Media Description for IKE in the Session Description Protocol (SDP)

draft-saito-mmusic-sdp-ike-03

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

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 are draft documents 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."
The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on January 28, 2009.
Abstract
This document extends the protocol identifier of SDP so that it could
negotiate the use of IKE for media session in SDP offer/answer model.
And it also specifies the method to boot up IKE and generate IPsec SA
using self-signed certificate under the mechanism of comediatls.
This document extends RFC 4572. In addition, it defines a new
attribute "udp-setup", which is similar to "setup"
attribute defined
in RFC 4145, to enable endpoints to negotiate their roles in the IKE
session. Considering the case that pre-shared keys can be used for
authentication in IKE, a new attribute "psk-fingerprint" is also
defined.
Conventions used in this document
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
document are to be interpreted as described in [RFC2119].
Table of Contents
1. Introduction .............................. 4
1.1. Problem Statement ................. 4
1.2. Approach to Solution
1.3. Alternative Solution under Prior Relationship between
Two Nodes
2. Protocol Overview

7
3. Protocol Identifiers ........................................ 9
4. Example of SDP Offer and Answer Exchange without IPsec
NAT-Traversal .............................................. 10
5. Example of SDP Offer and Answer Exchange with IPsec
NAT-Traversal .......................... 12
5.1. Port Usage

... 12
5.2. Offer and Answer Exchange with ICE . . . . . . . . . . 12
6. Application to IKE .......................... 15
7. Specifications Assuming Prior Relationship between Two
Nodes .......................... 16
7.1. Certificates Signed by Trusted Third Party . . . . 16
7.2. Configured Pre-Shared Key ............... 17
8. Security Considerations .......................... 19
9. IANA Considerations .......................... 20
10. References ................................. 21
10.1. Normative References . . . . . . . . . . . . . . 21
10.2. Informative References ................. 22
Appendix A. Changes since draft-saito-mmusic-sdp-ike-02.

.... 23
Authors' Addresses ............................ 24
1. Introduction
In this section, the background of the problem in accessing home
network which this document tries to solve, and the approach to the
solution are described.
1.1. Problem Statement
When a device outside the home network connects to another device
inside the home network, it often becomes a problem to traverse a NAT
(Network Address Translation) device between them. One of the
effective solutions for this problem is VPN remote access to the NAT
device, usually a home router. With this approach, once the external
device participates in the home network securely, it will be easy to
establish connections with all the devices inside the home. On the
other hand, there are more difficult cases that a home router itself
is located inside the NAT. In such cases, it is also necessary to
consider NAT traversal of the remote access to the home router. In
any cases, because a global IP address of the home router is not
always fixed, it is necessary to make use of an effective name
resolution mechanism.
In addition, there is a problem how a remote client and a home router
authenticate each other over IKE [RFC4306] which establishes IPsec
[RFC4301] for remote access. It wouldn't be always possible that
both parties exchange a pre-shared key securely in advance. It would
be also impractical to distribute authentication certificates signed
by well-known root certification authority (CA) to all the devices
because of their cost and administrative overhead, and after all, it
is inefficient to publish a temporary certificate to the device which
does not have a fixed IP address or hostname. Therefore, if it is
possible to use a self-signed certificate for authentication
securely, that will be one of the effective solutions in this case.
1.2. Approach to Solution
In this document, we propose to use SIP [RFC3261] as a name.
resolution and authentication mechanism to initiate an IKE session.
There are three main advantages to use SIP as follows.
Delegation of Authentication to Third Party
By taking advantage of the authentication and authorization
mechanisms which SIP already has, the devices can be free from
managing signed certificates and their whitelists.
o UDP Hole Punching for IKE/IPsec
SIP has a cross-nat rendezvous mechanism such as ICE
[I-D.ietf-mmusic-ice]. This effective function can be used for
general applications as well as real-time media. It is difficult
to setup the session between devices without SIP if they are
inside various types of NAT.
o Reuse of Existing SIP Infrastructure
SIP servers are widely distributed as a scalable infrastructure,
and it is quite reasonable to reuse them without any
modifications.
