MN Identifier Types for RFC 4283 Mobile Node Identifier Option
draft-ietf-dmm-4283mnids-08.txt

Abstract

   Additional Identifier Type Numbers are defined for use with the
   Mobile Node Identifier Option for MIPv6 (RFC 4283).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

   The Mobile Node Identifier Option for MIPv6 [RFC4283] has proved to
   be a popular design tool for providing identifiers for mobile nodes
   during authentication procedures with AAA protocols such as Diameter
   [RFC3588]. To date, only a single type of identifier has been
   specified, namely the MN NAI. Other types of identifiers are in
   common use, and even referenced in RFC 4283. In this document, we
   propose adding some basic types that are defined in various
   telecommunications standards, including types for IMSI
   [ThreeGPP-IDS], P-TMSI [ThreeGPP-IDS], IMEI [ThreeGPP-IDS], and GUTI
   [ThreeGPP-IDS]. In addition, we specify the IPv6 address itself and
   IEEE MAC-layer addresses as mobile node identifiers. Defining
   identifiers that are tied to the physical elements of the device (

MAC address etc.) help in deployment of Mobile IP because in many
cases such identifiers are the most natural means for uniquely
identifying the device, and will avoid additional look-up steps that
might be needed if other identifiers were used.

2. Terminology

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

3. New Mobile Node Identifier Types

The following types of identifiers are commonly used to identify
mobile nodes. For each type, references are provided with full
details on the format of the type of identifer.

                Mobile Node Identifier Description

Identifier Type	Description	Reference
IPv6 Address		[RFC4291]
IMSI	International Mobile Subscriber Identity	[ThreeGPP-IDS]
P-TMSI	Packet-Temporary Mobile Subscriber Identity	[ThreeGPP-IDS]
GUTI	Globally Unique Temporary ID	[ThreeGPP-IDS]
EUI-48 address	48-bit Extended Unique Identifier	[IEEE802]
EUI-64 address	64-bit Extended Unique Identifier-64 bit	[IEEE802]
DUID	DHCPv6 Unique Identifier	[RFC3315]

                              Table 1

4. Descriptions of MNID types

In this section descriptions for the various MNID types are provided.

4.1. Description of the IPv6 address type

The IPv6 address [RFC4291] is encoded as a 16 octet string containing
a full IPv6 address which has been assigned to the mobile node. The
IPv6 address MUST be a unicast routable IPv6 address. Multicast

addresses, link-local addresses, and the unspecified IPv6 address
MUST NOT be used. IPv6 Unique Local Addresses (ULAs) MAY be used, as
long as any security operations making use of the ULA also take into
account the domain in which the ULA is guaranteed to be unique.

4.2. Description of the IMSI MNID type

The International Mobile Subscriber Identity (IMSI) [ThreeGPP-IDS] is
at most 15 decimal digits (i.e., digits from 0 through 9). The IMSI
MUST be encoded as a string of octets in network order (i.e., high-
to-low for all digits), where each digit occupies 4 bits. If needed
for full octet size, the last digit MUST be padded with 0xf. For
example an example IMSI 123456123456789 would be encoded as follows:

    0x12, 0x34, 0x56, 0x12, 0x34, 0x56, 0x78, 0x9f

4.3. Description of the EUI-48 address type

The IEEE EUI-48 address [IEEE802-eui48] is encoded as 6 octets
containing the IEEE EUI-48 address.

4.4. Description of the EUI-64 address type

The IEEE EUI-64 address [IEEE802-eui64] is encoded as 8 octets
containing the full IEEE EUI-64 address.

4.5. Description of the DUID type

The DUID is the DHCPv6 Unique Identifier (DUID) [RFC3315]. There are
various types of DUID, which are distinguished by an initial two-
octet type field. Clients and servers MUST treat DUIDs as opaque
values and MUST only compare DUIDs for equality.

5. Security Considerations

This document does not introduce any security mechanisms, and does
not have any impact on existing security mechanisms.

Mobile Node Identifiers such as those described in this document are
considered to be private information. If used in the MNID extension
as defined in [RFC4283], the packet including the MNID extension MUST
be encrypted so that no personal information or trackable identifiers
is inadvertently disclosed to passive observers. Operators can
potentially apply IPsec Encapsulating Security Payload (ESP)
[RFC4303], in transport mode, with confidentiality and integrity
protection for protecting the identity and location information in
Mobile IPv6 signaling messages.

Some MNIDs contain sensitive identifiers which, as used in protocols
specified by other SDOs, are only used for signaling during initial
network entry. In such protocols, subsequent exchanges then rely on
a temporary identifier allocated during the initial network entry.
Managing the association between long-lived and temporary identifiers
is outside the scope of this document.

