

Source: SA WG3 (Security)

Title: CR to 33.203 and 33.210: Addition of AES transform (Rel-6)

Document for: Approval

Agenda Item: 7.3.3

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-040153	33.203	064	-	Rel-6	Addition of AES transform	B	6.1.0	S3-040186	IMS-ASEC
SP-040153	33.210	015	-	Rel-6	Addition of AES transform	B	6.3.0	S3-040085	SEC-NDS-IP

CHANGE REQUEST

⌘ **33.203 CR 064** ⌘ rev **-** ⌘ Current version: **6.1.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Addition of AES transform		
Source:	⌘ SA WG3		
Work item code:	⌘ IMS-ASEC	Date:	⌘ 11/02/2004
Category:	⌘ B	Release:	⌘ Rel-6
	Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	⌘ Now AES-CBC mode encryption method is available and it is desirable to permit it to be used.
Summary of change:	⌘ The change introduces support for AES-CBC mode encryption.
Consequences if not approved:	⌘ IMS access security will not be able to offer the security protection by means of the AES based transform.

Clauses affected:	⌘ 2, 7.1, Annex I										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"> </td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications	Y	N		X		X		X	⌘	
Y	N										
	X										
	X										
	X										
Other comments:	⌘ -										

***** **First change** *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [2] 3GPP TS 22.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service Requirements for the IP Multimedia Core Network".
- [3] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia (IM) Subsystem".
- [4] 3GPP TS 21.133: "3rd Generation Partnership Project; T Technical Specification Group Services and System Aspects; Security Threats and Requirements".
- [5] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".
- [6] IETF RFC 3261 "SIP: Session Initiation Protocol".
- [7] 3GPP TS 21.905: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Vocabulary for 3GPP specifications".
- [8] 3GPP TS 24.229: "3rd Generation Partnership Project: Technical Specification Group Core Network; IP Multimedia Call Control Protocol based on SIP and SDP".
- [9] 3GPP TS 23.002: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, Network Architecture".
- [10] 3GPP TS 23.060: "3rd Generation Partnership Project: Technical Specification Group Services and System Aspects, General Packet Radio Service (GPRS); Service Description".
- [11] 3GPP TS 24.228: "3rd Generation Partnership Project: Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP".
- [12] IETF RFC 2617 (1999) "HTTP Authentication: Basic and Digest Access Authentication".
- [13] IETF RFC 2406 (1998) "IP Encapsulating Security Payload (ESP)".
- [14] IETF RFC 2401 (1998) "Security Architecture for the Internet Protocol".
- [15] IETF RFC 2403 (1998) "The Use of HMAC-MD5-96 within ESP and AH".
- [16] IETF RFC 2404 (1998) "The Use of HMAC-SHA-1-96 within ESP and AH".
- [17] IETF RFC 3310 (2002): "HTTP Digest Authentication Using AKA". April, 2002.
- [18] IETF RFC 3041 (2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".
- [19] IETF RFC 2402 (1998): "IP Authentication Header".

- [20] IETF RFC 2451 (1998): "The ESP CBC-Mode Cipher Algorithms ".
- [21] IETF RFC 3329 (2002): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".
- [22] [IETF RFC 3602 \(2003\): "The AES-CBC Cipher Algorithm and Its Use with IPsec".](#)

***** Next change *****

7.1 Security association parameters

For protecting IMS signaling between the UE and the P-CSCF it is necessary to agree on shared keys that are provided by IMS AKA, and a set of parameters specific to a protection method. The security mode setup (cf. clause 7.2) is used to negotiate the SA parameters required for IPsec ESP with authentication, but without confidentiality.

The SA parameters that shall be negotiated between UE and P-CSCF in the security mode set-up procedure are:

- Encryption algorithm

The encryption algorithm is either DES-EDE3-CBC as specified in RFC ~~2451~~²⁵⁴⁴ [20] or AES-CBC as specified in RFC 3602 [22] with 128 bit key.

Both encryption algorithms shall be supported by both, the UE and the P-CSCF.

~~[Editors note: The encryption algorithm AES should be added as soon as it appears as an RFC in IETF.]~~

- Integrity algorithm

NOTE: What is called "authentication algorithm" in RFC 2406 [13] is called "integrity algorithm" in this specification in order to be in line with the terminology used in other 3GPP specifications and, in particular, to avoid confusion with the authentication algorithms used in the AKA protocol.

