Internet Engineering Task Force (IETF)
Request for Comments: 7859
Category: Experimental
ISSN: 2070-1721

C. Dearlove
BAE Systems

May 2016

# Identity-Based Signatures for Mobile Ad Hoc Network (MANET) Routing Protocols

## Abstract

This document extends RFC 7182, which specifies a framework for (and specific examples of) Integrity Check Values (ICVs) for packets and messages using the generalized packet/message format specified in RFC 5444. It does so by defining an additional cryptographic function that allows the creation of an ICV that is an Identity-Based Signature (IBS), defined according to the Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI) algorithm specified in RFC 6507.

## Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7859.

Table of Contents

## 1. Introduction

[RFC7182] defines Integrity Check Value (ICV) TLVs for use in packets and messages that use the generalized MANET packet/message format defined in [RFC5444]. This specification extends the TLV definitions therein by defining two new cryptographic function code points from within the registries set up by [RFC7182]. This allows the use of an Identity-Based Signature (IBS) as an ICV. An IBS has an additional property that is not shared by all of the previously specified ICVs; it not only indicates that the protected packet or message is valid, but also verifies the originator of the packet/message.

This specification assumes that each router (i.e., each originator of [RFC5444] format packets/messages) has an identity that may be tied to the packet or message. The router may have more than one identity but will only use one for each ICV TLV. The cryptographic strength of the IBS is not dependent on the choice of identity.

Two options for the choice of identity are supported (as reflected by the two code points allocated). In the first option, the identity can be any octet sequence (up to 255 octets) included in the ICV TLV. In the second option, the octet sequence is preceded by an address, either the IP source address for a Packet TLV or the message originator address for a Message TLV or an Address Block TLV. In particular, the second option allows just the address to be used as an identity.

Identity-based signatures allow identification of the originator of information in a packet or message. They thus allow additional security functions, such as revocation of an identity. (A router could also then remove all information recorded as from that revoked originator; the Optimized Link State Routing Protocol Version 2 (OLSRv2) [RFC7181], an expected user of this specification, can do this.) When applied to messages (rather than packets), this can significantly reduce the damage that a compromised router can inflict on the network.

Identity-based signatures are based on forms of asymmetric (public key) cryptography - Identity-Based Encryption (IBE). Compared to symmetric cryptographic methods (such as HMAC and AES), IBE and IBS methods avoid requiring a shared secret key that results in a single point of failure vulnerability. Compared to more widely used asymmetric (public key) cryptographic methods (such as RSA and ECDSA), IBE and IBS methods have a major advantage and a major disadvantage.

The advantage referred to is that each router can be configured once (for its key lifetime) by a trusted authority, independently of all

other routers. Thus, a router can connect to the authority (typically in a secure environment) to receive a private key or can have a private key delivered securely (out of band) from the authority. During normal operation of the MANET, there is no need for the trusted authority to be connected to the MANET or even to still exist. Additional routers can be authorized with no reference to previously authorized routers (the trusted authority must still exist in this case). A router's public key is its identity, which when tied to a packet or message (as is the case when using an address as, or as part of, the identity) means that there is no need for public key certificates or a certificate authority, and a router need not retain key material for any other routers.

The disadvantage referred to is that the trusted authority has complete authority, even more so than a conventional certificate authority. Routers cannot generate their own private keys, only the trusted authority can do that. Through the master secret held by the trusted authority, it could impersonate any router (existing or not). When used for IBE (not part of this specification), the trusted authority can decrypt anything. However, note that the shared secret key options described in [RFC7182] also have this limitation.

There are alternative mathematical realizations of identity-based signatures. This specification uses one that has been previously published as [RFC6507], known as Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI). Similar to other IBE/IBS approaches, it is based on the use of elliptic curves. Unlike some, it does not use "pairings" (bilinear maps from a product of two elliptic curve groups to another group). It thus may be easier to implement and more efficient than some alternatives, although with a greater signature size than some. This specification allows the use of any elliptic curve that may be used by [RFC6507].

