**3GPP TSG SA WG3 Security — S3#18** **S3-010223**

**21 - 24 May, 2001**

**Phoenix, USA**

---

Source: Alcatel

Subject: comments on draft-arkko-map-doi-01.txt (tagged with [OP])

> Network Working Group J. Arkko
> INTERNET-DRAFT R. Blom
> Category: Informational Ericsson
> <draft-arkko-map-doi-01.txt> 22 February 2001
>
> The MAP Security Domain of Interpretation for ISAKMP
>
> Status of this Memo
>
> This document is an Internet Draft and is in full conformance with
> all provisions of Section 10 of RFC2026 [Bra96]. Internet Drafts are
> working documents of the Internet Engineering Task Force (IETF), its
> areas, and 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 inapproporiate 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.
>
> 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 (Australia), ds.internic.net (US East Coast), or
> ftp.isi.edu (US West Coast).
>

>    The distribution of this memo is unlimited. It is filed as <draft-
>    arkko-map-doi-01.txt>, and expires August 15, 2001. Please send
>    comments to the authors.
>
> Contents
>

>
>
>

>
>
>
>
>

>
>

>
> 1. Abstract
>
> In the Global Mobile System (GSM) and Universal Mobile
> Telecommunication System (UMTS) networks, the MAP protocol
> plays a central role in the signaling communications between
>
>
>

>
>
>
>
>

>
>
> the Network Elements (NEs). The Internet Security Association and
> Key Management Protocol (ISAKMP) defines a framework for security
> association management and cryptographic key establishment for the
> Internet. This framework consists of defined exchanges, payloads,
> and processing guidelines that occur within a given Domain of
> Interpretation (DOI). This document defines the MAP Security DOI
> (MAPSEC DOI), which instantiates ISAKMP for use with MAP when MAP
> uses ISAKMP to negotiate security associations.
>
> 2. Terms and Definitions
>
> The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD,
> SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this
> document, are to be interpreted as described in [RFC 2119].
>
> 3. Introduction
>
> 3.1. MAP
>
> In the Global Mobile System (GSM) and Universal Mobile
> Telecommunication System (UMTS) networks, the MAP protocol
> plays a central role in the signaling communications between
> the Network Elements (NEs). User profiles, authentication, and
> mobility management are performed using MAP. MAP is an SS7 protocol
> and runs over the TCAP, SCCP, and MTP protocol layers, typically
> using dedicated PCM links.
>
> The mobile networks are moving towards IP-based solutions, and
> completely IP based networks and new protocols such as SIP
> will in few years time replace MAP. However, MAP and SS7
> signaling networks have to be supported during the transition
> time, and beyond, due to the need to retain legacy equipment

>    in networks.
>
> 3.2. Requirements for a DOI
>
>    Within ISAKMP, a Domain of Interpretation is used to group related
>    protocols using ISAKMP to negotiate security associations.  Security
>    protocols sharing a DOI choose security protocol and cryptographic
>    transforms from a common namespace and share key exchange protocol
>    identifiers.  They also share a common interpretation of DOI-specific
>    payload data content, including the Security Association and
>    Identification payloads.
>
>    Overall, ISAKMP places the following requirements on a DOI
>    definition:
>
>      o  define the naming scheme for DOI-specific protocol identifiers
>
>
>

>
>
>
>
>

>
>
>      o  define the interpretation for the Situation field
>      o  define the set of applicable security policies
>      o  define the syntax for DOI-specific SA Attributes (Phase II)
>      o  define the syntax for DOI-specific payload contents
>      o  define additional Key Exchange types, if needed
>      o  define additional Notification Message types, if needed
>
>    For instance, the IP Security DOI [IPDOI] describes the use of
>    ISAKMP in the context of IP Security AH and ESP and the IP
>    Compression protocols. The IP Security DOI also includes the
>    details for how phase 1 authentication and protection of ISAKMP
>    itself is performed between two IP nodes.

>
> 3.3. MAP Security
>
> Due to the role of MAP in the authentication process
> of GSM phones, operators are concerned about its lack of
> cryptographic security support. For this reason a new protocol
> header has been developed to protect MAP messages, much
> in the same way as IPsec ESP protects IP packets. Also
> similarly, a key management mechanism is needed for MAP.
> The intention of the standardization entities working on
> MAP is to reuse an existing key management mechanism,
> namely ISAKMP, and parts of IKE and the IPsec DOI.
> The reasons for wishing to reuse ISAKMP include the
> following:
>
> o Avoiding the security and complexity pitfalls involved
> in new protocol design
>
> o Benefits of using the same protocol that IP-based
> (especially IPv6) nodes already use for other purposes.
>
> The use of IKE and IPsec DOI for MAP Security is possible since the
> networks employing MAP Security will always have also
> network-to-network IP connectivity even if MAP and SS7
> are still used for the signaling.
>
> The remainder of this document details the instantiation of these
> requirements for using the GSM MAP protocol and its security to
> provide authentication, integrity, and/or confidentiality for MAP
> messages sent between cooperating Network Elements.
>
> For a description of the GSM and MAP architecture, see [???] and
> [???].
>
> 3.4. Network Architecture
>
>
>
>

>
>
>
>
>

>
>
> The MAP Security protocol may provide confidentiality, integrity, and
> replay protection services to the MAP messages it transports.

[OP] authentication is also provided.