6. IANA Considerations

The new mobile node identifier types defined in the document should
be assigned values from the "Mobile Node Identifier Option Subtypes"
registry. The following values should be assigned.

New Mobile Node Identifier Types

```
+-----------------+------------------------+
| Identifier Type | Identifier Type Number |
+-----------------+------------------------+
| IPv6 Address    | 2                      |
| IMSI            | 3                      |
| P-TMSI          | 4                      |
| EUI-48 address  | 5                      |
| EUI-64 address  | 6                      |
| GUTI            | 7                      |
| DUID-LLT        | 8                      |
| DUID-EN         | 9                      |
| DUID-LL         | 10                     |
| DUID-UUID       | 11                     |
|                 | 12-15 reserved         |
|                 | 16-255 unassigned      |
+-----------------+------------------------+
```

Table 2

See Section 4 for additional information about the identifier types.
Future new assignments are to be made only after Expert Review
[RFC8126]. The expert must ascertain that the identifier type allows
unique identification of the mobile device; since all MNIDs require
encryption there is no additional privacy exposure attendent to the
use of new types.

7. Acknowledgements

The authors wish to acknowledge Hakima Chaouchi, Tatuya Jinmei, Jouni
Korhonen, Sri Gundavelli, Suresh Krishnan, Dapeng Liu, Dale Worley,
Joseph Salowey, Linda Dunbar, and Mirja Kuehlewind for their helpful
comments.

8. References

8.1. Normative References

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

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins,
           C., and M. Carney, "Dynamic Host Configuration Protocol
           for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July
           2003, <https://www.rfc-editor.org/info/rfc3315>.

[RFC4283] Patel, A., Leung, K., Khalil, M., Akhtar, H., and K.
           Chowdhury, "Mobile Node Identifier Option for Mobile IPv6
           (MIPv6)", RFC 4283, DOI 10.17487/RFC4283, November 2005,
           <https://www.rfc-editor.org/info/rfc4283>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
           Architecture", RFC 4291, DOI 10.17487/RFC4291, February
           2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)",
           RFC 4303, DOI 10.17487/RFC4303, December 2005,
           <https://www.rfc-editor.org/info/rfc4303>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for
           Writing an IANA Considerations Section in RFCs", BCP 26,
           RFC 8126, DOI 10.17487/RFC8126, June 2017,
           <https://www.rfc-editor.org/info/rfc8126>.

8.2. Informative References

[EANUCCGS]
           EAN International and the Uniform Code Council, "General
           EAN.UCC Specifications Version 5.0", Jan 2004.

[EPC-Tag-Data]
           EPCglobal Inc., "EPC(TM) Generation 1 Tag Data Standards
           Version 1.1 Rev.1.27
           http://www.gs1.org/gsmp/kc/epcglobal/tds/
           tds_1_1_rev_1_27-standard-20050510.pdf", January 2005.

[IEEE802] IEEE, "IEEE Std 802: IEEE Standards for Local and
           Metropolitan Networks: Overview and Architecture", 2001.

[IEEE802-eui48]
          IEEE, "Guidelines for 48-Bit Global Identifier (EUI-48)
          https://standards.ieee.org/develop/regauth/tut/eui48.pdf",
          2001.

[IEEE802-eui64]
          IEEE, "Guidelines for 64-Bit Global Identifier (EUI-64)
          https://standards.ieee.org/develop/regauth/tut/eui.pdf64",
          2001.

[RFC3588] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., and J.
          Arkko, "Diameter Base Protocol", RFC 3588,
          DOI 10.17487/RFC3588, September 2003,
          <https://www.rfc-editor.org/info/rfc3588>.

[RFID-DoD-spec]
          Department of Defense, "United States Department of
          Defense Suppliers Passive RFID Information Guide (Version
          15.0)", January 2010.

[RFID-framework]
          Institut National des Telecommunication, ""Heterogeneous
          RFID framework design, analysis and evaluation"", July
          2012.

[ThreeGPP-IDS]
          3rd Generation Partnership Project, "3GPP Technical
          Specification 23.003 V8.4.0: Technical Specification Group
          Core Network and Terminals; Numbering, addressing and
          identification (Release 8)", March 2009.

[TRACK-IoT]
          IPv6.com, ""Heterogeneous IoT Network : TRACK-IoT"", March
          2012.

[Using-RFID-IPv6]
          IPv6.com, ""Using RFID & IPv6"", September 2006.

