Use Cases for Identity Enabled Networks
draft-padma-ideas-use-cases-00

Abstract

This document describes some use cases for Identity Enabled networks using a Generic Resilient Identity Services infrastructure.

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 13, 2017.
Table of Contents

1.  Introduction .................................................. 3
2.  Specification of Requirements ............................... 3
3.  Definition of Terms .......................................... 3
4.  Common Control Plane Infrastructure .................... 5
   4.1.  ID-Based Protocols .................................. 5
   4.2.  Need for a Generic Resilient Identity Services in IoT .. 6
   4.3.  Case 1: Smart Home .................................. 8
   4.4.  Case 2: Smart City .................................. 9
   4.5.  Case 3: Industrial IoT Services ..................... 9
5.  Network Simplification ..................................... 10
   5.1.  Case 4: Proximity Services and Scopes ................. 10
   5.2.  Case 5: Ease of troubleshooting and Management ...... 11
   5.3.  Case 6: Application of Common policies ............... 11
6.  Ease of Provisioning ........................................ 11
   6.2.  Case 8: Active User-Driven Provisioning ............ 12
7.  Mobility ...................................................... 12
   7.1.  Case 9: Mobility within a single provider network ... 12
   7.2.  Case 10: Roaming across Mobile Networks ............. 15
   7.3.  Case 11: Mobility of a Subnet ....................... 16
8.  Heterogeneous Multi-Access Environments (hetnet) ........ 18
   8.1.  Case 12: Dynamic Mobility across Cellular and Wi-Fi .. 18
   8.2.  Case 13: Ad-hoc Networks Mobility across Hetnet .... 18
   8.3.  Case 14: Multi-network Access Support ................ 19
   8.4.  Case 15: Disconnection-tolerant routing ............. 20
9.  Security ...................................................... 20
10. Discovery of devices ......................................... 21
    10.1.  Case 17: Low Cost Asset tracking .................. 21
11. Security Considerations .................................... 21
12. IANA Considerations ........................................ 21
1. Introduction

The problem statement document for Identity Enabled Networks (IDEAS) advocates for a standardized infrastructure, secured common control plane with data integrity and allowing for different data-plane solutions [IDEAS-PS].

This infrastructure is called Generic Resilient Identity Services (GRIDS). The GRIDS will support functionalities such as traditional mapping and resolution of Identifiers (ID), as well as secured identifier registration, subscription, discovery, updates with data integrity. In addition, it is designed to allow future extensions.

This memo describes some use cases for Identity-based protocols that will benefit from such an infrastructure.

2. Specification of Requirements

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. Definition of Terms

This document makes use of the terms that have been already defined in the problem statement draft of IDEAS [IDEAS-PS]. They are included here for reader’s convenience. In case of any discrepancies between the two drafts, the problem statement draft overrides.

Entity : An entity is a communication endpoint. It can be a device, a node, or a (software) process, that needs to be identified. An entity may have one or multiple identifiers simultaneously. An entity is reached by the resolution of one or more of its identifiers to one or more locators.

Entity Collection: A set of entities with its own identifier, e.g., a multicast group, or an ad-hoc vehicular network that needs to be uniquely identified (e.g., a train entity may represent a Closed User Group (CUG) and may contain all the passengers’ devices that share the same fate for connectivity).
Identifier (ID): denotes information to unambiguously identify an entity within a given scope. There is no constraint on the format, obfuscation or routability of an ID. The ID may or may not be present in the packet whose format is defined by ID-based protocols.

Locator (LOC): denotes information that is topology-dependent and which is used to forward packets to a given entity attached to a network. An entity can be reached using one or multiple locators; these locators may have a limited validity lifetime.

Identity: the essence of "being" of a specific entity. An identity is not to be confused with an identifier: while an identifier may be used to refer to an entity, an identifier’s lifecycle is not necessarily tied to the lifecycle of the identity it is referencing. On the other hand, the identity’s lifecycle is inherently tied to the lifecycle of the entity itself.