> The purpose of the MAP Security header in the protocol is to
> provide enough information to determine the MAP SA and Protection
> Modes used in securing the MAP operation that follows the
> header.
>
> Typically, two NEs belong to two different operator networks.
> The arrangement is shown in Figure 1.
>
>
>
>

```
>  (Operator 1 Network)                    (Operator  2  Network)
>
>
>        _-----------MAP DOI over ISAKMP over IP----------_
>       /                                                 \
>       |                                                 |
>    +------+                                          +------+
>    |      |                                          |      |
>    |      |                                          |      |
>    | NE_1 |------MAP over MAP Security over SS7------>| NE_2 |
>    |      |                                          |      |
>    |      |                                          |      |
>    +------+                                          +------+
>
>
>
```

```
>       Figure 1. Simple network architecture for MAP Security
>
>
>
>
>  (Operator 1 Network)                    (Operator 2 Network)
>
>
>
>        _----------IPSEC DOI over ISAKMP over IP----------_
>       /                                                   \
>       |  _---------MAP DOI over ISAKMP over IP---------_   |
>       | /                                               \  |
>       | |                                               | |
>     +------+                                          +------+
>     |      |                                          |      |
>     |      |------MAP over MAP Security over SS7------>|      |
>     | NE_1 |                                          | NE_2 |
>     |      |------Protocol X over IPsec over IP------->|      |
>
>
>
```



```
>
>
>
>
>
```



```
>
>
>     |      |                                          |      |
>     +------+                                          +------+
>
>
>
>       Figure 2. Use of IKE for two purposes.
>
>
>    One benefit of using IKE can be seen in Figure 2. As the network
```

> elements use both MAP and another, IP-based protocol X they
> can use ISAKMP/IKE to negotiate keys for both. In this case,
> IKE phase 1 needs to be run just once.
>
> In an alternative network arrangement, the Network Elements
> do not have key management support or direct IP connections
> to other networks. In this case a Key Administration Center
> (KAC) handles the negotiations on the behalf of the NEs. This
> is shown in Figure 2.
>
>

```
>  (Operator 1 Network)                    (Operator 2 Network)
>
>
>    +------+                                +------+
>    |      |                                |      |
>    | KAC_1|--------MAP DOI over ISAKMP over IP--------|KAC_2 |
>    |      |                                |      |
>    +------+                                +------+
>       |                                       |
>       |                                       |
>       |                                       |
>    +------+                                +------+
>    |      |                                |      |
>    |      |                                |      |
>    | NE_1 |------MAP over MAP Security over SS7------>| NE_2 |
>    |      |                                |      |
>    |      |                                |      |
>    +------+                                +------+
>
>
>
>       Figure 3. Complex network architecture for MAP Security
>
```

[OP] It is understood that only scenario 3 is applicable for release 4. The first two scenarios should therefore be removed.

>
>

> In this arrangement, the security of the communications
> between the NEs and the KAC is of great importance. Security
> mechanisms or transport protocols for that purpose are, however,
>
>
>
> Arkko & Blom Informational [Page 6]
>
>
>
>
>
> INTERNET-DRAFT MAPSEC DOI 22 February 2001
>
>
> not discussed in this document though as an example, IPsec/IKE,
> IPsec/KINK, MPLS VPNs [MPLS], or ATM Permanent Virtual Connections
> could be used.

[OP] MPLS and ATM-based VPNs certainly do not provide the same level of
security as IPsec-based VPNs, for the simple reason that the formers are
not crypto-based. We would therefore either suppress the whole list of
examples or just keep the IPsec-based ones.

>
> Only one SA (pair) needs to exist between two networks in
> this arrangement, even if there is a large number of NEs
> communicating to the NEs of the other network. (Note
> that MAP Security employs time stamps instead of sequence
> numbers, making the simultaneous use of the same SA in
> multiple NEs possible.)
>
> 3.5. Reuse of IPSEC DOI and IKE
>
> The MAP DOI for ISAKMP is always used in devices that have
> IP connectivity to the peer device. There are no additional
> requirements set forth by the MAP Security or MAP protocols
> regarding the identification and authentication of the communicating
> peers. Therefore, all IPSEC DOI definitions and IKE procedures
> regarding phase 1 of IKE are used unchanged in the MAPSEC DOI.

>
> Furthermore, the IKE procedures regarding phase 2 are used
> unchanged, with the following exceptions:
>
> o Identity types used in phase 2 are different.
>
> o SA payloads are different.
>
> o There are no MAPSEC-specific phase 2 notifications.
>
> o The procedure for creating keys for MAP Security
> is different than that for IPsec.
>
> Systems implementing the MAP Security DOI MUST support
> this DOI using ISAKMP/IKE. However, MAP Security DOI
> does not require the implementations to support full
> ISAKMP/IKE. Specific MAP Security ISAKMP/IKE profile
> is given below.
>
> The requirements set forth in the IKE [ISAKMP,
> IKE] and IPsec DOI [IPSDOI] MUST be followed with the
> exception of the following:

[OP] it is quite disturbing to refer to IPsec DOI requirements from MAPsec DOI. MAPsec DOI is supposed to be independent from IPsec DOI and something different. So, any applicable requirements should appear in this document (or the 3gpp spec if that type of material is eventually moved to the 3gpp spec and referred from this one).

>
> o Perfect Forward Secrecy (PFS) SHOULD be
> supported in Phase 2.

[OP] this is not clear. The above sentence means that implementors are "advised" to implement PFS (which does not mean it must be used). SA3 decided to make it optional but it does not help with clarity. It must be explicitly stated whether we mean optional to implement or/and optional to use. Also, we should specify what to do if entity A receives phase 2 IKE messages with PFS (ie KE payload present) from entity B. Should we assume that both operators have a pre-agreement on that ?

In our view, PFS should be left optional to implement (hence to use) at
this stage. This is because it is a single phase 2 SA which
is set up between two given operators. When renegotiating a new SA from
time to time, it is not believed to be a hard job to renegotiate both
phase 1 and phase 2 SA's. This is indirectly achieving PFS.

>     o  In contrast to the requirements set in [IKE],
>        Aggressive Mode MUST be implemented and Main
>        Mode SHOULD be implemented.

[OP] SA3 reverted this suggestion and we agree with mandating main mode
as in IKE.