The computational load imposed by ECCSI (and, perhaps more so by other IBS methods) is not trivial, though it depends significantly on the quality of implementation of the required elliptic curve and other mathematical functions. For a security level of 128 bits, the ICV data length is 129 octets, which is longer than for alternative ICVs specified in [RFC7182] (e.g., 32 octets for the similar strength HMAC-SHA-256). The signature format used could have been slightly shortened (to 97 octets) by using a compressed representation of an elliptic curve point, however, at the expense of some additional work when verifying a signature and loss of direct compatibility with [RFC6507], and implementations thereof.

The trusted authority is referred to in [RFC6507] as the Key Management Service (KMS). That term will be used in the rest of this specification.

## 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].

Additionally, this document uses the terminology of [RFC5444], [RFC6507], and [RFC7182].

## 3. Applicability Statement

This specification adds an additional option to the framework specified in [RFC7182] for use by packets and messages formatted as described in [RFC5444]. It is applicable as described in [RFC7182] and is subject to the additional comments in Section 6, particularly regarding the role of the trusted authority (KMS).

Specific examples of protocols for which this specification is suitable are Neighborhood Discovery Protocol (NHDP) [RFC6130] and OLSRv2 [RFC7181].

## 4. Specification

### 4.1. Cryptographic Function

This specification defines a cryptographic function named ECCSI that is implemented as specified as the "sign" function in Section 5.2.1 of [RFC6507]. To use that specification:

- The ICV is not calculated as cryptographic-function(hash-function(content)) as defined in [RFC7182] but (like the HMAC ICVs defined in [RFC7182]) uses the hash function within the cryptographic function. The option "none" is not permitted for hash-function, and the hash function must have a known fixed length of N octets (as specified in Section 4.2).

- M, used in [RFC6507], is "content" as specified in [RFC7182].

- ID, used in [RFC6507], is as specified in Section 4.3.

- Key Management Service Public Authentication Key (KPAK), Secret Signing Key (SSK), and Public Validation Token (PVT), which are provided by the KMS, are as specified in Sections 4.2 and 5.1.1 of [RFC6507].

The length of the signature is 4N+1 octets (as specified in [RFC6507]) whose affine coordinate format (including an octet valued 0x04 to identify this) is used unchanged.

Verification of the ICV is not implemented by the receiver recalculating the ICV and comparing with the received ICV, as it is necessarily incapable of doing so. Instead, the receiver evaluates the "verify" function described in Section 5.2.2 of [RFC6507], which may pass or fail.

To use that function M, KPAK, SSK, and PVT are as specified above, while the Identifier (ID) is deduced from the received packet or message (as specified in Section 4.3) using the <key-id> element in the <ICV-value>. This element need not match that used by the receiver, and thus when using this cryptographic function, multiple ICV TLVs differing only in their <key-id> or in the choice of cryptographic function from the two defined in this specification SHOULD NOT be used unless routers are administratively configured to recognize which to verify.

Routers MAY be administratively configured to reject an ICV TLV using ECCSI based on part or all of <key-id>: for example, if this encodes a time after which this identity is no longer valid (as described in Section 4.3).

## 4.2. ECCSI Parameters

Section 4.1 of [RFC6507] specifies parameters n, N, p, E, B, G, and q. The first of these, n, is specified as "A security parameter; the size in bits of the prime p over which elliptic curve cryptography is to be performed." For typical security levels (e.g., 128, 192, and 256 bits), n must be at least twice the required bits of security; see Section 5.6.1 of [NIST-SP-800-57].

Selection of an elliptic curve, and all related parameters, MUST be made by administrative means, and known to all routers. Following [RFC6507], it is RECOMMENDED that the curves and base points defined in Appendix D.1.2 of [NIST-FIPS-186-4] be used (note that n in that document is q in [RFC6507]). However, an alternative curve MAY be used.

The parameter that is required by this specification is N, which is defined as Ceiling(n/8). The hash function used must create an output of size N octets. For example, for 128 bit security, with n = 256 and N = 32, the RECOMMENDED hash function is SHA-256. The signature (i.e., <ICV-data>) length is 4N+1 octets, i.e., 129 octets for N = 32.

