IP Routing for Wireless/Mobile Hosts (mobileip) WG
INTERNET DRAFT
Date: 09 July 2001
Expires: January 2002

S. Jacobs, S. Belgard
Verizon Laboratories

Mobile IP Public Key Based Authentication
<draft-jacobs-mobileip-pki-auth-03.txt>

Status of This Memo

Abstract

This document proposes an extension to the Mobile IP base protocol (RFC 2002) to allow Mobile Nodes (Hosts) and Mobility Agents (both home network and foreign network) to use X.509 digital certificates, public keys and digital signatures as the basis of authenticating Mobile IP control messages in addition to secret key authentication. The use of these mechanisms will allow Mobile IP to scale from small research environments to potentially millions of mobile nodes across thousands of networks owned-operated by different organizations and service providers. A Public Key Infrastructure is proposed that focuses specifically on authentication of Mobile IP knowledgeable nodes, NOT general use for authenticating individuals.

1. Introduction

The Mobile IP base protocol [RFC2002] provides a scalable mechanism for node mobility. When examining the various types of Mobile IP deployments being considered, one sees significantly different networking environments. Research test beds are relatively benign environments, provide network bandwidth from a few Kbps to Gbps within

a single organization. Office and warehouse networks face a greater level of threats, are typically a mixture of wired and wireless media

with bandwidth ranging from Mbps to Gpbs, and may span a number of organizations. Service provider deployments are focused on a wireless environment, face many possible threats, provide bandwidth from 4.8Kbps to a few 100Kbps, interoperability across many organizations, and assure the ability to account and bill for services rendered.

The number and frequency of protocol control messages has a direct impact on a protocol like Mobile IP; especially for frequently roaming nodes. The impact of control message size and control message size frequency have a direct impact on network bandwidth. As available network bandwidth decreases, network control overhead needs to be minimized. Frequent network control messages increase network overhead. Mobile IP deployment environments face different types of threats and associated degrees of risk ranging from very few threats and low risks to many threats and very high risks. A Mobile IP deploying organization faces a trade-off between their expected threats, the degree of risk acceptable and the cost in network security overhead necessary to mitigate risk in a specific threat context.

There are a number of Mobile IP control message authentication methodologies, such as manually distributed Secret Keys, IPsec negotiated security associations, AAA negotiated security associations, self-signed Certificates containing Public Keys, and CA signed Certificates containing Public Keys. For each authentication method there are advantages and disadvantages (trade-offs) between bandwidth consumed, scaleability, complexity and performance. All authentication solutions are based on arriving at a compromise between these trade-offs.

As the number of nodes deployed increases, the number of secret keys increases even faster, namely ((#nodes * (#nodes-1))**2)/2, which increases complexity yet have a positive impact on performance as they are relatively easy to compute and process. With public keys, the number of keys needed = the number of nodes, reducing complexity yet have a negative impact on performance as they are more expensive to compute and process than secret keys.

Manual key distribution approaches necessitate distributing key information to all nodes prior to deployment, reducing scaleability, yet have no impact on network overhead. Dynamic key distribution approaches eliminate pre-deployment key distribution, thereby increasing scaleability, yet increase network overhead as keys are established/exchanged over the network.

Dynamic key distribution and security association negotiation methods vary greatly regarding:

- number of messages used
- complexity of supporting protocols
- number of participants involved
- supporting infrastructure required
- computing resources consumed
- robustness and integrity of resulting security associations.

The primary dynamic approaches under consideration are:

- IPsec protocols
- Authentication, Authorization and Accounting Protocols (AAA).

The IPsec suite of IKE and ISAKMP provide a general purpose approach to establishing and negotiating Security Associations (SAs) between communicating systems on a peer-to-peer basis. The use of this authentication method with Mobile IP will:

- increase the number of discreet messages exchanged between a Mobile Node (MN) and a Foreign Agent (FA) by three (3) if "aggressive mode" is used or by six (6) messages if "main mode" is used for IKE phase one. A like number of extra messages will have to be exchanged between the FA and the MN's Home Agent (HA), as well as between the MN and its HA. IKE phase two communication adds an additional 3 messages between MN and FA, FA and HA, and HA and MN. Using IKE results in at least 18, and as many as 27, additional messages, beyond those directly necessary for Mobile IP, being exchanged to establish IPsec SAs.
- require the exchange of Public key digital certificates, as part of the IKE protocol, unless these are pre-distributed. Given that an MN does not necessarily know apriori where it will roam, pre-distributing certificates to FAs becomes nearly impossible.
- regardless of which IKE mode used, each network node will have to either generate/verify one digital signature or perform one public/private key encryption/decryption as part of the IKE phase one protocol.
- The IKE protocol does not include certificate validation or certificate revocation and the network overhead managing certificates.

The leading AAA approach is based on the DIAMETER protocol. DIAMETER:

- does not increase the number of discreet messages exchanged between a Mobile Node (MN) and a Foreign Agent (FA) or between the MN and its HA.
- requires the use of AAA Servers to perform the actual authentication function for FAs and HAs increasing the number of required participants significantly.
- primarily focuses on the use of secret keys for establishing identity authenticity and expects the AAA servers to dynamically generate these secret keys in real-time as needed.
- does not provide a secure method for distributing the dynamically

generated secret keys unless one has pre-distributed static secret keys to
all mobility aware nodes.

This document proposes an extension to the Mobile IP base protocol that defines how Mobile Nodes (MNs) and Mobility Agents (both HAs and FAs) may:

- use public key based authentication via digital signatures.
- use X.509 digital certificates
  - issued by Certificate Authorities (CAs)
  - issued by the subject of the certificate (self-signed certificates for a PGP-like informal web of trust)
- use a Network Access Identifier (NAI) for identifying mobile nodes and mobility agents
- ahndle digital certificate revocation and verification.

These Mobile IP authentication extensions are designed to minimally change the Mobile IP defined in [RFC-2002]. The extensions make use of a few reserved fields in the existing Mobile IP message definitions. Given the increased functionality of this approach the RFC-2002 authentication extension has been modified to accommodate different authentication types, different sizes of authenticators (digital signatures) and the use of Network Access Identifier for identifying mobile nodes and mobility agents. These changes to Mobile IP do not prevent using Mobile IP with DHCP on visited networks (if one is willing to forgo visited network authentication, access control and non-repudiation). The security benefit from these extensions is achieved when using Foreign Agents.

2. Terminology

Certification Authority (CA)
: A third party trusted by one or more users to create and assign digital certificates.

Certificate-Revocation List (CRL)
: A data structure that contains information about certificates whose validity an issuer has prematurely revoked. The information consists of an issuer name, the time of issue, the next scheduled time of issue, and a list of certificate serial numbers and their associated revocation times. The CRL is signed by the issuer. The data structure is defined in [RFC1422]

Certificate Subject (Subject)
: A Certificate Subject, or Subject, is the entity referred to by the NAI contained within the Certificate.