>     o  Only one identity type, ID_FQDN, MUST be
>
>
>
> Arkko & Blom                    Informational          [Page 7]
>
>
>
>
>
> INTERNET-DRAFT               MAPSEC DOI              22 February 2001
>
>
>        implemented for phase 1. Other identity types
>        specified in [IPSDOI] SHOULD be implemented.
>     o  Only the 3DES encryption algorithm SHA1 algorithms
>        MUST be implemented as ISAKMP encryption and hash
>        operations.

[OP] SA3 decided on AES in CBC for encryption and SHA-1 as the basic
hashing function, which we agree with.

>     o  SA lifetime notifications will not be allowed
>        [see section 4.5.3].

[OP] our understanding from IPsec DOI is that it is mandatory to implement but optional to use for IPsec DOI. If MAPsec DOI does not need it (and it does not), why mentioning it ? Again this is coming from the fact that MAPsec DOI refers to IPsec DOI, which it should not.

> o SA deletetion will not be allowed (this is
> required in order to ensure that pull-based
> schemes can be used between network elements
> and the KAC when the architecture in Figure 3
> is used.)

[OP] We think that SA deletion should be possible between KAC's (ie between operators). At this stage, it is premature to argue on pull-based vs pushed-based vs mixtures intradomain key distributing schemes. And SA deletion is useful after key compromise or key lost.

>
> Note that IKE [IKE] specifies that all implementations
> MUST support authentication through pre-shared secrets
> and SHOULD support public key based authentication.

[OP] We do not see the purpose of this sentence apart from reminding the reader. Since MAPsec would be used in a "close" environment, psk-based authentication is to be made mandatory for support at least.

>
> 3.6. Reuse of KKMP
>
> The KINK protocol [KINK] uses centralized authenticatin
> from Kerberos to bypass IKE phase 1 and offer a faster
> alternative to IKE phase 2. KINK uses directly ISAKMP
> and IPSEC DOI payload formats, and therefore anything
> negotiable normally
>
> Systems implementing the MAP Security DOI SHOULD support
> this DOI using KINK.

[OP] Given the immaturity of KINK at this stage, this should be removed (as agreed at SA3 already anyway). Moreover, we do no see any benefit in using Kerberos-based key distribution in a context where you set up the SA between two KACs. KINK would require the use of a central server trusted by both KACs.

>
> 4. Definition
>
> 4.1 Naming Scheme
>
> Within ISAKMP, all DOI’s MUST be registered with the IANA in the
> "Assigned Numbers" RFC [STD-2]. The IANA Assigned Number for the
> MAP Security DOI (MAPSEC DOI) is TBD (N). Within the MAP Security
> DOI, all well-known identifiers MUST be registered with the IANA
> under the MAPSEC DOI. Unless otherwise noted, all tables within this
> document refer to IANA Assigned Numbers for the MAPSEC DOI. See
> Section 6 for further information relating to the IANA registry for
> the MAPSEC DOI.
>
> All multi-octet binary values are stored in network byte order.
>
> 4.2 MAPSEC Situation Definition
>
> Within ISAKMP, the Situation provides information that can be used by
> the responder to make a policy determination about how to process the
> incoming Security Association request. For the MAPSEC DOI, the
>
>
>

>
>
>
>
>

>
>
> Situation field is a four (4) octet bitmask with the following
> value.
>
> Situation Value
> --------- -----

>      SIT_IDENTITY_ONLY          0x01
>
> 4.2.1 SIT_IDENTITY_ONLY
>
>    The SIT_IDENTITY_ONLY type specifies that the security association
>    will be identified by source identity information present in an
>    associated Identification Payload.  See Section 4.6.2 for a complete
>    description of the various Identification types.  All MAPSEC DOI
>    implementations MUST support SIT_IDENTITY_ONLY by including an
>    Identification Payload in at least one of the Phase I Oakley
>    exchanges ([IKE], Section 5) and MUST abort any association setup
>    that does not include an Identification Payload.
>
> 4.3 MAPSEC Security Policy Requirements
>
>    The MAPSEC DOI does not impose specific security policy requirements
>    on any implementation.  Host system policy issues are outside of the
>    scope of this document.
>
>    However, the following sections touch on some of the issues that must
>    be considered when designing a MAPSEC DOI host implementation.  This
>    section should be considered only informational in nature.
>
> 4.3.1 Protection Profiles
>
>    In order to make it possible to establish as small number of
>    SAs as possible in large meshed operator network, and to
>    limit the protection to the most critical MAP messages, the
>    concept of MAP protection profiles has been introduced.
>    For instance, one profile could mandates the use of MAP Security
>    for all MAP messages, while another could require the use of MAP
>    Security only for all messages containing mobile terminal
>    authentication vectors, and no security for other messages.
>
>    These actual profiles are numbered and standardized by the 3GPP
>    [NDSEC] and are not listed here.
>
>    During the IKE phase 2 negotiations between two nodes or networks,
>    they agree on a common protection profile and create a single SA
>    (pair) between themselves. The SA is then either used or not used

>    for individual MAP messages, based on the standardized rules
>    in the particular selected profile.

[OP] the exact mechanism of protection profiles is not fully specified yet so it may be difficult to fully understand what the above implies but let us try. Both KACs will set up a single SA which will be used for the one (or several ?) protection profiles associated to that negotiated SA. Could we have different PPs for the two directions ? Could we combine several basic PPs to be associated to the same SA ?

