ATIS-I-0000042

ATIS Trust and Identity (T&I) Focus Group White Paper

July 2013

As a leading technology and solutions development organization, ATIS brings together the top global ICT companies to advance the industry's most-pressing business priorities. Through ATIS committees and forums, nearly 200 companies address cloud services, device solutions, emergency services, M2M communications, cyber security, ehealth, network evolution, quality of service, billing support, operations, and more. These priorities follow a fast-track development lifecycle — from design and innovation through solutions that include standards, specifications, requirements, business use cases, software toolkits, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). ATIS is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of oneM2M, a member and major U.S. contributor to the International Telecommunication Union (ITU) Radio and Telecommunications sectors, and a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit < www.atis.org >.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

The *ATIS Trust and Identity (T&I) Focus Group White Paper* was developed for the **Technical and Operations (TOPS) Council**.

Published by
Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

Printed in the United States of America.

Table of Contents

ATIS Trust and Identity (T&I) Focus Group White Paper

1 Executive Summary

The ATIS Trust and Identity (T&I) Focus Group analyzed the activity map created by the T&I Landscape Team for activities that meet three criteria:

1. *The activity must have common interest among ATIS service providers*. These are areas where multiple ATIS service providers are working on standardization or deployment of a particular technology.
2. *It must have the potential for collaborative service interaction and reuse*. These are service elements that support either service portability or service interoperability across providers. The service element must also have use in more than one implementation. Services that do not have the potential for reuse will be excluded.
3. *The Identity Management (IdM) service components must have industry support, including evidence of current or planned implementation*.

This whitepaper identifies functions that meet all three criteria, and recommends next steps. It is not this Focus Group's intent to redesign mature architectures such as IMS, but rather to identify existing assets that ATIS member companies can leverage, as well as areas where ATIS is positioned to help address identified business requirements.

2 Background

Previously, the ATIS Trust and Identity Landscape Team completed an assessment of trust and identity activities across multiple industries. This assessment provided a map of trust and identity (T&I) activities for further evaluation of relevance to ATIS member companies. The analysis highlighted the level of industry acceptance for each activity. In general, the landscape study noted that most of the activities were very tactical, and that there is a lack of strategic focus in this space.

3 Industry Activities

The following section identifies relevant trust and identity activities where some aspect of the service may be useful for reuse.

3.1 Local Number Portability (LNP)

Local Number Portability provides the ability to move a phone number between operators and/or geographic locations. There are technical and regulatory limitations on the implementation, but the intent is to allow customers to make changes in service without changing phone number. The phone number is the user's identity in the PSTN.

3.2 Open Identity Exchange (OIX) Telecom Data Trust Framework

This trust framework exemplifies what a trust framework does, but it is specific to the exchange of information related to Line Information Database (LIDB). It also incorporates strong authentication and support for interoperability between service providers. The OIX Telecom Data Trust Framework is effectively a single service vertical (i.e., LIDB) which may limit its broader applicability, but a number of capabilities could contribute to a comprehensive solution.

3.3 OAuth 2.0

OAuth 2.0 is a framework that enables authorization services across administrative domains. When a service uses OAuth 2.0, a third-party service or application can get limited access to resources provided by that service, as authorized by the resource owner. OAuth 2.0 does this in a way that does not expose the resource owner's login credentials or other private information to the third-party.

OAuth 2.0 is one piece of the identity management ecosystem. As an authorization system, it depends upon proper authentication of appropriate parts of the transactions – authentication of the resource owner to the authorization service, for example. OpenID Connect is an identity layer built on top of OAuth 2.0.

There is significant industry momentum, from Google, Facebook, Twitter, AT&T, and others, to use OAuth 2.0 to control access to APIs. When such use of OAuth 2.0 is in place, a third-party application can only access a user's Google services, for example, after the user (the resource owner) authorizes the access with Google through OAuth 2.0. This provides an additional layer of protection that prevents accidental or unexpected exposure to rogue applications.