Digital Certificate (Certificate)
: A Digital Certificate, or Certificate, is a data structure that binds an entity's NAI to a public key with a digital signature. This data structure is defined in [X.509]. and contains information, such as identify and public key, about an entity where an authority, called a Certification Authority, has cryptographicly linked the information together using a

digital signature.

Digital Certification

Digital Certification is the mechanism in which a Certification Authority (CA) "signs" a special data structure containing the name of some entity, or Subject, and their public key in such a way that anyone can "verify" that the message was signed by no one other than the certification authority and thereby develop trust in the subject's public key.

Digital Signature

the content to be signed is first reduced to a message digest with a message-digest algorithm (such as MD5), and then the octet string containing the message digest is encrypted with the private key of the signer of the content.

Message-Digest Algorithm

A message-digest algorithm is a method of reducing a message of Any length to a string of a fixed length, called the message digest, in such a way that it is computationally infeasible to find a collision (two messages with the same message digest) or to find a message with a given, predetermined message digest. MD2 and MD5 are message-digest algorithms described in [RFC1319] and [RFC1321]. Each inputs an arbitrary message and outputs a 128-bit message digest.

Mobile Security Association (MSA)

A collection of security contexts, between a pair of nodes, which may be applied to Mobile IP control messages exchanged between them. Each context indicates an authentication algorithm and mode.

Network Access Identifier (NAI)

A string of octets as defined in [RFC2486] for identifying mobile nodes and mobility agents.

Public-key algorithm

An algorithm for encrypting or decrypting data with a public or Private key. When a private key is used to encrypt a message digest the public-key algorithm is called a message-digest encryption algorithm and the encrypted output is called a Digital Signature. This algorithm transforms a message of any length under a private key to a signature in such a way that it

is computationally infeasible to find two messages with the same signature, to find a message with a given, predetermined signature, or to find the signature of a given message without knowledge of the private key. Typically, a digital signature is created by computing a message digest on the message, then encrypting the message digest with the private key.

Public-key cryptography
: Public-key cryptography is the technology first identified by Diffie and Hellman [Diffie76] in which encryption and Decryption involve different keys. The two keys are the public key and the private key, and either can encrypt or decrypt data. A user gives his or her public key to other users, keeping the Private key to himself or herself.

RSA
: RSA is a public-key algorithm invented by Rivest, Shamir, and Adleman [RSA78] involving exponentiation modulo the product of two large prime numbers. The difficulty of breaking RSA is generally considered to be equal to the difficulty of factoring integers that are the product of two large prime numbers of approximately equal size.

Security Context
: A security context between two nodes defines the manner in which these two nodes choose to mutually authentication each other, and indicates an authentication algorithm and mode.

Security Parameter Index (SPI)
: An index, used with Secret Key authentication mechanisms, identifying a security context between a pair of Nodes among the contexts available.

Self-Signed Digital Certificate (Self-Signed Certificate)
: A Digital Certificate, or Certificate, is a Digital Certificate that has been signed by the entity to which the Certificate appies to. This data structure is defined in [X.509] and contains information, such as identify and public key, about an entity where the entity itself has cryptographicly linked the information together using a digital signature.

X.509 Digital Certificate
: An X.509 Digital Certificate is a data structure that binds an entity's NAI to a public key with a digital signature. This data structure is defined in [X.509].

X.509 Digital Certification
: X.509 Digital Certification is the mechanism in which a Certification Authority (CA) "signs" a special data structure containing the name of some entity, or Subject, and their public key in such a way that anyone can "verify" that the message was signed by no one other than the Certification Authority and thereby develop trust in the subject's public key.

3. Specification Language

This document uses the terms "MUST", "SHOULD", and "MAY" as defined in RFC-2119, along with the negated forms of those terms.

4. Security Enhancement

The design goal of the approach presented herein is to add scaleable strong authentication to Mobile IP. This approach works exactly the same way as the base protocol except for the mechanism responsible for generating/verifying message authenticators (digital signatures) and the data structures supporting the proposed digital signature based authenticators.

The Co-located Care-of Address (COA) mode (sometimes referred to as "pop-up" mode) relies on the use of DHCP [RFC1541] which assumes that nodes requesting DHCP assigned addresses either belong to the same organization operating the DHCP server or these nodes will be authenticated for network use outside of DHCP.

Each extended Mobile IP Node SHOULD be able to support multiple authentication options ranging from simple to complex, while also permitting the possibility of no authentication (the default mode). Mobile IP messages between Mobile Nodes and Mobility Agents are authenticated with an Authentication Extension. The Authentication Extension identifies the Authentication type to be used and a Security Context between a pair of Mobile IP Nodes and is fundamental to defining the Mobility Security Association (MSA) between these nodes. The Authentication Extension MAY be followed by a Certificate Extension if the MSA, between the Mobile Nodes utilizes public key based authentication and Certificates.

The Certificate Extension includes a copy, or copies, of Certificates that bind system "distinguished names" to public keys using a digital signature. A Certificate Extension will always contain at least one Certificate which applies to the sender of a Mobile IP message. There may also be present in the Certificate Extension, Certificates belonging to one of more CAs. When Mobile Nodes share a common CA, the Certificate of the common CA would appear in the Certificate Extension. In the case where the communicating Nodes do not share a common CA then the Certificate Extension may contain multiple CA Certificates from which a trust hierarchy path Between the CA of one Node and the CA of the other Node may be established.

4.1. Message and Extension Formats

The changes described herein include:

- the use of a NAI extension with all MIP messages to identify the messages sender via a unique Network Access Identifier indipendant of IP addresses.

- a modified Advertisement extension that now includes authentication information

- a modified Registration Request extension that identifies the form of authentication

- a modified Registration Reply extension that identifies the form of authentication

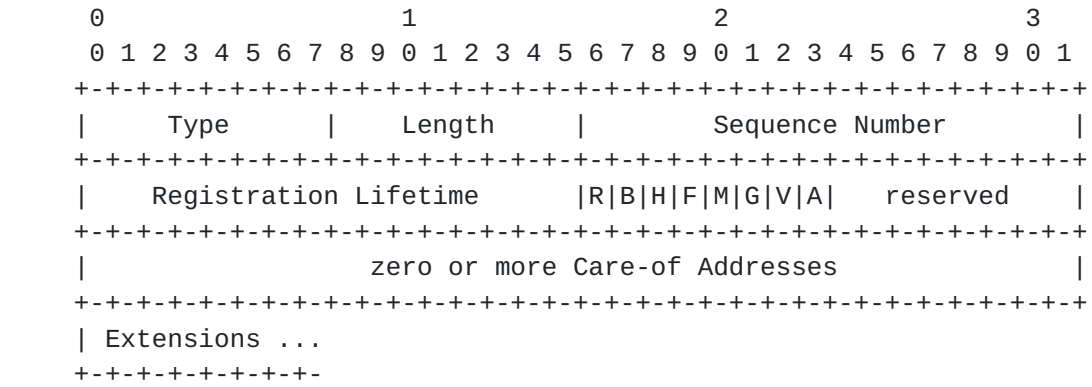
- a modified Authentication extension that may now include public key digital signature authentication information

