Mobile Ad Hoc Networking Working Group
INTERNET DRAFT
5 September 2006

Manel Guerrero Zapata
Technical University
of Catalonia (UPC)

Simple Ad hoc Key Management (SAKM)

draft-guerrero-manet-sakm-01.txt

Intellectual Property Rights Statement

Status of this Memo

Copyright

Abstract

The Simple Ad hoc Key Management (SAKM) is a key management system that allows to the nodes of an ad hoc network to use asymmetric cryptography with zero configuration. It is intended to be applied to MANET routing protocols that provide security features that require the use of asymmetric cryptography (like SAODV).

Table of Contents

1. Introduction

The Simple Ad hoc Key Management (SAKM) is a key management system that allows to the nodes of an ad hoc network to use asymmetric cryptography with zero configuration. It is intended to be applied to MANET routing protocols that provide security features that require the use of asymmetric cryptography (like SAODV[1] and SDYMO[2]). Although, recent modifications to the DYMO draft render SDYMO obsolete (since the techniques used by SDYMO cannot be applied anymore to current DYMO draft).

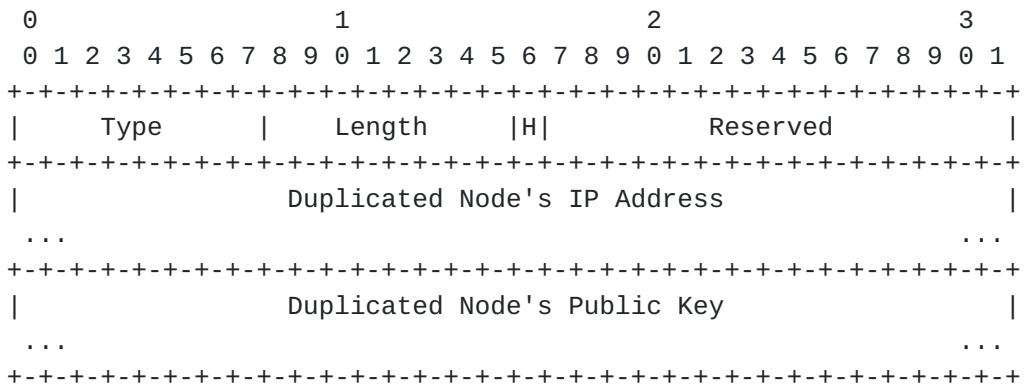
SAKM messages will be sent through the same port as the routing protocol (be it SAODV or some other).

SAKM protects the non-mutable fields of the routing messages. It is assumed that mutable fields (like hop count) are protected by some other means.

2. Terminology

This memo uses the conventional meanings [3] for the capitalized words MUST, SHOULD and MAY. It also uses terminology taken from the specification of IPSec [4].

3. Duplicated Address (DADD) Detected Message



Type 64

Length The length of the type-specific data, not including the Type and Length fields of the message in bytes.

