X.509 Encoding of Diffie-Hellman Public Values
<draft-ietf-ipsec-skip-x509-00.txt>

Status of this Memo

This document is a submission to the IETF Internet Protocol Security (IPSEC) Working Group. Comments are solicited and should be addressed to the working group mailing list (ipsec@ans.net) or to the authors.

This document is an Internet-Draft. Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working Groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts draft documents are valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), nic.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

Distribution of this memo is unlimited.
Abstract

1. Encoding of DH public values

The X.509 certificate format is defined by the following ASN.1 syntax:
Certificate ::= SIGNED SEQUENCE {
  version [0]           Version DEFAULT v1988,
  serialNumber          CertificateSerialNumber,
  signature             AlgorithmIdentifier,
  issuer                Name,
  validity              Validity,
  subject               Name,
  subjectPublicKeyInfo  SubjectPublicKeyInfo
}

Version ::= INTEGER { v1988(0) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
  notBefore UTCTime,
  notAfter UTCTime
}

SubjectPublicKeyInfo ::= SEQUENCE {
  algorithm    AlgorithmIdentifier,
  subjectPublicKey     BIT STRING
}

AlgorithmIdentifier ::= SEQUENCE {
  algorithm       OBJECT IDENTIFIER,
  parameters      ANY DEFINED BY algorithm OPTIONAL
}

The encoding of a Diffie-Hellman public value in an X.509 certificate will be in the form of an INTEGER. The algorithm identifier will be as defined in PKCS #3 [3].
Thus,

DHPublicKey ::= INTEGER

AlgorithmIdentifier ::= SEQUENCE {
  algorithm OBJECT IDENTIFIER
  SEQUENCE {
    prime INTEGER, -- p
    base INTEGER, -- g
    privateValueLength INTEGER OPTIONAL
  }
}

with the OBJECT IDENTIFIER value being,

dhKeyAgreement OBJECT IDENTIFIER ::= {
  iso(1) member-body(2) US(840)
    rsadsi(113549) pkcs(1) 3 1
}

The DHPublicKey gets encapsulated as the BIT STRING in SubjectPublicKeyInfo of an X.509 certificate in the following manner. First the DHPublicKey is encoded as an INTEGER, and then this INTEGER is encoded as the payload of the BIT STRING.

The certificate and Certificate Revocation List (CRL) encoding is the same as in RFC 1422. CRLs can be used with SKIP in accordance with each site’s certificate/CRL management policies.

2. Encoding of the Distinguished Name (DN)

When the name space is the IP address space, a certificate is allowed to bind multiple IP addresses to a single public value to accommodate cases where a single IP node has multiple IP addresses. The SEQUENCE-OF construct in a DN readily allows for this. What is needed is an ASN.1 OBJECT IDENTIFIER for an AttributeType specifying an IP address.
This is defined here as,

ipAddress ATTRIBUTE
   WITH ATTRIBUTE-SYNTAX
       PrintableString (SIZE(1 .. ub-ipAddress))
   ::= { 1, 3, 6, 1, 4, 1, 42, 2, 11, 2, 1 }

ub-ipAddress ::= 256

The DN in the certificate can contain multiple of these by iterating on the SEQUENCE-OF construct of the Relative Distinguished Name Sequence.

The PrintableString contains either the hexadecimal representation or standard dot notation representation of an IP address. Note that all three conventional forms for representing IPv6 addresses [7] as text strings are allowed by this definition.

When individual users are identified using DNs, then the certificate naturally contains their DNs. The SKIP internet draft [5] describes how DNs may be used with SKIP, by identifying the DN name space using the Source and destination NSID bytes in the SKIP header.

3. Security Considerations

Security issues are not discussed in this document.

Acknowledgements

We would like to thank all of the people who helped make this draft possible.

References


Author’s Address(es)

Ashar Aziz
Sun Microsystems, Inc.
M/S PAL1-550
2550 Garcia Avenue
Mountain View, CA 94043

Email: ashar.aziz@eng.sun.com
Alternate email address: ashar@incog.com

Tom Markson
Sun Microsystems, Inc.
M/S PAL1-550
2550 Garcia Avenue
Mountain View, CA 94043

Email: markson@incog.com
Alternate email address: markson@eng.sun.com

Hemma Prafullchandra
Sun Microsystems, Inc.
M/S PAL1-550
2550 Garcia Avenue
Mountain View, CA 94043

Email: hemma@eng.sun.com
Alternate email address: hemma@incog.com