Note that [RFC6507] actually refers to the predecessor to [NIST-FIPS-186-4], but the latest version is specified here; there are no significant differences in this regard.

### 4.3. Identity

There are two options for ID as used by [RFC6507], which are indicated by there being two code points allocated for this cryptographic function, see Section 5.

- For the cryptographic function ECCSI, ID is the element <key-id> defined in Section 12.1 of [RFC7182]. This MUST NOT be empty.

- For the cryptographic function ECCSI-ADDR, ID is the concatenation of an address (in network byte order) and the element <key-id> defined in Section 12.1 of [RFC7182], where the latter MAY be empty.

  * For a Packet TLV, this address is the IP source address of the IP datagram in which this packet is included.

  * For a Message TLV or an Address Block TLV, this address is the message originator address (the element <msg-orig-addr> defined in [RFC5444]) if that address is present; if it is not present and the message is known to have traveled only one hop, then the IP source address of the IP datagram in which this message is included is used. Otherwise, no address is defined and the message MUST be rejected. (Note that HELLO messages specified in NHDP [RFC6130] and used in OLSRv2 [RFC7181] always only travel one hop; hence, their IP source address SHOULD be used if no originator address is present.)

The element <key-id> MAY be (for the cryptographic function ECCSI-ADDR) or include (for either cryptographic function) a representation of the identity expiry time. This MAY use one of the representations of time defined for the TIMESTAMP TLV in [RFC7182]. A RECOMMENDED approach is to use the cryptographic function ECCSI-ADDR with element <key-id> containing the single octet representing the type of the time, normally used as the TIMESTAMP TLV Type Extension (defined in [RFC7182], Table 9), or any extension thereof, followed by the time as so represented, normally used as the TIMESTAMP TLV Value.

Note that the identity is formatted as specified in [RFC6507] and thus does not need a length field incorporated into it by this specification.

## 5. IANA Considerations

IANA has allocated the following two new values in the "Cryptographic Functions" registry under "Mobile Ad Hoc NETwork Parameters" registry and modified the unassigned range accordingly.

| Value | Algorithm | Description | Reference |
|---|---|---|---|
| 7 | ECCSI | ECCSI [RFC6507] | RFC 7859 |
| 8 | ECCSI-ADDR | ECCSI [RFC6507] with an address (source or originator) joined to identity | RFC 7859 |
| 9-251 | | Unassigned; Expert Review | |

Table 1: Cryptographic Function Registry

## 6. Security Considerations

This specification extends the security framework for MANET routing protocols specified in [RFC7182] by adding cryptographic functions (in two forms, according to how identity is specified).

This cryptographic function implements a form of IBS; a stronger form of ICV that verifies not just that the received packet or message is valid but that the packet or message originated at a router that was assigned a private key for the specified identity.

It is recommended that the identity include an address unique to that router: for a message, its originator address, and for a packet, the corresponding IP packet source address. If additional information is included in the identity, this may be to indicate an expiry time for signatures created using that identity.

In common with other forms of IBS, a feature of the form of IBS (known as ECCSI) used in this specification is that it requires a trusted KMS that issues all private keys and has complete cryptographic information about all possible private keys. However, to set against that, the solution is scalable (as all routers can be independently keyed) and does not need the KMS in the network. If no future keys will be required, then the KMS's master secret can be destroyed. As routers are individually keyed, key revocation (by blacklist and/or time expiry of keys) is possible.

ECCSI is based on elliptic curve mathematics. This specification follows [RFC6507] in its recommendation of elliptic curves, but any suitable (prime power) elliptic curve may be used; this must be

administratively specified. Implementation of this specification will require an available implementation of suitable mathematical functions. Unlike some other forms of IBS, ECCSI requires only basic elliptic curve operations; it does not require "pairings" (bilinear functions of a product of two elliptic curve groups). This increases the available range of suitable mathematical libraries.

### 6.1. Experimental Status

The idea of using identity-based signatures for authentication of ad hoc network signaling goes back at least as far as 2005 [Dearlove]. The specific implementation of an IBS used in this specification, ECCSI, was published as an Internet Draft in 2010 before publication as an Informational RFC [RFC6507]. ECCSI is now part of standards such as [ETSI] for LTE Proximity-based Services. An open-source implementation of cryptographic software that includes ECCSI is available, see [SecureChorus].

