Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 16, 2012

A. Garcia-Martinez
M. Bagnulo
UC3M

October 14, 2011

Management Information Base for Cryptographically Generated Addresses (CGA)
draft-garcia-martinez-cgamib-03

Abstract

This memo defines a portion of the Management Information Base (MIB) for managing Cryptographically Generated Addresses (CGA).

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 April 16, 2012.

Copyright Notice

Table of Contents

1. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410]. Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

2. Overview

This document defines the portion of the Management Information Base (MIB) to be used for managing Cryptographically Generated Addresses (CGA) [RFC3972]. CGA addresses are IPv6 addresses for which the interface identifier is generated by computing a one-way hash function from a public signature key and some auxiliary parameters. Therefore, CGA are represented in this MIB module as values of the InetAddressIPv6 type defined in [RFC4001].

Two tables are defined, cgaLocalTable for representing the information about CGA local to the managed node, and cgaRemoteTable for representing CGA of nodes with which the managed node is communicating to.

Rows in the cgaLocalTable may be created by means of the management protocol. Once a row for a CGA has been created in the cgaLocalTable, it can be used as a local address by the node when the configuration of the corresponding rows in the ipAddressTable [RFC4293] is completed. A discrete spin lock object is used to coordinate the creation of rows by different managers.

Rows in the cgaRemoteTable are created as a result of CGA-aware protocol operation, such as SEND [RFC3971] or Shim6 [RFC5533] operation.

3. Conventions

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 RFC 2119 [RFC2119].