3.4 Roaming

There is a robust and reliable mechanism for access and financial settlement related to roaming between operators. Today roaming works with voice calls, text messages, and data access. Roaming requires technology compatibility between the user’s device and the visited network. There are real-time trust and identity mechanisms to support roaming, such as authenticating a user in a visited network, but these are out of scope for the analysis in this white paper. Here we are interested in the business and financial framework negotiated between service providers to support roaming. That framework includes a well-established network of clearinghouses.

One area where roaming differs from some other trust and identity mechanisms is the degree of reciprocity between roaming partners. Roaming agreements support roaming in both directions and are very much agreements between peers. Trust and identity agreements between a service provider and a service consumer would have different requirements that must be taken into account.

3.5 Communications

Identity is an important aspect of all communications services, and service provider networks incorporate a number of implicit and explicit identity mechanisms. This section considers a number of these solutions. Each of these solutions uses a purpose-built architecture to provide communications capability for a specific endpoint type. Each model incorporates technology-specific implementations that are not necessarily compatible with other models.

3.5.1 Rich Communication Services (RCS)

RCS is a series of GSMA specifications that extend the capabilities of current voice and text messaging solutions to add instant messaging, video communications, and file sharing across multiple devices and networks. RCS provides an inter-provider alternative to vertical Over the Top (OTT) communications offerings. Over the Top (OTT) services are delivered in such a way that the network carries the IP traffic but is not aware of the details of the application. One of the core functions of RCS is a common trust and identity model that is used across the supported services and across operators. RCS is intended to be a true global solution across all devices and service providers, in contrast to OTT services, which are typically restricted to a single service ecosystem.

3.5.2 Unified Visual Communications

Unified visual communications (e.g., telepresence) is a service that gives geographically distributed users or groups of users the experience of meeting in the same room. This experience is created through a

combination of multimedia communication including at least one audio channel and video channel. Typically the service incorporates HD voice and multiple high quality video channels to enhance the quality of the experience. Collaboration tools are often included as well. Existing unified visual communications services incorporate some form of identity, but this is generally service and vendor specific.

Unified visual communications provides a multi-user framework for a variety of communications offerings including video, voice, messaging, collaboration, and document sharing. While some existing solutions optimize a specific set of communications functions across a single domain, there is a business requirement to expand this to include interconnectivity across domains. For example, immersive Telepresence is an optimized and managed service that provides a life-like video communications experience. Unified visual communication does not redefine Telepresence, but rather broadens the scope, and looks at how other domains such as RCS and WebRTC can interconnect with the Telepresence domain. This use case raises some specific trust and identity questions:

- Telepresence, RCS, and WebRTC domains have different addressing, authentication, and profile models.
- How is information shared between these domains to facilitate user discovery, inter-domain communications, and maintenance of each domain's trust model?

3.5.3 Over-the-Top (OTT)

As an example of an OTT service, Apple Facetime and iMessage provide video calling and text messaging services. The video calling capability only works between Apple devices. The messaging service works between Apple devices, but Apple devices with a cellular radio can also send text-only messages to an SMS address. In addition to text, the messaging service can send photos, videos, locations, links, contacts, and other attached content. Both services can work over WiFi and cellular. The Apple identity model works differently than the mobile identity model. Devices equipped with a cellular radio will have a phone number. All Apple devices can also have one or more identities formatted and validated as email addresses. These additional identities provide flexibility for call and message routing as well as a way to contact devices without a phone number. These email-formatted identities do not work outside the Apple ecosystem.

3.5.4 ORCA

Open Real-time Communications API (ORCA) provides a simple mechanism to allow web application developers to use network infrastructure – initially IMS infrastructure – to simplify signaling when adding real-time communications to web applications. This effectively allows web applications to leverage the IMS identity and addressing model. Although this has not been addressed by ORCA, explicitly offering web applications a unified trust and identity model that could be applicable to a range of services (UVC, RCS, VoLTE, etc.) would make ORCA more valuable to application developers, and would generate more usage revenue for service providers. Explicitly including T&I in ORCA should be considered in this context.