Today, SIP is applied to not only VoIP but also various applications
and recognized as a general protocol for session initiation.
Therefore, it can be used to initiate IKE/IPsec sessions, too.
On the other hand, there is also a specification which uses a self-
signed certificate for authentication in the SIP/SDP
[RFC4566]
framework. Comedia-tls [RFC4572] specifies the method to exchange a
fingerprint of self-signed certificate to establish a TLS [RFC4346]
connection. This specification defines a mechanism that allows self-
signed certificates can be used securely, provided that the integrity
of the SDP description is assured. Because a certificate itself can
be used for authentication not only in TLS but also in IKE, this
mechanism will be applied to the establishment of IPsec SA by
extending the protocol identifier of SDP so that it could specify
One of the easy methods to protect the integrity of SDP description,
which is the premise of this spec, is to use SIP identity [RFC4474]
mechanism. This approach is also referred in
[I-D.fischl-sipping-media-dtls]. Because SIP identity mechanism can
protect the integrity of a body part as well as the value of From
header in a SIP request by a valid Identity header, the receiver of
the request can establish the secure IPsec connections with the
sender by confirming that the hash value of the certificate sent
during IKE negotiation matches the fingerprint in the SDP. Although
SIP identity does not protect the identity of the receiver of the SIP
request, SIP connected identity [RFC4916] does it.
Considering above background, this document defines new media formats
"ike-esp" and "ike-esp-udpencap" which can be used when the protocol
identifier is "UDP" to enable the negotiation of using IKE for media
session over SDP exchange on condition that the integrity of SDP
description is assured. And it also specifies the method to setup
IPsec SA by exchanging fingerprints of self-signed certificates based
on comedia-tls, and notes the example of SDP offer/answer [RFC3264]
and the points which implementation should take care. Because there
is a chance that devices are inside NAT, it also covers the method to
combine IKE/IPsec NAT-Traversal [RFC3947][RFC3948] with ICE. In
addition, it defines an attribute "udp-setup" for UDP media sessions,
similar to the "setup" attribute for TCP-based media transport
defined in RFC 4145 [RFC4145]. It is used to negotiate the role of
each endpoint in the IKE session.
1.3. Alternative Solution under Prior Relationship between Two Nodes
Under quite limited conditions, certificates signed by trusted third
parties or pre-shared keys between endpoints could be used for
authentication in IKE, with using SIP servers only for name
resolution and authorization of session initiation. We address such
limited cases in chapter 7.
2. Protocol Overview
As shown in Figure 1, for example, there is a case of VPN remote
access from a device outside the home to the home router whose IP
address is not fixed. In this case, the external device, a remote
client recognizes Address of Record of the home router, but does not
have any information about its contact address and certificate.
Generally, it is difficult to establish IPsec SA dynamically and
securely in this situation. However as specified in comedia-tls, if
the integrity of SDP session descriptions is assured, it is possible
for the home router and the remote client to have a prior
relationship with each other by exchanging certificate fingerprints,
secure one-way hashes of the DER (distinguished encoding rules) form
of the certificates.
+---------| Proxy |<--------+
| | INVITE +-----------+ | |
Net. | +----------+ IKE (Media Session) +----------+
<table>
<thead>
<tr>
<th></th>
<th>Remote</th>
<th></th>
<th>Router</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Client =========(4)====================
|          |      IPsec SA       +--------+
|          |                        |
Figure 1: Remote Access to Home Network
1. Both Remote Client and Home Router generate secure signaling
channels. They may REGISTER to SIP Proxy using TLS.
2. Both Remote Client (SDP offerer) and Home Router (SDP answerer)
exchange the fingerprints of their self-signed certificates in
SDP during an INVITE transaction.
3. After SDP exchange, Remote Client (SDP offerer) initiates IKE
with the SDP answerer to establish IPsec SA. Both the offerer
and the answerer validate that the certificate presented in the
IKE exchange has a fingerprint that matches the fingerprint from
SDP. If they match, IKE negotiation proceeds as normal.