4. Definitions

```
CGA-MIB DEFINITIONS ::= BEGIN

IMPORTS

   MODULE-IDENTITY,
   OBJECT-TYPE,
   mib-2,
   zeroDotZero                                  FROM SNMPv2-SMI
   TEXTUAL-CONVENTION,
   TestAndIncr,
   RowStatus,
   StorageType,
   TimeStamp,
   RowPointer                                   FROM SNMPv2-TC
   MODULE-COMPLIANCE,
   OBJECT-GROUP                                 FROM SNMPv2-CONF
   InetAddressIPv6                      FROM INET-ADDRESS-MIB;

cgaMIB MODULE-IDENTITY
    LAST-UPDATED "201102020000Z"
    ORGANIZATION "IETF CSI (Cga & Send Maintenance) Working Group"
    CONTACT-INFO
           "Editor:

           Alberto Garcia-Martinez
           U. Carlos III de Madrid
           Avenida Universidad, 30
```

```
            Leganes, Madrid 28911
            Spain
            Email: alberto.garcia@uc3m.es"

        DESCRIPTION
            " The MIB module for managing Cryptographically Generated
            Addresses (CGA) [RFC3972].

            Copyright (c) 2011 IETF Trust and the persons identified
            as the document authors.  All rights reserved.
            This version of this MIB module is part of RFC yyyy; see
            the RFC itself for full legal notices."

        -- RFC Ed.: replace yyyy with actual RFC number & remove this
        -- note

        REVISION "201102020000Z"
```



```
        DESCRIPTION
            "Initial version, published as RFC yyyy."

               -- RFC Ed.: replace yyyy with actual RFC number & remove
               -- this note

        ::= { mib-2 XXX }

           -- RFC Ed.: replace XXX with actual number assigned by IANA
           -- & remove this note


    --
    -- The textual conventions we define and use in this MIB.
    --

    CgaModifier ::= TEXTUAL-CONVENTION
        DISPLAY-HINT "16x"
        STATUS current
        DESCRIPTION
            "This is a binary string of 16 octets in network byte-
            order representing a 128-bit unsigned integer, which
```

```
            models the 'Modifier' parameter of the CGA."
        SYNTAX OCTET STRING (SIZE (16))

    CgaCollisionCount ::= TEXTUAL-CONVENTION
        STATUS current
        DESCRIPTION
            "This enumerated integer models the 'Collision Count'
            parameter of the CGA."
        SYNTAX INTEGER {
            zerocollisions(0),
            onecollision(1),
            twocollisions(2)
        }

    CgaKeyInfo::= TEXTUAL-CONVENTION
        DISPLAY-HINT "1024x"
        STATUS current
        DESCRIPTION
            "Variable-length field containing the key (either public
            or private) of the address (CGA) owner.  The key MUST be
            formatted as a DER-encoded [CCITT.X690.2002] ASN.1
            structure of the type SubjectPublicKeyInfo, defined in the
            Internet X.509 certificate profile [RFC5280].  When RSA is
            used, the algorithm identifier MUST be 'rsaEncryption',
            which is 1.2.840.113549.1.1.1, and the RSA public key MUST
            be formatted by using the RSAPublicKey type as specified
```



```
            in Section 2.3.1 of RFC 3279 [RFC3279].
            The length of this field is determined by the ASN.1
            encoding."
        REFERENCE "RFC 3279, RFC 5280, ITU-T Recommendation X.690"
        SYNTAX OCTET STRING (SIZE (0..1024))

