Mobile Operators as Identity Brokers

Ajit Raghavan
Technology & System Management, BUSS R&D
Ericsson India Global Services
Gurgaon, India
ajit.r.raghavan@ericsson.com

Kirti Girdhar
Technology & System Management, BUSS R&D
Ericsson India Global Services
Gurgaon, India
kirti.girdhar@ericsson.com

***Abstract* — In this paper, we discuss how a mobile communication service provider (Mobile Operator) can act as an intermediary between the end user and the digital service providers. This enables a more trustful relationship between the end user and service provider, and brings out compelling value. In addition to being a trusted broker, a mobile operator can also provide various value-added services to the end users and service providers.**

Keywords - Telecommunication; Digital Services Over the Top; Online Services; Identity Management; Identity Federation; Digital Identity Profile; Ease of Use; Security; Circle of Trust; E-commerce; M2M

I. INTRODUCTION

In a connected society, where a significant number of applications and services are available over the Internet, a user is faced with daunting challenges of maintaining multiple identities for various services. Usually, every application or service requires some authentication and establishing the identity of the appropriate user. It is done with an identity coupled with a password.

A user needs to maintain identities for each of the applications. However, there is a drawback in this approach. The end users tend to reuse the same identity and password across all services, which make them vulnerable to risks of identity thefts or identity pilferage.

In future, it is expected that the number of the services is going to grow exponentially [1]. It will be difficult for an end user to manage identities across all the services. In addition, the increasing number of devices associated with the user (for example, connected cars or home security systems) is also going to magnify these identity management problems.

Digital services like online banking or trading, require a secure identity establishment. However, digital services like e-mail or social networking need basic identity establishment.

For all the digital service providers, it is a big challenge to maintain and establish the identities of their users.

In this paper, we discuss how the mobile operator can act as an intermediary between the user and the service provider. It enables a more trustful relationship between the end user and the service provider. For example, it would be great for an end user to use single identity across mobile networks, Wi-Fi hot spots, broadband, utility, or cable TV. If mobile operators are able to provide an identity brokerage service between the end user and their service providers, it will help them monetize the brokerage services as well as increase the loyalty of their end users.

There are some initiatives ([2][3][4]), where mobile operators are playing a global identity provider role. This paper leverages on these initiatives, and presents how mobile operators can provide more compelling value to end users and service providers.

This paper talks about:

- The previous work done on identity management.
- The future requirements and actors in value chain.
- How mobile operator can provide identity broker services and other value added service.
- The challenges mobile operator's may have.
- How end users can be subscribed to the services provided by a mobile operator.
- The solution framework and its components.
- The case studies and the conclusion.

II. BACKGROUND

Many service providers allow subscriber authentication using popular service provider identities, for example, Facebook, LinkedIn, or Google account. This concept is known as Identity Federation. It enables end users to reuse their existing identities without registering to every service provider. There is a lot of work done towards standardization of the identity federation with protocols, such as, Security Assertion Markup Language (SAML) [5], Liberty Alliances [6], OAuth [7] gaining significance. Organizations like GSMA [8] are involved in driving these standardizations.

There are few success stories around this concept; however, they still need to achieve a mass adaptation. Also, mobile operators perceive this a potential revenue stream.

III. THE FUTURE NEED

The future need indicates that number of services is going to grow exponentially [1]. However, it also indicates the following points:

- It is a pain for end users to register and maintain their identities (including identities related to their devices) across multitudes of services. It also acts as a deterrent for the end users from trying out new services unless there is a need.

 ISBN: 978-1-61208-345-2

- It is a pain for various service providers to maintain end users identity, authentication, and comply with local regulations.

Service providers have a strong requirement to differentiate between a genuine end user and a fraudulent end user.

An Identity Broker is required in the connected world, which can provide validated information of end users and service providers.

A secure identity establishment and identity exchange enables innovative use cases. For example:

- Digital voting
- Seamless access to connected devices
- Secured access to corporate Intranet or government portals

IV. ACTORS IN THE VALUE CHAIN

In the identity establishment and exchange flow, the following actors play an important role:

- End User: The subscriber of mobile operator and a digital service provider, whose identity is established before giving access to a service.
- Mobile Operator: The connectivity provider having the infrastructure available for securing the communication channel and also have detailed information about the end user.
- Digital Service Provider: The digital service provider to the end user over the Internet. It uses the connectivity provided by mobile operator to offer services.

