

Mobile IP Public Key Based Authentication

<draft-jacobs-mobileip-pki-auth-01.txt>

Proposes an extension to the Mobile IP base protocol.

Allows Mobile Nodes (Hosts) and Mobility Agents (both home network and foreign network) to use

- Secret keys and Keyed MD5 <new>
- CA signed digital certificates
- Self signed digital certificates <new>
- IP address or host name as certificate subject <new>
- public keys

as the basis of authenticating Mobile IP control messages.

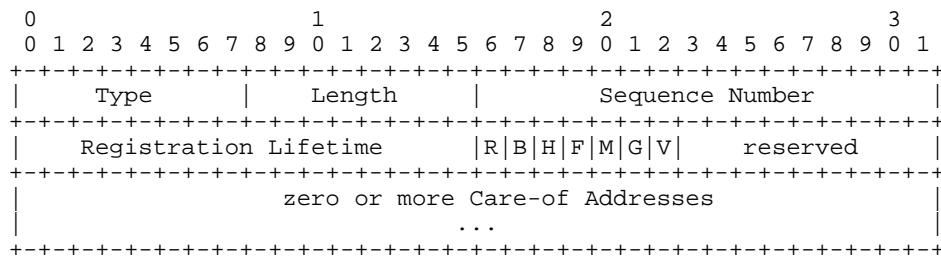
Authentication types.

Auth Type Value	Authentication Algorithm	Key Length in bits	Digital Signature Length in bytes
001	MD5	128	16
002 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

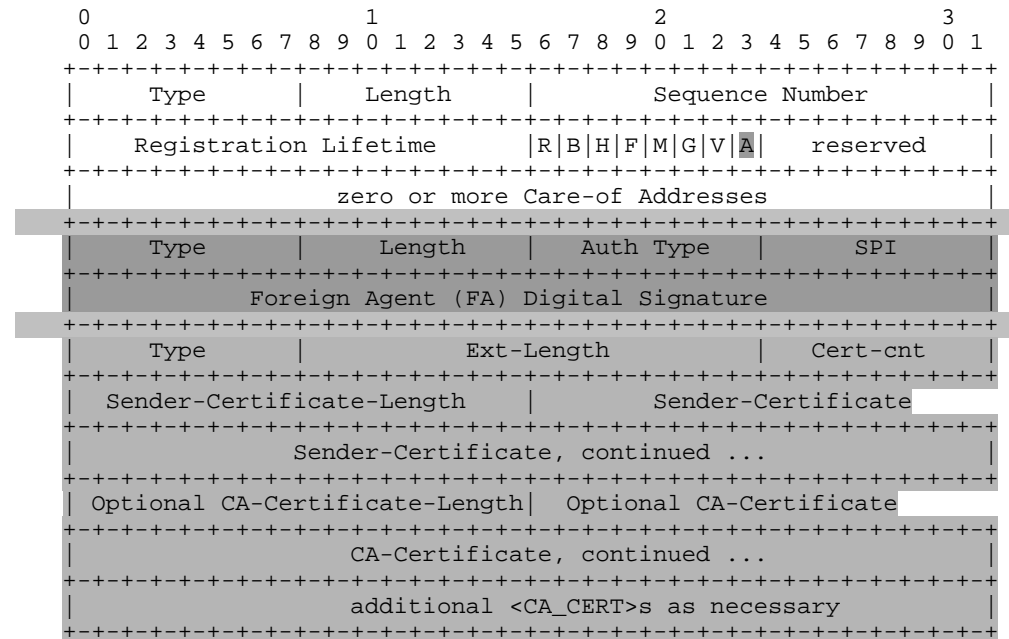
Auth Type = 001 then authentication is performed in a Prefix-Postfix keyed MD5 fashion as specified in RFC-2002.