The integrity algorithm is either HMAC-MD5-96 [15] or HMAC-SHA-1-96 [16].

Both integrity algorithms shall be supported by both, the UE and the P-CSCF as mandated by RFC 2406 [13]. In the unlikely event that one of the integrity algorithms is compromised during the lifetime of this specification, this algorithm shall no longer be supported.

NOTE: If only one of the two integrity algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. clause 7.2) will then ensure that the other integrity algorithm is selected.

- SPI (Security Parameter Index)

The SPI is allocated locally for inbound SAs. The triple (SPI, destination IP address, security protocol) uniquely identifies an SA at the IP layer. The UE shall select the SPIs uniquely, and different from any SPIs that might be used in any existing SAs (i.e. inbound and outbound SAs). The SPIs selected by the P-CSCF shall be different than the SPIs sent by the UE, cf. clause 7.2. In an authenticated registration, the UE and the P-CSCF each select two SPIs, not yet associated with existing inbound SAs, for the new inbound security associations at the UE and the P-CSCF respectively.

NOTE: This allocation of SPIs ensures that protected messages in the uplink always differ from protected messages in the downlink in, at least, the SPI field. This thwarts reflection attacks. When several applications use IPsec on the same physical interface the SIP application should be allocated a separate range of SPIs.

The following SA parameters are not negotiated:

- Life type: the life type is always seconds;
- SA duration: the SA duration has a fixed length of $2^{32}-1$;

NOTE: The SA duration is a network layer concept. From a practical point of view, the value chosen for "SA duration" does not impose any limit on the lifetime of an SA at the network layer. The SA lifetime is controlled by the SIP application as specified in clause 7.4.

- Mode: transport mode;
- Key length: the length of the integrity key IK_{ESP} depends on the integrity algorithm. It is 128 bits for HMAC-MD5-96 and 160 bits for HMAC-SHA-1-96.

- Key length: the length of the encryption key depends on the encryption algorithm. The entropy of the key shall at least be 128 bits.

Selectors:

The security associations (SA) have to be bound to specific parameters (selectors) of the SIP flows between UE and P-CSCF, i.e. source and destination IP addresses, transport protocols that share the SA, and source and destination ports.

- IP addresses are bound to two pairs of SAs, as in clause 6.3, as follows:
 - inbound SA at the P-CSCF:
The source and destination IP addresses associated with the SA are identical to those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.
 - outbound SA at the P-CSCF:
the source IP address bound to the outbound SA equals the destination IP address bound to the inbound SA;
the destination IP address bound to the outbound SA equals the source IP address bound to the inbound SA.

NOTE: This implies that the source and destination IP addresses in the header of the IP packet in which the protected SIP REGISTER message was received by the P-CSCF need to be the same as those in the header of the IP packet in which the initial SIP REGISTER message was received by the P-CSCF.

- The transport protocol selector shall allow UDP and TCP.
- Ports:
 1. The P-CSCF associates two ports, called *port_ps* and *port_pc*, with each pair of security associations established in an authenticated registration. The ports *port_ps* and *port_pc* are different from the standard SIP ports 5060 and 5061. No unprotected messages shall be sent from or received on the ports *port_ps* and *port_pc*. From a security point of view, unprotected messages may be received on any port which is different from the ports *port_ps* and *port_pc*. The number of the ports *port_ps* and *port_pc* are communicated to the UE during the security mode set-up procedure, cf. clause 7.2. These ports are used with both, UDP and TCP. The use of these ports may differ for TCP and UDP, as follows:

UDP case: the P-CSCF receives requests and responses protected with ESP from any UE on the port *port_ps* (the "protected server port"). The P-CSCF sends requests and responses protected with ESP to a UE on the port *port_pc* (the "protected client port").

TCP case: the P-CSCF, if it does not have a TCP connection towards the UE yet, shall set up a TCP connection from its *port_pc* to the port *port_us* of the UE before sending a request to it..

NOTE: Both the UE and the P-CSCF may set up a TCP connection from their client port to the other end's server port on demand. An already existing TCP connection may be reused by both the P-CSCF or the UE; but it is not mandatory.

NOTE: The protected server port *port_ps* stays fixed for a UE until all IMPUs from this UE are de-registered. It may be fixed for a particular P-CSCF over all UEs, but there is no need to fix the same protected server port for different P-CSCFs.

NOTE: The distinction between the UDP and the TCP case reflects the different behaviour of SIP over UDP and TCP, as specified in section 18 of RFC 3261 [6].