    cga OBJECT IDENTIFIER ::= { cgaMIB 1 }

    --
    -- Information related to local CGA
    --

    cgaLocalSpinLock OBJECT-TYPE
        SYNTAX TestAndIncr
        MAX-ACCESS read-write
```

```
        STATUS current
        DESCRIPTION
                "An advisory lock used to allow cooperating SNMP managers
                to coordinate their use of the set operation in creating
                or removing rows within the cgaLocalTable.  Note that the
                rows in the cgaLocalTable MUST remain unmodified (except
                for the RowStatus columnar object) once the cgaLocalStatus
                columnar object has been set to enabled(2).
                In order to use this lock to coordinate the use of set
                operations, managers SHOULD first retrieve
                cgaLocalSpinLock.  They SHOULD then determine the
                appropriate row to create or remove (setting the
                appropriate value to the cgaLocalRowStatus object).
                Finally, they SHOULD issue the appropriate set command,
                including the retrieved value of cgaLocalSpinLock.  If
                another manager has created or destroyed the row in the
                meantime, then the value of cgaLocalSpinLock will have
                changed, and the creation will fail as it will be
                specifying an incorrect value for cgaLocalSpinLock.  It is
                suggested, but not required, that the cgaLocalSpinLock be
                the first var bind for each set of objects representing a
                'row' in a PDU."
        ::= { cga 1 }

    cgaLocalTable OBJECT-TYPE
        SYNTAX SEQUENCE OF CgaLocalEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "This table contains information describing the CGA
                parameters which can be used to configure local addresses
                in the managed system."
```



```
                ::= { cga 2 }

    cgaLocalEntry OBJECT-TYPE
        SYNTAX CgaLocalEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "Each row defines the information required to configure
```

and use a CGA as a local address in the managed system. In order to have a local IP address configured as a CGA, two conditions MUST be fulfilled:

+ A row in the cgaLocalTable with cgaLocalStatus set to enabled(2). The enabled(2) value can only be set if the information held in the columnar objects of the row is valid according to the verification process defined in section 5 of [RFC3972].
+ A row IP-MIB:ipAddressTable with a IP-MIB:ipAddressAddr value equal to the cgaLocalAddr, with a IP-MIB:ipAddressRowStatus value set to active(1), and with an appropriate IP-MIB:ipAddressStatus value - for example, not invalid(3) or inaccessible(4).

If the cgaLocalStatus of a row is set to enabled(2) when the corresponding row in IP-MIB:ipAddressTable does not exist, this row SHOULD be created and its IP-MIB:ipAddressRowStatus value should be set to active(1). In this case, the address MUST behave as a CGA since its very activation as an IP address: For example, in a node with SEND operation enabled, the Duplicate Address Detection procedure for this address will be performed as described in the SEND specification [RFC3971], using the CGA-specific information.