Mobility Agent Advertisement Extension

RFC 2002 MIP

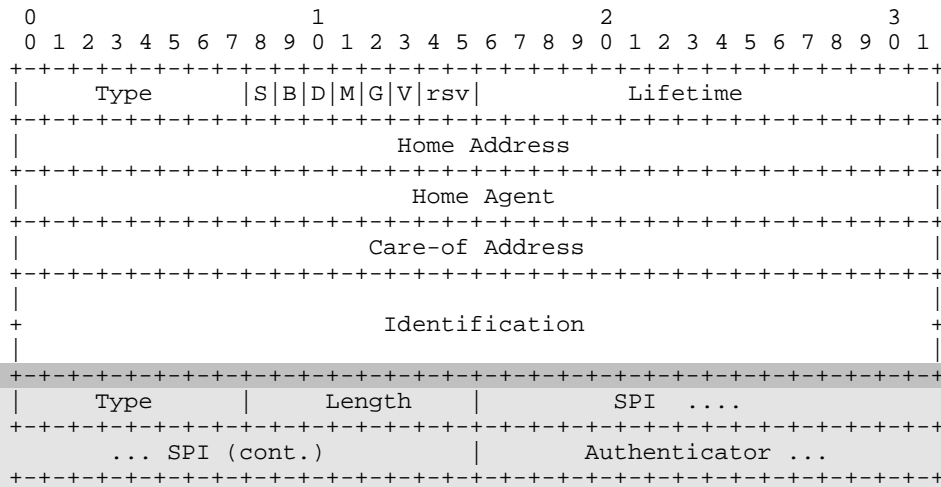


SSA MIP

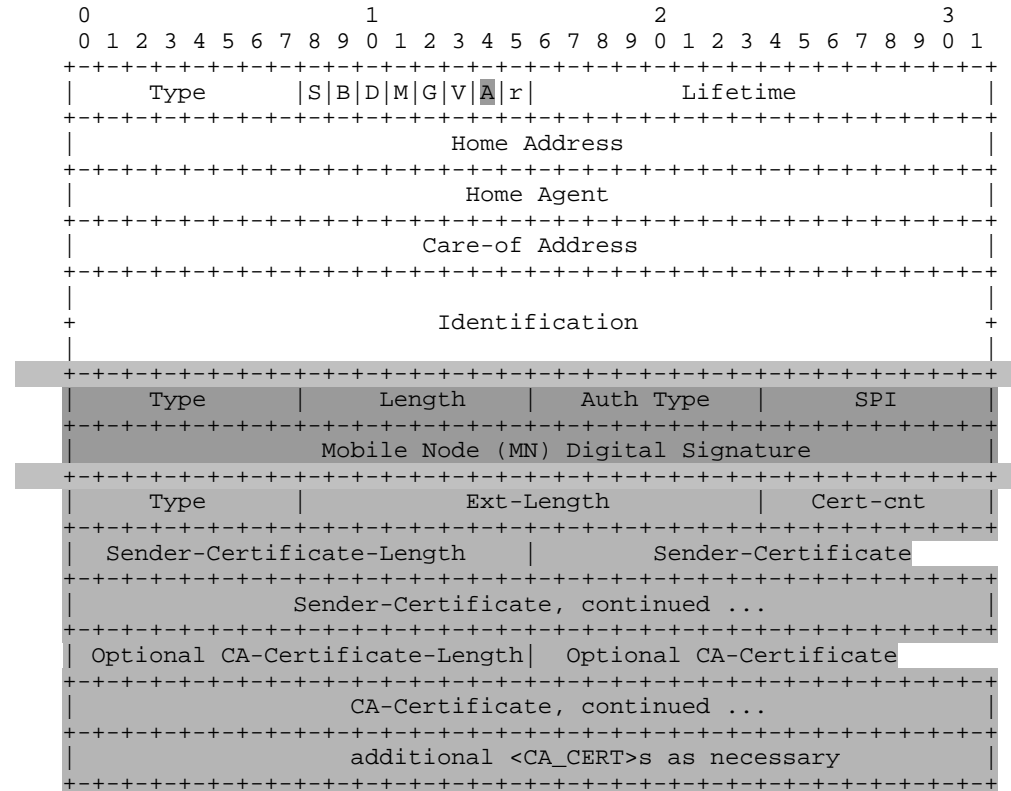


Registration Request Message received by a Foreign Agent

RFC 2002 MIP