4 Requirements

4.1 Separation of Authentication & Authorization

Each of the examples above identifies the user and then authorizes one or more capabilities. OAuth 2.0 is frequently used for API authorization. IMS authorizes a user for specific services which may include RCS. Consistent delineation between the authentication of an identity and the authorization of that identity for specific capabilities provides an opportunity to mix and match these capabilities. An example may be using IMS authentication to support OAuth2.0 authorization of API access. The inverse would be to use OpenID authentication for a WebRTC client which then used IMS services to authorize access.

4.2 Graduated Authorization

Graduated authorization acknowledges the need to support an agile framework for user identity validation (e.g., user/password, certificates, biometric, multi-factor, etc.). Over time, new methods and tools will be introduced to identify users. These new identity methods will continue to coexist with existing methods. It should be noted that the Federal ICAM Trust Framework (applicable to U.S. Government departments and agencies) already includes the concept of an Assurance Level (or Level of Assurance – "LOA") that includes information on the trustworthiness of an authentication. The ICAM Trust Framework also specifies the type of token that is acceptable for higher LOAs. The identity framework should be extensible so that these new methods can be accommodated without impacting the services that rely on the identity assertions produced by the framework.

In addition, service providers should be able to make authorization decisions based on attributes related to the identity of users as well as the methods with which a user identity was determined. For example, a service may choose to provide access to health records for doctors only when the doctor has performed a multi-factor authentication. However, it is possible that within an identity framework, a user is identified as a doctor, but for which that doctor's identity was proven only with a password. For some services a password may be sufficient, but for others, stronger validation may be required. If a user has been Authenticated using a relatively weak mechanism (e.g., password) and later tries to access a service that requires stronger validation, this would trigger a second Authentication with the stronger mechanism (e.g., biometric). The T&I framework must be able to distinguish between authentication by one method (e.g., password) and by another method (e.g., biometric). The T&I framework should assert not only the identity of the user, but also information about how the identity was proven so that the services consuming identity assertions can make appropriate authorization decisions.

Currently, there is no concept of "multi-factor Authorization", only "multi-factor Authentication". However, Authentication and Authorization build on each other, and at the implementation level the same effect can be achieved in multiple ways. For example, it is possible for an Authentication outcome to be binary (you are either authenticated, or you are not) and then allow a range of Authorization options, determined by policy applied to a variety of other factors. On the other hand, it is also possible to have a range of Authentication outcomes based on different sets of attributes that reflect the LOA, and then have the Authorization outcome be binary (a given Authenticated individual is either Authorized or not Authorized) based on policy applied to a variety of other factors. At the implementation level these two approaches can appear identical. In either case, the designation of access entitlements are generally determined offline during initial proofing/registration, or during ongoing administrative procedures. There is no industry consensus on which of these two approaches is the best one to follow.

4.3 Single Sign On

It is desirable for a trust and identity solution to minimize interaction with the end users of the service and to make identity as unobtrusive to the end user as possible. Minimizing the frequency of end-user identity credential verification makes it more palatable for users to utilize more complex and therefore stronger credentials for authentication (e.g., multi-factor or long complex passwords). It is suggested that a goal for the T&I framework should be to support the ability of a user to "log in" at the beginning of a session and then be free to utilize any service from any service provider participating in the framework without requiring explicit user interaction to repeat authentication (simply because the user crossed service provider boundaries during the session). However, in the case where a user was Authenticated using a relatively weak mechanism (e.g., password), and later tried to access a service that required a stronger mechanism (e.g., biometric), the user would need to Authenticate again, using the stronger identity mechanism. This could happen when the user logged into one portal, and then accessed a different portal that dictates a higher Assurance Level Authentication. Alternatively, it could happen when the user accesses a more restricted service through the same portal.

This use case implies either a single “universal” identity framework or a federated identity framework, while recognizing that there may be multiple levels of Authorization within the identity framework, and that additional Authentication may be required to access higher Authorization levels.