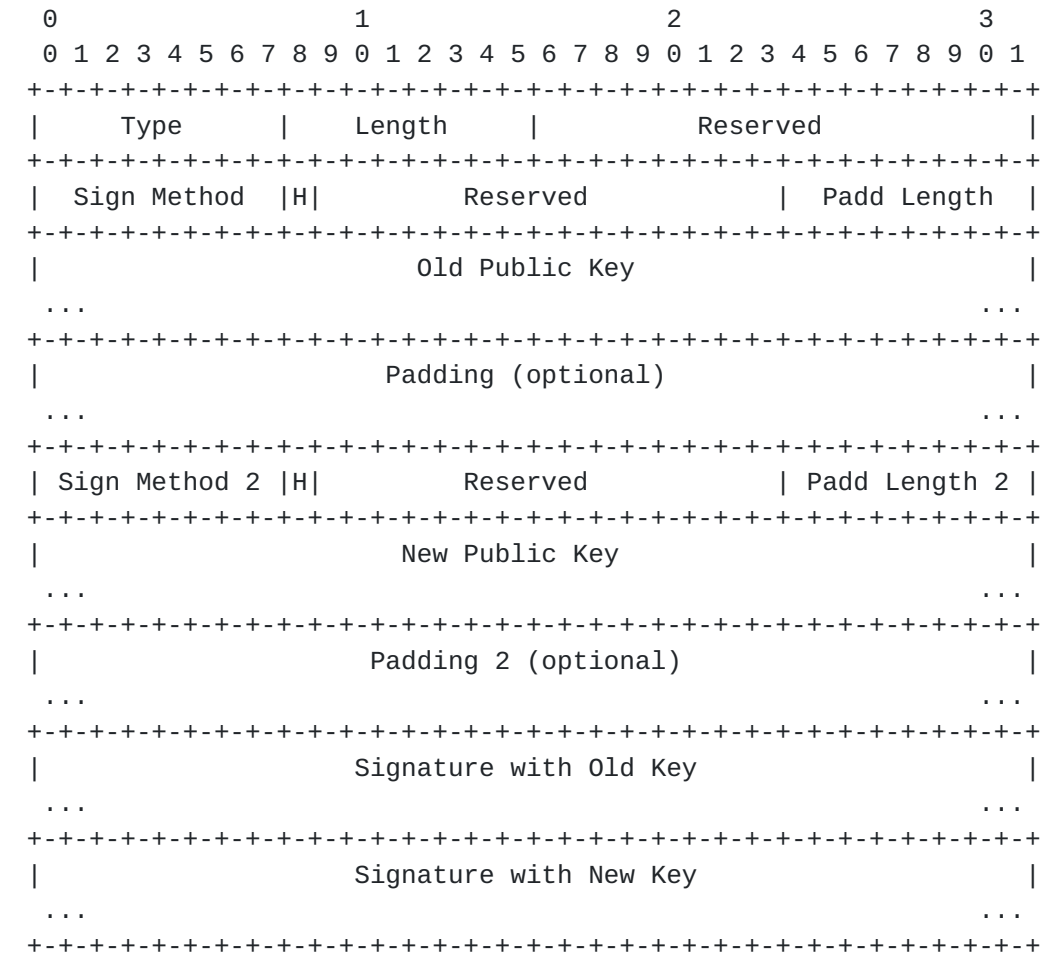
H Half Identifier flag. If it is set to '1' indicates the use of HID and if it is set to '0' the use of FID.

Reserved Sent as 0; ignored on reception.

Duplicated Node's IP Address
The IP Address of the node that uses a Duplicated IP Address.

Duplicated Node's Public Key
The Public Key of the node that uses a Duplicated IP Address.

4. New Address (NADD) Notification Message



Type 65

Length The length of the type-specific data, not including the Type and Length fields of the message in bytes.

Reserved Sent as 0; ignored on reception.

Signature Method ... Padding
The same than in RREQ (Single) Signature Extension. Corresponds to the 'Signature with Old Public Key'

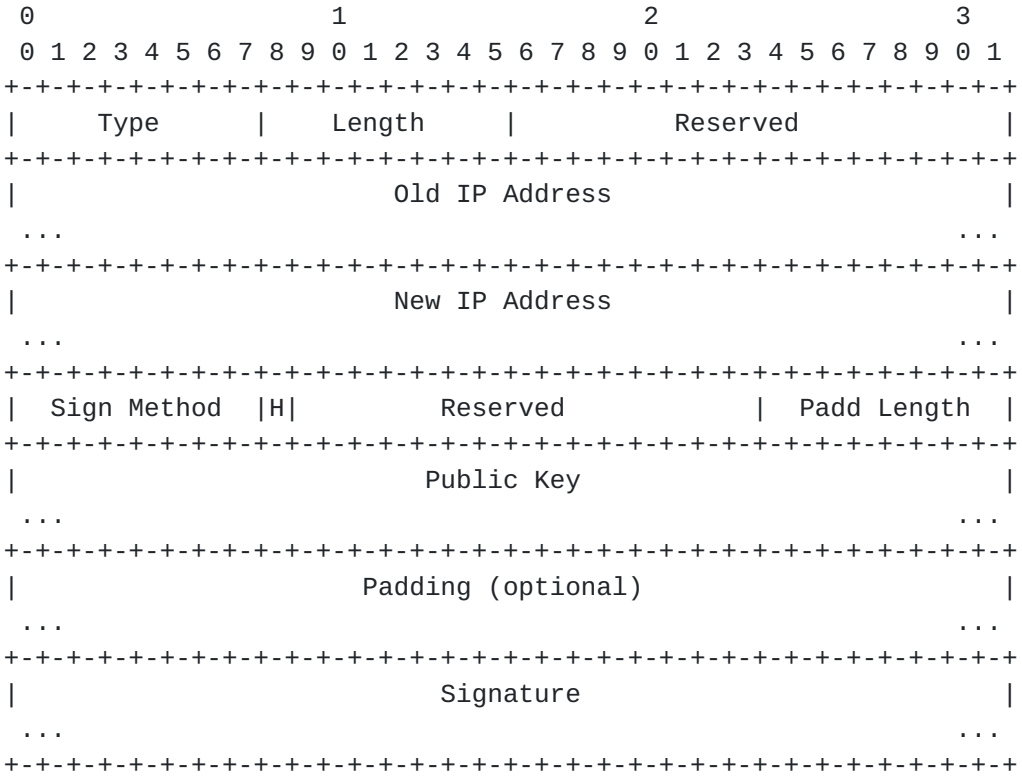
signature.