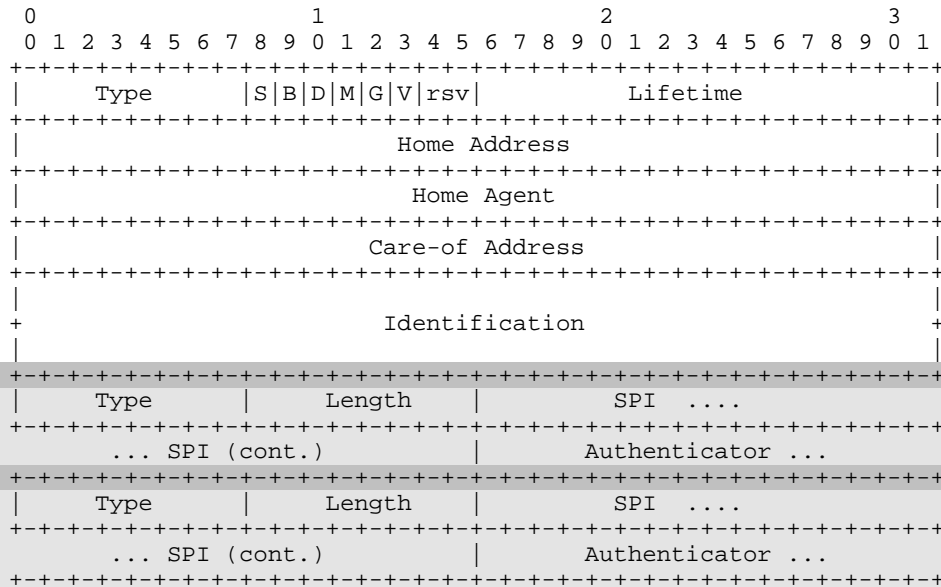


SSA MIP

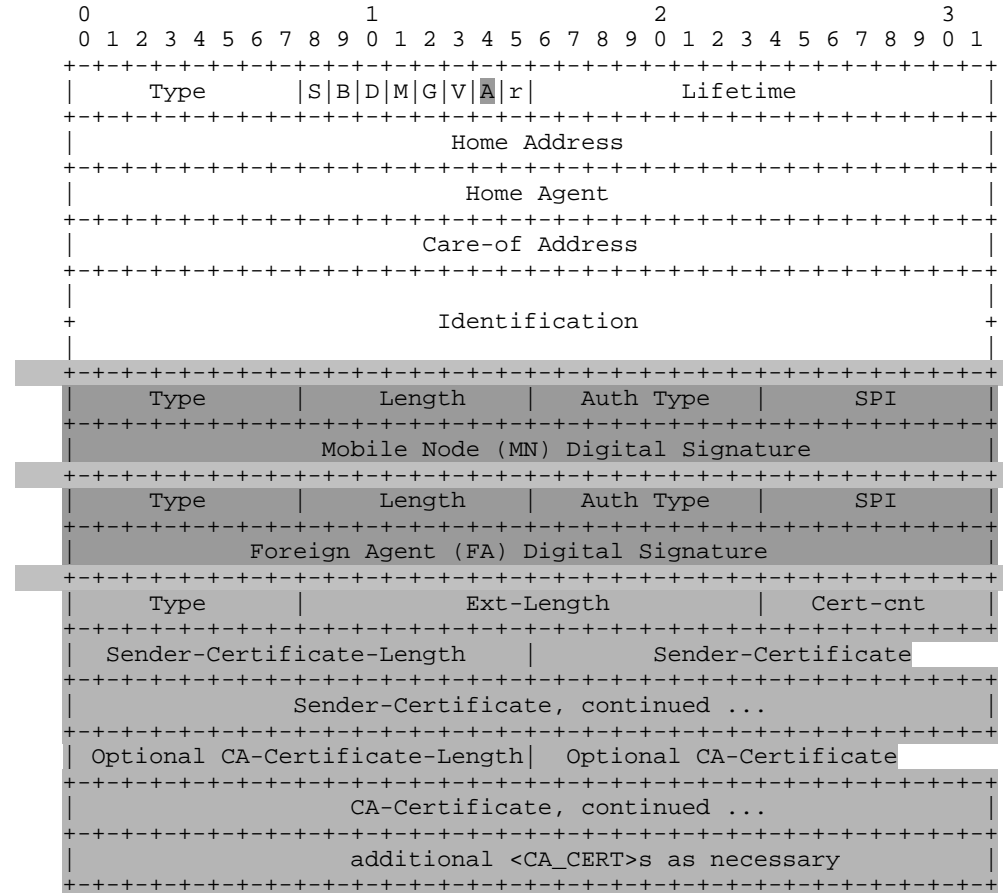


Registration Request Message Received by a Home Agent

RFC 2002 MIP

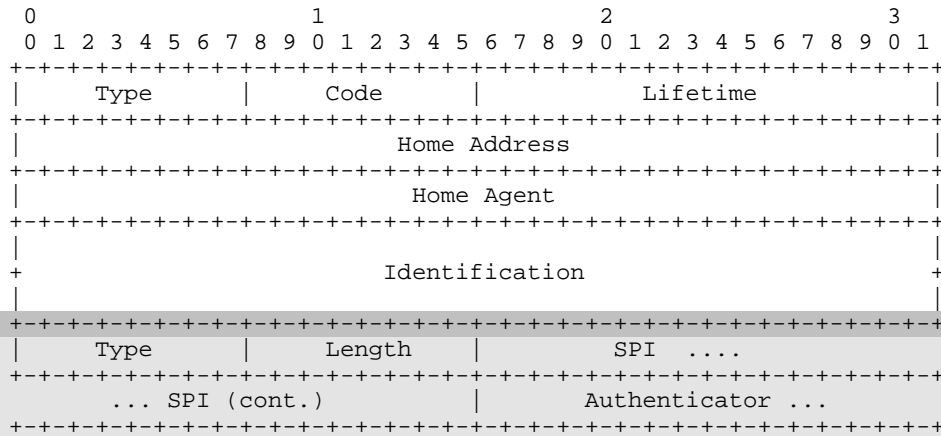


SSA MIP

