modern
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2017

C. Wendt
Comcast

March 13, 2017

Identity Registry (idreg)
draft-wendt-modern-identity-registry-01

Abstract

This document will describe an approach for how a distributed identity registry model might look. It will consider both public registry components of the data model necessary for routing calls from one globally routable identity to another. It will also consider part of the private registry components a provider may need to manage associations with users or customers. Other topics include provider associations, application or service association, and the ability to support multiple identities associated with a user/ subscriber (e.g. telephone number and e-mail identity).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 14, 2017.

Table of Contents

1. Introduction

There are many useful VoIP and user to user communications applications that desire the ability to provide services that don't depend on a single entity or provider to manage the end-to-end identities associated with that application. For example, using the VoIP protocol, SIP [RFC3261], the telephone network provides a federated mechanism that using a publicly known identity, the telephone number, a customer of a telephone provider A can call a customer of telephone provider B based on managed routing databases and routing rules. XMPP [RFC6120] is another example of a protocol that allowed federation of communications based on the username and domain of the host of the XMPP server. Each of these examples uses service specific databases or registries that are generally protocol or application specific, however today application providers general provide many applications or services for a user which generally share the use of common communications identities like telephone numbers, e-mail identities, or identities associated with web based IdPs.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

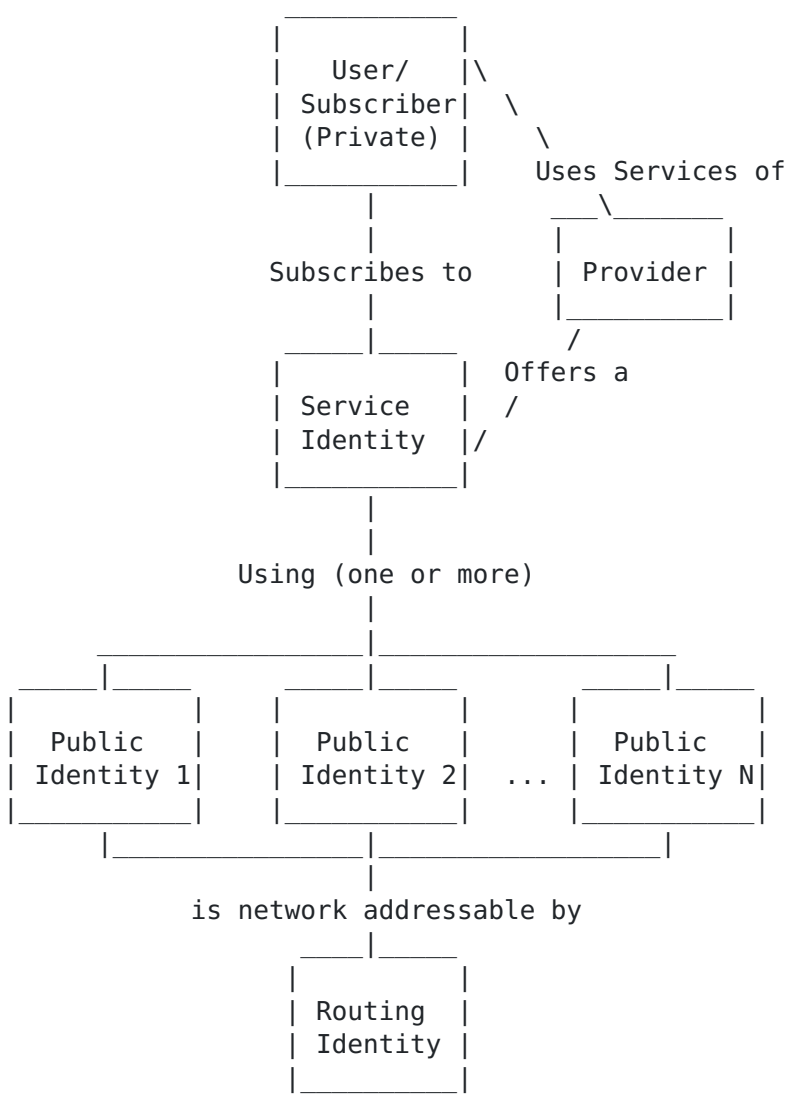
3. Overview

The identity registry model proposed in this document supports the model where there are a few actors in the model relevant to providing communications services.

- Provider - An entity that provide a service to customers and manages there identity in the network.
- User/Subscriber - The entity that is using the services of the provider.
- Service Identity - A globally unique identifier representing a application or service being made available to users/subscribers by multiple providers.
- Public Identity - A publicly known identity that the user associates with a service. This identity must be globally unique to a user/subscriber. It must also be provably associated to a given user/subscriber that claims the association.
- Routing Identity - A uniquely and globally routable identity used specifically in signaling calls between users.

This data model can be used to build the shared data between providers that support the federated service in order for users that are associated with one provider to call another provider.

