data is populated automatically by the different legacy provisioning systems of the operator, using LDAP protocol. However, we have implemented in the Data Federation business logic layer of one CSP the ability to auto-provision new services in UIR if certain eligibility criteria are fulfilled for the same Person (Identity Profile), allowing cross-product discounts and loyalty programs. The case in question required to provision the entitlement to access for free a specific Sport channel from any wireless device if the subscriber has Service 1 (Wireless Data Plan of 10GB), Service 2 (Internet with no data limit), Account is active and residential and lives in states X,Y,Z. Please note that none of the legacy systems in the CSP were able to register this condition, as they were deployed with the typical silo approach, and only in UIR the operator was able to see for the first time all services the subscriber has purchased, and so offer a new service for free to create stickiness. This auto-provisioning is triggered by the provisioning of any Service 1, Service 2, Account update and/or location update.

4. Features

Data Federation key features are:

- Real Time Protocols for both Northbound and Southbound interface: HTTPS, REST, SOAP, JDBC, LDAP, Diameter, RADIUS client/server/proxy with advanced access control, TLS support
- Messaging format supported: XML, JSON, HTML
- Supports synchronous and asynchronous requests for both northbound and southbound interfaces
- Onboarding of Consumer Applications: Who access What attribute with What API

- OOB GUIs: Data Modelling Studio, Configuration Editor, File Service Workflow, Rule Chain Visualization, App Deployment Visualization, Operations Console, Deployment Manager, O&AM Workflow, Common Codec Framework
- NFV ready and cloud scalability: Level 3 Scale in/out
    - Dataless Micro service architecture, paving the way to 5G and Wi-Fi 6
    - VNF Manager (new component for NFV/MANO integration) and O&AM Workflow
    - EMS Management enhancement: NFV Templates and Operations Console Extensibility
    - Load Balancer for Real Time
- Management enhancement: statistics threshold with alarm, resource utilization chart, SNMP v2c and v3 support, Management HA support
- Reference Data Manager and Services enhancement: extend control for admin to manage reference data that drives business logic, advanced querying and caching

In addition, Data Federation provides optionally an Access Feature including the following two functions:

- **Access Control:**
    - Allow only **trusted clients/applications** to access UIR DF by providing mutual authentication using HTTPS Two-Way SSL
    - Authenticate and Authorize the users accessing UIR DF by checking against its LDAP database where user information, credentials and user's **access control list** (user, roles and privileges objects) data is stored
    - Provide **secure communication channel** between the clients and UIR Data Federation platform: TLS 1.2
- **Access Filtering:**
    - Ability to include service types / privileges / instructions as URL parameters, which enable a client to ask for a subset of the data that it is entitled to (e.g. {BASE_URL}/{RELATIVE_PATH_TO_ACCOUNT_VIEW}?pname=qamTV&pname=xyz)
    - Ability to include instructions, as URL parameters, which request UIR Federation to ignore one or more external data sources (e.g. {RELATIVE_PATH_TO_ACCOUNT_VIEW}?pname=qamTV&pname=xyz&exclude=LOCATION_SYSTEM&exclude=TV_RATINGS)

Access Control function:

- Allows only **trusted clients/applications** to access UIR DF by providing mutual authentication using HTTPS Two-Way SSL
- Authenticates and Authorizes the users accessing UIR DF by checking against its LDAP database where user information, credentials and user's **access control list** (user, roles and privileges objects) data is stored

- Provides **secure communication channel** between the clients and UIR Data Federation platform: TLS 1.2

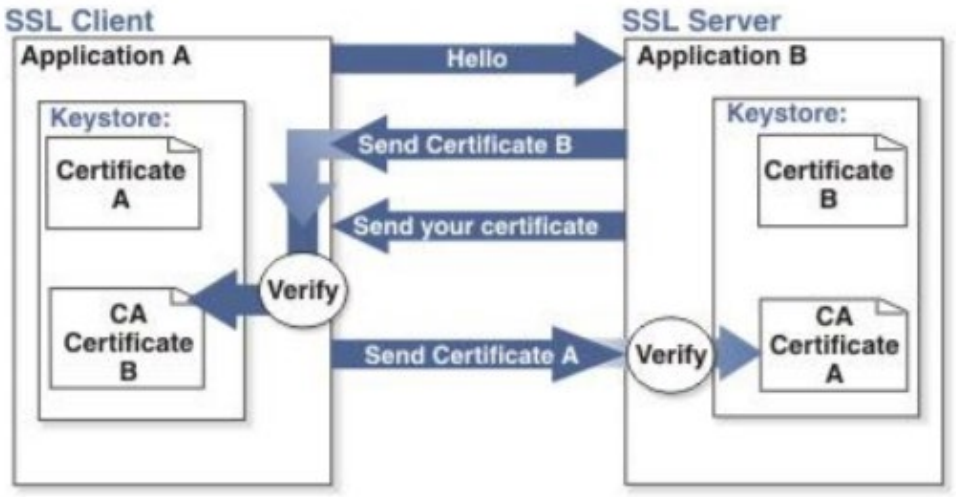


Figure 4 - Data Federation ACL Feature

Data Federation internally will leverage UIR LDAP Database where the Access Control List for a User is stored. The Access Control list would consist of User Role and Its Privileges and other artifacts. Data Federation will provide only those information elements to a user allowed by Access Control List, using the data model shown in Figure 5.
Data Access is enabled for the Account View to:

- Access to services, by type.
- Access to Service attributes, by name
- Access to Devices, by type.
- Access to Device attributes, by name
- Access to Person Role Map. By Id

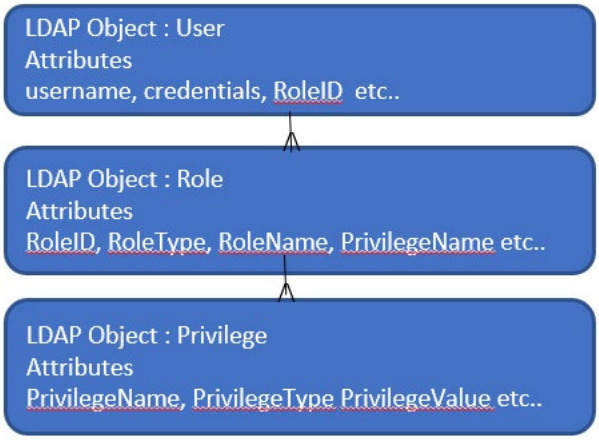


Figure 5 - Data Federation Access Control Data Model

5. Sample Deployment

This section describes a production implementation of the solution in one Quad Play operator in North America with 3 Million Subscribers. Here different provisioning, CRM and billing systems are implemented, for Cable, Wireless and Wireline access technologies, with dedicated flows for residential and enterprise customers. The main goal was to provide to any external application a consolidated view of the subscriber profile, accessed using different keys. Depending on the entitlement query type, defined by the external APP, a different view is presented.

Table 1 - Performance Metrics: Operator with 3M Subscribers - Payload

View	Average TPS	Max TPS	Average Response Time (ms)	Payload size
Account Lite View	5	80	75	Average – 405KB
Account View	19	300	200	Max- 3.3MB
Person View	7	20	10	Average – 1KB Max- 30KB
Mobile App View	4	73	188	Average – 2.5KB Max- 8KB
TV Guide View	9	290	200	Average – 18KB Max- 224KB
VOD Auth View	24	47	140	Average – 3.5KB Max- 17KB
Wifi View	2	26	2	Average – 1.3KB Max- 5KB
TOTAL	**70**	**500**		

As indicated in Table 1, two Account views were implemented, as there are APP that only require a "Lite" version of the account, indicating list of accounts associated to a subscriber ID, while the other version (called "Account View" in the table) lists all accounts, for each account all services and devices, for each service all instances, for each device all instances, etc. Therefor you can see that the payload for this full view is quite high, up to 3.3MB, and its data is retrieved in an average of 200 milliseconds. On the other side of the spectrum, you have the WiFi Application, that is just concerned about QoS associated to the subscriber, and so payload is just 5KB maximum. The platform was sized for 500 TPS queries, measured from the northbound interface, and each query can trigger multiple queries to the UIR, which in turn, according to the business logic of the entitlement query selected by the APP, can query one or multiple external data sources, some of them using JDBC protocol (i.e Oracle DBs), or webservices, for location information.

Figure 6 displays UIR LDAP reads and writes over time, where the number of TPS for reads is greater than the northbound entitlement requests, as the first query to LDAP is associated to Authentication, and the second and onwards with Authorization to retrieve details of the account, service and device.
Provisioning requests, coming from legacy systems, are classified into Inserts (ADD), Updates (MODIFY) and Delete (DEL).