Using this method, the self-signed certificates of both parties are
used for authentication in IKE, but SDP itself is not concerned with
all the negotiations related to key-exchange such as those of
encryption and authentication algorithms. These negotiations are up
to IKE. And in many cases that IPsec is used for remote access, a
remote client needs to obtain a private address inside the home
network dynamically while initiating the remote access, therefore
IPsec security policy also needs to be set dynamically at the same
time. However, such a management function of security policy is on
the responsibility of the high-level application. SDP is not
concerned with it. The roles of SDP here are to determine the IP
addresses of both parties used for IKE connection with c-line in SDP,
and exchange fingerprints of certificates used for authentication in
IKE with fingerprint attribute in SDP.
If the high-level application thinks a VPN session as the media
session, it MAY discard the IPSec SA and terminate IKE when that
media session is terminated by BYE request. Therefore the
application MUST NOT send a BYE request as long as it needs the IPSec
SA. By the way, each party can cache the certificate of the other
party as described in Security Consideration of comedia-tls.
The above example is for tunnel mode IPsec used for remote access,
but the actual usage of negotiated IPsec is not limited. For
example, IKE can negotiate transport mode IPsec to encrypt multiple
media sessions between two parties with only a pair of IPsec security
associations. Only one thing that SDP offer/answer model is
responsible for is to exchange the fingerprints of certificates used
for IKE, therefore, it does not take care of security policy.
3. Protocol Identifiers
This document defines new media format descriptions "ike-esp" and
"ike-esp-udpencap", which can be used when the protocol identifier is
"UDP" and indicate that the described media are IKE and IPsec coming
after it. Both offerer and answerer can negotiate IKE by specifying
"UDP" in the "proto" field and "ike-esp" or "ike-esp-udpencap" in the
"fmt" field in SDP. "ike-esp" denotes the normal IKE process and
IPsec ESP [RFC4303], while "ike-esp-udpencap" does the process of
IPsec NAT-Traversal that is specified in RFC3947 and RFC3948.
In addition, this document defines a new attribute "udp-setup", which
can be used when the protocol identifier is "UDP" and the "fmt" field
is "ike-esp" or "ike-esp-udpencap", in order to describe how
endpoints should perform the IKE session setup procedure. The "udp-
setup" attribute indicates which of the end points should initiate
the IKE session establishment. The "udp-setup" attribute is charset-
independent and can be a session-level or a media-level attribute.
The following is the ABNF of the "udp-setup" attribute.
udp-setup-attr = "a=udp-setup:" role
role = "active" / "passive" / "actpass"
'active' : The endpoint will initiate an outgoing session.
'passive' : The endpoint will accept an incoming session.
'actpass' : The endpoint is willing to accept an incoming
session or to initiate an outgoing session.
As defined in 4.1 of RFC 4145, both endpoints negotiate the value of
"udp-setup" using the offer/answer model. However, "holdconn"
defined in RFC 4145 is not defined here because UDP doesn't establish
a connection.
| Offer | Answer |
active       passive
passive      active
actpass  active / passive
The semantics of "active", "passive", and "actpass" in the offer/
answer exchange is the same as the definition described in 4.1 of RFC
The default value of the udp-setup attribute is "active" in
the offer and "passive" in the answer.
4. Example of SDP Offer and Answer Exchange without IPsec NAT-Traversal
If IPsec NAT-Traversal is not necessary, SDP negotiation to setup IKE
is quite simple. The example of SDP exchange is as follows.
(Note: due to RFC formatting conventions, this document splits SDP)
across lines whose content would exceed 72 characters. A backslash
character marks where this line folding has taken place. This
backslash and its trailing CRLF and whitespace would not appear in
actual SDP content.)
offer SDP
m=application 500 UDP ike-esp
c=IN IP4 192.0.2.10
a=fingerprint:SHA-1 \
answer SDP
m=application 500 UDP ike-esp
c=IN IP4 192.0.2.20
a=udp-setup:passive
a=fingerprint:SHA-1 \
Following comedia-tls specification, the fingerprint attribute may be
either a session-level or a media-level SDP attribute. If it is a
session-level attribute, it applies to all IKE sessions and TLS
sessions for which no media-level fingerprint attribute is defined.