3.1. Identity Data Model



3.2. Other identity registry attributes

The identity registry MUST support functions such as the following:

- The ability to query for available/unused identities for the purposes of either identifying conflicts before committing to the registry or identify unused identities that are part of a pool (e.g. telephone numbers)

- The ability to allocate identities for future use at individual levels or at block levels, such as NPA-NXX level telephone numbers or perhaps wildcard identities, e.g. *@example.com.

- The ability to update/transfer/port identities from one provider to another provider.

- The ability to digitally sign transactions to a provider for validation of legitimate transactions. Or forensic analysis of illegitimate transactions.

It is anticipated that this identity registry would be used with [I-D.wendt-modern-drip] for supporting a continuously and timely updated local registry for a given service identity the provider is offering.

4. Message and Control Flows

4.1. Queries

Typical queries for finding a globally routable identity should be in the context of a public identity and service identity for an allocated routing identity.

4.2. Allocation/Assignment

When a provider customer has decided to allocate a given single or block level set of telephone numbers there is a PUT command that allocates the number, given the number wasn't already allocated between the GET and the PUT. As a result of a successful allocation, the telephone number will be removed from the unallocated bucket.

4.2.1. API definition

Request:

PUT /idreg/createidentity

Pass the following object (JSON) in the body.

Property	Type	Description
user_type	string	(MAND) Type representing user/sub
user_type_id	string	(MAND) ID associated with user Example: accountID of user
user_info	stringified JSON	(OPT) User specific metadata
service_id	string	(MAND) Service type identifier Example: "pstn", "voip". "volte"
public_id	string	(MAND) User associated service identifier. Example: telephone number

An Authorization Header MUST be included with a JWT including timestamp, x5u, and signature that will be associated with this transaction.

Response:

Code	Status
201	user profile created, associate public id, returns new routing ID
200	user profile and public id association already exists returns the same routing ID (Idempotent)
204	service identifier not found
400	input errors
401	unauthorized API access - Signature validation failed
5xx	errors related to DB access and other system anomalies

For HTTP/1.1 200 OK and HTTP/1.1 201 Created responses:

Property	Type	Description
user_id	string	Globally Unique ID (UUID) for user.
routing_id	string	routing ID

4.2.2. Example

As part of the allocation, the service provider will be required to provide following information:

- publicID: telephone number in e.164 format (e.g., +12155551212).
- serviceID: "voip" by default, other services potentially in future.
- routingID: SIP URI with telephone number + domain representing service provider of record (e.g., sip:+12155551212@voip.example.com).
- timestamp: a timestamp retrieved from a common NTP server representing time of allocation, used for validating which service provider allocated first in race condition scenarios, and just for logging and historical reference in general.
- x5u: used for validation of signature
- signature: using a provider level [RFC5280] based private key/ certificate, the provider MUST sign the information above to validate the change to the registry.

4.3. Update Entry/Port

If a provider needs to update information related to an allocated entry, such as adding a publicID, modify routingID, etc. or if there is a port where a new service provider will overwrite the entry with new information, the API should be the same.

There is a GET operation to read the current entry information, if the provider needs this information, (e.g., read/modify/write). There also is a PUT operation that will write the updated entry information. This will require a new timestamp and signature to validate the security of the operation and logging/historical purposes.

4.3.1. API definition

The PUT /idreg/createidentity API can be used for updates to entries as it's an idempotent API. For porting of telephone numbers either createidentity or a combination of the delete described in the next section and createidentity can be used.

4.4. Removal/de-allocation

If a provider wants to remove an entry for the case where a customer removes his service and no longer wants to own or associate a public identity, a DELETE operation will be provided that will delete the entry, and for the case of a telephone number, will put the telephone number back in the pool of unallocated numbers.

4.4.1. API definition

Request:

DELETE /idreg/identitymapping/serviceid/:id/publicid/:id

Pass the following object (JSON) in the body.

Property	Type	Description
service_id	string	(MAND) Service type identifier Example: "pstn", "voip". "volte"
public_id	string	(MAND) User associated service identifier. Example: telephone number

An Authorization Header MUST be included with a JWT including timestamp, x5u, and signature that will be associated with this transaction.

Response:

Code	Status
200	public ID association deleted
204	record with service_id and public_id in request URI not found
400	input errors
401	unauthorized API access - Signature validation failed
5xx	errors related to DB access and other system anomalies

For HTTP/1.1 200 OK and HTTP/1.1 201 Created responses:

Property	Type	Description
user_id	string	Globally Unique ID (UUID) for user.
routing_id	string	routing ID

5. Security Considerations

TBD

6. Acknowledgements

Thanks to Harsha Bellur for collaboration on developing this model and it's implementation.

7. References

7.1. Normative References

[I-D.wendt-modern-drip]
Bellur, H. and C. Wendt, "Distributed Registry Protocol", draft-wendt-modern-drip-01 (work in progress), July 2016.

7.2. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, DOI 10.17487/RFC3261, June 2002, <http://www.rfc-editor.org/info/rfc3261>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <http://www.rfc-editor.org/info/rfc6120>.

Author's Address

Chris Wendt
Comcast
One Comcast Center
Philadelphia, PA 19103
USA

Email: chris-ietf@chriswendt.net