2. The UE associates two ports, called *port_us* and *port_uc*, with each pair of security associations established in an authenticated registration. The ports *port_us* and *port_uc* are different from the standard SIP ports 5060 and 5061. No unprotected messages shall be sent from or received on the ports *port_us* and *port_uc*. From a security point of view, unprotected messages may be received on any port which is different from the ports *port_us* and *port_uc*. The number of the ports *port_us* and *port_uc* are communicated to the P-CSCF during the security mode set-up procedure, cf. clause 7.2. These ports are used with both, UDP and TCP. The use of these ports may differ for TCP and UDP, as follows:

UDP case: the UE receives requests and responses protected with ESP on the port *port_us* (the "protected server port"). The UE sends requests and responses protected with ESP on the port *port_uc* (the "protected client port").

TCP case: the UE, if it does not have a TCP connection towards the P-CSCF yet, shall set up a TCP connection to the port *port_ps* of the P-CSCF before sending a request to it.

NOTE: Both the UE and the P-CSCF may set up a TCP connection from their client port to the other end's server port on demand. An already existing TCP connection may be reused by both the P-CSCF or the UE, but it is not mandatory.

NOTE: The protected server port *port_us* stays fixed for a UE until all IMPUs from this UE are de-registered.

NOTE: The distinction between the UDP and the TCP case reflects the different behaviour of SIP over UDP and TCP, as specified in section 18 of RFC 3261 [6]

3. The P-CSCF is allowed to receive only REGISTER messages and error messages on unprotected ports. All other messages not arriving on a protected port shall be either discarded or rejected by the P-CSCF.
4. The UE is allowed to receive only the following messages on an unprotected port:
 - responses to unprotected REGISTER messages;
 - error messages.

All other messages not arriving on a protected port shall be rejected or silently discarded by the UE.

The following rules apply:

1. For each unidirectional SA which has been established and has not expired, the SIP application at the P-CSCF stores at least the following data: (UE_IP_address, UE_protected_port, P-CSCF_protected_port, SPI, IMPI, IMPU1, ... , IMPUn, lifetime) in an "SA_table". The pair (UE_protected_port, P-CSCF_protected_port) equals either (*port_uc*, *port_ps*) or (*port_us*, *port_pc*).

NOTE: The SPI is only required when initiating and deleting SAs in the P-CSCF. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

2. The SIP application at the P-CSCF shall check upon receipt of a protected REGISTER message that the source IP address in the packet headers coincide with the UE's IP address inserted in the Via header of the protected REGISTER message. If the Via header does not explicitly contain the UE's PI address, but rather a symbolic name then the P-CSCF shall first resolve the symbolic name by suitable means to obtain an IP address.
3. The SIP application at the P-CSCF shall check upon receipt of an initial REGISTER message that the pair (UE_IP_address, UE_protected_client_port), where the UE_IP_address is the source IP address in the packet header and the protected client port is sent as part of the security mode set-up procedure (cf. clause 7.2), has not yet been associated with entries in the "SA_table". Furthermore, the P-CSCF shall check that, for any one IMPI, no more than six SAs per direction are stored at any one time. If these checks are unsuccessful the registration is aborted and a suitable error message is sent to the UE.

NOTE: According to clause 7.4 on SA handling, at most six SAs per direction may exist at a P-CSCF for one user at any one time.

4. For each incoming protected message the SIP application at the P-CSCF shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the triple (UE_IP_address, UE_protected_port, P-CSCF_protected_port) in the "SA_table". The SIP application at the P-CSCF shall further check that the IMPU associated with the SA in the "SA_table" and the IMPU in the received SIP message coincide. If this is not the case the message shall be discarded.
5. For each unidirectional SA which has been established and has not expired, the SIP application at the UE stores at least the following data: (UE_protected_port, P-CSCF_protected_port, SPI, lifetime) in an "SA_table". The pair (UE_protected_port, P-CSCF_protected_port) equals either (*port_uc*, *port_ps*) or (*port_us*, *port_pc*).

NOTE: The SPI is only required to initiate and delete SAs in the UE. The SPI is not exchanged between IPsec and the SIP layer for incoming or outgoing SIP messages.

6. When establishing a new pair of SAs (cf. clause 6.3) the SIP application at the UE shall ensure that the selected numbers for the protected ports do not correspond to an entry in the "SA_table".