By the way, it is possible that an offerer becomes IKE responder and
an answerer becomes IKE initiator. For example, when RAS server
sends INVITE to RAS client, the server may expect the client to
become an IKE initiator. In this case, the server sends
offer SDP
with udp-setup:passive and the client sends back answer
SDP with udp-
setup:active as follows.
offer SDP
m=application 500 UDP ike-esp
c=IN IP4 192.0.2.10
a=udp-setup:passive
a=fingerprint:SHA-1 \
Media Description for IKE in the SDP

July 2008
answer SDP
m=application 500 UDP ike-esp
c=IN IP4 192.0.2.20
a=udp-setup:active
a=fingerprint:SHA-1 \
5. Example of SDP Offer and Answer Exchange with IPsec NAT-Traversal
If either of endpoints that negotiate IKE is inside the NAT, they
need to transmit both IKE and IPsec packets over NAT. That mechanism
is specified in RFC3947 and RFC3948 that both endpoints encapsulate
IPsec-ESP packets with UDP header and multiplex them into the UDP
session which IKE generates. On the other hand, they also need to
decide their transport addresses (combination of IP address and port)
before starting IKE making use of ICE framework. In this chapter, a
method to coordinate IPsec NAT-Traversal and ICE is described.
5.1. Port Usage
IKE uses local UDP port 500 in general, but IPsec NAT-Traversal spec
requires the port transition to UDP port 4500 during IKE negotiation
because there is a possible problem that IPsec-aware NAT would
derive. This transition imposes ICE to generate an additional UDP
session soon after the first IKE starts, and it would be an
inefficient overhead. However, IPsec NAT-Traversal allows IKE
session to use local UDP port 4500 from the beginning. Therefore the
endpoints SHOULD use their local UDP port 4500 for IKE session from
the beginning because when they are ready to use ICE, they should
also be ready to use IPsec NAT-Traversal.
When using ICE, a responder's IKE port observed by an initiator is
not necessarily 500 or 4500. Therefore, IKE initiator MUST allow any
destination ports in addition to 500 and 4500 for the IKE packets
which itself sends.
5.2. Offer and Answer Exchange with ICE
We consider the following scenario here.
| Internet |
| offerer | answerer |
Figure 2: NAT-Traversal Scenario
As shown above, an offerer is on the Internet but an answerer is
inside the NAT. The offerer cannot initiate IKE session unless the
answerer prepares a global routable transport address which accepts
IKE packets. In this case, the following offer/answer exchange will
take place.
offer SDP
a=ice-pwd:YH75Fviy6338Vbrhlp8Yh
a=ice-ufrag:9uB6
m=application 4500 UDP ike-esp-udpencap
c=IN IP4 192.0.2.10
a=udp-setup:active
a=fingerprint:SHA-1 \
a=candidate:1 1 UDP 2130706431 192.0.2.10 4500 typ host
answer SDP
a=ice-pwd:asd88fgpdd777uzjYhagZg
a=ice-ufrag:8hhY
m=application 45664 UDP ike-esp-udpen cap
c=IN IP4 192.0.2.20
a=udp-setup:passive
a=fingerprint:SHA-1 \
a=candidate:1 1 UDP 2130706431 10.0.1.1 4500 typ host
a=candidate:2 1 UDP 1694498815 192.0.2.20 45664 typ srflx \
raddr 10.0.1.1 rport 4500
Conformed to ICE, they start STUN [I-D.ietf-behave-rfc3489bis]
connectivity check after SDP exchange. Then the offerer initiates
the IKE session making use of UDP session generated by STUN packets.