If a local IP address is configured as a CGA, but the corresponding row in the cgaLocalTable is made unusable or the cgaLocalStatus value is set to a value different to enabled(2), the CGA SHOULD continue to be usable as an IP address, although CGA-aware protocols SHOULD stop using it as a CGA. For example, Shim6 could keep the communications established, although may not use the CGA information for new communications; or could tear down all communications using Shim6, and stop using the CGA.

If a row in the IP-MIB:ipAddressTable exists with its IP-MIB:ipAddressRowStatus set to active(1) exists, but there is no correspondent entry in the cgaLocalTable or the corresponding entry has a cgaLocalStatus object set to a value different to enabled(2), then the IP address is configured, but it does not behave as a CGA. Then, cgaLocalStatus value of the corresponding row in the

cgaLocalTable is set to to enabled(2), the node SHOULD

```
                start using the address as a CGA for the operation of the
                CGA-aware protocols.
                If a row in the cgaLocalTable with the cgaLocalStatus
                object set to enabled(2) exists, but the IP address is not
                configured because there is no correspondent row in the
                IP-MIB:ipAddressTable (for example, because it has been
                removed after creation of the CGA) or the IP-
                MIB:ipAddressRowStatus is not set to active(1), and then
                the value IP-MIB:ipAddressRowStatus is set to active(1),
                the node SHOULD start using the address as a CGA for the
                operation of the CGA-aware protocols.
                Once the value of the cgaLocalStatus of an entry has been
                set once to enabled(2), the cgaLocalModifier,
                cgaLocalCollisionCount, cgaLocalPublicKey,
                cgaLocalPrivateKey and cgaLocalExtensionFields columnar
                objects of the entry MUST remain unmodified.
                The agent may generate new entries by other means than
                network management."
        INDEX { cgaLocalAddr }
        ::= { cgaLocalTable 1 }

    CgaLocalEntry ::= SEQUENCE {
            cgaLocalAddr InetAddressIPv6,
            cgaLocalModifier CgaModifier,
            cgaLocalCollisionCount CgaCollisionCount,
            cgaLocalPublicKey CgaKeyInfo,
            cgaLocalPrivateKey CgaKeyInfo,
            cgaLocalExtensionFields OCTET STRING,
            cgaLocalStatus INTEGER,
            cgaLocalAddrInfo RowPointer,
            cgaLocalRowStatus RowStatus,
            cgaLocalStorageType StorageType
        }

    cgaLocalAddr OBJECT-TYPE
        SYNTAX InetAddressIPv6
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
                "The CGA address to which this entry's information
                pertains."
        ::= { cgaLocalEntry 1 }

    cgaLocalModifier OBJECT-TYPE
        SYNTAX CgaModifier
```

```
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
                "Binary string of 16 octets in network byte-order
                representing a 128-bit unsigned integer, which models the
                'Modifier' parameter.
                This object MUST NOT be modified once the
                cgaLocalRowStatus object has been set to enabled(2)."
        ::= { cgaLocalEntry 2 }

    cgaLocalCollisionCount OBJECT-TYPE
        SYNTAX CgaCollisionCount
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
                "This enumerated integer models the 'Collision Count'
                parameter of the CGA.
                This object MUST NOT be modified once the
                cgaLocalRowStatus object has been set to enabled(2)."
        ::= { cgaLocalEntry 3 }

    cgaLocalPublicKey OBJECT-TYPE
        SYNTAX CgaKeyInfo
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
                "Variable-length field containing the public key of the
                address owner which models the 'Public Key' parameter of
                the CGA.
                Upon a set operation, an 'inconsistentValue' error MUST be
                returned if the value is not a DER-encoded ASN.1 structure
                of the type SubjectPublicKeyInfo.
                This object MUST NOT be modified once the
                cgaLocalRowStatus object has been set to enabled(2)."
        REFERENCE "RFC 3279, RFC 5280, ITU-T Recommendation X.690"
        ::= { cgaLocalEntry 4 }

    cgaLocalPrivateKey OBJECT-TYPE
        SYNTAX CgaKeyInfo
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
                "Variable-length field containing the private key of the
                address owner which corresponds to the public key in
                cgaLocalPublicKey.
                Upon a set operation, an 'inconsistentValue' error MUST be
```

```
            This object MUST NOT be modified once the
            cgaLocalRowStatus object has been set to enabled(2).
            Note that read access to this object by an unintended
            party allows this party to impersonate the identity
            defined by any CGA of the node."
        REFERENCE "RFC 3279, RFC 5280, ITU-T Recommendation X.690"
        ::= { cgaLocalEntry 5 }

    cgaLocalExtensionFields OBJECT-TYPE
        SYNTAX OCTET STRING (SIZE (0..1024))
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "Optional variable-length field, defined as an opaque
            type, modeling the 'Extension Fields' field of the CGA.
            This object MUST NOT be modified once the
            cgaLocalRowStatus object has been set to enabled(2)."
        ::= { cgaLocalEntry 6 }

    cgaLocalStatus OBJECT-TYPE
        SYNTAX INTEGER {
            notReady(1),
            enabled(2),
            invalid(3) }
        MAX-ACCESS read-create
        STATUS current
        DESCRIPTION
            "This columnar object indicates whether the row can be
            used as a CGA in the managed system or not.
            If the row is created but this object has not been set,
            its value is notReady(1).  In this state, the information
            of the row MUST NOT be used for address configuration.  In
            addition, it cannot be assumed that the information is
            valid according to the rules stated in section 5 of
            [RFC3972]
            If the administrator wants to made the CGA information in
            this row ready to be used, he MUST set this columnar
            object to enabled(2).  The managed node MUST then check
            the validity of the CGA according to the rules stated in
```