However, although this specification has been implemented for use in an OLSRv2 [RFC7181] routed network, there are only limited reports of such use. There are also no reports of the use of ECCSI within the IETF, other than in this specification. There are no reports of independent public scrutiny of the algorithm, although ECCSI is reported [RFC6507] as being based on [ECDSA] with similar properties.

This specification is thus published as Experimental in order to encourage its use and encourage reports on its use. Once experiments have been carried out and reported on (and when some public analysis of the underlying cryptographic algorithms is available), it is intended to advance this specification, with any changes identified by such experimentation and analysis, to Standards Track.

## 7. References

### 7.1. 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, <http://www.rfc-editor.org/info/rfc2119>.

[RFC5444] Clausen, T., Dearlove, C., Dean, J., and C. Adjih, "Generalized Mobile Ad Hoc Network (MANET) Packet/Message Format", RFC 5444, DOI 10.17487/RFC5444, February 2009, <http://www.rfc-editor.org/info/rfc5444>.

[RFC6507] Groves, M., "Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI)", RFC 6507, DOI 10.17487/RFC6507, February 2012, <http://www.rfc-editor.org/info/rfc6507>.

[RFC7182] Herberg, U., Clausen, T., and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)", RFC 7182, DOI 10.17487/RFC7182, April 2014, <http://www.rfc-editor.org/info/rfc7182>.

## 7.2. Informative References

[Dearlove] Dearlove, C., "OLSR Developments and Extensions", Proceedings of the 2nd OLSR Interop and Workshop, July 2005, <http://interop.thomasclausen.org/Interop05/Papers/Papers/paper-01.pdf>.

[ECDSA] American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62-2005, November 2005.

[ETSI] ETSI/3GPP, "Universal Mobile Telecommunications System (UMTS); LTE; Proximity-based Services (ProSe); Security aspects", ETSI TS 33.303, V13.2.0, Release 13, January 2016, <http://www.etsi.org/deliver/etsi_ts/133300_133399/133303/13.02.00_60/ts_133303v130200p.pdf>.

[NIST-FIPS-186-4] National Institute of Standards and Technology, "Digital Signature Standard (DSS)", FIPS 186-4, DOI 10.6028/NIST.FIPS.186-4, July 2013.

[NIST-SP-800-57] National Institute of Standards and Technology, "Recommendation for Key Management - Part 1: General (Revision 3)", NIST Special Publication 800-57, Part 1, Revision 3, DOI 10.6028/NIST.SP.800-57pt1r4, July 2012.

[RFC5497] Clausen, T. and C. Dearlove, "Representing Multi-Value Time in Mobile Ad Hoc Networks (MANETs)", RFC 5497, DOI 10.17487/RFC5497, March 2009, <http://www.rfc-editor.org/info/rfc5497>.