- a Network Access Identifier extension that contains a unique identifier for Mobile IP aware nodes

- a Certificate extension that is used for exchanging X.509 digital certificates

4.1.1. Mobility Agent Advertisement Extension

The Mobility Agent Advertisement Extension follows the ICMP Router Advertisement fields. It is used to indicate that an ICMP Router Advertisement message is also an Agent Advertisement being sent by a mobility agent. The Mobility Agent Advertisement Extension is defined as follows:



Type 16 (Mobility Agent Advertisement)

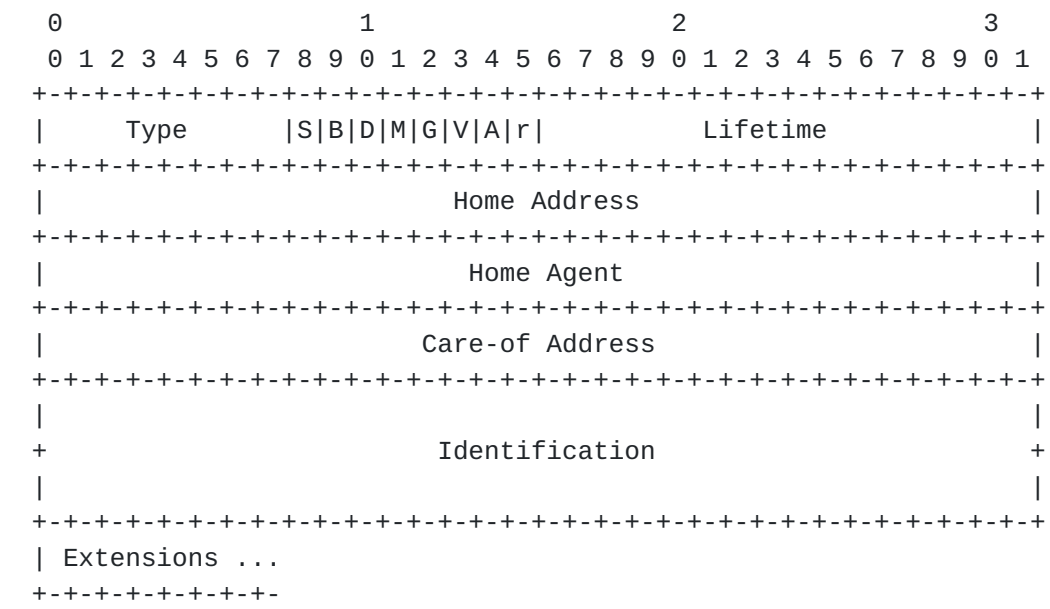
Length Unchanged from base Mobile IP protocol.

Sequence Number	Unchanged from base Mobile IP protocol.

Registration Lifetime	Unchanged from base Mobile IP protocol.
R bit	Unchanged from base Mobile IP protocol.
B bit	Unchanged from base Mobile IP protocol.
H bit	Unchanged from base Mobile IP protocol.
F bit	Unchanged from base Mobile IP protocol.
M bit	Unchanged from base Mobile IP protocol.
G bit	Unchanged from base Mobile IP protocol.
V bit	Unchanged from base Mobile IP protocol.
A bit	(New) Previously reserved in RFC-2002. If bit not set then this is a traditional RFC 2002 Advertisement extension. If set then this is an authenticated advertisement and is followed by a Network Access Identifier extension, Authentication Extension, and Certificate extension.
Care-of Address(es)	Unchanged from base Mobile IP protocol.
Extensions	When A bit = 0, No extensions follow When A bit = 1, Usage is as follows - Foreign Agent Network Access Identifier extension appended - Foreign Agent Authentication extension appended - Foreign Agent Certificate extension is appended

4.1.2. Registration Request Message

An MN registers with its HA using a Registration Request message so that its HA can create or modify a mobility binding for that MN. The Request MAY be relayed to the HA by an FA through which the MN is registering. The UDP header is followed by the Mobile IP fields shown below:



Type	1 (Registration Request)
S bit	Unchanged from base Mobile IP protocol.
B bit	Unchanged from base Mobile IP protocol.
D bit	Unchanged from base Mobile IP protocol.
M bit	Unchanged from base Mobile IP protocol.
G bit	Unchanged from base Mobile IP protocol.
V bit	Unchanged from base Mobile IP protocol.
A bit	(New) Previously reserved in RFC-2002. If bit not set then this is a traditional RFC 2002 Registration Request extension. If set then this is a modified registration request and is followed by a Network Access Identifier extension, Authentication extension And Certificate Extension.
r bit	Unchanged from base Mobile IP protocol.
Lifetime	Unchanged from base Mobile IP protocol.
Home Address	Unchanged from base Mobile IP protocol.
Home Agent	Unchanged from base Mobile IP protocol.
Care-of Address	Unchanged from base Mobile IP protocol.

Identification Unchanged from base Mobile IP protocol.

Extensions When A bit = 0, Usage is as follows between Mobile Node and Foreign Agent

- RFC 2002 formatted Mobile Node Authentication extension is appended.

When A bit = 0, Usage is as follows between Foreign Agent and Home Agent

- RFC 2002 formatted Mobile Node Authentication extension is appended.
- RFC 2002 formatted Foreign Agent Authentication extension is appended.

When A bit = 1, Usage is as follows between Mobile Node and Foreign Agent

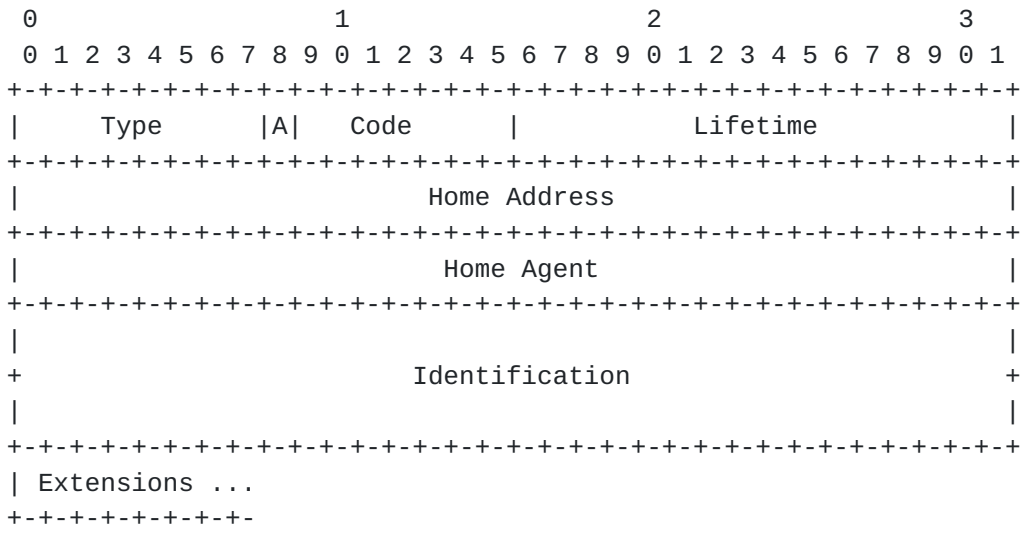
- Mobile Node Network Access Identifier extension is appended.
- Modified Mobile Node Authentication extension is appended.
- Mobile Node Certificate extension is appended.