Appendix A. RFID types

The material in this non-normative appendix was originally composed
for inclusion in the main body of the specification, but was moved
into an appendix because there was insufficient support for
allocating RFID types at this time. It was observed that RFID-based
mobile devices may create privacy exposures unless confidentiality is
assured for signaling. A specification for eliminating unauthorized
RFID tracking based on layer-2 addresses would be helpful.

Much of the following text is due to contributions from Hakima Chaouchi. For an overview and some initial suggestions about using RFID with IPv6 on mobile devices, see [Using-RFID-IPv6].

In the context of IoT and industry 4.0 vertical domain, efficient inventory and tracking items is of major interest, and RFID technology is the identification technology in the hardware design of many such items.

The "TRACKIOT: Heterogeneous IoT control" project ([TRACK-IoT], [RFID-framework]) explored Mobile IPv6 as a mobility management protocol for RFID-based mobile devices.

1. Passive RFID tags (that have no processing resources) need to be handled by the gateway (likely also the RFID Reader), which is then the end point of the mobility protocol. It is also the point where the CoA will be created based on some combination such as the RFID tag and the prefix of that gateway. The point here is to offer the possibility to passive RFID items to get an IPv6 address and take advantage of the mobility framework to follow the mobile device (passive tag on the item). One example scenario that has been proposed, showing the need for mobility management of passive RFID items, would be pieces of art tagged with passive tags that need to be monitored while transported.

2. Using active RFID tags (where processing resource is available on the tag), the end point of the mobility protocol can be pushed up to the RFID Active tag. We name it also an identification sensor. Use cases include active RFID tags for traceability of cold food respect during mobility (transport) of food. Mobility of cars equiped with active RFID tags that we already use for toll payement can be added with mobility management.

One major effort of connecting IETF efforts to the EPCGlobal (RFID standardisation) led to the ONS (DNS version applied for RFID logical names and page information retrieval). Attempts have tried to connect IPv6 on the address space to RFID identifier format. Other initiatives started working on gateways to map tag identifiers with IPv6 addresses and build signaling protocols for the application level. For instance tracking of mobile items equipped with a tag can be triggered remotely by a remote correspondent node until a visiting area where a mobile item equipped with an RFID tag is located. An RFID reader will be added with an IPv6 to RFID tag translation. One option is to build a Home IPv6 address of that tagged item by using the prefix of the Home agent combined with the tag RFID identifier of the mobile item; as the tag ID is unique, the home IPv6 address of that item will be also unique. Then the visiting RFID reader will compose the IPV6 care of address of the tagged mobile item by combining the prefix of the RFID reader with the tag ID of the item).

   MIPv6 can then provide normally the mobility management of that RFID
   tagged item. A different useful example of tagged items involves
   items of a factory that can be tracked while they are transported,
   especially for real time localisation and tracking of precious items
   transported without GPS. An automotive car manufacturer can assign
   IPv6 addresses corresponding to RFID tagged cars or mechanical car
   parts, and build a tracking dataset of the mobility not only of the
   cars, but also of the mechanical pieces.

   The Tag Data standard promoted by Electronic Product Code(TM)
   (abbreviated EPC) [EPC-Tag-Data] supports several encoding systems or
   schemes, which are commonly used in RFID (radio-frequency
   identification) applications, including

   o RFID-GID (Global Identifier),
   o RFID-SGTIN (Serialized Global Trade Item Number),
   o RFID-SSCC (Serial Shipping Container),
   o RFID-SGLN (Global Location Number),
   o RFID-GRAI (Global Returnable Asset Identifier),
   o RFID-DOD (Department of Defense ID), and
   o RFID-GIAI (Global Individual Asset Identifier).

   For each RFID scheme except GID, there are three representations:

   o a 64-bit binary representation (for example, SGLN-64) (except for
      GID)
   o a 96-bit binary representation (SGLN-96)
   o a representation as a URI

   The URI representation for the RFID is actually a URN. The EPC
   document has the following language:

      All categories of URIs are represented as Uniform Reference Names
      (URNs) as defined by [RFC2141], where the URN Namespace is epc.

   The following list includes the above RFID types.