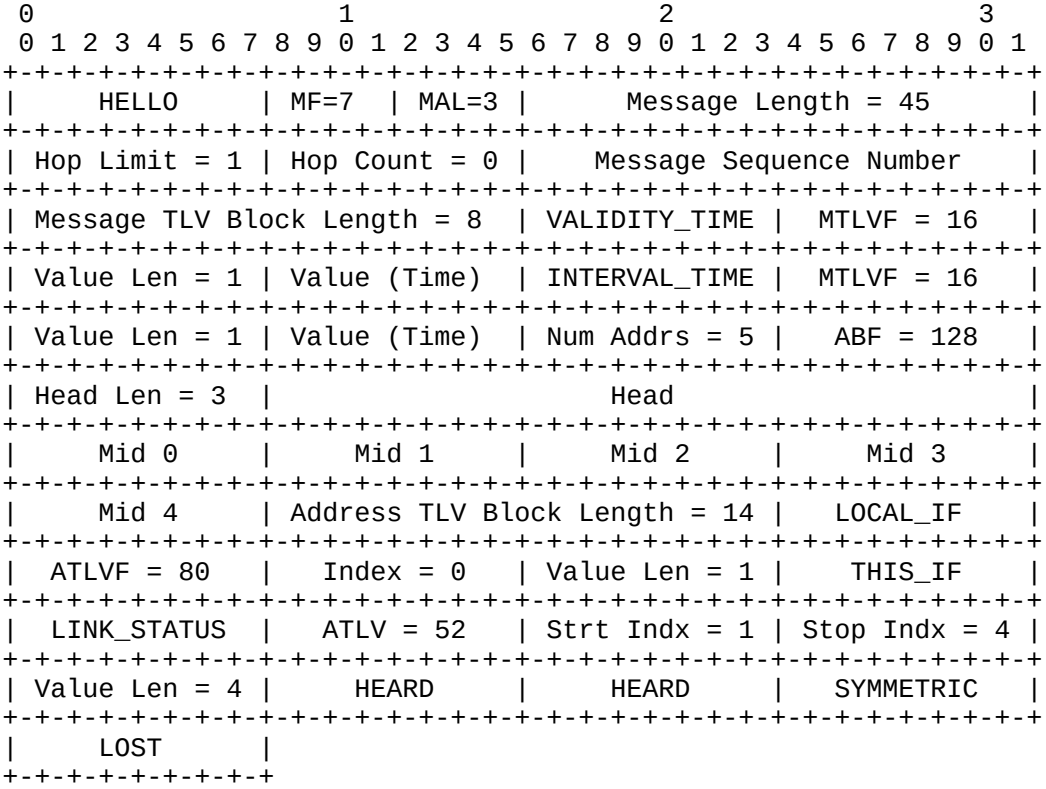
[RFC6130] Clausen, T., Dearlove, C., and J. Dean, "Mobile Ad Hoc Network (MANET) Neighborhood Discovery Protocol (NHDP)", RFC 6130, DOI 10.17487/RFC6130, April 2011, <http://www.rfc-editor.org/info/rfc6130>.

[RFC7181] Clausen, T., Dearlove, C., Jacquet, P., and U. Herberg, "The Optimized Link State Routing Protocol Version 2", RFC 7181, DOI 10.17487/RFC7181, April 2014, <http://www.rfc-editor.org/info/rfc7181>.

[SecureChorus] "Secure Chorus: Interoperable and secure enterprise communications", <http://www.securechorus.com/>.

## Appendix A. Example

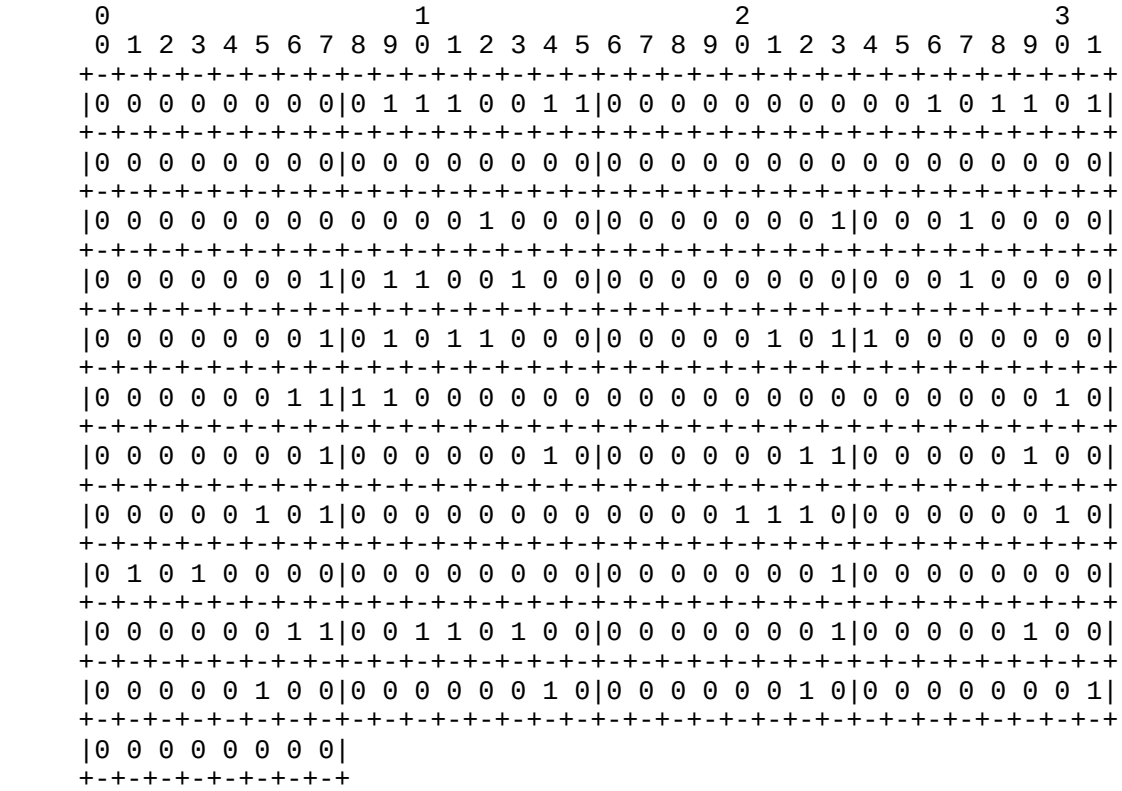
Appendix C of [RFC6130] contains this example of a HELLO message. (Note that normally a TIMESTAMP ICV would also be added before the ICV TLV, but for simplicity, that step has been omitted here.)