Digital service providers need to partner with mobile operator to leverage on the assets which the operators have.

Operator's partners can be, for example, Over-the-Top (OTT) service providers, Wi-Fi hot spot providers, or Broadband providers.

V. OPERATORS AS A TRUSTED IDENTITY BROKERS AND MORE

The operators have unique position in a connected society. The operators have following capabilities:

- Verify customer information as per the local regulations.
- Contact/Billing addresses of the end user.
- Support for multiple communication interfaces like Unstructured Supplementary Service Data (USSD) [12], Short Message Service (SMS) [13], E-mail, and Voice.
- Self-care/Customer care
- Fraud management
- Established relationship with the end user.
- Charging and Billing infrastructure
- Extensive reach to the customers and dealer/agent network.
- Marketing infrastructure to enable service providers to get more end users.

The operator can leverage these capabilities:

- To act as an identity broker.
- To provide value added services to end users and service providers.
- To enable a low entry barrier for new service providers for offering their services to the end users.

It is not the identity brokerage service which is provided, but a complete bouquet of services made available to service providers enabling them to focus on best quality service delivery aspects.

The end users can enjoy a seamless and secure access to all the trusted partner services.

VI. THE CHALLENGES

The mobile operators have the following challenges:

- SIM-based Security: It is built in as part of the SIM [15] card or device, which has its pros and cons. There should be authentication mechanism for following scenarios:

Multiple devices per end user (including devices without SIM, for example, tablets, home security systems)

Shared family devices or accounts

- SIM tied to the operator: Here an end user might have multiple SIM cards from multiple operators. The challenge is how the identity brokering work is done when we have other services like Wi-Fi, fixed line, or broadband.
- Access Dependence: Connected devices may not be using operator's access network. For example, power line communications for a smart meter, home security solution over fixed Broadband, or Wi-Fi access over SIM less devices.

The proposal on how these challenges can be mitigated is discussed in the Proposed Solution Framework Section.

VII. GET END USERS SUBSCRIBED TO THE SERVICE

It is essential to get maximum number of end users subscribed to the service to enable mobile operator successfully monetize the identity brokerage service. However, there should be sufficient leverages for the end users to subscribe to the services. It will be difficult for the end users to subscribe to the services if there is no significant benefit for them.

The possible benefits which the mobile operator can provide to the end users are:

- Increased Security: No need to share personal information to multiple online services (about whom end users do not have sufficient trust level information). It protects the user from identity proliferation issues and associated threats.
- Partner Risk Score Information: Operator verifying the partner and providing a trust level score to the end user enables the end user to take good decision about the services.
- User Profile Sharing based on Partner's Risk Score and User Preferences: Risk scoring done by operator and recommending end user what to share and what not to share. User can use the trust level score and recommendations to decide his preferences for the service provider.

 ISBN: 978-1-61208-345-2

- Special Tariffs and Quality of Services for Partners: Offer end users special tariffs (for example, no charge, quota usage, or higher speeds) for specific service providers, based on the mobile operator's agreement with the service provider. For example, online retail sites, giving higher speed and priority with discounted data tariffs.
- Allowing end user seamless access to various partner services. This is a unique selling point.
- Offering a digital signature to the end user, which can be used across critical services of service provider (for example, digitally signed financial transactions).
- Provide a generic loyalty point service for all partner service providers, which offers end user to use the loyalty points across service providers.
- A simplified mechanism allowing end user to opt-in and opt-out for this service anywhere and anytime is essential. For example, at a click of few buttons on the self-care App, end user should be able to register and create different digital identities and set preferences.
- The solution should be intelligent to understand the end user usage pattern, and quickly map various existing identities of the user to the centralized identity. For example, an end user of the service trying to log in to a partner's site (for example, Yahoo) should be offered an option of mapping his local identity (yahoo id) to his centralized identity with operator.
- Agreeing with service provider to allow end users subscription with their operator maintained identity. Since the end user's access request is coming from a trusted partner (through the mobile operator's network), the service provider can identify the end user using the security token inserted by the operator as part of the access request header. For example, an end user accessing a partner bank's URL on his smart phone is automatically identified by the bank.
- Mobile operator can also act as a seamless payment gateway. Service provider sites can provide an option to end user to pay via the mobile operator. Mobile operator may provide a wallet service to the end users. Another offer can be payment through prepaid account or a postpaid bill by the mobile operator.