Identity Enabled Networks (IDEAS): IDEAS are networks that support the identifier/locator decoupling. Reaching an entity is achieved by the resolution of identifier(s) to locator(s).

Identifier-based (ID-based): When an entity is only reachable through one or more communication access then a protocol or a solution is said to be ID-based if it uses an ID-LOC decoupling and a mapping system (MS) as base components of the architecture.

Identity-capable (ID-capable): An application is said to be ID-capable if it makes use of an Identifier of an entity to establish communication. For example, an application that initiates its sessions using an ID. An application may use an IP-address as a proxy for an ID if the network resolves this ambiguity. We regard such an application as being ID-capable.

Generic Resilient Identity Services (GRIDS): GRIDS is a set of services to manage the lifecycle of IDs, to map and resolve identifiers and locators, and to associate metadata (META) with entities and entity collections. It is a distributed system that stores the ID, the associated LOC(s), and metadata (META) in the form of tuples (ID, LOC, and META).

Metadata (META): is data associated with an Identity. The metadata may contain information such as the nature of the entity for example.

5G: Fifth generation wireless broadband technology [NEWS-3GPP].
Scope: denotes the domain of applicability or usability of an ID. A scope may be limited (e.g., considered local with geographic proximity, or private within an administrative domain) or be global.

User Equipment (UE): A user equipment is an entity per definition in [IDEAS-PS]

Mapping gateway (MGW): A mapping gateway is a node in the network which may host the GRIDS. It has access to the ID/LOC mappings. It may also be able to update the destination address of a packet based on the changes in the network.

4. Common Control Plane Infrastructure

4.1. ID-Based Protocols

ID-based protocols currently rely upon a customized mapping infrastructure and they do not interoperate with each other. Therefore, it would be difficult to deploy multiple ID-based protocols in the same network due to the overhead generated by the operation of various mapping functions. Hence, only one ID protocol is usually deployed even though there exist the need to deploy specific solutions to address various contexts.
4.2. Need for a Generic Resilient Identity Services in IoT

The IoT landscape is comprised of diverse devices and protocols. Often, specific protocols are chosen due to constraints in the deployment solution. For example, a small CPU/Memory footprint may not allow for the formation of IPv6 packets or the battery-operated nature of the device is not compatible with the "always-reachable" nature of an IP stack.

In many scenarios, there is little commonality and almost no interoperability between various IoT device technologies especially when they are provided by different vendors. Meanwhile, the IoT implementations are solely depended on their own network enablers. The use of gateways within IoT solution is a common feature allowing
IoT solutions to satisfy different applications. By adopting multiple gateways in individual IoT domains, the convergent point for global IoT interconnections is usually at a higher layer, such as through adapting non-IP IoT protocols to IP-enabled reachability.

Whilst such an approach has allowed for rapid innovation in terms of IoT applications, it also encourage the proliferation of siloed networks. The ability of GRIDS to take into account various (IoT-inferred) naming and addressing schemes is a possible solution. The proper operation of cross-platform IoT services, that may deployed at various scales - metro, region, country, may also encourage privately operated mapping systems.

For example, an e-health service portfolio would include dynamic biometric data monitoring which would involve an IoT network provider (to forward data collected by sensor bracelets towards the nearest dispatch emergency unit (as a function of the location of the patient), an e-health service provider (e.g., ministry of health), possibly associated with an e-health application service provider (bracelet management, privacy data management, etc.). In this use case, the different players may use specific naming schemes which may solicit different mapping systems - one operated by the IoT network provider (typical IP address resolution for example), the other by the ASP or the IoT service provider.

However, it has to be realized that consolidating a vast array of IoT datasets to a single, common form is likely to be unachievable without compromising the quality of the data; the scope of IoT data is too broad for them to be a single presentation that would suit every application. In turn, this leads to the conclusion that IoT will continue to comprise a large number of access technologies and protocols, that are designed and optimized for their target application, environment or devices.
Therefore, any exchange of data must happen at a layer above the current network as illustrated in the figure 2. The solution lies in an overlay addressing scheme to which all devices subscribe and are aware of, but which allows for-purpose network stacks and local addressing schemes to remain in place.