>
>
>
>
> Arkko & Blom                    Informational           [Page 9]
>
>
>
>
>
> INTERNET-DRAFT                 MAPSEC DOI              22 February 2001
>
>
>    Note that this is in contrast to the mechanisms used in the IPSEC
>    DOI, where several SA (pairs) may be negotiated, one for each
>    different class of traffic.
>
>    The protection profile mechanism is also used to provide a way
>    for two nodes to agree that they will not use security at all.
>    A protection profile that doesn't use MAPSEC for any MAP message
>    is defined in [NDSEC].
>
> 4.3.2 Key Management Issues
>
>    It is expected that many systems choosing to implement ISAKMP will
>    strive to provide a protected domain of execution for a combined IKE
>    key management daemon.  On protected-mode multiuser operating
>    systems, this key management daemon will likely exist as a separate
>    privileged process.
>

>    In such an environment, a formalized API to introduce keying material
>    into the TCP/IP kernel may be desirable.  The IP Security
>    architecture does not place any requirements for structure or flow
>    between a host TCP/IP kernel and its key management provider.

[OP] The above sentence does not seem applicable in the MAPsec context since we are not in an IPsec context where the IKE application daemon is "co-located" with the IPsec kernel module. In the envisaged scenario, the keying material must be distributed to other network nodes (out of scope as written above).

>
> 4.3.3 Static Keying Issues
>
>    Static keying is not supported in MAP Security.

[OP] This is clearly not true if we use psk for phase 1 authentication.

>
> 4.3.4 Host Policy Issues
>
>    It is not realistic to assume that the  transition  to  MAP  Security
>    will occur overnight.  Host systems must be prepared to implement
>    flexible policy lists that describe which systems they desire to
>    speak securely with and which systems they require  to  speak
>    securely  to them. Some notion of proxy firewall addresses may also
>    be required.
>
>    A minimal approach is probably a static list of Public Land Mobile
>    Network  Identities  (PLMN  IDs).  A  PLMN  ID  is   constructed  by
>    concatenating  the  Mobile Country Code (MCC) and  by  the  Mobile
>    Network Code (MNC).
>
> 4.3.5 Certificate Management
>
>    Host systems implementing a certificate-based authentication scheme
>    will need a mechanism for obtaining and managing a database of
>    certificates.
>
>    Secure DNS is to be one certificate distribution mechanism, however

>    the pervasive availability of secure DNS zones, in the short term, is
>
>
>

>
>
>
>
>

>
>
>    doubtful for many reasons.  What's far more likely is that hosts will
>    need an ability to import certificates that they acquire through
>    secure, out-of-band mechanisms, as well as an ability to export their
>    own certificates for use by other systems.

[OP] The above statement, taken from "good old" IPsec DOI, probably needs reconsideration. Secure DNS (in terms of being able to store certificates - not securing DNS transactions themselves) can easily be deployed in a "close" environment as an operator's backbone, for use between operators. Other technologies can also be used such as LDAP or other (future ?) solutions for CRL handling specified by PKIX.

>
>    However, manual certificate management should not be done so as to
>    preclude the ability to introduce dynamic certificate discovery
>    mechanisms and/or protocols as they become available.

[OP] As stated above, such mechanisms exist and can be deployed without all the burden that would be required on a global Internet scale.

>
> 4.4 MAPSEC Assigned Numbers
>
>    The following sections list the Assigned Numbers for the MAPSEC DOI:
>    Protocol  Identifiers,   MAPSEC   Transform   Identifiers,   Security
>    Association  Attribute Type Values, ID Payload Type  Values,  and
>    Notify  Message Type  Values.

>
> 4.4.1 MAPSEC DOI Number
>
> This number is TBD.
>
> 4.4.1 MAPSEC Security Protocol Identifier
>
> The ISAKMP proposal syntax was specifically designed to allow for the
> simultaneous negotiation of multiple Phase II security protocol
> suites within a single negotiation. As a result, the protocol suites
> listed below form the set of protocols that can be negotiated at the
> same time. It is a host policy decision as to what protocol suites
> might be negotiated together.
>
> The following table lists the values for the Security Protocol
> Identifiers referenced in an ISAKMP Proposal Payload for the MAPSEC
> DOI.
>
> Protocol ID Value
> ----------- -----
> RESERVED 0
> PROTO_ISAKMP 1
> PROTO_MAPSEC_MAPSEC TBD

[OP] Interestingly enough, the described mechanism only enables to set up encrypted SAs. Iow one cannot set up an SA which only provides integrity/authentication since the only transform defined is AES for encryption (and authentication is an attribute of that transform). Is this a restriction we really want ?

>
> 4.4.1.1 PROTO_ISAKMP
>
> The PROTO_ISAKMP type specifies message protection required during
> Phase I of the ISAKMP protocol. The specific protection mechanism
> used for the MAPSEC DOI is described in [IKE]. All implementations
> within the MAPSEC DOI MUST support PROTO_ISAKMP.
>
> NB: ISAKMP reserves the value one (1) across all DOI definitions.
>

>
>
>

>
>
>
>
>

>
>
> This is exactly as it is in the IPSEC DOI.
>
> 4.4.1.2 PROTO_MAPSEC_MAPSEC
>
> The PROTO_MAPSEC_MAPSEC type specifies the use of the MAP
> Security to protect MAP messages.
>
>
> 4.4.2 MAPSEC ISAKMP Transform Identifiers
>
> As part of an ISAKMP Phase I negotiation, the initiator's choice of
> Key Exchange offerings is made using some host system policy
> description. The actual selection of Key Exchange mechanism is made
> using the standard ISAKMP Proposal Payload. The following table
> lists the defined ISAKMP Phase I Transform Identifiers for the
> Proposal Payload for the MAPSEC DOI.
>
> Transform Value
> --------- -----
> RESERVED 0
> KEY_IKE 1
>
> Implementor's note: This is exactly as it is in the IPSEC DOI.
>
> 4.4.2.1 KEY_IKE
>
> The KEY_IKE type specifies the hybrid ISAKMP/Oakley Diffie-Hellman
> key exchange (IKE) as defined in the [IKE] document. All

> implementations within the MAPSEC DOI MUST support KEY_IKE.
>
> 4.4.3 MAPSEC Transform Identifiers
>
> The following table lists the defined MAPSEC AES Transform
> Identifiers.
>
> Transform ID Value
> ------------ -----
> RESERVED 0-1
> MAPSEC_AES TBD
>
> 4.4.3.1 MAPSEC_AES
>
> The MAPSEC_AES type specifies a generic MAP Security transform using
> AES. The actual protection suite is determined in concert with
> an associated SA attribute list.