When A bit = 1, Usage is as follows between Foreign Agent and Home Agent

- Mobile Node Network Access Identifier extension is appended.
- Modified Mobile Node Authentication extension is appended.
- Foreign Agent Network Access Identifier extension is appended.
- Foreign Agent Authentication extension is appended.
- Foreign Agent Certificate extension is appended.

4.1.3. Registration Reply

A mobility agent (FA or HA) returns a Registration Reply message to an MN which was the source of a Registration Request message. The UDP header is followed by the Mobile IP fields shown below:



Type	3 (Registration Reply)
A bit	(New) Replaces high order bit in RFC-2002 Code field. If A bit = 0, then this is a Traditional RFC 2002 Registration Reply extension. If A bit = 1, then this is a modified registration reply and is followed by a Network Access Identifier extension, Authentication extension and Certificate extension.
Code	A value indicating the result of the Registration Request. Currently defined Code values are shown In Table 2.3 below.(redefined from 8 bits in RFC-2002 to now 7 bits)
Lifetime	Unchanged from base Mobile IP protocol.
Home Address	Unchanged from base Mobile IP protocol.
Home Agent	Unchanged from base Mobile IP protocol.
Care-of Address	Unchanged from base Mobile IP protocol.
Identification	Unchanged from base Mobile IP protocol.

Extensions	When A bit = 0,Usage is as follows between Home Agent and Foreign Agent - RFC 2002 formatted Home Agent Authentication extension is appended. When A bit = 0,Usage is as follows between Foreign Agent and Mobile Node - RFC 2002 formatted Home Agent Authentication extension is appended. - RFC 2002 formatted Foreign Agent Authentication extension is appended. When A bit = 1, Usage is as follows between Home Agent and Foreign Agent - Home Agent Network Access Identifier extension is appended. - Modified Home Agent Authentication extension is appended. - Home Agent Certificate extension is appended. When A bit = 1,Usage is as follows between Foreign Agent and Mobile Node - Home Agent Network Access Identifier extension is appended. - Modified Home Agent Authentication extension is appended. - Foreign Agent Network Access Identifier extension is appended. - Foreign Agent Authentication extension is appended.

Table 2.3 -- Currently defined Code values are

0 = Unchanged from base Mobile IP protocol.
1 = Unchanged from base Mobile IP protocol.
64 = Unchanged from base Mobile IP protocol.
65 = Unchanged from base Mobile IP protocol.
66 = Unchanged from base Mobile IP protocol.
67 = Unchanged from base Mobile IP protocol.
68 = Unchanged from base Mobile IP protocol.
69 = Unchanged from base Mobile IP protocol.
70 = Unchanged from base Mobile IP protocol.
71 = Unchanged from base Mobile IP protocol.
72 = Unchanged from base Mobile IP protocol.
73 = Unchanged from base Mobile IP protocol.
80 = Unchanged from base Mobile IP protocol.
81 = Unchanged from base Mobile IP protocol.
82 = Unchanged from base Mobile IP protocol.

88 = Unchanged from base Mobile IP protocol.
89 = foreign agent failed authentication

4.1.4. Mobile IP Authentication Extensions

The extended Mobile IP uses Authentication extensions appended to Agent Advertisements, Registration Requests and Registration Reply messages to provide receiving nodes the information to verify the authenticity and integrity of received Mobile IP control messages.

The digital signature computed for each authentication Extension MUST protect the following fields from the registration message:

- the UDP payload (that is, the Registration Request or Registration Reply data),
- all prior Extensions in their entirety, and
- the Type and Length of this Extension.

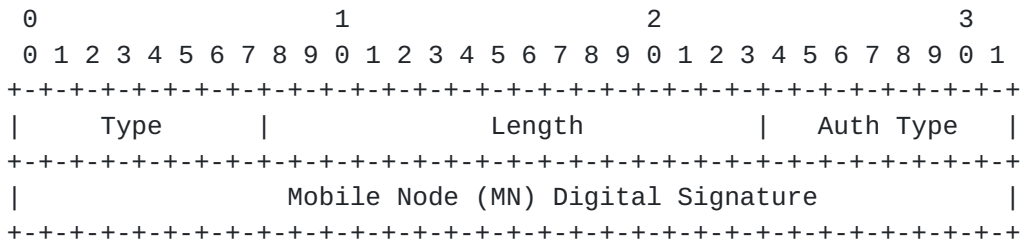
Note that the digital signature field itself and the UDP header are NOT included in the computation of the digital signature value.

Table 2.4 -- Valid Authentication types, when A bit = 1.

Auth Type Value	Authentication Algorithm	Key Length in bits	Digital Signature Length in bytes
001 to 009	User Defined	User Defined	User Defined
011	RSA	512	64
012	RSA	768	97
013	RSA	1024	128
014	RSA	2048	256
021	Elliptic Curve	80	10
022	Elliptic Curve	120	15
023	Elliptic Curve	160	20
030	DSA	512	64

4.1.4.1. Mobile Node Authentication Extension

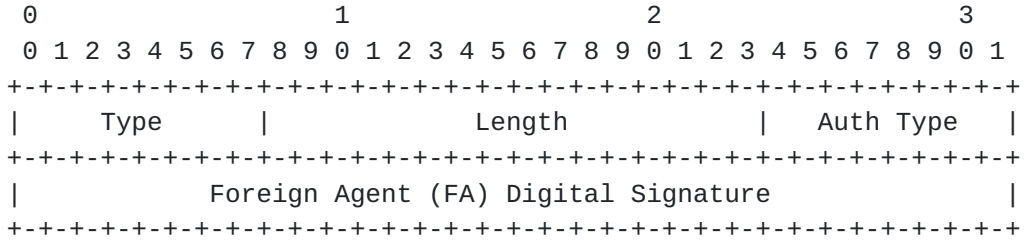
Exactly one Mobile Node Authentication Extension MUST be appended to all Registration Requests. The format of the Mobile Node Authentication Extension is:



Type	32 (Mobile Node Authentication Extension)
Length	4 plus the number of bytes in the digital signature
Auth Type	When the A bit is set, the Auth Type identifies the public key cryptographic method (algorithm) and key Length used to generate digital signatures. Valid Authentication types are shown in Table 2.4.
Mobile Node Digital Signature	The computed MN Private key based Digital Signature.