The ability to "route" between different technologies should be enabled by the exchange of or notification of, or dynamic discovery of the location of the GRIDS. It is expected that within a single domain, such an ID scheme would allow data exchange between gateways onto the existing IoT networks. A single ID solution therefore has the ability to bind multiple, silo-ed IoT solutions into a logical whole, allowing for the exchange of data between applications. (e.g., telemedicine IoT devices monitoring different health indicators).

4.3. Case 1: Smart Home

In a smart home, there usually exist heterogeneous consumer products made by different manufacturers, such as TV, air conditioner, refrigerator, surveillance camera, washing machine, and so forth. As a prominent trend for those home appliances becoming smart, they are able to be controlled in a wireless manner by respective control applications (e.g., be installed in a Smart Phone acting as the controller). However, one serious problem is that each specific home product provider often request to have its customized application with the associated protocol to enable device connectivity. This results in siloed administration domains, and causes significant inconvenience for customers, while tens of applications might be needed for controlling all the appliances at home.
The management of a plethora of IoT devices regardless of underlying technology is a challenge for the user and a common mechanism is needed. Such a mechanism requires to have unified identifier, interoperable protocol, compatible data format, and the like. For example, the user may operate his/her own IoT Mapping System, with or without the support of the network provider or the IoT service provider. In case of support from a provider, a Customer Premise Equipment (CPE) may function as an Internet gateway with an embedded GRIDS. Hence, connected IoT devices may be accessed by a remote controller.

Note that a cross-domain unified identifier and a set of management policies upon such identifier plays an essential role in this case, especially when every connected device at home is equipped with intelligence for wired or wireless control in near future.

4.4. Case 2: Smart City

In current smart city constructions, lots of function-oriented closed-loop applications have created information silos in distinct industries, which are independent of each other. Accordingly, the full interconnection and interoperability among various systems and applications in smart city environment have not been extensively realized. One of the key problems is the lack of unified identifier service along with a resilient resolution method. As a result, different sectors cannot mutually interoperate or need to shoulder a heavy cost to achieve interconnection.

With the assistance of a common identifier layer and the resolution service of fetching all relevant information of any identifier, many vertical industries such as Transportation, Healthcare, Tourism, Environment etc., can provide services that can be better managed whenever participating service components share a common communication infrastructure. For example, one traveler in a city can request information about instant traffic, near-term weather, and shopping guidance of one specific place of interest by issuing a single query to the corresponding service identifier.

4.5. Case 3: Industrial IOT Services

In some scenarios, a publishing entity might not be able directly communicate with multiple entities to send the same data due to energy constraints. For example, a temperature sensor may send the temperature readings to a GRIDS. Eventually, subscribers could access the readings without direct interaction with the sensor allowing it to save energy. In these cases, a local and private GRIDS may act as helper by implementing a pub/sub model on the
sensor’s behalf. The GRIDS may receive and store the information in the metadata associated with the entity or the data could be stored remotely to a server referenced in the metadata. Furthermore, the GRIDS could leverage its own access policy control features so that the data can only be accessed by authorized users or entities. This scheme protects the publishing entity from possible attack by obfuscating its locator and preventing direct access to it.

5. Network Simplification

Whilst the term IoT encompasses a wide range of applications ranging from short, low data-rate communications through to latency-sensitive haptic control loops, the ability to reduce network overhead through the simplification and potential removal of addresses at specific points on the network has several benefits.

5.1. Case 4: Proximity Services and Scopes

In a system generating small amounts of data, the relative size of the addressing which can be considered to be network operator overhead compared to the size of the data payload which is customer data can be very high to the point where the addressing and control data vastly outsizes the customer data. In a traditional IT network, this is not often the case; the address and management data is very-much smaller than the payload and is thus an acceptable tax on the overall communication. Small data IoT applications require a solution to address the imbalance which now exists between the payload and the overhead.