Signature Method 2 ... Padding 2
: The whole block of fields is repeated. Corresponds to the 'Signature of the New Public Key' signature.

Signature with Old Key
: The signature (with the old key) of the all the fields in the routing message that are before this field. This field has variable length, but it must be 32-bits aligned.

Signature with New Key
: The signature (with the new key) of the all the fields in the routing message that are before this field. This field has variable length, but it must be 32-bits aligned.

5. New Address Acknowledgment (NADD-ACK) Message



Type 66

Length The length of the type-specific data, not including the Type and Length fields of the message in bytes.

Reserved Sent as 0; ignored on reception.

Old IP Address
The old IP address.

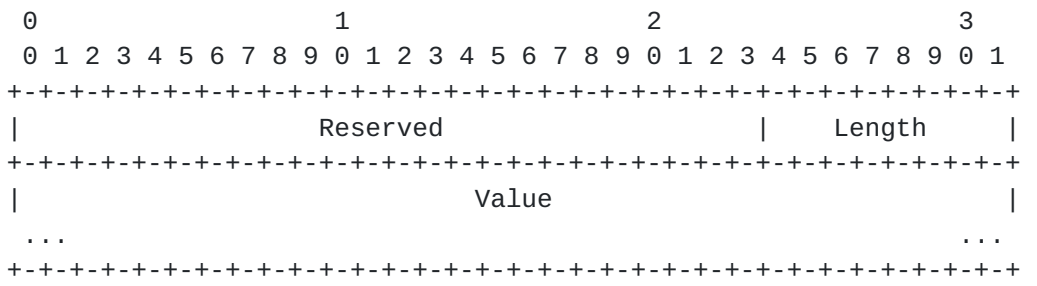
New IP Address
The new IP address.

Signature Method ... Padding
The same than in RREQ (Single) Signature Extension.

Signature The signature of the all the fields in the routing message that are before this field. This field has variable length, but it must be 32-bits aligned.

6. Encoding of Public Key and Signature

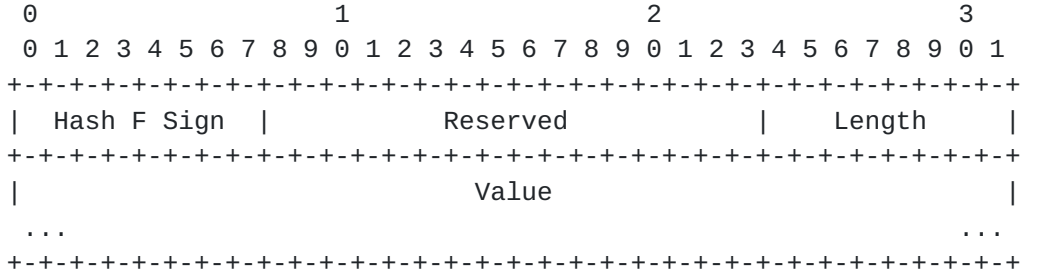
Encoding of each of the components of Public Key will be done in the following manner unless stated otherwise:



Reserved Sent as 0; ignored on reception.

Length The length of the Value field, (not including the Length and Reserved fields) in 32-bit units.

Encoding of the Signature will be done in the following manner unless stated otherwise:



Hash F Sign The hash function used to compute the hash that will be signed. Because, typically you don't want to sign the whole message, you sign a hash of the message.