section 5 of [RFC3972]. If the validation is successful, the state is changed to enabled(2). Otherwise, an 'inconsistentValue' error is returned, and the state is set to invalid(3).
The administrator can set this columnar object to notReady(1) to indicate that the information of the CGA is no longer usable.

Note that the invalid(3) value cannot be requested to be set."
DEFVAL { notReady }
::= { cgaLocalEntry 7 }

cgaLocalAddrInfo OBJECT-TYPE
SYNTAX RowPointer
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"Points to the corresponding row in IP-MIB:ipAddressTable if the CGA address is locally configured in the managed system.
If the CGA is not configured as a local address of the node, it contains { 0 0 }."
DEFVAL { zeroDotZero }
::= { cgaLocalEntry 8 }

cgaLocalRowStatus OBJECT-TYPE
SYNTAX RowStatus
MAX-ACCESS read-create
STATUS current
DESCRIPTION
"The status of this conceptual row.
A conceptual row can not be made active until all the columnar objects, except for the cgaLocalStatus, have been assigned a value. Note that validity of the CGA information (according to to the rules stated in section 5 of [RFC3972]) is not required for this object to be active(1)"
::= { cgaLocalEntry 9 }

```
   cgaLocalStorageType OBJECT-TYPE
       SYNTAX StorageType
       MAX-ACCESS read-create
       STATUS current
       DESCRIPTION
              "The storage type for this conceptual row.  If this object
              has a value of 'permanent', then no other objects are
              required to be able to be modified.
              The values of the cgaLocalStorageType and of the
              corresponding IP-MIB:ipAddressStorageType SHOULD be the
              same."
       DEFVAL { volatile }
       ::= { cgaLocalEntry 10 }
```



```
   --
   -- table to store information about the valid CGAs corresponding
   -- to remote nodes
   --

   cgaRemoteTable OBJECT-TYPE
       SYNTAX SEQUENCE OF CgaRemoteEntry
       MAX-ACCESS not-accessible
       STATUS current
       DESCRIPTION
              "List of valid CGA addresses of remote nodes.  Only valid
              CGAs, according to the validation rules of section 5 of
              [RFC3972], MUST appear in this table.
              The agent populates the entries in this table with the
              information obtained using a CGA-aware protocol (i.e.
              SEND or Shim6), and operation with these protocols is
              responsible for deleting the entry according to the rules
              defined for their operation.  Protocol-specific
              information associated with the CGA MUST be managed in a
              MIB specific for the considered protocol.  Note that many
              protocols could be using the same remote CGA.
              Note in addition that each protocol may require different
              rules for validating a CGA (for example, may vary in the
              minimum bits required for the key length).
              All the objects in this table are defined as read-only."
```

```
        ::= { cga 3 }

    cgaRemoteEntry OBJECT-TYPE
        SYNTAX CgaRemoteEntry
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
               "Information related with a remote CGA."
        INDEX { cgaRemoteAddr }
        ::= { cgaRemoteTable 1 }

    CgaRemoteEntry ::= SEQUENCE {
            cgaRemoteAddr InetAddressIPv6,
            cgaRemoteModifier CgaModifier,
            cgaRemoteCollisionCount CgaCollisionCount,
            cgaRemotePublicKey CgaKeyInfo,
            cgaRemoteExtensionFields OCTET STRING,
            cgaRemoteCreated TimeStamp
        }

    cgaRemoteAddr OBJECT-TYPE
```



```
        SYNTAX InetAddressIPv6
        MAX-ACCESS not-accessible
        STATUS current
        DESCRIPTION
               "The CGA IPv6 address of a remote node to which this
               entry's information is associated."
        ::= { cgaRemoteEntry 1 }

    cgaRemoteModifier OBJECT-TYPE
        SYNTAX CgaModifier
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION
               "Binary string of 16 octets in network byte-order
               representing a 128-bit unsigned integer, which models the
               'Modifier' parameter."
        ::= { cgaRemoteEntry 2 }
```

```
   cgaRemoteCollisionCount OBJECT-TYPE
       SYNTAX CgaCollisionCount
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "Enumerated integer which models the 'Collision Count'
              parameter of the CGA."
       ::= { cgaRemoteEntry 3 }

   cgaRemotePublicKey OBJECT-TYPE
       SYNTAX CgaKeyInfo
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "Variable-length field containing the public key of the
              remote node owner of the address, which models the 'Public
              Key' parameter of the CGA."
       ::= { cgaRemoteEntry 4 }

   cgaRemoteExtensionFields OBJECT-TYPE
       SYNTAX OCTET STRING (SIZE (0..1024))
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "Optional variable-length field.  Defined as an opaque