It is possible to imagine local services within a scope that require only a small ID within a scope and can communicate with a local GRIDS to resolve its mapping and location services if it is only communicating with local devices such as local networked sensors. Such an example could sensors be in a factory.
5.2. Case 5: Ease of troubleshooting and Management

Trouble-shooting a complex, multi-layer network where data is handed from one encapsulation to another is complex. It is already seen in solutions such as SIP that having embedded naming structures vastly improves the ability to determine a data-path in a trouble-shooting instance. Similarly, an ID-based solution would apply from the data producer to the consumer and can also be used to improve data-traceability thereby resulting in lower operational costs.

The presence of a GRIDS can improve on managing the data paths as they are stored in their mappings. Such improvement can be especially beneficial if GRIDS capabilities interact with a SDN-based computation logic, whose service-inferred policy-based decision making process may choose to redirect traffic onto alternate paths as a function of the nature of the service, the load status of the primary path, etc. Application of such dynamics can be critical for specific IoT services, such as e-health services. Data analytics on the GRIDS may also be logging events for easier postmortem if there are issues.

5.3. Case 6: Application of Common policies

A Mapping System can contribute to enforce a set of common policies for a given connectivity service by providing a global, consistent identification and resolution service to any participating device involved in the forwarding of the corresponding traffic.

6. Ease of Provisioning

The ease of provision becomes crucial with the foreseen deployment of several (tens of) billions of connected devices come online. There are two main scenarios where ID may simplify provisioning:

6.1. Case 7: Automatic Bootstrapping

Vastly improved operational efficiency is a requirement for Industrial IoT (IIoT). The fast bring up, management and optimized use of assets are crucial to industry automation. (For example, diverse entities such as industrial robots or sensors having an ID may access the factory network and be redirected to a private GRIDS. They may then authenticate and register themselves with the GRIDS. If the GRIDS has some metadata for configuration stored for these IDs, the entities could be automatically bootstrapped. Changes of configuration need only be done on the local private GRIDS in the future without individually accessing each device.
6.2. Case 8: Active User-Driven Provisioning

IoT devices deployed in large numbers in a given coverage area (e.g., Smart Agriculture for herd inventory) should be provisioned and authenticated in bulk. Similarly, lightweight simplified device configuration such as health monitors and Pet tracking devices would benefit from bulk pre-provisioning.

7. Mobility

This section considers some scenarios of mobility in Identity Enabled Networks. We assume that mobility should be seamless and transparent to the application and user as far as possible. In particular, data communication sessions should not be disrupted across mobility events.

Seamless and transparent mobility in the network layer is achieved in Identity Enabled Networks by updating the mapping database to reflect changes.

From the perspective of user equipment (UE) (e.g., smartphone, automobile, airplane...) there are three common mobility scenarios:

- Mobility of nodes within a single provider network
- Mobility of nodes between provider networks
- Mobility of subnet (within a provider network or between them)

7.1. Case 9: Mobility within a single provider network

Figure 4 provides an example of the topology of a single mobile carrier network. UE.A, UE.B, and UE.C are devices connected to the mobile network and are themselves mobile. UE.A and UE.B are currently connected to base station Base1 and UE.C is currently connected to Base2. The base stations are connected to the radio access network (RAN) of the provider. The RAN is connected to the Internet via a mapping gateway (MGW) which co-hosts the GRIDS for all ID services. Host1 Host1 and Host2 are hosts in the Internet that are communicating with the UEs. In this example we assume that ID functionality is handled within the network and is transparent to the UEs or hosts.
The role of the MGW is to leverage the GRIDS that maps destination addresses on ingress packets into the network to deliver packets to the destination. The GRIDS maintain a list of ID-to-LOC mappings. Hosts on the Internet only know the identifier of the mobile nodes. Depending on the dataplane solution packets forwarded from the Internet may be routed to a MGW that is able to retrieve the mapping ID to the destination LOC to facilitate delivery.