In addition, UDP encapsulated ESP packets are multiplexed into the
same UDP session as IKE. Thus it is necessary to multiplex the
different three packets, STUN, IKE, and UDP-encapsulated ESP into the
same UDP session.
5.3. Multiplex of UDP Messages
As described above, STUN, IKE, and UDP-encapsulated ESP packets are
multiplexed into the same UDP session. This section describes how to
demultiplex these three packets.
At the first step, the endpoint which received a UDP packet at the
multiplexed port MUST check the first 32 bits of UDP payload. If
they are all 0, which is defined as non-ESP marker, that packet MUST
be treated as an IKE packet.
Otherwise it is judged as an ESP packet in IPsec NAT-Traversal spec,
however it is furthermore necessary to distinguish STUN from ESP.
Therefore the bits 32-64 from the beginning of the UDP payload MUST
be checked. If it doesn't match the magic cookie of STUN
0x2112A442
(most packets don't match), it is treated as an ESP packet because it
is no longer a STUN packet.
However if it matches the magic cookie, an additional test is
necessary to determine it is STUN or ESP. The magic cookie field of
STUN overlaps the sequence number filed of ESP, so there still
remains a possibility that the sequence number of ESP coincides with
0x2112A442. In this additional test, the validity of the fingerprint
attribute of STUN message MUST be checked. If there is a valid
fingerprint in the message, it is judged as a STUN packet, otherwise
it is an ESP packet.
The above logic is expressed as follows.
if SPI-field-is-all-zeros
{ packet is IKE }
else
if bits-32-through-64 == stun-magic-cookie-value
and
bits-0-through-1 == 0 and
bits-2-through-15 == a STUN message type and
bits-16-through-32 == length of this UDP packet
fingerprint_found ==
parse_for_stun_fingerprint();
if fingerprint_found == 1
{ packet is STUN }
else
{ packet is ESP }


}
else
{ packet is ESP }
6. Application to IKE
After sharing fingerprints of both parties securely over the SDP
exchange, the IKE initiator MAY start the IKE session to the other
party. To follow this specification, digital signature MUST be
chosen as an authentication method in IKE phase 1. In this process,
certificate whose hashed value matches the fingerprint exchanged over
SDP MUST be used. If the certificate used in IKE does not match the
original fingerprint, the endpoint MUST terminate the IKE session
with detecting an authentication failure.
In addition, each party MUST present a certificate and be
authenticated by each other.
7. Specifications Assuming Prior Relationship between Two Nodes
This section describes the specification for the limited cases such
that certificates signed by trusted third parties or pre-shared keys
between endpoints can be used for authentication in IKE. Because
endpoints already have a prior relationship between them in this
case, they use SIP servers just for name resolution and
authorization. However, even in this case, the integrity of SDP
description MUST be assured.
7.1. Certificates Signed by Trusted Third Party
The protocol overview in this case is the same as in chapter 2. SDP
offer/answer procedure is also the same as in chapter 4 and 5. Both
endpoints have a prior relationship through the trusted third
parties, and SIP servers are used for name resolution and
authorization of session initiation. Even so, they MAY exchange
fingerprints in the SDP because one device can have several
certificates and it would be necessary to specify in advance which
certificate will be used for the following IKE authentication. By
this process, authorization in SIP and authentication in IKE become
consistent with each other. The following figure shows VPN remote
access from a device outside the home to the home router whose IP
address is not fixed (same as chapter 2).
| (1) | SIP   | (1) |
Net. | +---------+ IKE(Media Session) +---------+
<table>
<thead>
<tr>
<th>Remote</th>
<th>Router</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Figure 3: Remote Access to Home Network
1. Both Remote Client and Home Router generate secure signaling
channels. They may REGISTER to SIP Proxy using TLS.
2. Both Remote Client (SDP offerer) and Home Router (SDP answerer)
exchange the fingerprints of their certificates signed by trusted
third parties in SDP during an INVITE transaction.