4.4 Service Provider Interoperability

A number of capabilities, such as single sign on, require some level of interoperability among service providers for identity information or identity assertions. This interoperability creates greater collective scale and increases the value of the services being offered in accordance with Metcalf’s law. Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system.[1] In specific areas (such as PSTN calling, roaming, and SMS), service providers have realized “universal” interoperability. However, extension of interoperability beyond PSTN capabilities has been elusive.

4.5 Identity Portability

Linking an identity permanently to an identity provider creates additional complexity for the user. Multiple identities must be created, linked, managed, and deleted. The ability to federate identity partially addresses this issue, but not fully. Ideally, a degree of “identity portability” would be supported in much the same way that number portability is currently supported in the PSTN and IP environments. Unlike the PSTN, where users are free to retain an E.164 number as they move between service providers, social networking users are locked into a single vertical ecosystem and cannot port their identities or applications to other providers. Social networking sites have started developing partnerships to expand the scope of services that can be accessed within their ecosystem, but this does not change the fact that users are locked inside a “walled garden” of sanctioned services.

E.164 numbers can be ported between service providers, and to some degree are extensible to new services. Phone numbers can be used for PSTN calls, for SMS, and for RCS services. It may be possible to extend E.164 numbers to cover IP services as well. Some other services already take advantage of E.164 numbers – for example, Apple FaceTime and Blackberry BBM can be linked to E.164 numbers. Extending this to other IP services would require further study.

Unfortunately, portability of web identities is unlikely to occur without significant effort. Portability of E.164 numbers required the addition of the LNP database and the Location Routing Number (LRN). These functions provided the ability to determine which identities had been ported and what network element currently owned the identity. This mechanism does not exist with today’s web-based identities. Instead, the web provides the ability to delineate between identity provider and service provider. For example, many companies support third-party OAuth 2.0 identities such as Facebook and Google. This allows the user to segregate his or her services from the identity. Users can add new services without adding new identities, but they should choose the identity provider carefully because of the barrier to change. An additional alternative is the use of identity management tools that facilitate the creation and management of identities. These systems are a form of aliasing where the user accesses one application that subsequently maps a specific username and credential pair to a desired service. These services provide a similar user experience to OAuth 2.0, but do not eliminate the multiple identities.

4.6 Identity Relationships

In addition to the authentication of the user and the authorization of services to that user, there are also requirements for the interaction between users.

For example, the ability to assign rights and obligations in a way that clearly differentiates between the user of a service, and the subscriber (who owns and pays for a service), provides significant value. This concept is completely absent from Application Service Provider frameworks. Operator frameworks use an

[1] ”Metcalfe’s Law” (page 532), *Netwon’s Telecom Dictionary*, 16th Edition. Telecom Books: New York, NY. ©2000.

account PIN for limited circumstances such as account access. Layering biometrics and other information as a means of identifying the user can generate significantly more value if implemented in a standardized way.

In addition, there are also relationships within enterprises, families, and other groups. These relationships are further outlined in ATIS-1000044.2011, *ATIS Identity Management: Requirements and Use Cases Standard.*

4.7 Anonymized/Compartmentalized Information

Establishing trust usually implies using mechanisms that strongly identify (authenticate) a specific (individually identifiable) user. However, some verticals – such as eHealth – are mandated to restrict unauthorized disclosure of individually identifiable health Protected Health Information (PHI). This is normally accomplished through institutional policies applied to its employees and internal systems.

There are at least two ongoing issues with maintaining privacy in this environment:

- In spite of various policies, laws, and regulations, individual breaches involving thousands of individuals continue for a wide range of reasons[2],
- There are still circumstances where aggregated and anonymized information is disclosed for analysis and reporting purposes.

The above issues are out of scope of this analysis. However, identity mechanisms may be explored that allow the vertical's applications/systems to invoke underlying network capabilities (e.g., RCS, Telepresence, ORCA) in a way that allows privacy tools such as anonymization, pseudonymization, and compartmentalization to be used within the vertical's application/system domain. In other words, invoke underlying network services, but "do no harm" to data privacy.