Consider that Host1 sends a packet to UE.A. The destination address of the packet is the identifier address of UE.A. The packet is sent by Host1 and is forwarded across the Internet to the provider’s network based on the identifier address. A MGW receives the packet. The destination address of a packet (identifier) is looked up in the mapping table. The return result is the LOC for UE.A. The MGW modifies the packet so that the destination address is the LOC for UE.A (either by encapsulation or address translation). The packet is then forwarded to Base1. At Base1 the destination is changed back to the identifier address and forwarded to the UE.

In the case that two UEs need to communicate the process is similar. Consider that UE.A sends a packet to UE.C. Again, UE.A only knows the identifier address of UE.C. UE.A sends a packet into the network and it is forwarded to a MGW. The MGW maps the destination address of UE.C to its locator and forwards the packet to Base2 which translates the destination back to an identifier address.

In order to reduce latency and improve performance, a mapping cache may be implemented at or near the base stations. A mapping cache would maintain a subset of mappings in the network that are being
used for communications by the attached UEs to other devices in the network. A protocol would be run between the base stations and MGWs to populate and invalidate entries in the cache.

Now consider that UE.B changes locations so that it is now attached to Base2 (figure 5).

The MGWs are updated to reflect UE.B’s new location. As updating location is not instantaneous across all the mapping gateways in the network, it is possible that a packet is forwarded to an old destination. Several possible solutions exist today:

1. Predictive routing. Pre-populating the (ID,LOC) tuple in the GRIDS itself so that multiple packets may get delivered ahead of the move as described in [LISP-PRED]. A predictive algorithm can be used to forward packets ahead of the move with minimum duplication.

2. Late binding. This method refers to rebinding of identifiers to addresses after a packet enters the network. This capability makes it possible for routers in the network to redirect packets whose end-point address might have changed due to fast mobility or rapid changes in radio link association or multicast group membership. This type of dynamic rerouting can help to improve network efficiency and reduce packet drops. Late binding generally requires in-network elements such as routers and base stations to be able to store data packets temporarily and access the ID to address mapping (name resolution) service.
3. Traditional Redirection. For instance, Basel may receive packets for a UE.B after it has moved to Base2. A "care of address" could be set on Basel for some period after the move. When Basel receives a packet for UE.B it can map the destination address to reflect UE.B's new location and forward the packet.

7.2. Case 10: Roaming across Mobile Networks

Consider the example network topology in figure 6. In this case UE.A and UE.B are connected to one provider network and UE.C is connected to another. We assume that the UEs are respectively customers of these attached networks and that they are assigned identifiers from the pool of each carrier (their "home network"). In this configuration connectivity to the UEs is achieved as described above.

When a UE moves between different carrier networks, the ID continues to work if distinct GRIDS can share mapping information across the networks. Consider that UE.B moves to the other carrier network (figure 7).
Suppose Host1 sends a packet destined to UE.B. The identifier address for UE.B is set in the destination address of the packet. The packet is forwarded to the home network for UE.B since the identifier was assigned from that carrier’s pool. In order to handle this the packet can be mapped at the MGW to indicate the location of the current carrier network for UE.B. This can be done in at least two ways:

1. The new carrier provides the full LOC (mapping to Base_station2) and the MGW sends the packet directly to that LOC

2. The packet is mapped so that it is forwarded to an MGW in the new network and that MGW in turn maps the packet to its final destination.

While #1 has the advantage of being more direct, it requires a higher rate of sharing mappings, for instance if UE.B moves to a new base station in the remote carrier network each change in the mapping would need to be propagated to the MGWs UE.B’s home network. In #2 movement within a remote network would be transparent to MGW in the home network.