Mobile Node RFID Identifier Description

```
+----------------+-------------------------------+----------------+
| Identifier     | Description                   | Reference      |
| Type           |                               |                |
+----------------+-------------------------------+----------------+
| RFID-SGTIN-64  | 64-bit Serialized Global Trade| [EPC-Tag-Data] |
|                | Item Number                   |                |
| RFID-SSCC-64   | 64-bit Serial Shipping        | [EPC-Tag-Data] |
|                | Container                     |                |
| RFID-SGLN-64   | 64-bit Serialized Global      | [EPC-Tag-Data] |
|                | Location Number               |                |
| RFID-GRAI-64   | 64-bit Global Returnable Asset| [EPC-Tag-Data] |
|                | Identifier                    |                |
| RFID-DOD-64    | 64-bit Department of Defense  | [RFID-DoD-spec]|
|                | ID                            |                |
| RFID-GIAI-64   | 64-bit Global Individual Asset| [EPC-Tag-Data] |
|                | Identifier                    |                |
| RFID-GID-96    | 96-bit Global Identifier      | [EPC-Tag-Data] |
| RFID-SGTIN-96  | 96-bit Serialized Global Trade| [EPC-Tag-Data] |
|                | Item Number                   |                |
| RFID-SSCC-96   | 96-bit Serial Shipping        | [EPC-Tag-Data] |
|                | Container                     |                |
| RFID-SGLN-96   | 96-bit Serialized Global      | [EPC-Tag-Data] |
|                | Location Number               |                |
| RFID-GRAI-96   | 96-bit Global Returnable Asset| [EPC-Tag-Data] |
|                | Identifier                    |                |
| RFID-DOD-96    | 96-bit Department of Defense  | [RFID-DoD-spec]|
|                | ID                            |                |
| RFID-GIAI-96   | 96-bit Global Individual Asset| [EPC-Tag-Data] |
|                | Identifier                    |                |
| RFID-GID-URI   | Global Identifier represented | [EPC-Tag-Data] |
|                | as URI                        |                |
| RFID-SGTIN-URI | Serialized Global Trade Item  | [EPC-Tag-Data] |
|                | Number represented as URI     |                |
| RFID-SSCC-URI  | Serial Shipping Container      | [EPC-Tag-Data] |
|                | represented as URI            |                |
| RFID-SGLN-URI  | Global Location Number        | [EPC-Tag-Data] |
|                | represented as URI            |                |
| RFID-GRAI-URI  | Global Returnable Asset       | [EPC-Tag-Data] |
|                | Identifier represented as URI |                |
| RFID-DOD-URI   | Department of Defense ID      | [RFID-DoD-spec]|
|                | represented as URI            |                |
| RFID-GIAI-URI  | Global Individual Asset       | [EPC-Tag-Data] |
|                | Identifier represented as URI |                |
+----------------+-------------------------------+----------------+
```

Table 3

A.1. Description of the RFID types

   The General Identifier (GID) that is used with RFID is composed of
   three fields - the General Manager Number, Object Class and Serial
   Number. The General Manager Number identifies an organizational
   entity that is responsible for maintaining the numbers in subsequent
   fields. GID encodings include a fourth field, the header, to
   guarantee uniqueness in the namespace defined by EPC.

   Some of the RFID types depend on the Global Trade Item Number (GTIN)
   code defined in the General EAN.UCC Specifications [EANUCCGS]. A
   GTIN identifies a particular class of object, such as a particular
   kind of product or SKU.

   The EPC encoding scheme for SGTIN permits the direct embedding of
   EAN.UCC System standard GTIN and Serial Number codes on EPC tags. In
   all cases, the check digit is not encoded. Two encoding schemes are
   specified, SGTIN-64 (64 bits) and SGTIN-96 (96 bits).

   The Serial Shipping Container Code (SSCC) is defined by the EAN.UCC
   Specifications. Unlike the GTIN, the SSCC is already intended for
   assignment to individual objects and therefore does not require
   additional fields to serve as an EPC pure identity. Two encoding
   schemes are specified, SSCC-64 (64 bits) and SSCC-96 (96 bits).

   The Global Location Number (GLN) is defined by the EAN.UCC
   Specifications. A GLN can represent either a discrete, unique
   physical location such as a warehouse slot, or an aggregate physical
   location such as an entire warehouse. In addition, a GLN can
   represent a logical entity that performs a business function such as
   placing an order. The Serialized Global Location Number (SGLN)
   includes the Company Prefix, Location Reference, and Serial Number.

   The Global Returnable Asset Identifier (GRAI) is defined by the
   General EAN.UCC Specifications. Unlike the GTIN, the GRAI is already
   intended for assignment to individual objects and therefore does not
   require any additional fields to serve as an EPC pure identity. The
   GRAI includes the Company Prefix, Asset Type, and Serial Number.

   The Global Individual Asset Identifier (GIAI) is defined by the
   General EAN.UCC Specifications. Unlike the GTIN, the GIAI is already
   intended for assignment to individual objects and therefore does not
   require any additional fields to serve as an EPC pure identity. The
   GRAI includes the Company Prefix, and Individual Asset Reference.