4.1.4.2. Foreign Agent Authentication Extension

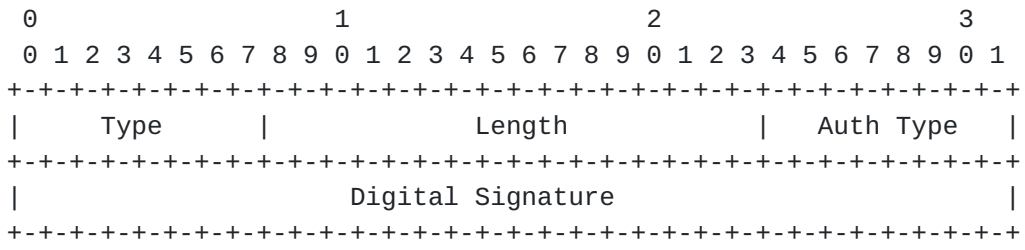
Exactly one Foreign Agent Authentication Extension must be appended to all Registration Requests being passed from an FA to an HA or Registration Replies sent from an FA to a MN. The format of the Foreign Agent Authentication Extension is:



Type	33 (Foreign Agent Authentication Extension)
Length	4 plus the number of bytes in the digital signature
Auth Type	When the A bit is set, the Auth Type identifies the public key cryptographic method (algorithm) and key Length used to generate digital signatures. Valid Authentication types are shown in Table 2.4.
Foreign Agent Digital Signature	The computed FA Private key based Digital Signature.

4.1.4.3. Home Agent Authentication Extension

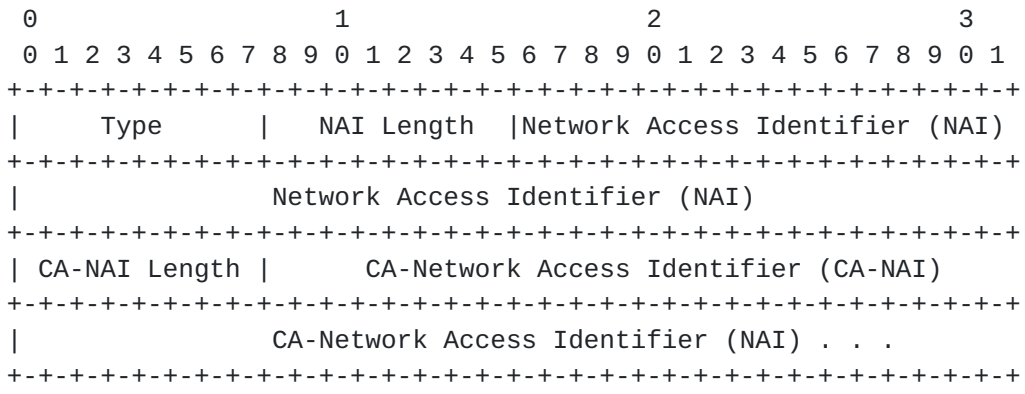
Exactly one Home Agent Authentication Extension must be appended to all Registration Replies being sent from an HA to an MN. The format of the Home Agent Authentication Extension is:



Type	34 (Home Agent Authentication Extension)
Length	4 plus the number of bytes in the digital signature
Auth Type	When the A bit is set, the Auth Type identifies the public key cryptographic method (algorithm) and key Length used to generate digital signatures. Valid Authentication types are shown in Table 2.4.
Home Agent Digital Signature	The computed HA Private key based Digital Signature.

4.1.4.4. Network Access Identification extension

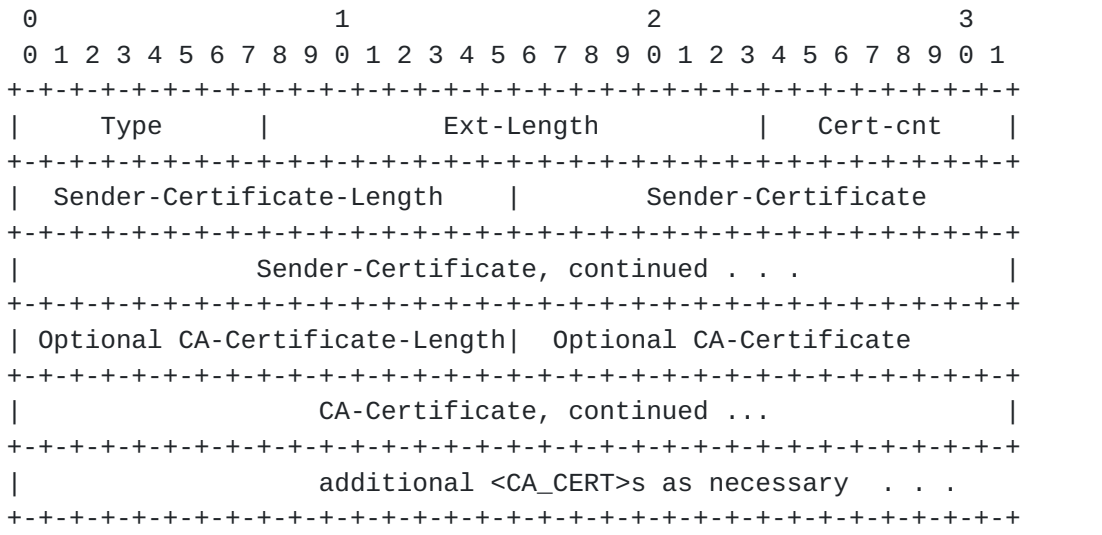
A Network Access Identification extension must preceed an Authentication extension. The format of the Network Access Identification extension is:



Type	11 (Network Access Identification extension)
Network Access Identifier Length	Length in bytes of the Network Access Identifier
Network Access Identifier	The Network Access Identifier (NAI) is an ASCII text string of up to XXXX bytes of an arbitrary format and length that uniquely identifies the network node. The NAI MUST match the subject identifier contained in an X.509 digital certificate for this network node.
CA Network Access Identifier Length	Length in bytes of the CA Network Access Identifier
CA Network Access Identifier	The Certificate Authority (CA) Network Access Identifier (CA-NAI) is an ASCII text string of up to XXXX bytes of an arbitrary format and length that uniquely identifies a certificate Authority. The CA-NAI MUST match the signing CA identifier contained in the X.509 digital certificate for this network node.

4.1.4.5 Certificate Extension

The Certificate Extension is used to transfer authentication information (Certificates) between MNs, FAs and HAs. The fields of the Certificate Extension are:



Type: 10 Identifies this as a Certificate Extension.

Ext Length: The length of the Certificate Extension in bytes. set to 6 + value of Sender-Certificate-Length field The value is increased again for each additional certificate in the Extension by 2 plus the value found in each additional CA-Certificate-Length Field.

Sender-Certificate-Length: Length in bytes of the X.509 Type 3 formatted Certificate of the message sender.

Sender-Certificate: The X.509 Type 3 Formatted Certificate of the message sender which contains the public key of the message sender.

CA-Certificate-Length: Length in bytes of the X.509 Type 3 formatted certificate of a Certificate Authority (CA). This field MUST be present if authentication relies on public keys and Certificate Authorities.

CA-Certificate: The X.509 Type 3 formatted certificate of a CA which contains the public key of the CA used to sign Certificates. This field MUST be present if authentication relies on public keys and

Certificate Authorities.