[OP] In particular, we believe that the key length attribute could be used to specify the chosen key length, rather than defining separate transforms for AES. The transform identifier should still specify the mode (ie CBC in our case).

>
> All implementations within the MAPSEC DOI MUST support this
> transform. The MAPSEC_AES transform is defined in [NDSEC].
>
>
>

>
>
>
>
>

>
>
> 4.5 MAPSEC Security Association Attributes
>

> The following SA attribute definitions are used in Phase II of an IKE
> negotiation. Attribute types can be either Basic (B) or Variable-
> Length (V). Encoding of these attributes is defined in the base
> ISAKMP specification.
>
> Attributes described as basic MUST NOT be encoded as variable.
> Variable length attributes MAY be encoded as basic attributes if
> their value can fit into two octets. See [IKE] for further
> information on attribute encoding in the MAPSEC DOI. All
> restrictions listed in [IKE] also apply to the MAPSEC DOI.
>
> Implementor's note: In general, the attributes describe here
> behave exactly as the corresponding ones in the IPSEC DOI.
> The attributes Encapsulation Mode, Compression Dictionary Size,
> and Compression Private Algorithm are not supported by MAPSEC DOI.

[OP] Only the attributes required for MAPsec should be mentioned: SA Life Type and Duration, Group Description, Authentication Algorithm, Key Length (if we use this to announce AES key length)and MAP PP. All others are irrelevant.

This also brings an issue on numbering of those attribute types. Current text keeps numbering aligned with the one defined in IPsec DOI. However, we can see IPsec DOI and MAPsec DOI as completely separate, including wrt naming spaces. Hence, we should not bother on keeping IPsec DOI numbers as reserved (we should start from scratch). On the other hand, we understand that to ease code re-use it is better to keep those numbers the same.

Also, it is noteed that the SA Life Type attribute is not really needed since the type is always "seconds".

```
>
>     Attribute Types
>
>          class          value        type
>     -------------------------------------------------
>     SA Life Type           1           B
>     SA Life Duration       2           V
>     Group Description      3           B
```

> Encapsulation Mode 4 B
> Authentication Algorithm 5 B
> Key Length 6 B
> Key Rounds 7 B
> Compress Dictionary Size 8 B
> Compress Private Algorithm 9 V
> MAP Protection Profile TBD B
>
> Class Values
>
> SA Life Type
> SA Duration
>
> Specifies the time-to-live for the overall security
> association. When the SA expires, all keys negotiated under
> the association (AH or ESP) must be renegotiated. The life
> type values are:
>
> RESERVED 0
> seconds 1
>
> Values 3-61439 are reserved to IANA. Values 61440-65535 are
> for private use. For a given Life Type, the value of the
>
>
>

>
>
>
>
>

>
>
> Life Duration attribute defines the actual length of the
> component lifetime -- in number of seconds.
>
> If unspecified, the default value shall be assumed to be
> 28800 seconds (8 hours).

>
> An SA Life Duration attribute MUST always follow an SA Life
> Type which describes the units of duration.
>
> See Section 4.5.3 for additional information relating to
> lifetime notification.
>
> Implementor's note: The semantics and values for these
> attributes are exactly as they are in the IPSEC DOI, except
> that kilobyte lifetimes are not supported.
>
> Group Description
>
> Specifies the Oakley Group to be used in a PFS QM
> negotiation.  For a list of supported values, see Appendix A
> of [IKE].
>
> Implementor's note: The semantics and values for these
> attributes are exactly as they are in the IPSEC DOI.
>
> Authentication Algorithm
>
> RESERVED 0
> HMAC-MD5 1
> HMAC-SHA 2
> DES-MAC 3
> KPDK 4
> AES-MAC 5

[OP] Only HMAC-SHA and AES-MAC should be identified as these are the only ones envisaged for short and longer term. Also, a special value should be predefined for "no auth algorithm" in case we do not want an auth algorithm to be negotiated (for example when both partners really do not want authentication or when AES encryption will be used in a mode that also provides integrity/authentication). Unless absence means no auth algorithm ?

>
> Values 5-61439 are reserved to IANA.  Values 61440-65535 are
> for private use.

>
> There is no default value for Auth Algorithm, as it must be
> specified to correctly identify the applicable transform.
>
> Implementor's note: The semantics of the first five
> values for this attribute is exactly as they are in the IPSEC
> DOI.
> This specification requires additionally that only AES-MAC
> and the omission of the algorithm are mandatory for all MAP
> Security implementations. The semantics of the AES-MAC are
> defined in [NDSEC].
>
>
>
>

>
>
>
>
>

>
>
> Key Length
>
> RESERVED 0
>
> There is no default value for Key Length, as it must be
> specified for transforms using ciphers with variable key
> lengths. For fixed length ciphers, the Key Length attribute
> MUST NOT be sent.
>
> Implementor's note: The semantics and values for this
> attributes is exactly as it is in the IPSEC DOI.
>
> Key Rounds
>
> RESERVED 0
>