In order to provide an example of an ECCSI ICV Message TLV that may be added to this message, the fields shown need to all have numerical values, both by inserting defined numerical values (e.g., 0 for HELLO) and by selecting example values where needed. The latter means that

- The message sequence number will be zero.
- The five addresses will be 192.0.2.1 to 192.0.2.5.
- The message validity time will be six seconds and the message interval time will be two seconds, each encoded with a constant value C = 1/1024 seconds (as described in [RFC5497] and as referenced from [RFC6130]).

In addition, when calculating an ICV, the hop count and hop limit are both set to zero. This results in the message:




Or, in hexadecimal form:

```
M         := 0x 0073002D  00000000  00080110  01640010
                01580580  03C00002  01020304  05000E02
                50000100  03340104  04020201  00
```

The ICV TLV that will be added will have cryptographic function ECCSI-ADDR and hash function SHA-256. This message has no originator address, but it travels a single hop and its IP source address can be used. This will be assumed to be 192.0.2.0 with an empty <key-id>; thus, the sender’s identity will be (in hexadecimal form):

```
ID        := 0x  C0000200
```

Parameters for [RFC6507] will thus be n = 256, N = 32. The same parameters and master key will be used as in Appendix A of [RFC6507], i.e., the elliptic curve P-256, with parameters:

```
p     := 0x  FFFFFFFF 00000001 00000000 00000000
             00000000 FFFFFFFF FFFFFFFF FFFFFFFF

B     := 0x  5AC635D8 AA3A93E7 B3EBBD55 769886BC
             651D06B0 CC53B0F6 3BCE3C3E 27D2604B

q     := 0x  FFFFFFFF 00000000 FFFFFFFF FFFFFFFF
             BCE6FAAD A7179E84 F3B9CAC2 FC632551

G     := 0x  04
             6B17D1F2 E12C4247 F8BCE6E5 63A440F2
             77037D81 2DEB33A0 F4A13945 D898C296
             4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16
             2BCE3357 6B315ECE CBB64068 37BF51F5

KSAK  := 0x  12345;

KPAK  := 0x  04
             50D4670B DE75244F 28D2838A 0D25558A
             7A72686D 4522D4C8 273FB644 2AEBFA93
             DBDD3755 1AFD263B 5DFD617F 3960C65A
             8C298850 FF99F203 66DCE7D4 367217F4
```