VIII. Required Technical Capabilities

The required technical capabilities for this solution are described below:

- Secure token exchange for seamless identity exchange with service provider. Using intelligent URL inspection, service provider site identification, and exchanging the end user profile information in secure manner as part of the security token embedded in the HTTP header. For example, scenario of an end user accessing a bank's URL on his smart phone. Mobile operator identifies this service from a trusted source, and then embeds the configured security token in the request header. The secure token also includes the required end user profile as agreed by the end user and the bank. The bank's online service will check the presence of this token, parse and verify the token with the mobile operator's secure verification services and then allow the end user access to the bank's service.
  Advanced identity federation and security platform is required to maintain the end user's digital identity profiles to authenticate and authorize, and to share the required user profile towards service provider.

IX. The Proposed Solution Framework

A mobile operator needs a collaboration platform, which enables effective collaboration between digital service providers and operators.

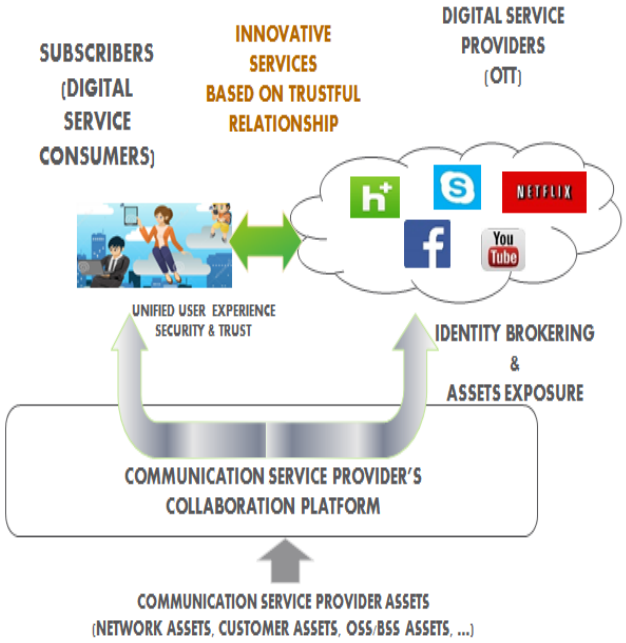

Figure 1: Enabling monetization via effective collaboration

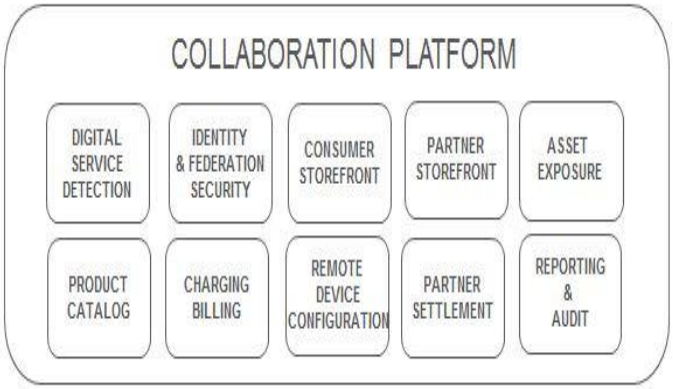

Figure 2: Collaboration Platform Functional Architecture

Collaboration platform hosts capabilities for any digital service provider to self-register at the mobile operator's site and use of the mobile operator's assets and available capabilities.

The functional architecture of the collaboration platform is shown in Figure 2. The components of the architecture are described below:

- Partner Storefront: It enables digital service providers quickly register as partners. The partner lifecycle management including agreements is handled within this storefront.
- Consumer Storefront: It enables consumers quickly browse through available products from a mobile operator or a service provider.
- Identity Federation and Security: It enables the mobile operators act as a secure and trusted identity broker and federates the identities between end user and digital service providers. It enables secure exchange of customer information such as profile, preferences, and segmentation with the service provider.
- Service Detection: It is an intelligent service detection based on URL, packet intercept, and partner identification. Based on the partner identification, a secure channel can be established where the customer profile information can be shared with the digital service provider. The profile information exchange happens using a secure token to ensure that critical customer information is not compromised.
- Asset Exposure: It is a platform for exposing the mobile operator's assets (for example, authentication, location, or charging) in a secure manner as REST-based API's. This can be leveraged by service providers to build innovative services for the end users.
- Charging, Billing and Quality of Service Control: It enables differentiated charging and special Quality of Service (QoS) for the service provider's service usage session. A specialized charging & billing platform is required which in runtime can change the QoS parameters for the data session.
- Partner Settlement: It enables billing the service provider for a value added service session and exchanging settlement files/invoices with the service providers.
- Remote Device Configuration: It enables digital service providers and mobile operators to configure the end user devices (for example, mobile phones or any M2M device) to install a digital certificate or application.
- Reporting and Auditing: It enables analysis and reporting of Key Performance Indicators (KPI) for service providers. It allows mobile operators to determine their profitable service providers and provide more incentive to them.

X. CASE STUDY

Authentication services Mobile-ID are implemented in Estonia [2]. The Mobile-ID service is built and launched by mobile operator EMT [14], which in 2009 made its platform available to the other operators (Elisa and Tele2). This was recognized as key to driving scale among users and encouraging service providers to join the service. Mobile-ID service allows a client to use a mobile phone as a secure electronic ID. Just like an ID card, it can be used for accessing secure e-services and digitally signing documents. The private keys are stored on the SIM card with a small application for authentication and signing.

Turkcell's Mobillmza mobile signature solution was launched in 2007 in Turkey [3].

XI. CONCLUSION

There have been initiatives by the mobile operators across the world to offer Identity Provider Services to service providers and application developers. However, the success stories around it are still limited. If the operators have to achieve success from their Identity Brokerage Service, they need to provide more compelling value to service providers and their end users. With current assets and customer knowledge, operators are in a unique position to provide compelling values. The requirement is to build a collaboration platform which can package all the operator capabilities together and provide as services to the service providers and end users.

ACKNOWLEDGMENT

We would like to thank Dr. Piyush Maheshwari and Rajeev Kumar Tiwari at Ericsson India for their valuable feedback and support.

REFERENCES

[1] Prediction from CISCO http://www.businessinsider.com/cisco-predicts-mobile-2013-5?IR=T&tru=J8YD9#before-we-begin-cisco-has-a-great-track-record-with-its-internet-predictions-1 [Accessed May, 2014].

[2] Mobile-ID e-Estonia, http://e-estonia.com/component/mobile-id/ [Accessed April, 2014].

[3] Mobile Signature in Turkey, MobilImza service, http://www.gsma.com/mobileidentity/mobile-signature-in-turkey-a-ase-study-of-turkcell-mobilimza [Accessed April, 2014].

[4] GSMA Mobile Identity project, http://www.gsma.com/mobileidentity/ [Accessed April, 2014].

[5] Security Assertion Markup Language, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security. [Accessed April, 2014].

[6] Liberty Alliances, http://www.projectliberty.org/. [Accessed May, 2014].

[7] Oauth protocol, http:/oauth.net/. [Accessed May, 2014].

[8] GSMA, http://www.gsma.com/. [Accessed April, 2014].

[9] Mobile Identity UK Research Summary http://www.gsma.com/mobileidentity/wp-content/uploads/2013/12/GSMA_Mobile_Identity_Research_June_2013.pdf [Accessed May, 2014].

[10] Dialog Connect, http://www.gsma.com/mobileidentity/wp-content/uploads/2013/06/GSMA-Mobile-Identity_Case-Study_Dialog-Connect_May2013.pdf [Accessed May, 2014].

 ISBN: 978-1-61208-345-2

[11] Mobile Birth Registration in Sub-Saharan Africa:A case study of Orange Senegal and Uganda Telecom solutions http://www.gsma.com/mobileidentity/wp-content/uploads/2013/05/Mobile-Birth-Registration-in-Sub-Saharan-Africa.pdf [Accessed May, 2014].

[12] Unstructured Supplementary Service Data http://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data [Accessed May, 2014].

[13] Short Message Service http://en.wikipedia.org/wiki/Short_Message_Service [Accessed May, 2014].

[14] Mobile operator EMT https://www.emt.ee/en/liitu [Accessed May, 2014].

[15] Subscriber identity module http://en.wikipedia.org/wiki/Subscriber_identity_module [Accessed May, 2014].

 ISBN: 978-1-61208-345-2