>     There is no default value for Key Rounds, as it must be
>     specified for transforms using ciphers with varying numbers
>     of rounds.
>
>     Implementor's note: The semantics and values for this
>     attributes is exactly as it is in the IPSEC DOI.
>
>    MAP Protection Profile
>
>     The value of this attribute is as defined in [NDSEC].
>
> 4.5.1 Required Attribute Support
>
>  To ensure basic interoperability, all implementations MUST be
>  prepared to negotiate all of the following attributes.
>
>     SA Life Type
>     SA Duration
>     Auth Algorithm
>     MAP Protection Profile
>
> 4.5.2 Attribute Negotiation
>
>  If an implementation receives a defined MAPSEC DOI attribute (or
>  attribute value) which it does not support, an ATTRIBUTES-NOT-
>  SUPPORTED SHOULD be sent and the security association setup MUST be
>  aborted, unless the attribute value is in the reserved range.
>
>  If an implementation receives an attribute value in the reserved
>  range, an implementation MAY chose to continue based on local policy.
>
>  Implementor's note: This is exactly as it is in the IPSEC DOI.
>
>
>

>
>
>
>

>

>
>
> However, there are no special lifetime attribute parsing
> requirements as only time-based lifetimes are supported.
>
> 4.5.3 Lifetime Matching
>
> Offered and locally acceptable SA lifetimes must match
> exactly under MAPSEC in order for the responder to select
> an SA.
>
> Implementor's note: This is simplified from the IPSEC DOI
> which required notifications.
>
> 4.6 MAP Security Payload Content
>
> The following sections describe those ISAKMP payloads whose data
> representations are dependent on the applicable DOI.
>
> 4.6.1 Identification Payload Content
>
> The Identification Payload is used to identify the initiator of the
> Security Association. The identity of the initiator SHOULD be used
> by the responder to determine the correct host system security policy
> requirement for the association.
>
> During Phase I negotiations, the ID port and protocol fields MUST be
> set to zero or to UDP port 500. If an implementation receives any
> other values, this MUST be treated as an error and the security
> association setup MUST be aborted. This event SHOULD be auditable.

[OP] In phase 2, the protocol ID and port fields should be '0' since
this has no meaning for MAP messages.

>
> The following diagram illustrates the content of the Identification
> Payload.
>

```
>     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
>    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
>    !  Next Payload !   RESERVED    !        Payload Length         !
>    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
>    !   ID Type     !  Protocol ID  !             Port              !
>    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
>    ~                     Identification Data                       ~
>    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
>
>                   Figure 2: Identification Payload Format
>
>    The Identification Payload fields are defined as follows:
>
>      o  Next Payload (1 octet) - Identifier for the payload type of
>         the next payload in the message.  If the current payload is the
>         last in the message, this field will be zero (0).
>
>
>
```



```
>
>
>
>
>
```



```
>
>
>      o  RESERVED (1 octet) - Unused, must be zero (0).
>
>      o  Payload Length (2 octets) - Length, in octets, of the
>         identification data, including the generic header.
>
>      o  Identification Type (1 octet) - Value describing the identity
>         information found in the Identification Data field.
>
>      o  Protocol ID (1 octet) - Value specifying an associated IP
>         protocol ID (e.g. UDP/TCP).  A value of zero means that the
>         Protocol ID field should be ignored.
>
```

>     o  Port (2 octets) - Value specifying an associated port.  A value
>        of zero means that the Port field should be ignored.
>
>     o  Identification Data (variable length) - Value, as indicated by
>        the Identification Type.
>
>   The legal Identification Type field values in phase 1 are as
>   defined in the IPSEC DOI. However, phase 2 identities should MUST
>   conform to the following. The table lists the assigned values
>   for the Identification Type field found in the Identification
>   Payload.
>
>      ID Type                 Value
>      -------                 -----
>      RESERVED                  0
>      ID_KEY_ID                 11
>
>   For types where the ID entity is variable length, the size of the ID
>   entity is computed from size in the ID payload header.
>
>   The ID_KEY_ID type specifies an opaque byte stream. In MAPSEC DOI,
>   the contents of the data MUST be the the PLMN ID of the initiating
>   or responding party.
>
> 4.6.2 IPSEC Notify Message Types
>
>   The IPSEC DOI Notify Message types are used in phase 1. In phase
>   2, no new notify messages are specified beyond those provided
>   by ISAKMP. Implementor's note: MAPSEC does not allow turning
>   replay protection on or off which make the use of REPLAY-STATUS
>   unnecessary. Responder lifetimes are required to be exactly the
>   same as the initiator lifetimes, which makes the use of RESPONDER-
>   LIFETIME unnecessary.

[OP] Again, we find it confusing to rely for some parts on IPsec DOI. MAPsec DOI should clearly define its own notification types it needs. It does not need REPLAY-STATUS nor RESPONDER-LIFETIME so do not even mention these. But what about INITIAL-CONTACT ? Do we really need it ? If so, we should explicitly specify it in here, even if that the same as the one used in IPsec DOI.

>
>
> 4.7 MAPSEC Key Exchange Requirements
>
>
>

>
>
>
>
>

>
>
> The MAPSEC DOI introduces no additional Key Exchange types.
>
> 5. Security Considerations
>
> This entire memo pertains to the Internet Key Exchange protocol
> ([IKE]), which combines ISAKMP ([ISAKMP]) and Oakley ([OAKLEY]) to
> provide for the derivation of cryptographic keying material in a
> secure and authenticated manner. Specific discussion of the various
> security protocols and transforms identified in this document can be
> found in the associated base documents and in the cipher references.
>
> 6. IANA Considerations
>
> This document contains many "magic" numbers to be maintained by the
> the standardization bodies. In the case of the MAPSEC DOI, the
> 3GPP handles the assignment of numbers instead of IANA. This
> section explains the criteria to be used by the 3GPP to
> assign additional numbers in each of these lists. All values not
> explicitly defined in previous sections are reserved to 3GPP.
> (IANA will still define the DOI numbers, including the DOI
> number for this DOI.)
>
> 6.1 MAPSEC Situation Definition
>