5. Protocol Overview

For this extended Mobile IP, a complete registration cycle consists of:

a) the MN receiving a Mobility Agent Advertisement
b) the MN sending a Registration Request to the FA
c) the FA preprocessing the received Registration Request and, if tentatively approved, passing the Registration Request to the MN's HA
d) the HA receiving the Registration from the MN, via the FA
e) the HA processing the Registration Request and sending a Registration Reply to the FA
f) the FA receiving the Registration Reply, updating visiting MN data structures
g) the FA sending the completed Registration Reply to the visiting MN.

Proposed authentication changes apply to the messages associated with both the Agent Discovery and the Registration procedures..

When secret key based authentication is being used then MNs, FAs and HAs follow the procedures specified in RFC-2002. The Following sections (3.1 through 3.12) describe Mobile IP authentication based upon public keys.

5.1. Agent Discovery with Public key Authentication

FAs advertise their presence via a Mobility Agent Advertisement Extension appended to ICMP Router Advertisements generated by Mobility Agents acting as Foreign Agents. The visiting MN obtains a Care-OF-Address (COA) from these Mobility Agent Advertisement Extensions (Agent Advertisements).

Our extended Agent Advertisement has appended to it:

- a Foreign Agent Network Access Identifier (NAI) Extension appended which contains the NAI of the FA and the NAI of a Certificate Authority that has signed an X.509 digital certificate for this FA.
- a Foreign Agent Authentication Extension containing a digital signature that is used to authenticate the contents of the Agent Advertisement message.
- a Certificate Extension so that MNs can quickly obtain a authentic copy of the FA's public key.

The specific authentication related steps the FA follows are:

1. The FA creates the Agent Advertisement, as per RFC-2002, and sets the new A bit to "1"
2. The FA creates the Agent NAI Extension and appends it to the Advertisement
3. The FA uses it's private key to produce a digital signature

spanning all Agent Advertisement fields and NAI extension fields and places this digital signature in a Foreign Agent Authentication Extension.

4. The FA creates a Certificate Extension placing a copy of its Certificate, and any Certificates belonging to CAs necessary for

trust hierarchy creation, into the Certificate Extension.
5. The FA appends the Foreign Agent Authentication Extension and the Certificate Extension to the Agent Advertisement, plus NAI extension, message.

The FA follows RFC-2002 regarding the transmission of Agent Advertisement messages.

5.2. MN Processing of Agent Advertisements with Public key Authentication

When the MN receives an Agent Advertisement, the MN follows the base Mobile IP protocol except for the following authentication actions:

1. The MN extracts the Certificates necessary for trust hierarchy creation from the Certificate Extension and, in the case where the FA and the MN share the same CA, the MN uses the CA's public key to validate the FA's Certificate.
2. In the case where the MN and the FA do not share a common CA, the MN uses any other CA Certificates contained in the Certificate Extension to establish a trust hierarchy path between the MN's CA and the FA's CA
3. In the case where the MN is unable to establish a trust hierarchy path between the CAs, the MN ceases further authentication processing and considers the Agent Advertisement message not authentic, the sending FA as not a valid candidate to register with and the MN ignores this Agent Advertisement message.
4. Should the MN be able to establish a trust hierarchy path between CAs, the MN proceeds down the path verifying CA Certificates stopping when the Certificate of the advertising FA has been verified.
5. Upon verification of the FA's Certificate, the MN uses the FA's public key from the FA Certificate to verify the digital signature in the Foreign Agent Authentication Extension, created using the FA's private key.
6. Upon successful verification of the Foreign Agent Authentication Extension digital signature, the MN continues with normal processing of the Agent Advertisement message as specified in the base Mobile IP protocol.

Should the Agent Advertisement digital signature not pass verification, the MN ceases further processing and considers the Agent Advertisement message as not authentic, the sending FA as not a valid candidate to register with and the MN ignores this Foreign Agent Advertisement message.

5.3. MN Registration Request Generation

When the MN generates a Registration Request message, the MN follows the base Mobile IP protocol except for the following authentication actions:

1. The MN sets the new A bit, in the Registration Request to "1".

2. The MN creates the MN NAI Extension and appends it to the Registration Request

3. The MN uses it's private key to produce a digital signature spanning all Registration Request fields and NAI extension fields and places this digital signature in a Mobile Node Authentication Extension.
4. The MN then creates a Certificate Extension placing a copy of its Certificate, and any Certificates belonging to CAs necessary for trust hierarchy creation, into the Certificate Extension.
5. The MN appends the Certificate Extension to the end of the Registration Request message following the Mobile Node Authentication Extension.

The MN continues with the actions specified in RFC-2002 for sending out Registrations Requests.

5.4. Registration Request Processing by FA

When the FA receives a Registration Request from an MN, the FA follows the base Mobile IP protocol except for the following authentication actions:

1. The FA extracts the Certificates from the Certificate Extension and, in the case where the FA and the MN share the same CA, the FA uses the CA's public key to validate the MN's Certificate.
2. In the case where the MN and the FA do not share a common CA, then the FA uses any other CA Certificates contained in the Certificate Extension to establish a trust hierarchy path between the FA's CA and the MN's CA.
3. In the case where the FA is unable to establish a trust hierarchy path between the CAs, the FA ceases further authentication processing and considers the Registration Request message not authentic, the sending MN as not allowed to attach to the FA's network, the FA logs the authentication failure and creates a Registration Reply message informing the MN that the MN's Registration Request is not allowed having failed authentication.
4. Should the FA be able to establish a trust hierarchy path between CAs. The FA proceeds down the path verifying CA Certificates stopping when the Certificate of the MN has been verified.
5. The FA uses the MN's public key from the MN Certificate to verify the digital signature in the Mobile Node Authentication Extension, created using the MN's private key.
6. Upon successful verification of the Mobile Node Authentication Extension digital signature, the FA continues with normal processing of the Registration Request message as specified in the base Mobile IP protocol except for authentication actions.
7. Should the Mobile Node Authentication Extension digital signature not pass verification, the FA ceases further authentication processing and considers the Registration Request message not authentic, the sending MN as not allowed to attach to the FA's network, the FA logs the authentication failure and creates a Registration Reply message informing the MN that the MN's Registration Request is not allowed having failed authentication.

5.5. FA Forwarding Registration Requests to HA

When the FA finishes basic Registration Request processing and is preparing to forward the Registration Request to the MN's Home Agent (HA), the FA performs the following authentication actions:

1. The FA deletes the received Certificate Extension.
2. The FA creates the Foreign Agent NAI Extension and appends it to the Advertisement
3. The FA uses it's private key to produce a digital signature spanning all Registration Request fields and NAI extension fields and places this digital signature in a Foreign Agent Authentication Extension.
2. The FA uses it's private key to produce a digital signature spanning all Registration Request message fields and places the digital signature in a Foreign Agent Authentication Extension appended following the NAI extension.
3. The FA places a copy of its Certificate, and copies of any other Certificates necessary for establishing a trust hierarchy, into a new Certificate Extension.
4. The FA appends the Certificate Extension to the end of the Registration Request message following the Foreign Agent Authentication Extension.
5. The FA continues with the actions specified in RFC-2002 for sending out Registrations Requests.