7.3. Case 11: Mobility of a Subnet

Figure 8 presents a topology where UE.A, UE.B, and UE.C are connected to a subnet and the whole subnet may itself be mobile (for instance a Wi-Fi network on a bus). To treat the subnet as an aggregate devices, the subnet identification is reflected in the identifier address. A single mapping entry then could then represent this
subnet where the identifier is the prefix for the subnet and the locator reflects the location of the subnet (Base1 in this case)

When the subnet moves the mappings to the identifier, the prefix for the subnet is updated in the MGWs (figure 9). Note that a UE could also move out of its subnet and attach to the network on its own, for instance a UE might switch from using Wi-Fi to using a mobile network. This will work if a specific mapping for UEs is allowed in the mapping database, and that mapping is preferred over the aggregate mapping since it has a longer identifier prefix.

Similar to the case of a UE moving between carrier networks, a subnet can move between carrier networks if the networks share identifier locator mappings that include identifier prefixes. Also, subnet mobility can modify community management and therefore impact GRIDS service operation: if UE.A, UE.B, and UE.C have subscribed to
different services where, for example, UE.A exchanges information with UE.B but not with UE.C, whereas, UE.C exchanges information with UE.B but not UE.A, the mobile subnet may support different "closed user groups" that may be serviced by different GRIDS. When the subnet moves, other GRIDS may be invoked to make sure communication within the said closed user groups is not disrupted.

8. Heterogeneous Multi-Access Environments (hetnet)

8.1. Case 12: Dynamic Mobility across Cellular and Wi-Fi

In this case, the UE is multi-homed and moves seamlessly between the cellular network to a Wi-Fi network where the Wi-Fi provider may be different from the cellular provider. In order to achieve session continuity in this case, the UE can rely on ID/LOC mappings with the use of GRIDS.

```
+-----+   /          \
/---| enb |--|  Wireless  +---\______
| LTE ++++-+   /      /      /      (          )    +-----+
\-----+/   \          /          \          /          ( Internet ) +--|Host |

| UE |

+-----+/   \          \________/ (           ) (+-----+)

\ Wi-Fi | hot |---+   |    |
\-------+    \________/ ( Internet ) +--|Host |
```

8.2. Case 13: Ad-hoc Networks Mobility across Hetnet

As smartphones move across various mobility domains, their points of attachment to the Internet can change easily and rapidly. The need for supporting mobility arises when an individual node or a group of nodes move and reconnect to the Internet.

Frequent disconnections and IP address change on re-association to new access points interrupt the data transmission sessions. Solutions like transparent handover between base stations in cellular networks, which let users retain their static IP address, are practical only for intra-network mobility purposes.
Furthermore, there are opportunities for a network to be formed between groups of vehicles on the highway, and these networks should be able to quickly peer along the edge with different networks encountered during mobility. As another emerging use-case consider Google’s Project Loon, which proposes to beam LTE access in developing countries from a network of aerial balloons. The Facebook’s Internet provider drones that aims to provide online access with wireless antennas, lasers, and satellites.

Managing a global scale of unmanned and highly mobile base-stations is challenging, despite the partial solution that BGP currently provides for airline connectivity. Decoupling identity from location provides inherent support for mobility, provided the mapping system is scalable and supports fast query and minimum lookup latencies. Optimizations such as "late binding", in which identity of in-transit packets can be bound to a locator closer to the edge of the network to account for highly mobile vehicular scenarios can be further developed based on the GRIDS.

The Ad-hoc networks of the future such as driverless cars will need secured services and communications. Today, the cost of reestablishing both the session and any security association is prohibitive in real-time applications. The local and proximity services on the GRIDS could be leveraged to provide the session continuity and security features.

8.3. Case 14: Multi-network Access Support

A typical mobile device (smartphones, cars, ..) can see multiple available networks at the same time and can be multi-homed. Although the majority of current business models generally restrict a user to a single cellular network provider, with the increasing popularity of "hetnet" mobile services, mobile device might be soon able to simultaneously connect to a dynamically changing set of cellular, WiFi and future 5G networks.