The other fields work just like the ones of the encoding of the components of Public Key.

This is the list of possible values of the 'Hash F Sign' field:

Hash F Sign	Hash length	Value
RESERVED	-	0
MD2	(128 bit)	1
MD5	(128 bit)	2
SHA1	(160 bit)	3
SHA256	(256 bit)	4
SHA384	(384 bit)	5
SHA512	(512 bit)	6
Reserved	-	7-127
Implementation dependent	-	128-255

All the implementations MUST support the SHA1 option.

MD2 is a relatively slow hash function, but I decided to include it anyway. About SHA512 and SHA384, somebody might argue that nowadays they generate a much longer hash that what it is needed. But I believe they will be needed in the future.

7. Signature Methods

This is the list of possible values of the Signature Method field that MAY be included in the routing message (otherwise it is assumed to be RSA):

RESERVED	0
RSA	1
DSA	2
ElGamal	3
Reserved	4-127
Implementation dependent	128-255

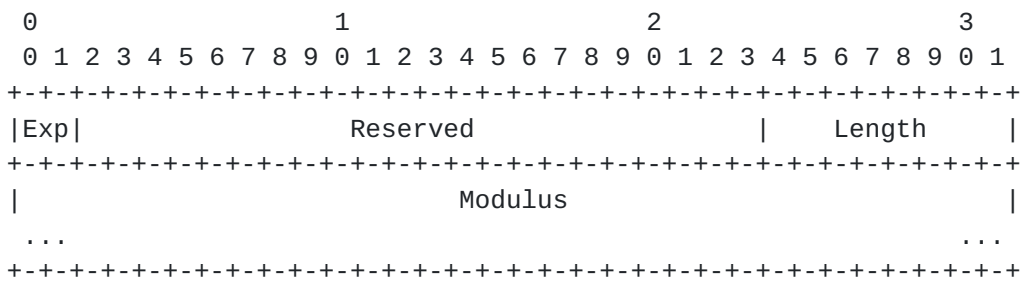
All the implementations MUST support the RSA option.

7.1. Signature Method #1 (RSA)

Public Key is composed of:
- Modulus (n)
- Exponent (e)

Signature is composed of:
- Signature

Where all these components may be encoded in the standard way or in the following way:



Reserved — Sent as 0; ignored on reception.

Length — The length of the Modulus field, (not including the Length and Reserved fields) in 32-bit units.

Exp — The Exponent (e):
- 00 — The components are encoded in the standard way. The Exponent (e) will be specified after the Modulus (n).
- 01 — Specifies that Exponent (e) is 65537 (2^16+1).
- 10 — Specifies that Exponent (e) is 17 (2^4+1).
- 11 — Specifies that Exponent (e) is 3.

A message that uses any of these 'smartly chosen' exponents MUST include random padding (in the Padding field). There is no security problem with everybody using the same exponent.

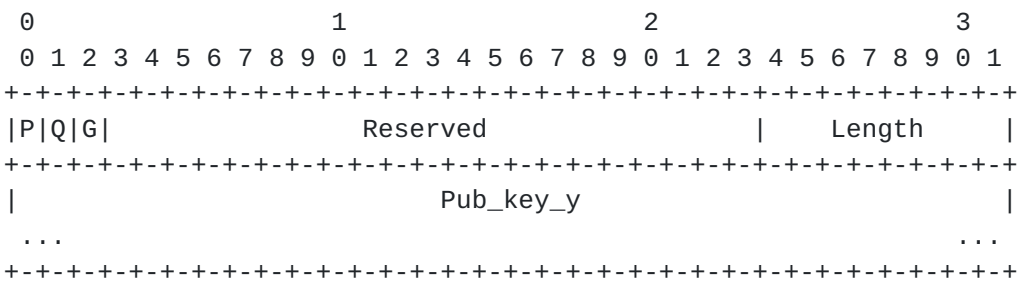
7.2. Signature Method #2 (DSA)

Public Key is composed of:
- Pub_key_y (y = g^x mod p)
- Prime (p)
- Group_order (q)
- Group_generator (g)

Signature is composed of:

- Signature

Where all these components may be encoded in the standard way or in the following way:



Reserved Sent as 0; ignored on reception.

Length The length of the Modulus field, (not including the Length and Reserved fields) in 32-bit units.