5.6. Registration Request Authentication verification by HA

When the HA receives a Registration Request forwarded from an FA, the HA follows the base Mobile IP protocol except for the following authentication actions:

1. The HA extracts the Certificates from the Certificate Extension and, in the case where the FA and the HA share the same CA, the HA uses the CA's public key to validate the FA's Certificate.
2. In the case where the HA and the FA do not share a common CA, then the HA uses any other CA Certificates contained in the Certificate Extension to establish a trust hierarchy path between the HA's CA and the FA's CA.
3. In the case where the HA is unable to establish a trust hierarchy path between the CAs, the HA ceases further authentication processing and considers the Registration Request message invalid, the forwarding FA as untrustworthy as a Foreign Agent, the HA logs the authentication failure and creates a Registration Reply message informing the FA that the MN's Registration Request is not allowed having failed FA authentication.
4. Should the HA be able to establish a trust hierarchy path between CAs. The HA proceeds down the path verifying CA Certificates stopping when the Certificate of the FA has been verified.
5. The HA uses the FA's public key from the FA Certificate to verify

the FA digital signature in the Foreign Agent Authentication Extension, created using the FA's private key.

6. The HA uses the MN's public key, from the MN Certificate that the HA already possesses, to verify the MN digital signature in the Mobile Node Authentication Extension, created using the MN's private key.
7. Upon successful verification of the Registration Request message digital signatures, the HA continues with normal processing of the Registration Request message as specified in the base Mobile IP protocol except for authentication actions.
8. Should the Registration Request message digital signatures not pass verification, the HA ceases further authentication processing and considers the Registration Request message not authentic, the requested registration as prohibited, the HA logs the authentication failure and creates a Registration Reply message informing the FA and the MN that the MN's Registration Request is not allowed having failed authentication.

5.7. HA Generation of Registration Reply

When the HA generates a Registration Reply message, the HA follows the base Mobile IP protocol except for the following authentication actions:

1. The FA sets the new A bit to "1".
2. The FA creates the Agent NAI Extension and appends it to the Registration Reply message.
3. The HA uses it's private key to produce a digital signature spanning all Registration Reply fields and NAI extension fields and places this digital signature in a Home Agent Authentication Extension which it appends to the Registration Reply.
2. The HA then creates a Certificate Extension placing a copy of its Certificate into the Certificate Extension.
3. The HA appends the Certificate Extension to the end of the Registration Request message following the Home Agent Authentication Extension.
4. The HA continues with the actions specified in RFC-2002 for sending out Registrations Requests.

5.7.2. HA Generation of Registration Reply With DHCP Involved

When the HA generates a Registration Reply message, the HA follows RFC-2002 except for the following authentication actions:

1. The HA uses it's private key to produce a digital signature spanning all Registration Request message fields and places the digital signature in an Home Agent Authentication Extension which it appends to the Registration Reply.
2. The HA continues with the actions specified in RFC-2002 for sending out Registrations Requests.

5.8. Registration Reply Authentication verification by FA

When the FA receives a Registration Reply from an HA, the FA follows the base Mobile IP protocol except for the following authentication actions:

1. The FA extracts the HA's Certificate from the Certificate Extension and uses the public key from the Certificate of the HA's CA to validate the HA's Certificate.
2. The FA uses the HA's public key from the HA Certificate to verify the digital signature in the Home Agent Authentication Extension, created using the HA's private key.
3. Upon successful verification of the Home Agent Authentication Extension digital signature, the FA continues with normal processing of the Registration Reply message as specified in the base Mobile IP protocol except for authentication actions.
4. Should the Registration Reply message digital signature not pass verification, the FA ceases further authentication processing and considers the Registration Reply message not authentic, the sending HA as not a valid HA, the FA logs the authentication failure and creates a Registration Reply message informing the MN that the MN's Registration Request is not allowed having failed authentication.

5.9. FA Forwarding Registration Reply to MN

When the FA finishes basic Registration Reply processing and is preparing to forward the Registration Reply to the MN, the FA performs the following authentication actions:

1. The FA deletes the Certificate Extension received from the HA.
2. The FA uses it's private key to produce a digital signature spanning all Registration Reply message fields and places the digital signature in a Foreign Agent Authentication Extension following the Home Agent Authentication Extension.
3. The FA continues with the actions specified in RFC-2002 for sending out Registrations Replies.

5.10. MN Receipt of Registration Reply

When the MN receives a Registration Reply forwarded from an FA, the MN follows the base Mobile IP protocol except for the following authentication actions:

1. The MN uses the FA's public key from the FA Certificate, that the MN already possesses, to verify the FA digital signature in the Foreign Agent Authentication Extension, created using the FA's private key.
2. The MN uses the HA's public key, from the HA Certificate, that the MN already possesses, to verify the HA digital signature in the Home Agent Authentication Extension, created using the HA's private key.

3. Upon successful verification of the Registration Reply message digital signatures, the MN continues with normal processing of the

Registration Reply message as specified in the base Mobile IP protocol except for authentication actions.

4. Should the Registration Reply message digital signatures not pass verification, the MN ceases further authentication processing and considers the Registration Reply message not authentic, the MN logs the authentication failure and restarts its efforts to find a foreign network the MN can register with.

5.11. FA Generation of Registration Reply

When the FA generates a Registration Reply message rejecting an MN's request to register with the FA's network, the FA follows the base Mobile IP protocol except for the following authentication actions:

1. The FA uses it's private key to produce a digital signature spanning all Registration Rely message fields and places the digital signature into a Foreign Agent Authentication Extension appended to the Registration Reply.
2. The FA continues with the actions specified in RFC-2002 for sending out Registrations Replies.

5.12. MN Receipt of Registration Reply

When the MN receives a Registration Reply generated by an FA, the MN follows the base Mobile IP protocol except for the following authentication actions:

1. The MN uses the FA's public key from the FA Certificate, which the MN already possesses, to verify the FA digital signature in the Foreign Agent Authentication Extension, created using the FA's private key.
2. Upon successful verification of the Registration Reply message FA digital signature, the MN continues with normal processing of the Registration Reply message as specified in the base Mobile IP protocol except for authentication actions.
3. Should the Registration Reply message FA digital signature not pass verification, the MN ceases further authentication processing and considers the Registration Reply message not authentic, the MN logs the authentication failure and restarts its efforts to find a foreign network the MN can register with.

6. Certificates

This extended Mobile IP provides for two forms of certificates:

1) certificates signed by Certificate Authorities and issued on behalf of the certificate subject by the Certificate Authority and
2) certificates signed by the subject of the certificate and issued by the subject.