> The Situation Definition is a 32-bit bitmask which represents the
> environment under which the IPSEC SA proposal and negotiation is
> carried out.  Requests for assignments of new situations must be
> accompanied by a 3GPP contribution which describes the interpretation
> for the associated bit.
>
> The upper two bits are reserved for private use amongst cooperating
> systems.
>
> 6.2 MAPSEC Security Protocol Identifiers
>
> The Security Protocol Identifier is an 8-bit value which identifies a
> security protocol suite being negotiated.  Requests for assignments
> of new security protocol identifiers must be accompanied by a 3GPP
> contribution which describes the requested security protocol.
>
> The values 249-255 are reserved for private use amongst cooperating
> systems.
>
> 6.3 MAPSEC ISAKMP Transform Identifiers
>
> The ISAKMP Transform Identifier is an 8-bit value which
> identifies a key exchange protocol to be used for the negotiation.
> Requests for assignments of new ISAKMP transform identifiers must be
>
>
>

>
>
>
>
>

>
>
> accompanied by a 3GPP contribution which describes the requested key
> exchange protocol.
>
> The values 249-255 are reserved for private use amongst cooperating

> systems.
>
> 6.4 MAPSEC MAP Security Transform Identifiers
>
> The MAP Security Transform Identifier is an 8-bit value which
> identifies a particular algorithm to be used to provide security
> protection for MAP messages. Requests for assignments of new
> transform
> identifiers must be accompanied by a 3GPP contribution which
> describes
> how to use the algorithm within the framework.
>
> The values 249-255 are reserved for private use amongst cooperating
> systems.
>
> 6.5 MAPSEC Security Association Attributes
>
> The MAPSEC Security Association Attribute consists of a 16-bit type
> and its associated value. MAPSEC SA attributes are used to pass
> miscellaneous values between ISAKMP peers. Requests for assignments
> of new MAPSEC SA attributes must be accompanied by an Internet Draft
> which describes the attribute encoding (Basic/Variable-Length) and
> its legal values. Section 4.5 of this document provides an example
> of such a description.
>
> The values 32001-32767 are reserved for private use amongst
> cooperating systems.
>
> 6.6 MAPSEC Identification Type
>
> The MAPSEC Identification Type is an 8-bit value which is used as a
> discriminant for interpretation of the variable-length Identification
> Payload. Requests for assignments of new Identification Types
> must be accompanied by a 3GPP contribution which describes how to use
> the identification type.
>
> The values 249-255 are reserved for private use amongst cooperating
> systems.
>
> 6.7 MAPSEC Notify Message Types

>
> The MAPSEC Notify Message Type is a 16-bit value taken from the range
> of values reserved by ISAKMP for each DOI. There is one range for
> error messages (8192-16383) and a different range for status messages
>
>
>

>
>
>
>
>

>
>
> (24576-32767). Requests for assignments of new Notify Message Types
> must be accompanied by a 3GPP contribution which describes how to use
> the identification type.
>
> The values 16001-16383 and the values 32001-32767 are reserved for
> private use amongst cooperating systems.
>
> 6.8 MAPSEC Protection Profiles
>
> The MAPSEC Protection Profile values are 8-bit values used
> in decisions regarding actual protection of individual MAP
> messages. The values are defined [NDSEC] and new values must
> be accompanied by a 3GPP contribution which describes the
> semantics of the profile.
>
> The values 64-255 are reserved for private use amongst cooperating
> systems.
>
> 7. Key Derivation for MAP Security
>
> 7.1 IKE
>
> MAP Security requires two sets of keys, one for each direction,
> just as in the case of IPSEC SAs. Both need authentication and

> encryption keys. For one direction of an SA, these two keys are
> taken from the key material as follows (see also Figure 4.)
>
> o The authentication key is taken first and then
> the encryption key.
>
>
>
>

```
>             +---------------+---------------+
>             |Message auth   |Message encr   |
>             +---------------+---------------+
```

>
>
>
> Figure 4. Use of derived key material for MAPSEC
>
>
>
> Furthermore, it is possible that the Key Administration
> Centers (KACs) are used. Then just one key is negotiated on behalf
> of the whole set of NEs. Note that MAP Security uses timestamps
> instead of sequence numbers in order to prevent replay attacks,
> so the same SAs can be used by multiple senders.

[OP] This is somewhat an overstatement. It depends at which granularity level the timestamp is created and yet it is theoretically possible that two different NEs generate the same timestamp value.

>
>
>

>
>
>
>
>

>

>

[OP] In the KEYMAT generation below, we fail to see the usefulness of the protocol field as it should always be set to the value '0'.

> If PFS is not needed, and KE payloads are not exchanged, the new
> keying material is defined as
>
> KEYMAT = prf(SKEYID_d, protocol | SPI | Ni_b | Nr_b).
>
> If PFS is desired and KE payloads were exchanged, the new keying
> material is defined as
>
> KEYMAT = prf(SKEYID_d, g(qm)^xy | protocol | SPI | Ni_b | Nr_b)
>
> The referenced symbols are defined as follows:
>
> o prf is the negotiated, keyed pseudo-random function-- often a
> keyed hash function-- used to generate a deterministic output
> that appears pseudo-random.
>
> o SKEYID_d is defined by IKE [IKE].
>
> o g(qm)^xy is the shared secret from the ephemeral Diffie-
> Hellman exchange of this Quick Mode.
>
> o "protocol" and "SPI" are from the ISAKMP Proposal
> Payload that contained the negotiated Transform.
>
> o Ni_b indicates the body of the initiator's Nonce payload
> from IKE [IKE].
>
> o Nr_b indicates the body of the responder's Nonce payload
> from IKE [IKE].
>
> A single SA negotiation results in two security assocations-- one
> inbound and one outbound. Different SPIs for each SA (one chosen by
> the initiator, the other by the responder) guarantee a different key
> for each direction. The SPI chosen by the destination of the SA is
> used to derive KEYMAT for that SA.