The remaining steps to creating a private key for the ID use the same "random" value v as Appendix A of [RFC6507] and are:

```
   v         := 0x  23456

   PVT       := 0x  04
                    758A1427 79BE89E8 29E71984 CB40EF75
                    8CC4AD77 5FC5B9A3 E1C8ED52 F6FA36D9
                    A79D2476 92F4EDA3 A6BDAB77 D6AA6474
                    A464AE49 34663C52 65BA7018 BA091F79

   HS        := hash( 0x 04
                         6B17D1F2 E12C4247 F8BCE6E5 63A440F2
                         77037D81 2DEB33A0 F4A13945 D898C296
                         4FE342E2 FE1A7F9B 8EE7EB4A 7C0F9E16
                         2BCE3357 6B315ECE CBB64068 37BF51F5
                         04
                         50D4670B DE75244F 28D2838A 0D25558A
                         7A72686D 4522D4C8 273FB644 2AEBFA93
                         DBDD3755 1AFD263B 5DFD617F 3960C65A
                         8C298850 FF99F203 66DCE7D4 367217F4
                         C0000200
                         04
                         758A1427 79BE89E8 29E71984 CB40EF75
                         8CC4AD77 5FC5B9A3 E1C8ED52 F6FA36D9
                         A79D2476 92F4EDA3 A6BDAB77 D6AA6474
                         A464AE49 34663C52 65BA7018 BA091F79 )

          = 0x  F64FFD76 D2EC3E87 BA670866 C0832B80
                B740C2BA 016034C8 1A6F5E5B 5F9AD8F3
```

The remaining steps to creating a signature for M use the same "random" value j as Appendix A of [RFC6507] and are:

```
   j         := 0x  34567

   J         := 0x  04
                    269D4C8F DEB66A74 E4EF8C0D 5DCC597D
                    DFE6029C 2AFFC493 6008CD2C C1045D81
                    6DDA6A13 10F4B067 BD5DABDA D741B7CE
                    F36457E1 96B1BFA9 7FD5F8FB B3926ADB

   r         := 0x  269D4C8F DEB66A74 E4EF8C0D 5DCC597D
                    DFE6029C 2AFFC493 6008CD2C C1045D81

   HE        := hash( 0x
                      F64FFD76 D2EC3E87 BA670866 C0832B80
                      B740C2BA 016034C8 1A6F5E5B 5F9AD8F3
                      269D4C8F DEB66A74 E4EF8C0D 5DCC597D
                      DFE6029C 2AFFC493 6008CD2C C1045D81
                      0073002D 00000000 00080110 01640010
                      01580580 03C00002 01020304 05000E02
                      50000100 03340104 04020201 00       )

                = 0x  FE236B30 CF72E060 28E229ED 5751D796
                      91DED33C 24D2F661 28EA0804 30D8A832

   s'        := 0x  C8C739D5 FB3EFB75 221CB818 8CAAB86A
                    2E2669CF 209EA622 7D7072BA A83C2509

   s         := 0x  C8C739D5 FB3EFB75 221CB818 8CAAB86A
                    2E2669CF 209EA622 7D7072BA A83C2509

   Signature := 0x  269D4C8F DEB66A74 E4EF8C0D 5DCC597D
                    DFE6029C 2AFFC493 6008CD2C C1045D81
                    C8C739D5 FB3EFB75 221CB818 8CAAB86A
                    2E2669CF 209EA622 7D7072BA A83C2509
                    04
                    758A1427 79BE89E8 29E71984 CB40EF75
                    8CC4AD77 5FC5B9A3 E1C8ED52 F6FA36D9
                    A79D2476 92F4EDA3 A6BDAB77 D6AA6474
                    A464AE49 34663C52 65BA7018 BA091F79
```

## Acknowledgments

The author would like to thank his colleagues who have been involved in identity-based security for ad hoc networks, including (in alphabetical order) Alan Cullen, Peter Smith, and Bill Williams. He would also like to thank Benjamin Smith (INRIA/Ecole Polytechnique) for independently recreating the signature and other values in Appendix A to ensure their correctness, and Thomas Clausen (Ecole Polytechnique) for additional comments.

## Author's Address

Christopher Dearlove
BAE Systems Applied Intelligence Laboratories
West Hanningfield Road
Great Baddow, Chelmsford
United Kingdom

Phone: +44 1245 242194
Email: chris.dearlove@baesystems.com
URI: http://www.baesystems.com/