              type, containing the 'Extension Fields' of the CGA."
       ::= { cgaRemoteEntry 5 }

   cgaRemoteCreated OBJECT-TYPE
```



```
       SYNTAX TimeStamp
       MAX-ACCESS read-only
       STATUS current
       DESCRIPTION
              "The value of the sysUpTime object at the time this entry
              was created.  If this entry was created prior to the last
              re-initialization of the local network management
              subsystem, then this object contains a zero value."
       ::= { cgaRemoteEntry 6 }
```

```
--
-- conformance information
--


cgaMIBConformance OBJECT IDENTIFIER ::= { cgaMIB 2 }

cgaMIBCompliances OBJECT IDENTIFIER ::= { cgaMIBConformance 1 }

cgaMIBGroups OBJECT IDENTIFIER ::= { cgaMIBConformance 2 }

cgaMIBFullCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
           "When this MIB is implemented for read-create access to
           the information related to the local CGA, the
           implementation can claim full compliance."
    MODULE -- this module
    MANDATORY-GROUPS { cgaLocalGroup, cgaRemoteGroup }

    OBJECT cgaLocalRowStatus
    SYNTAX RowStatus { active(1) }
    WRITE-SYNTAX RowStatus { active(1),
           createAndGo(4), destroy(6) }
    DESCRIPTION
           "Support for createAndWait and notInService is not
           required."

    ::= { cgaMIBCompliances 1 }

cgaMIBReadOnlyCompliance MODULE-COMPLIANCE
    STATUS current
    DESCRIPTION
           "When this MIB is implemented without read-create access
           to the information related to the local CGA, the
           implementation can claim read-only compliance.
```



```
           In this case the cgaLocalPrivateKey may or may not be
           accessible."
    MODULE -- this module
    MANDATORY-GROUPS { cgaLocalGroup, cgaRemoteGroup }
```

```
OBJECT cgaLocalSpinLock
MIN-ACCESS not-accessible
DESCRIPTION
       "An agent is not required to implement this object.
       However, if an agent provides write access to any of the
       other objects in the cgaLocalGroup, it SHOULD provide
       write access to this object as well."

OBJECT cgaLocalModifier
MIN-ACCESS read-only
DESCRIPTION
       "An agent is not required to provide write or create
       access to this object."

OBJECT cgaLocalCollisionCount
MIN-ACCESS read-only
DESCRIPTION
       "An agent is not required to provide write or create
       access to this object."

OBJECT cgaLocalPublicKey
MIN-ACCESS read-only
       DESCRIPTION
       "An agent is not required to provide write or create
       access to this object."

OBJECT cgaLocalPrivateKey
MIN-ACCESS not-accessible
DESCRIPTION
       "An agent is not required to provide write or create
       access to this object.  Read access to this object is also
       not required.  If write access is not provided to other
       objects in the cgaLocalGroup, or for security reasons, the
       cgaLocalPrivateKey MAY not be readable."

OBJECT cgaLocalExtensionFields
MIN-ACCESS read-only
DESCRIPTION
       "An agent is not required to provide write or create
       access to this object."
```

```
        OBJECT cgaLocalStatus
        MIN-ACCESS read-only
        DESCRIPTION
               "An agent is not required to provide write or create
               access to this object."

        OBJECT cgaLocalRowStatus
        SYNTAX RowStatus { active(1) }
        MIN-ACCESS read-only
        DESCRIPTION
               "An agent is not required to provide write or create
               access to this object.  In this case, the only value
               permitted is active(1)."

        OBJECT cgaLocalStorageType
        MIN-ACCESS read-only
        DESCRIPTION
               "An agent is not required to provide write or create
               access to this object.  If an agent allows this object to
               be written or created, it is not required to allow this
               object to be set to readOnly, permanent, or nonVolatile."

        ::= { cgaMIBCompliances 2 }



    -- group definitions


    cgaLocalGroup OBJECT-GROUP
        OBJECTS {
            cgaLocalSpinLock, cgaLocalModifier, cgaLocalCollisionCount,
            cgaLocalPublicKey, cgaLocalPrivateKey,
            cgaLocalExtensionFields, cgaLocalStatus, cgaLocalAddrInfo,
            cgaLocalRowStatus, cgaLocalStorageType }
        STATUS current
        DESCRIPTION
               "The group of the elements representing the components of
               the CGA Parameters data structure for the local node."
        ::= { cgaMIBGroups 1 }

    cgaRemoteGroup OBJECT-GROUP
        OBJECTS {
            cgaRemoteModifier, cgaRemoteCollisionCount,
            cgaRemotePublicKey, cgaRemoteExtensionFields,
            cgaRemoteCreated }
```

```
        STATUS current
        DESCRIPTION
                "The group of the elements representing the components of
                the CGA Parameters data structure for remote nodes."
        ::= { cgaMIBGroups 2 }

    END
```