4.8 OIX Trust Framework

The Telecom Data Trust Framework was specified to support using LIDB information with third-party applications. It demonstrates how a trust framework is used to set rules of interaction between parties, but it is too specific to be used for other purposes. A different OIX Trust Framework could be driven by a broader set of criteria according to varied communities of interest. OIX provides a means of scaling beyond a principal group of participants. Metadata listing is provided to facilitate potentially large-scale adoption.

4.9 Aliasing

Certain services may require the use of temporary identities, or identities that are used only within the service provider network(s) and are not used in the public domain for identification or addressing of a user or user device. Such identities commonly are required when they are associated with a piece of hardware which may be broken, lost, or stolen; and which should be replaceable without affecting the users' services. They are also used where routing translation is based on a different categorization from that used in the corresponding public address space, or where there is a need for a minimalist identity to save signaling overhead that is only allocated to active users. The use of non-public identities also provides an additional layer of security, which is of great benefit where that identity is used as the basis for subscription authentication.

The association of these aliases with their corresponding public identities occurs within a database operated by the service provider. The format of the alias may be standardized, where is it required for interchange between service providers, or proprietary if only used by the individual SP.

[2] < http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html >

A classic example of the use of such aliases is the use of IMSI and TMSI in mobile wireless voice and tele-services supported by 3GPP standards.

The public identity used for these services is an E.164 “phone number”, which is commonly allocated on a geographic basis. However, within and between the mobile network(s), subscription verification and routing uses International Mobile Station Identities (IMSIs) per ITU E.212, which, at the user end, are each stored on a specific piece of hardware, on a removable or embedded Subscription Identity Module (SIM) in the mobile device. If the terminal or SIM is lost, stolen, or destroyed, the SIM, and its corresponding IMSI can be replaced without changing the public identities of the user; the service provider merely provisions the terminal with the new IMSI and updates the translation records in their databases.

Mobile wireless networks also may dynamically allocate short temporary identities (Temporary Mobile Station Identities; TMSIs) for use over signaling channels with restricted capacity, such as the broadcast paging channels. These are issued only to active user devices within a given network zone, which can occupy a very small sub-set of the total available IMSI address space; for example, there may be 5 million active mobiles in NYC, they can be individually addressed using 4-byte addresses, but these are a very small fraction of the total world population of several billion IMSIs that are approximately twice that length. The association between the temporary ID and the IMSI (and public IDs) is stored on a local database within the wireless provider’s network. This dynamic allocation of a random ID that is used over a broadcast wireless channel also provides another layer of security for the user and service provider, as even the non-public IMSI of a user’s device may become public (e.g., though operator employee data theft), which would allow tracking of the user device, were it not hidden behind the TMSI.

Aliasing is also used in the web and financial industries to shield a user’s identity from third-parties. These aliases may be specific to the user, session, transaction, or other identifier. For example, a service provider may integrate a third-party API into a finished application. The service provider does not want to expose the user’s identity to the third-party, so it maps the user’s identity to an alias transaction id prior to conducting the third-party API call. Financial institutions also support this behavior. Some credit card companies support one-time account numbers for financial transactions. These numbers are requested and used by the user in lieu of their primary account number. This method protects the user’s information and reduces the potential for fraud.

5 Challenges

5.1 Fragmentation

All of the services identified in this white paper (Telepresence, RCS, VoLTE, ORCA, unified visual communications), plus many OTT services such as Apple FaceTime and Skype, have similar identity requirements. However, each is implementing independently, leading to similar, but not identical, implementations. As a result, these implementations are not interoperable without an interworking function. As real-time communication web applications proliferate, the challenges will only increase. This fragmentation creates opportunities for the OTT services like Apple FaceTime, which can offer global services. These services are limited to devices from a single supplier ecosystem, but nonetheless they can provide a global unified service across any service provider access network.