3. After SDP exchange, Remote Client (SDP offerer) initiates IKE
with the SDP answerer to establish IPsec SA. Both the offerer
and the answerer validate that the signed certificate presented
in the IKE exchange has a fingerprint that matches the
fingerprint from SDP. If they match, IKE negotiation proceeds as
normal.
7.2. Configured Pre-Shared Key
If a pre-shared key for IKE authentication is installed in both
endpoints in advance, they need not exchange fingerprints of their
certificates. However they may still need to specify which pre-
shared key they will use in the following IKE authentication in SDP
because they may have several pre-shared keys. Therefore, a new
attribute "psk-fingerprint" is defined to exchange a fingerprint of
pre-shared key over SDP. It also has a role of making authorization
in SIP consistent with authentication in IKE. "psk-fingerprint" is
applied to pre-shared keys as "fingerprint" defined in RFC4572 is
applied to certificates. The following is the ABNF of the
"psk-
fingerprint" attribute. The use of "psk-fingerprint" is OPTIONAL.
attribute =/ psk-fingerprint-attribute
psk-fingerprint-attribute = "psk-fingerprint" ":" hash-func SP
psk-fingerprint
hash-func = "sha-1" / "sha-224" / "sha-256" /
"sha-384" / "sha-512" /
"md5" / "md2" / token
can only come ; Additional hash functions
; from updates to RFC 3279
psk-fingerprint = 2UHEX *(":" 2UHEX)
separated ; Each byte in upper-case hex,
; by colons.
UHEX uppercase = DIGIT / %x41-46 ; A-F
An example of SDP negotiation for IKE with pre-shared key
authentication without IPsec NAT-Traversal is as follows.
offer SDP
m=application 500 UDP ike-esp
c=IN IP4 192.0.2.10
a=psk-fingerprint:SHA-1 \
answer SDP
m=application 500 UDP ike-esp
c=IN IP4 192.0.2.20
a=udp-setup:passive
a=psk-fingerprint:SHA-1 \
8. Security Considerations
This entire document concerns itself with security, but the security
considerations applicable to SDP in general is described in SDP
specification. And the security issues which should be considered in
using comedia-tls are described in Section 7 in its specification.
This section describes the security considerations specific in the
negotiation of IKE using comedia-tls.
Offering IKE in SDP (or agreeing to one in SDP offer/answer mode)
does not create an obligation for an endpoint to accept any IKE
session with the given fingerprint. On the other hand, the endpoint
must engage in the standard IKE negotiation procedure to ensure that
the IPsec security associations (including encryption and
authentication algorithms) chosen meet the security requirements of
the higher-level application. When IKE has finished negotiating, the
decision to conclude IKE and establish an IPsec security association
with the remote peer is entirely the decision of each endpoint. This
procedure is similar to how VPNs are typically established in the
absence of SIP.
In the general authentication process in IKE, subject DN or
subjectAltName is recognized as the identity of the remote party.
However by using SIP identity and SIP connected identity mechanisms
in this spec, certificates are used just as a carrier for the public
keys of the peers and there is no need for the information about who
is the signer of the certificate and whom subject DN indicates.
In this document, the purpose of using IKE is launching the IPsec SA,
and it is not for the security mechanism of RTP and RTCP packets.
Actually, this mechanism cannot provide end-to-end security inside
the virtual private network as long as using tunnel mode IPsec,
therefore other security methods such as SRTP must be used to secure
them.
9. IANA Considerations
This document defines a session and media level SDP attribute, "udp-
setup". This attribute should be registered by the IANA under
"Session Description Protocol (SDP) Parameters" under "att-field"
(both session and media level)".
This document defines media formats "ike-esp" and "ike-esp-udpencap".
These media format values should be registered by the IANA. Media
formats "ike-esp" and "ike-esp-udpencap" are associated with a proto
value "UDP".
This document defines a session and media level SDP attribute, "psk-
fingerprint". This attribute should be registered by the IANA under
"Session Description Protocol (SDP) Parameters" under "att-field"
(both session and media level)".