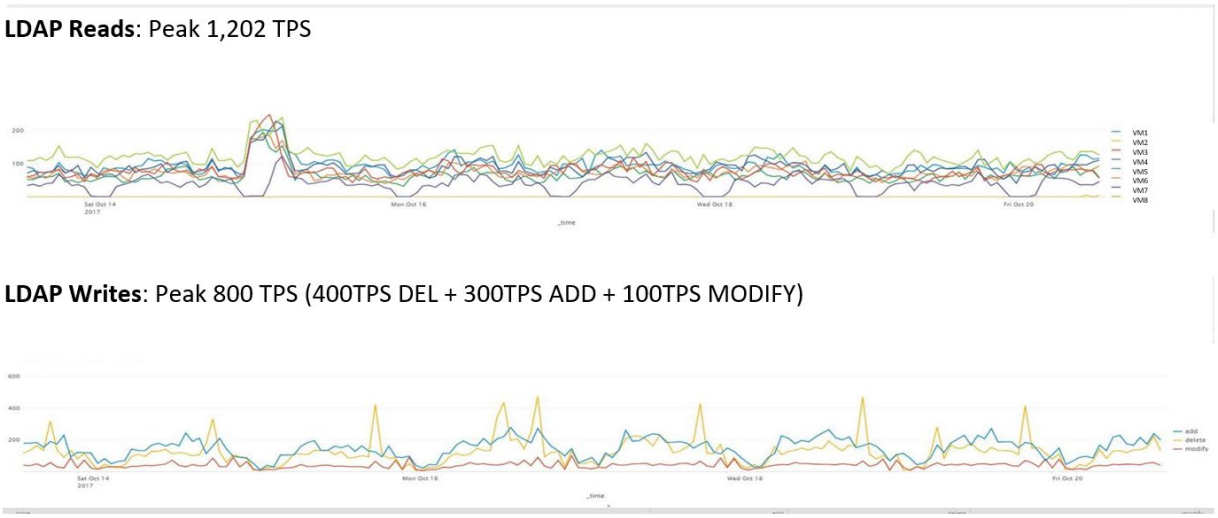


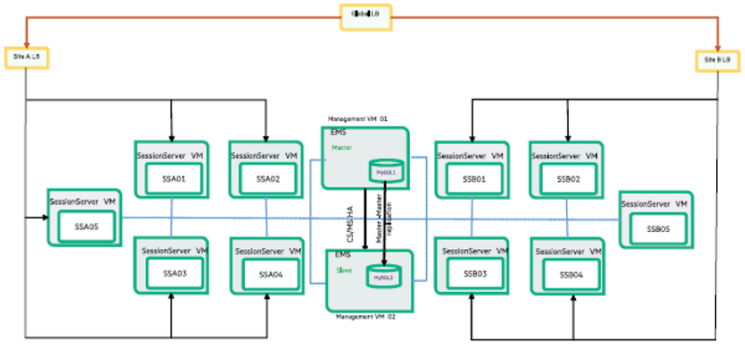
Figure 6. Performance Metrics: Operator with 3M Subscribers – LDAP

Finally, Figure 7 details the production deployment in two identical sites, where each site has five Virtual Machines with Data Federation, each one supporting up to 100 TPS query. The EMS component in each site is made up of an Operations Console, a web-based application designed for operators who need to monitor and manage micro services deployment on a daily basis. Among its capabilities, it can give you an at-a-glance, global view of the health of your deployment, view and monitor all the processes, as well as alarms and problems with your processes. You can also use it to create process groups for easier monitoring and management, and view history charts to show process activity over time. Operators can also perform routine

management operations, for example, starting and stopping processes and groups. The Operations Console also provides role-based security to limit operations capabilities for different users.

- Two identical sites
- Each site with 5 Session Servers VMs and 1 EMS VM, supporting up to 500TPS query
- Each VM with one Session Server containing the 3 layers: API Broker, Business Logic and Data Source Layer

	vCPU	vRAM (GB)	Disk (GB)
VM supporting 100 TPS	8	16	200
OS	RHEL 7.5 (x86-64)		
Hypervisor	VMWare		



• Multi site deployment is achieved with built in HA, that is, there is no need for third party clustering software (i.e. Red Hat Clustering)

• EMS: Single Config Server (CS) and Management Server (MS) run on HA mode with a replicated master-master MySQL database

Figure 7. Sample Production Deployment: Operator with 3M Subscribers

High availability is achieved by having each real time component (called Session Server, in eIUM) in active-active mode in both sites.

6. Conclusion

This paper described the HPE Subscriber Management Convergence solution, which leverages existing legacy data sources and streamlines the identity management process to produce a consistent customer experience across different access technologies and services involved. The solution introduces a centralized Subscriber Profile and Identity Repository along with Data Federation capabilities, so that when there is a need to check the authorization of a customer accessing a specific service from a particular device and location, this entitlement information can be retrieved from a single point. In addition, the authentication flow required to access the service will use the data already provided by the device making the request (i.e. IMSI in smartphone, eSIM in tablet, etc), without the need for the end customer to introduce user id and password whenever possible. These two improvements result in a better customer satisfaction and fast time to market to launch new services.

Abbreviations

HPE	Hewlett Packard Enterprise
CTG	Communication Technology Group
eSIM	Evolved Subscriber Identity Manager
eIUM	Enhanced Interactive Usage Manager
DB	Database
HTTP	Hypertext Transfer Protocol Secure is an extension of the Hypertext Transfer Protocol. It is used for secure communication over a computer network, and is widely used on the Internet
IPTV	Internet Protocol Television
JSON	Java Script Object Notation
REST	Representational State Transfer. Simple HTTP-based protocol that enables to contact the message broker through a Web browser
LDAP	Lightweight Directory Access
OPEX	Operating Expenses
OSS	Operation Support System
SOAP	Simple Object Access Protocol specification for exchanging structured information in the implementation of Web Services
TPS	Transactions Per Secong
UIR	Universal Identity Repository
XML	eXtended Markup Language

Bibliography & References

(1) HPE eIUM UIR Data Federation Delivery Guide

(2) HPE Universal Identity Repository Overview Manual