5.2 User & Developer Lock-In

Lock-in occurs as a result of fragmentation and lack of interoperability. Users or developers make investments of time and money in applications, content, configurations, and other platform-specific capabilities. These changes are locked-into the environment and are impossible or not easy to port into a different environment. For example, a developer may create an app for the Apple environment. The API definition and developer framework are specific to Apple. Deployment of the app on an Android or Windows device requires redevelopment, engagement in a new development ecosystem, and other platform specific investments.

Users have a similar challenge. Applications that are purchased in one environment do not translate to a different environment. Users also spend time customizing a device to their personal tastes. These changes are made manually and are lost when changing to a new device.

Social networking services that do not provide identity portability and interoperability create user lock-in and service fragmentation. It is common for users to maintain multiple equivalent systems (e.g., Yahoo Messenger, AIM, Google+, Facebook, etc.) with multiple identities to support communications with all their contacts.

5.3 Lack of Trusted Internet Identity

Most self-asserted internet identities (e.g., email addresses, website user names, and domain names) have a low barrier to acquisition and little or no recurring cost to the user. Because of these factors, illicit identities – including bot-controlled identities – proliferate. In the early evolution of the internet, advertising revenue driven by customer acquisition was more important that the cost incurred from fraudulent identities. Now, web business models are maturing, and the fraudulent identities cause two problems. One is the direct cost to current business models, such as Google's challenges from click fraud. The second is the lost opportunity to generate paying revenue.

There are ASP vertical ecosystems that implement some level of user validation or reputation. Examples of this include the Amazon "Real Name" badge and eBay buyer and seller rankings, but these examples are in the minority of web offerings.

6 Opportunities

6.1 Applicability of Transferred User or Device Authentication

One of the potential opportunities for operators may be to be able to extend their trust relationship with a customer to a third-party. However, when this is done, the applicability of the authentication scheme used in the provider domain to this external usage may need to be validated on a case by case basis.

For example, the authentication schemes that are adequate for the verification of a user to allow billing of a mobile phone service may or may not be adequate to verify billing for large purchases of goods from third-parties, but certainly would be adequate to verify that messages stemming from that subscription are from a specific device, which could prevent that terminal being used to host "bots", and rather validate that it was associated with a particular human or group of humans. This is a less--intrusive alternative to current bot checkers that attempt to identify valid identities by requiring the user to decipher warped letters in an image file. This image file is difficult for bot-driven optical character recognition (OCR) to recognize. The challenge is that OCR technology is always getting better, and the images are getting more difficult for human users to read. This test is known as a CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart).

6.2 Universal Identity

Service providers have natural strengths in the portability, interoperability, and consistent structure of identities. Many of these strengths are tightly coupled with specific, purpose-built technologies such as LIDB, LNP, and IMS/RCS. Adopting a unified "Trust and Identity" model that exposes these strengths in a broadly addressable way creates a natural focus for real-time communications.

6.3 User & Developer Portability

Addressing the portability opportunity requires a balance of interface standardization for developers and metadata standardization for users. Interface standardization enables developers to run applications in

conjunction with each operator environment without recoding the interfaces. Integrating to a new operator environment becomes a configuration exercise instead of today's higher cost redevelopment exercise.

For users, metadata standardization allows ported information to be easily moved from one operator to the other. Today, local number portability moves the phone number using user name, account number, and PIN. Device settings, applications, and other user specific information are lost during the port, unless they are captured as part of an application vertical such as a network-based address book service. User portability protects the user's investment in the operator ecosystem by standardizing the exchange of this information between operators.

6.4 Robust Communication Service Provider Identity

E.164 numbers provide a trusted identity within and between communication service provider networks. There is no equivalent standardized trusted identity for Internet applications. In fact, in some sense, E.164 is used as a trusted Internet identity. For example, a one-time password can be sent as a text message to a validated MSISDN associated with a mobile device. (MSISDN may be validated according to E.164 number schemes.) Additional work would be required to extend E.164 identity more broadly to a range of Internet applications.