P Shared Prime (p) flag. If it is set to '1' indicates that Prime (p) is shared among the nodes of the network.

Q Shared Group_order (q) flag.

G Shared Group_generator (g) flag.

After this block, the non shared values will be included in the usual order.

7.3. Signature Method #3 (ElGamal)

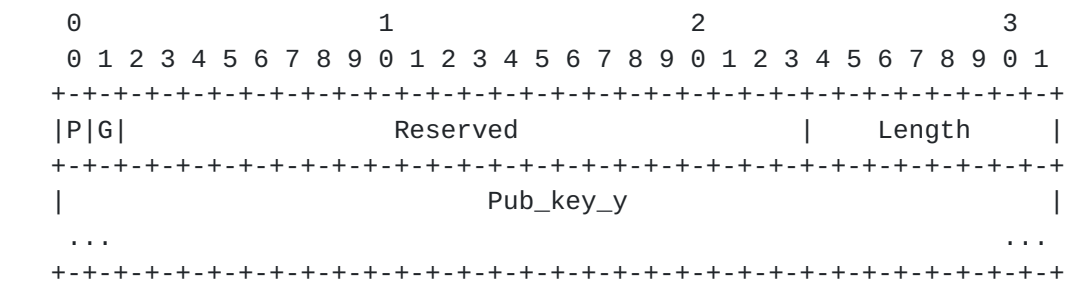
Public Key is composed of:

- Pub_key_y (y = g^x mod p)
- Prime (p)
- Group_generator (g)

Signature is composed of:

- Signature

Where all these components may be encoded in the standard way or in the following way:



Reserved Sent as 0; ignored on reception.

Length The length of the Modulus field, (not including the Length and Reserved fields) in 32-bit units.

P Shared Prime (p) flag. If it is set to '1' indicates that Prime (p) is shared among the nodes of the network.

G Shared Group_generator (g) flag.

After this block, the non shared values will be included in the usual order.

8. Delayed Verification of Signatures

The signatures in route requests and route replies will be verified after the node has forwarded the route reply. In this way transmissions of the route requests and replies occur without any kind of delay due to the verification of the signatures.

Routes pending of verification will not be used to forward any packet. If a packet arrives for a node for which there is a route pending of verification. The node will have to verify it before using that route. If the verification fails, it will delete the route and request a new one.

9. IP address generation

The first part of this section describes the key management scheme to be used with IPv6.

SAKM generates the IP addresses is very similar to the generation of SUCV (Statistically Unique and Cryptographically Verifiable) addresses [5]. SUCV addresses where designed to protect Binding Updates in Mobile IPv6. The main difference between SUCV and the method proposed in here is that SUCV addresses are generated by hashing an "imprint" in addition to the public key. That imprint (that can be a random value) is used to limit certain attacks related

to Mobile IP.

In SAKM, the address can be a network prefix of 64 bits with a 64 bit SAKM_HID (Half IDentifier) or a 128 bit SAKM_FID (Identifier). These two identifiers are generated almost in the same way than the sucvHID and the sucvID in SUCV (with the difference that they hash the public key instead of an imprint):

SAKM_HID = SHA1HMAC_64(PublicKey, PublicKey)

SAKM_FID = SHA1HMAC_128(PublicKey, PublicKey)

This is the list of what is used as PublicKey depending on which Signature Method is used:

Signature Method	PublicKey
1 (RSA)	Modulus (n)
2 (DSA)	Pub_key_y (y = g^x mod p)
3 (ElGamal)	Pub_key_y (y = g^x mod p)

There MAY be a flag in the routing message extensions (the 'H' flag) that will be set to '1' if the IP address is a HID and to '0' if it is a FID. Otherwise it the underlying protocol MUST specify which of them uses.

Finally, if it has to be a real IPv6 address, there is a couple of things that should be done [6].

If HID is used, then the HID behaves as an interface identifier and, therefore, its sixth bit (the universal/local bit) should be set to zero (0) to indicate local scope (because the IP address is not guaranteed to be globally unique).

And, if FID is used, then a format prefix corresponding to the MANET network should be overwritten to the FID. Format prefixes '010' through '110' are unassigned and would take only three bits of the FID. Format prefixes '1110' through '1111 1110 0' are also unassigned and they would take between 4 and 9 bits of the FID. All of these format prefixes required to have to have 64-bit interface identifiers in EUI-64 format, so universal/local bit should be set to zero (0).