5. Security Considerations

This document defines a MIB module which could be used to configure CGA local to a node, which provides address ownership capabilities. Since this configuration affects to the security services provided by other protocols (such as SEND or Shim6), access through a management protocol to this configuration data has to be carefully considered.

This document specifies two MODULE-COMPLIANCE statements, cgaMIBFullCompliance allowing read-create access to local CGA configuration, and cgaMIBReadOnlyCompliance allowing read-only access to local CGA configuration and (optionally) no access to the private key of the local CGA, cgaLocalPrivateKey. Therefore:

1. If read-only access is provided and cgaLocalPrivateKey is not-accessible, the information disclosed in the cgaLocalTable is the one provided by protocols using CGA to prove the identity of the node considered to other nodes communicating with it. An attacker could obtain in general this information by using a CGA-aware protocol to request the CGA of the node. However, filtering restrictions configured for these CGA-aware protocols may not be enforced in the same way at the management protocol. An additional concern is that an attacker could obtain the information about a CGA (or many CGAs) without knowing any (all) of them, since the attacker could use one of the addresses (may be even not a CGA) to retrieve information from all the CGAs of the node. In any case it must be noted that the information disclosed when this configuration is in use cannot be used to impersonate the identity of the node unless the CGA itself becomes vulnerable to factoring attacks, since the private key is not made available.
2. If read-only access is provided for all the objects of the

cgaLocalTable, including the cgaLocalPrivateKey columnar object, higher risks arise, since in this case any node accessing to this information could impersonate the node even if CGA-aware security protocols are used.

3. If read-create access is provided to the rows of the cgaLocalTable, besides the risks of accessing to cgaLocalPrivateKey, an attacker can delete or disable the entry associated to a CGA to prevent the node to benefit from the

authentication facilities provided by the combination of the CGA addresses and CGA-aware protocols. New CGAs can be introduced in the node, either to impersonate other nodes or to exhaust the resources of the node.

The risks associated to the last two configuration scenarios are so high that the following statement is made: the access to the managed node SHOULD be as secure or more secure than the services which are provided by the CGA. Only authorized administrators SHOULD be allowed to configure a device.

The risks associated to the access to the cgaRemoteTable are similar to the first case described when discussing the access to cgaLocalTable.

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPSec), even then, there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in this MIB module.

It is RECOMMENDED that implementers consider the security features as provided by the SNMPv3 framework (see [RFC3410], section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and privacy).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED to deploy SNMPv3 and to enable cryptographic security. It is then a customer/operator responsibility to ensure that the SNMP entity giving access to an instance of this MIB module, is properly configured to give access to the objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

6. IANA Considerations

The MIB module in this document uses the following IANA-assigned OBJECT IDENTIFIER values recorded in the SMI Numbers registry:

Descriptor	OBJECT IDENTIFIER value
cga-MIB	{ mib-2 XXX }

Editor's Note (to be removed prior to publication): the IANA is

requested to assign a value for "XXX" under the 'mib-2' subtree and to record the assignment in the SMI Numbers registry. When the assignment has been made, the RFC Editor is asked to replace "XXX" (here and in the MIB module) with the assigned value and to remove this note.

7. Acknowledgements

The work of Alberto Garcia-Martinez was supported in part by T2C2 project (TIN2008-06739-C04-01, granted by the Spanish Science and Innovation Ministry).

The authors would like to thank Suresh Krishnan for reviewing the document.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information

Version 2 (SMIv2)", STD 58, RFC 2578, April 1999.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, April 1999.

[RFC2580] McCloghrie, K., Perkins, D., and J. Schoenwaelder, "Conformance Statements for SMIv2", STD 58, RFC 2580, April 1999.

[RFC3279] Bassham, L., Polk, W., and R. Housley, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3279, April 2002.

[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, May 2008.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC4001] Daniele, M., Haberman, B., Routhier, S., and J. Schoenwaelder, "Textual Conventions for Internet Network Addresses", RFC 4001, February 2005.

[RFC4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009.

[CCITT.X690.2002]
International International Telephone and Telegraph Consultative Committee, "ASN.1 encoding rules: Specification of basic encoding Rules (BER), Canonical encoding rules (CER) and Distinguished encoding rules (DER)", CCITT Recommendation X.690, July 2002.

8.2. Informative References

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.

Authors' Addresses

Alberto Garcia-Martinez
Universidad Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
SPAIN

Phone: 34 91 6249500
Email: alberto@it.uc3m.es
URI: http://www.it.uc3m.es

Marcelo Bagnulo
U. Carlos III de Madrid
Av. Universidad 30
Leganes, Madrid 28911
Spain

Phone: +34 91 6248814
Email: marcelo@it.uc3m.es
URI: http://www.it.uc3m.es/