The other option is to apply the principles of operator assignment of E.164 numbers such as the validation process, credit check, address verification, etc., to communication service provider-specific web identities. There is a limited supply of E.164 numbers, and there is an unlimited supply of web-based identities. In addition, E.164 numbers are specific to communication services, and this model breaks down with web and hybrid services (e.g., machine-to-machine, WiFi, etc).

6.5 External Monetization of User or Device Authentication by the Provider

One of the major potential opportunities for operators may be to extend their trust relationship with a customer to a third-party. Whether this trust is established through electronic means, as in the case of subscription authentication in wireless networks, or by physical means in the case of "wired" service delivery, the provider has at least established a trusted relationship of adequate strength to meet their requirements for service billing, and this level of trust will be adequate to serve some third-party e-commerce applications.

There are challenges created by this re-use, as noted above, but the ability to use this established trust as the basis for an SSO scheme have yet to be fully exploited.

7 Recommendations

The current state of trust and identity is a juxtaposition of architectures designed for different purposes. On the one hand, we have a web ecosystem with rich services, but these services usually work within a single company and many rely on poorly validated identities. On the other hand, we have a limited set of mature communications capabilities that use robust, interoperable, and portable identities, but which are typically constrained to a limited number of services.

The opportunities section recommends five specific ways to bridge the gap between these ecosystems. Many of the core technologies for trust and identity are available and in use today. The challenge is that these capabilities are implemented for specific purposes with limited interoperability.

The Trust and Identity Focus Group recommends that the TOPS Council discuss and prioritize these five opportunities for prototyping and implementation across service providers. The opportunities take advantage of longstanding relationships in the PSTN and use a combination of trust framework, single sign on, and strong identity to address foundational weaknesses in current web solutions. Service providers can differentiate by binding identities to the user as well as to the device, and leveraging this

direct relationship to monetize across internal and third-party opportunities, including location, search profile, user consent management, personal data privacy management, and payment.

The T&I Focus group further recommends that the TOPS-prioritized technical work be completed as an extension of PTSC's current identity management efforts. This could include determining architecture required for the implementation of the trust framework, agreement on interoperability for single sign on, and technical implementation for service roaming.

In some cases, modifications may be required to the underlying standards to improve interoperability of these capabilities across operators. In those cases, it may be valuable to have a discussion with the design authorities for each of these activities to explore the feasibility of a converged approach.

8 Informative References

- **ATIS-1000035.2009: *Identity Management (IdM) Framework*[3]**
  - Provides an IdM framework for Next Generation Network (NGN).
  - Describes the fundamental concepts, functional components, and capabilities of IdM that can be used to organize and guide structured solutions and facilitate interoperability in an heterogeneous environment.
- **ATIS-1000044.2011: *Identity Management (IdM) Requirements and Use Cases Standard*[4]**
  - Provides IdM example use cases and requirements for the NGN and its interfaces.
  - IdM functions and capabilities are used to increase confidence in identity information and support and enhance business and security applications, including identity-based services.
  - The requirements provided in this standard are intended for NGN (i.e., managed packet networks) as defined in ATIS-1000018, *NGN Architecture*, and ITU-T Recommendation Y.2001.
- **ATIS-1000045.2012: *Identity Management (IdM) Mechanisms and Procedures Standard*[5]**
  - Describes the specific IdM mechanisms and suites of options that should be used to meet the requirements in the IdM Requirement standard (ATIS-1000044).
  - In addition, it provides best practices, guidelines to support interoperability, and other needs.
- **ATIS-0200008: *Trusted Information Exchange (TIE)*[6]**
  - The ATIS Trusted Information Exchange defines how to use a trust framework, identity management, and DNS in conjunction with a service to better address privacy concerns with data exchange. The document provides a functional view of the architecture.

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=25600 >.

[4] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=25632 >.

[5] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=26787 >.

[6] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street N.W., Suite 500, Washington, DC 20005 < https://www.atis.org/docstore/product.aspx?id=26798 >.