10. References
10.1. Normative References
"Session Traversal Utilities for (NAT) (STUN)",
draft-ietf-behave-rfc3489bis-17 (work in progress),
July 2008.
[I-D.ietf-mmusic-ice]
Rosenberg, J., "Interactive Connectivity Establishment"
(ICE): A Protocol for Network Address Translator (NAT)
Traversal for Offer/Answer Protocols
[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston,
Schooler, "SIP: Session Initiation Protocol",
RFC 3261,
June 2002.
with Session Description Protocol (SDP)

RFC 3264,
June 2002.
[RFC3947] Kivinen, T., Swander, B., Huttunen, A., and V. Volpe,
"Negotiation of NAT-Traversal in the IKE", RFC 3947,
January 2005.
Stenberg, "UDP Encapsulation of IPsec ESP Packets"
[RFC4572] Lennox, J., "Connection-Oriented Media Transport over the
Transport Layer Security (TLS) Protocol in the Session
Description Protocol (SDP)\textsuperscript{,} \url{RFC 4572}, July 2006.
10.2. Informative References
[I-D.fischl-sipping-media-dtls]
Fischl, J., "Datagram Transport Layer Security (DTLS)"
Protocol for Protection of Media Traffic
Established with
the Session Initiation Protocol",
draft-fischl-sipping-media-dtls-03 (work in progress),
[RFC4145] Yon, D. and G. Camarillo, "TCP-Based Media Transport in
the Session Description Protocol (SDP), RFC 4145,
September 2005.
[RFC4474] Peterson, J. and C. Jennings, "Enhancements for
Authenticated Identity Management in the Session
Initiation Protocol (SIP)" , RFC 4474, August 2006.
[RFC4916] Elwell, J., "Connected Identity in the Session Initiation
Protocol (SIP)\textsuperscript{a}, \texttt{RFC 4916}, June 2007.
Appendix A. Changes since draft-saito-mmusic-sdp-ike-02
Instruction to RFC Editor: please remove this section prior to
publication as an RFC
- Added the case that certificates signed by trusted third parties
or pre-shared keys can be used for authentication in IKE. And
defined a new attribute "psk-fingerprint" in chapter 7.
o Added an example that an SDP offerer becomes an IKE responder to
chapter 4.
o Added a description to 5.1 that when using ICE, IKE initiator MUST
allow any destination ports in addition to 500 and 4500 for the
IKE packets which itself sends.
o Modified media format descriptions from "IKE/ESP" and "UDP/IKE/"
ESP" to "ike-esp" and "ike-esp-udpencap".
Minor grammatical edits.
Authors' Addresses
Makoto Saito
3-20-2 Nishi-Shinjuku, Shinjuku-ku
Tokyo 163-1421
Japan
Email: ma.saito@nttv6.jp
Dan Wing
Cisco Systems
170 West Tasman Drive
San Jose, CA  95134
United States
Email: dwing@cisco.com
Full Copyright Statement
This document is subject to the rights, licenses and restrictions
contained in BCP 78, and except as set forth therein, the authors
retain all their rights.
This document and the information contained herein are provided on an
"AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS
OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND
THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS
OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT
THE USE OF
THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED
WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
Intellectual Property
The IETF takes no position regarding the validity or scope of any
Intellectual Property Rights or other rights that might be claimed to
pertain to the implementation or use of the technology described in
this document or the extent to which any license under such rights
might or might not be available; nor does it represent that it has
made any independent effort to identify any such rights. Information
on the procedures with respect to rights in RFC documents can be
found in BCP 78 and BCP 79.
Copies of IPR disclosures made to the IETF Secretariat and any
assurances of licenses to be made available, or the result of an
attempt made to obtain a general license or permission for the use of
such proprietary rights by implementers or users of this
specification can be obtained from the IETF on-line IPR repository at
The IETF invites any interested party to bring to its attention any
copyrights, patents or patent applications, or other proprietary
rights that may cover technology that may be required to implement
this standard. Please address the information to the IETF at
ietf-ipr@ietf.org.