The length of an IPv4 address is probably too short to provide the statistically uniqueness that this scheme requires when the number of nodes is very big. Nevertheless, if the number of nodes is assumed to be low, (let's say, under 100 nodes) it is not very unrealistic to expect that the statistically uniqueness property will hold.

The SAKM IPv4 address will have a network prefix of 8 bits and a SAKM_4ID (IPv4 Identifier). The network prefix can be any number between 1 and 126 (both included) with the exception of 14, 24 and 39 (see RFC3330). The network prefix 10 can only be used if it is granted that it will not be connected to any other network (RFC1918).

The SAKM_4ID will be the first bits of the SAKM_HID and the 'H' flag will be set.

9.1. Duplicated IP Address Detection

If a node 'A' receives a routing message that is signed by a node 'B' that has the same IP address than one of the nodes for which 'A' has a route entry (node 'C'), it will not process normally that routing message. Instead, it will inform 'B' (sending to it a Duplicated Address (DADD) Detected message) that it is using a duplicated IP and it will prove it by adding the public key of 'C' (so 'B' can verify the truthfulness of the claim).

When the node 'B' receives a DADD message that indicates that somebody else has the same IP address than itself (or it realizes about it by itself), it will have to generate a new pair of public/private keys. After that, it will derive its IP address from its public key and it MIGHT inform to all the nodes it finds relevant (through a broadcast) of which is its new IP address with an special message (New Address (NADD) Notification message) that contains: the two IP addresses (the old and the new ones) and the two public signatures (old and new) signed with the old private key and, all this, signed with the new private key. This unicast MIGHT be answered with the New Address Acknowledgment (NADD-ACK) Message by the receiver if it verifies that everything is in order.

After this, the node will generate a route error message for his old IP address. Its propagation will delete the route entries for the old IP address and, therefore, eliminate the duplicated addresses. This route error message may have a message extension that tells which is the new address. In this way, the nodes that receive the routing message can already create the route to the new IP address.

10. Security Considerations

Although it is true that there is no way to preclude a node of inventing many identities, that cannot be used to create an attack against the routing algorithm.

Delayed verification makes possible that a malicious node creates invalid route requests that could flood the network. But, the same malicious node can flood the network with perfectly valid route

requests. And there would be no easy way to know if it is trying to flood the network or if it is just trying to see if any of its friend nodes are present in the network (for instance).

An attacker cannot forge a public/private key pair from an IP address so the identity token becomes the IP address itself.

11. Modifications of the draft

Version 1

- The acknowledgment that SDYMO has been rendered obsolete due to changes in DYMO that make much more complicated to secure it.

Version 0

- This draft describes the key management system that was contained in the SAODV draft till its version 04.

12. Acknowledgments

I want to thank everybody who contributed to SAODV, since SAKM was originally part of it.

References

[1] M. Guerrero Zapata: Secure Ad hoc On-Demand Distance Vector (SAODV) Routing. draft-guerrero-manet-saodv-05.txt, February 2006.

[2] M. Guerrero Zapata: Secure Dynamic MANET On-Demand (SDYMO) Routing Protocol. draft-guerrero-manet-sdymo-00.txt, February 2006.

[3] S. Bradner: Key words for use in RFCs to Indicate Requirement Levels. RFC 2119, March 1997.

[4] S. Kent, R. Atkinson: Security Architecture for the Internet Protocol. RFC 2402, November 1998.

[5] Gabriel Montenegro, Claude Castelluccia: Statistically Unique and Cryptographically Verifiable (SUCV) Identifiers and Addresses. Network and Distributed System Security Symposium (NDSS '02). February 2002,

[6] R. Hinden and S. Deering: IP Version 6 Addressing Architecture. RFC 2373, July 1998.

Author's Address:

Questions about this memo can be directed to the author:

Manel Guerrero Zapata
Computer Architecture Department (DAC)
Technical University of Catalonia (UPC)
UPC-AC C6-123 Campus Nord
C. Jordi Girona 1-3
08034 Barcelona SPAIN
(+34) 93 4054044
guerrero@ac.upc.edu

Appendix A. Full Copyright Statement