   The DoD Construct identifier is defined by the United States
   Department of Defense (DoD). This tag data construct may be used to

encode tags for shipping goods to the DoD by a supplier who has
already been assigned a CAGE (Commercial and Government Entity) code.

A.1.1. Description of the RFID-SGTIN-64 type

The RFID-SGTIN-64 is encoded as specified in [EPC-Tag-Data]. The
SGTIN-64 includes five fields: Header, Filter Value (additional data
that is used for fast filtering and pre-selection), Company Prefix
Index, Item Reference, and Serial Number. Only a limited number of
Company Prefixes can be represented in the 64-bit tag.

A.1.2. Description of the RFID-SGTIN-96 type

The RFID-SGTIN-96 is encoded as specified in [EPC-Tag-Data]. The
SGTIN-96 includes six fields: Header, Filter Value, Partition (an
indication of where the subsequent Company Prefix and Item Reference
numbers are divided), Company Prefix Index, Item Reference, and
Serial Number.

A.1.3. Description of the RFID-SSCC-64 type

The RFID-SSCC-64 is encoded as specified in [EPC-Tag-Data]. The
SSCC-64 includes four fields: Header, Filter Value, Company Prefix
Index, and Serial Reference. Only a limited number of Company
Prefixes can be represented in the 64-bit tag.

A.1.4. Description of the RFID-SSCC-96 type

The RFID-SSCC-96 is encoded as specified in [EPC-Tag-Data]. The
SSCC-96 includes six fields: Header, Filter Value, Partition, Company
Prefix, and Serial Reference, as well as 24 bits that remain
Unallocated and must be zero.

A.1.5. Description of the RFID-SGLN-64 type

The RFID-SGLN-64 type is encoded as specified in [EPC-Tag-Data]. The
SGLN-64 includes five fields: Header, Filter Value, Company Prefix
Index, Location Reference, and Serial Number.

A.1.6. Description of the RFID-SGLN-96 type

The RFID-SGLN-96 type is encoded as specified in [EPC-Tag-Data]. The
SGLN-96 includes six fields: Header, Filter Value, Partition, Company
Prefix, Location Reference, and Serial Number.

A.1.7. Description of the RFID-GRAI-64 type

   The RFID-GRAI-64 type is encoded as specified in [EPC-Tag-Data]. The
   GRAI-64 includes five fields: Header, Filter Value, Company Prefix
   Index, Asset Type, and Serial Number.

A.1.8. Description of the RFID-GRAI-96 type

   The RFID-GRAI-96 type is encoded as specified in [EPC-Tag-Data]. The
   GRAI-96 includes six fields: Header, Filter Value, Partition, Company
   Prefix, Asset Type, and Serial Number.

A.1.9. Description of the RFID-GIAI-64 type

   The RFID-GIAI-64 type is encoded as specified in [EPC-Tag-Data]. The
   GIAI-64 includes four fields: Header, Filter Value, Company Prefix
   Index, and Individual Asset Reference.

A.1.10. Description of the RFID-GIAI-96 type

   The RFID-GIAI-96 type is encoded as specified in [EPC-Tag-Data]. The
   GIAI-96 includes five fields: Header, Filter Value, Partition,
   Company Prefix, and Individual Asset Reference.

A.1.11. Description of the RFID-DoD-64 type

   The RFID-DoD-64 type is encoded as specified in [RFID-DoD-spec]. The
   DoD-64 type includes four fields: Header, Filter Value, Government
   Managed Identifier, and Serial Number.

A.1.12. Description of the RFID-DoD-96 type

   The RFID-DoD-96 type is encoded as specified in [RFID-DoD-spec]. The
   DoD-96 type includes four fields: Header, Filter Value, Government
   Managed Identifier, and Serial Number.

A.1.13. Description of the RFID URI types

   In some cases, it is desirable to encode in URI form a specific
   encoding of an RFID tag. For example, an application may prefer a
   URI representation for report preparation. Applications that wish to
   manipulate any additional data fields on tags may need some
   representation other than the pure identity forms.

   For this purpose, the fields as represented the previous sections are
   associated with specified fields in the various URI types. For
   instance, the URI may have fields such as CompanyPrefix,

ItemReference, or SerialNumber. For details and encoding specifics, consult [EPC-Tag-Data].

Authors' Addresses

Charles E. Perkins
Futurewei Inc.
2330 Central Expressway
Santa Clara, CA 95050
USA

Phone: +1-408-330-4586
Email: charliep@computer.org

Vijay Devarapalli
Vasona Networks
2900 Lakeside Drive, Suite 180
Santa Clara, CA 95054
USA

Email: dvijay@gmail.com