Authenticator Creation/Verification

- Computation depends on the type of authentication algorithm, e.g. HMAC-MD5, HMAC-SHA, DSA or RSA-MD5.

- Input for this computation is the entire Mobile IP message to be protected upto and including the type, length and SPI fields of the authentication extension following the security parameter extension (same scope as defined previously in RFC 2002).

The hash addresses concerns with sending long certificates.

The Key ID field

Identifies the verification key in one of several ways:

OPAQUE the interpretation of the Key ID value is a local matter between communicating entities

X509_CERT Key ID field has a certificate containing the public key needed for verification.

X509_CERT_CHAIN as above but other certs are included for derived trust

CERT_MD5_HASH useful when recipient is known to have the certificate already

Motivation

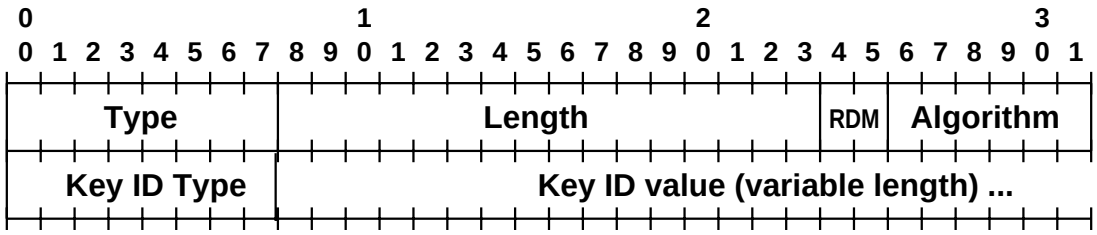
- Simplifies the use of public-key authentication w/ Mobile IP by allowing in-line exchange of public-key certificates (as in IKE).

- Provides a uniform mechanism for supporting both symmetric-key (HMAC-MD5, HMAC-SHA, prefix-suffix-MD5) and public-key (DSA, RSA-MD5) authentication methods.

- Allows mixing of public-key and symmetric-key authentication methods on different authentication extensions within the same Mobile IP message.

Currently a non-zero RDM field is only allowed when the following extension is a MN-HA extension.

Extension Format



- Must be followed immediately by an MN-HA, MN-FA or HA-FA authentication extension in which the SPI is a fixed TBD value.

- RDM: Replay Detection Mechanism (00 = none, 01 = timestamps*, 10 = nonces*)

- Algorithm: Determines how the authenticator (in the following extension) is computed.

- Key ID type and value identify the key needed to verify the authenticator.

Inline Security Parameter Extension for Mobile IP

<draft-gupta-mobileip-inline-secparams-00.txt>

Vipul Gupta
SUN Microsystems, Inc
901 San Antonio Road
Mailstop UMPK 15-214
Mountain View, CA 94043-1100

Email: vipul.gupta@eng.sun.com