6.1. Certificate Authority Signed Certificates

Certificate Authority Signed Certificates MUST include the following fields:

Distinguished Name - The Distinguished Name (DN) is the Network Access Identifier (NAI). The use of this field is a variation of the DN approach defined in [X.500].

Not Valid Before Date - Not Valid Before Date (NVBD) is that date prior to which the Certificate is not valid

Not Valid After Date - Not Valid After Date (NVAD) is that date After which the Certificate is not valid

CA Distinguished Name - The CA Distinguished Name (DN) is the Network Access Identifier (NAI) assigned to this CA.

Subject Public Key - Subject Public Key is the binary string of Octets containing the public key of the sender

Public Key Algorithm - Public Key Algorithm is the field that Identifies the type of public key algorithm the sender's public key must be used with

Public Key Size - Public Key Size is the field that identifies the size of the sender's public key in octets

CA Digital Signature - CA Digital Signature is the digital Signature generated by the sender's CA that binds the other fields of the Certificate together cryptocraphicly

Certificate Serial Number - A unique number assigned to a Certificate by the CA that creates and digitally signs the Certificate. This serial number is used to positively identify the Certificate

6.2 Self-Signed Certificates

With self-signed certificates each node acts as its own CA by creating a certificate for itself containing a public key that the node "certifies" as it's public key. This form of public key authentication is typically called an informal web of trust similar to that used with Pretty Good Privacy (PGP) public keys. Self-signed Certificates used with SSA Mobile IP MUST include the same fields as Certificate Authority Signed Certificates except for the following:

Signer Distinguished Name - This field replaces the CA Distinguished Name field and contains

the Network Access Identifier (NAI) of the node which created the certificate.

Signer Digital Signature - This field replace the CA Digital Signature field and contains the digital Signature, generated by the certificate creator, that binds the other fields of the Certificate together cryptocraphicly.

Certificate Serial Number - A unique number assigned to a Certificate by the node that creates and digitally signs the Certificate. This serial number is used to positively identify the Certificate

7. Trust Hierarchy Paths

A Trust Hierarchy Path is the establishment of a logical chain between two Certificate Authorities (CAs) and reflects a trust relationship that can be established through intervening CAs. Validation of a Certificate involves constructing a Trust Hierarchy Path between the sender Certificate, the CA that issued the sender Certificate and the CA of the validating system. The validity interval for every Certificate in this path must be checked. Establishing a trust hierarchy path MUST be performed to verify the authenticity and usability of Certificates within Mobile IP.

This process assumes that the receiver knows the public key of the Sender's CA. The receiver can develop trust in the public key of the Sender's CA recursively, if the receiver has a Certificate containing the CA's public key signed by a superior CA whom the receiver already trusts. In this sense, a certificate is a stepping stone in digital trust. Each certificate is processed in turn, starting with that signed using the input trusted public key.

The following checks are applied to all Certificates:
- Check that the signature verifies
- That dates are valid
- The subject and issuer names chain correctly
- The certificate has not been revoked.

If any of the above checks fails, the procedure terminates, returning a failure indication. If none of the above checks fail on each Certificate, the procedure terminates successfully.

8. Certificate Revocation Lists

Each CA signed digital certificate should be checked against the current Certificate Revocation List (CRL) from the issuing CA to

ensure that revoked Certificate are not employed. SSA Mobile IP

recognizes that network performance could be seriously degraded if

a receiving node always retrieves the most recent CRL when ever a new CA Signed Certificate is received. Consequently, a node (be it an MN, FA or HA) should cache received CA signed Certificates along with a value ("staleness value") that indicates the last time each Certificate was checked against a CRL from the issuing CA. The node should also provide a value that indicates the maximum degree ("staleness threshold") of Certificate staleness a given node may tolerate before the node has to retrieve the appropriate CRL and verify that the Certificate has not been revoked.

This staleness checking function is a compromise between the effect on available bandwidth vs. the risk of using a revoked Certificate. In those cases where the node has high network bandwidth available (usually FAs and HAs), via wired network attachments, then the staleness threshold should be set to a relatively low value (eg. 10 seconds). Where the node has less than good network bandwidth available (usually MNs) via wireless network attachments then the staleness threshold should be set to a higher value (eg. 10 minutes).

9. Security Considerations

Use of Mobile IP without authentication between the MN and the FA, such as with DHCP, do not provide for visited network access control and accounting. Likewise the MN has no basis to trust the visited network not to miss-direct or copy MN sourced packets.

Mobile IP relies on the use of the Address Resolution Protocol (ARP) for intercepting packets destined for a traveling MN. Unfortunately ARP does not include authentication mechanisms. Any wireless home network is consequently vulnerable to MN traffic stealing by having a hostile node on the wireless network issue ARP messages which cause these packets to be sent to a destination other than an MN, when at home, or the MN's HA when the MN is on the road. Ideally the ARP protocol should include authentication but this would require significant changes to the currently deployed protocol.

Staleness of Certificates and frequency for Certification Revocation List retrieval is a trade-off between exposure and potential threat resulting in a degree of risk from a revoked Certificate. By having implementations of SSA Mobile IP provide a user tunable staleness threshold the degree of risk becomes a user managed function.

Patent Issues

There are no patent issues at this time. The MIT patent (#4405829) governing

the RSA cryptography algorithm expired on December 15, 1999 and no longer applies.

References

[Diffie76] Diffie, W., Hellman, M. E., "New directions in cryptography", IEEE Transactions on Information Theory, IT-22(6):644--654, November 1976.

[NIST94] National Institute of Standards and Technology, NIST FIPS PUB 186, "Digital Signature Standard", US. Department of Commerce, May 1994

[RFC1319] Kaliski, B., "The MD2 Message-Digest Algorithm", April 1992.

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", April 1992.

[RFC1422] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", February 1993

[RFC1541] Droms, R., "Dynamic Host Configuration Protocol", October 1993

[RFC2002] Perkins, C., editor, "IP mobility support", October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Level", March 1997.

[RFC2486] Aboba, B., Beadles, M., "The Network Access Identifier", January 1999

[RSA78] Rivest, R.L., Shamir, A., Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Communications of the ACM, 21(2):120-126, February 1978.

[Schneier96] Schneier, B., "Applied Cryptography 2nd Edition", Chapter 22 pp. 513-514, John Wiley & Sons Inc., 1996

[X.500] "CCITT. Recommendation X.500: The Directory-Overview of Concepts, Models and Services", 1988

[X.509] "CCITT. Recommendation X.509: The Directory-Authentication Framework", 1988.

Authors' Address

Questions about this memo can also be directed to:

Stuart Jacobs
Network Security Group
Verizon Laboratories,
40 Sylvan Road,
Waltham, MA 02451-1128, USA.
Phone: 781-466-3076
Fax: 781-466-2838
Email: Stu.Jacobs@Verizon.com

Scott Belgard
Network Security Group
Verizon Laboratories,
40 Sylvan Road,
Waltham, MA 02451-1128, USA.
Phone: 781-466-2826
Fax: 781-466-2838
Email: Scott.Belgard@Verizon.com