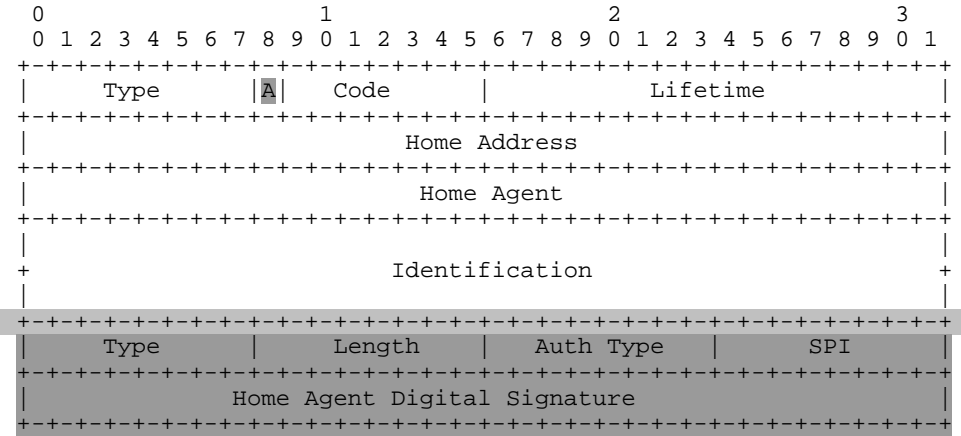


Registration Reply Message received by a Foreign Agent

RFC 2002 MIP

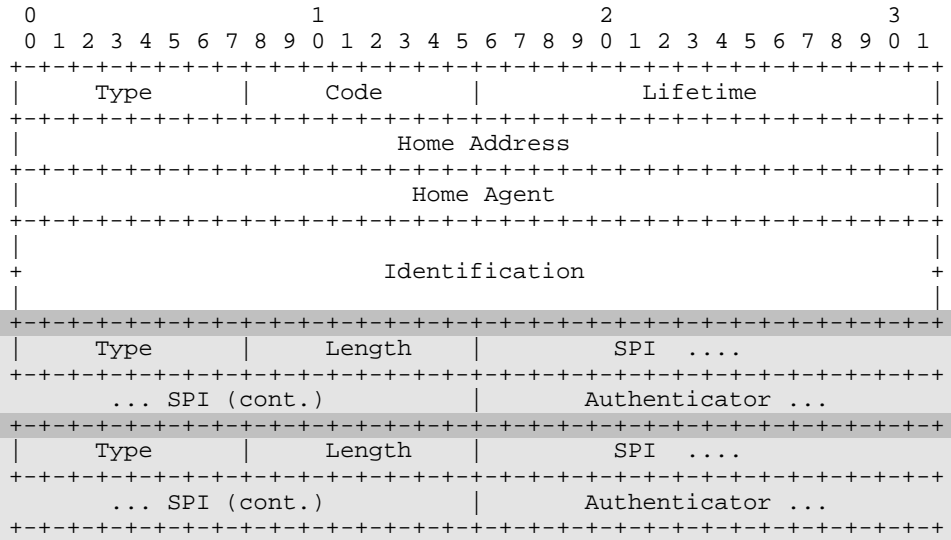


SSA MIP

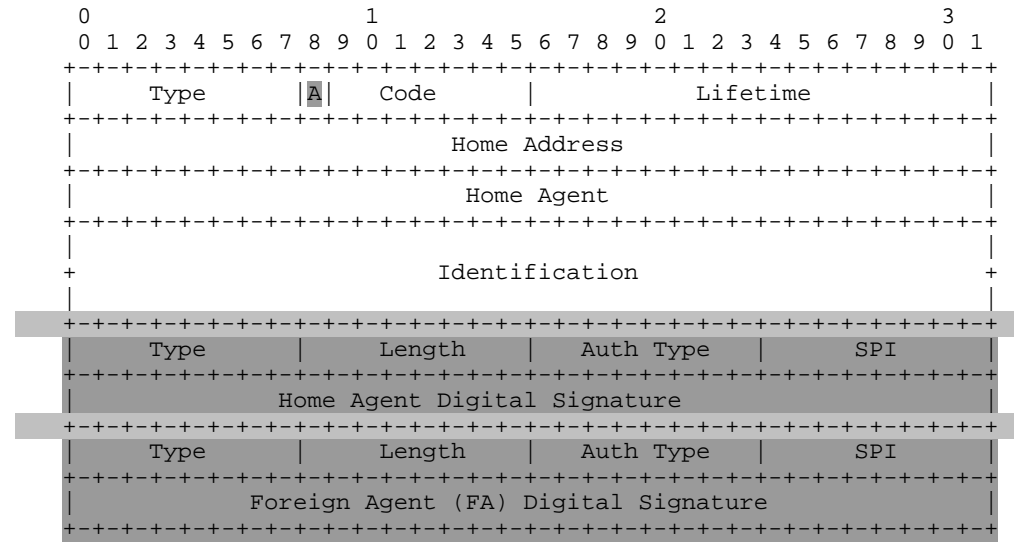


Registration Reply Message received by a Mobile Node

RFC 2002 MIP



SSA MIP



Authors' Address

Stuart Jacobs, Secure Systems Department
GTE Laboratories,
40 Sylvan Road,
Waltham, MA 02451-1128, USA.
Phone: 781-466-3076
sjacobs@gte.com