It is possible to consider a variety of service objectives for this scenario, ranging from "most cost-effective" to "highest throughput interface" to "all interfaces".

End-to-end solutions to support multi-path connectivity do exist, but supporting network-wide multi-homing has a very broad architectural implication. This implication stems from having more fine-grained control over network resources, complete information regarding forwarding path quality and load conditions and more adaptive response to congestion/loss. Since these networks will in general be in different Internet domains, autonomous systems need to support independent paths of connectivity for a single end-to-end flow.
Furthermore, there is a high cost associated with session continuity and security features for seamless and transparent switching between different networks. It is possible to create redundant connections (like MPTCP) over redundant networks. However, it is a very static solution and difficult to predict which network is being used if the switch is in the order of seconds. ID-based solutions may benefit use cases where cars trying to use V2V, V2X, 5G, 802.11p, etc. all at the same time.

8.4. Case 15: Disconnection-tolerant routing

While disconnection-tolerant (DTN) routing has been principally considered for ad-hoc disaster-relief, vehicular and tactical network scenarios, temporary disconnections during mobility also require support for store and forward capabilities of DTN.

Session-oriented transport protocols like TCP react adversely to disconnections and have a slow re-connection and end-to-end setup delays, whereas unreliable protocols like UDP simply drops packet on disconnection. Having in-network routers store in-transit packets while allowing a "rebinding" of identity to location would improve end-to-end transport and enable newer mobility-centric transport protocols for 5G.

9. Security

9.1. Case 16: Policy Access Control

For privacy or security reasons, an entity may only want a designated list of authorized entities to look up its locators and access it. To this end, the entity can specify an access control list in the GRIDS and let the GRIDS enforce the access control at the locator resolution phase. For example, when Alice wants to communicate with Bob, she has to look for the Bob’s ID in the GRIDS to get his locator. The GRIDS verifies Alice’s ID and checks the ID against Bob’s access control list. If Alice is authorized, the GRIDS returns Bob’s up-to-date locators; otherwise the GRIDS returns an error.
10. Discovery of devices

10.1. Case 17: Low Cost Asset tracking

Asset tracking with extremely low cost has become popular with offerings like bike sharing services. There is a need to track the exact location of individual bikes with low cost in long time span. In this case, there must have a module with a secure identifier of the bike and can be set up communications whenever needed. The information associated with the identifier should be maintained with efficient resolution capability for tracking the labeled asset.

11. Security Considerations

This document does not introduce any new security concerns.

12. IANA Considerations

This document has no actions for IANA.

13. Contributors

This present document is based on an extract of the first version of the draft. The authors and their affiliations on the original document are: D. Farinacci (lispers.net), D. Meyer (Brocade), D. Lake (Cisco Systems), T. Herbert (Facebook), M. Menthe (University of Tuebingen), Dipenkar Raychaudhuri (Rutgers University), Julius Mueller (ATT) and Padma Pillay-Esnault (Huawei).
There are two companion documents also extracted from the -00 version of the document above: Problem Statement for Identity Enabled Networks [IDEAS-PS] and GRIDS Requirements [IDEAS-REQ] which regroups all the authors above.

The authors would like to acknowledge the contributions of

Rutgers University: Parishad Karimi and Shreyasee Mukherjee
Huawei: Da Bin and Liu Binyang.

14. Acknowledgments

The authors would like to thank Kevin Smith, Alex Clemm, Uma Chunduri and Yingzhen Qu for their review and input on this document.

This document was produced using Marshall Rose’s xml2rfc tool.

15. References

15.1. Normative References


15.2. Informative References


Padma Pillay-Esnault (editor)
Huawei
2330 Central Expressway
Santa Clara, CA 95050
USA

Email: padma.ietf@gmail.com

Dino Farinacci
lispers.net
San Jose California
USA

Email: farinacci@gmail.com

Tom Herbert
Facebook

Email: tom@herbertland.com