>
> For situations where the amount of keying material desired is greater
> than that supplied by the prf, KEYMAT is expanded by feeding the
> results of the prf back into itself and concatenating results until
> the required keying material has been reached. In other words,
>
> KEYMAT = K1 | K2 | K3 | ...
> where
> K1 = prf(SKEYID_d, [ g(qm)^xy | ] protocol | SPI | Ni_b | Nr_b)
> K2 = prf(SKEYID_d, K1 | [ g(qm)^xy | ] protocol | SPI | Ni_b |
> Nr_b)
> K3 = prf(SKEYID_d, K2 | [ g(qm)^xy | ] protocol | SPI | Ni_b |
> Nr_b)
>
>
>
> Arkko & Blom Informational [Page 21]
>
>
>
>
>
> INTERNET-DRAFT MAPSEC DOI 22 February 2001
>
>
> etc.
>
> This keying material (whether with PFS or without, and whether
> derived directly or through concatenation) MUST be used with the
> negotiated SA.

[OP] section below to be removed.

>
> 7.2 KINK
>
> In KINK, during the establishment of SAs the initiator and responder
> each provide random nonces that add entropy to the KDC supplied
> session key in order to derive the SA keying material (KEYMAT).
>

>    KEYMAT = prf(Secret, Ni [ | Nr ])
>
>   where
>
>      o  prf is as presented in section 7.1.
>
>      o  Secret is the  secret  derived  from  the  Kerberos
>         ticket. It is as defined in KINK [KINK].
>
>      o  Ni and and Nr are the nonces of the initiator and
>         responder, respectively.
>
>   The function is initially called with the session key found in the
>   service ticket used for Secret and is called recursively with the
>   resulting KEYMAT until it has generated a proper number of bits.
>   Rules regarding the optionality of the Nr are as defined in KINK
>   [KINK].
>
> 8. Modification History
>
>   The following modifications have been made to the -01 version of
>   this draft:
>
>   o  Sections 3.5-3.6 now specify a profile for the use of
>      IKE and KINK.
>   o  All MAPSEC-specific phase 2 notifications have been removed
>      for simplicity.
>   o  AES-MAC has been specified instead of HMAC_SHA1. Note that
>      Phase 1 has been specified to use 3DES and SHA1 since
>      no RFC exists yet to define the use of AES and especially
>      AES-MAC for IKE Phase 1.
>   o  Some formatting modifications have been made.
>   o  Attribute parsing requirements were simplified since
>      only a single kind of lifetimes are supported.
>   o  MAP_BLOWFISH has been removed since 3GPP hasn't defined it.
>   o  MAP_NULL has been removed and protection profiles are
>
>
>

>
>
>
>
>

>
>
>    expected to be used instead to signify that no security
>    is needed.
>  o  Rules for assigning new numbers within this DOI have
>    been clarified.
>
> 9. Intellectual property rights
>
>  Ericsson has patent applications which may cover parts of this
>  technology. Should such applications become actual patents
>  and be determined to cover parts of this specification, Ericsson
>  intends to provide licensing when implementing, using or distributing
>  the technology under openly specified, reasonable, non-
>  discriminatory terms.
>
>
> 10. Acknowledgments
>
>  This document is derived from the work done by David Castellanos-
>  Zamora, Krister Boman, Anders Liljekvist, Eeva Munter and others at
>  Ericsson, and Tatu Ylonen and others at SSH Communications Security
>  Corp.
>
> 11. References
>
>  [AH]     Kent, S., and R. Atkinson, "IP Authentication Header", RFC
>          2402, November 1998.
>
>  [ARCH]   Kent, S., and R. Atkinson, "Security Architecture for the
>          Internet Protocol", RFC 2401, November 1998.
>
>  [ESP]    Kent, S., and R. Atkinson, "IP Encapsulating Security
>          Payload (ESP)", RFC 2406, November 1998.

>
> [IKE] Harkins, D., and D. Carrel, D., "The Internet Key Exchange
> (IKE)", RFC 2409, November 1998.
>
> [ISAKMP] Maughan, D., Schertler, M., Schneider, M., and J. Turner,
> "Internet Security Association and Key Management Protocol
> (ISAKMP)", RFC 2408, November 1998.
>
> [IPSDOI] D. Piper, "The Internet IP Security Domain of
> Interpretation for ISAKMP", RFC 2407, November 1998.
>
> [KINK] M. Froh, M. Hur, D. McGrew, S. Medvinsky, M. Thomas, J.
> Vilhuber, "Kerberized Internet Negotiation of Keys (KINK)",
> draft-ietf-kink-kink-00.txt, Cybersafe, Motorola, Cisco.
> Work In Progress, September 2000
>
>
>
>

>
>
>
>
>

>
>
> [OAKLEY] Orman, H., "The OAKLEY Key Determination Protocol", RFC
> 2412, November 1998.
>
> [NDSEC] 3rd Generation Partnership Project, Technical Specification
> Group SA3, Security "Network Domain Security (Release 4)",
> 3GPP TS 33.200, (Work In Progress), January, 2001.
>
> [MPLS] E. Rosen, Y. Rekhter, "BGP/MPLS VPNs", RFC 2547, March
> 1999.
>
> 12. Authors' Addresses
>

>    Jari Arkko
>    Oy LM Ericsson Ab
>    02420 Jorvas
>    Finland
>
>    Phone: +358 40 5079256
>    EMail: jari.arkko@ericsson.com
>
>    Rolf Blom
>    Ericsson Radio Systems AB
>    SE-16480 Stockholm
>    Sweden
>
>    Phone: +46 8 58531707
>    EMail: rolf.blom@era.ericsson.se
>
> Full Copyright Statement
>

>
>
>

>
>
>
>
>

>
>

>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>

>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>
>