NOTE: Regarding the selection of the number of the protected port at the UE it is generally recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. This is to thwart a limited form of a Denial of Service attack. UMTS PS access link security also helps to thwart this attack.

7. For each incoming protected message the SIP application at the UE shall verify that the correct inbound SA according to clause 7.4 on SA handling has been used. The SA is identified by the pair (UE_protected_port, P-CSCF_protected_port) in the "SA table".

NOTE: If the integrity check of a received packet fails then IPsec will automatically discard the packet.

***** Next change *****

Annex I (normative): Key expansion functions for IPsec ESP

Integrity Keys:

If the selected authentication algorithm is HMAC-MD5-96 then $IK_{ESP} = IK_{IM}$.

If the selected authentication algorithm is HMAC-SHA-1-96 then IK_{ESP} is obtained from IK_{IM} by appending 32 zero bits to the end of IK_{IM} to create a 160-bit string.

Encryption Keys:

Divide CK_{IM} into two blocks of 64 bits each:

$$CK_{IM} = CK_{IM1} \parallel CK_{IM2}$$

Where CK_{IM1} are the 64 most significant bits and CK_{IM2} are the 64 least significant bits.

The key for DES-EDE3-CBC is then defined to be:

$$CK_{ESP} = CK_{IM1} \parallel CK_{IM2} \parallel CK_{IM1},$$

after adjusting parity bits to comply with RFC 2451 [20].

[If selected encryption algorithm is AES-CBC as specified in RFC 3602 \[22\] with 128 bit key then \$CK_{ESP} = CK_{IM}\$](#)

~~[Editors Note: Should AES be implemented in Release 6 time frame the input key to AES shall be CK_{IM}].~~

CHANGE REQUEST

⌘ **33.210 CR 015** ⌘ rev **-** ⌘ Current version: **6.3.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

Proposed change affects: UICC apps ME Radio Access Network Core Network

Title:	⌘ Addition of AES transform		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC-NDS-IP	Date:	⌘ 02/02/2004
Category:	⌘ B	Release:	⌘ Rel-6
	<i>Use <u>one</u> of the following categories:</i> F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .		<i>Use <u>one</u> of the following releases:</i> 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	⌘ Support for the AES encryption was originally intended for Release 5, but due to delays in the IETF process the RFC was not ready in time for Release 5. Now when the transform is available it is desirable to permit it to be used by NDS/IP compliant IPsec solutions.
Summary of change:	⌘ The change introduces support for AES-CBC mode encryption.
Consequences if not approved:	⌘ NDS/IP will not be able to offer the confidentiality protection by means of the AES based transform.

Clauses affected:	⌘ 2, 5.3.3, 5.4										
Other specs affected:	<table border="1" style="display: inline-table; border-collapse: collapse; text-align: center;"> <tr> <td style="width: 20px;">Y</td> <td style="width: 20px;">N</td> </tr> <tr> <td style="width: 20px;"> </td> <td style="width: 20px;">X</td> </tr> <tr> <td style="width: 20px;"> </td> <td style="width: 20px;">X</td> </tr> <tr> <td style="width: 20px;"> </td> <td style="width: 20px;">X</td> </tr> </table> Other core specifications ⌘ Test specifications O&M Specifications	Y	N		X		X		X		
Y	N										
	X										
	X										
	X										
Other comments:	⌘ The proposed changes will update NDS/IP to reflect the current state of IPsec.										

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** First change *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TS 21.133: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements".
- [2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".
- [3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".
- [4] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".
- [5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".
- [6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".
- [7] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".
- [8] 3GPP TS 33.103: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines".
- [9] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".
- [10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".
- [11] RFC-2393: "IP Payload Compression Protocol (IPComp)".
- [12] RFC-2401: "Security Architecture for the Internet Protocol".
- [13] RFC-2402: "IP Authentication Header".
- [14] RFC-2403: "The Use of HMAC-MD5-96 within ESP and AH".
- [15] RFC-2404: "The Use of HMAC-SHA-1-96 within ESP and AH".
- [16] RFC-2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".
- [17] RFC-2406: "IP Encapsulating Security Payload".
- [18] RFC-2407: "The Internet IP Security Domain of Interpretation for ISAKMP".
- [19] RFC-2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

- [20] RFC-2409: "The Internet Key Exchange (IKE)".
- [21] RFC-2410: "The NULL Encryption Algorithm and Its Use With IPsec".
- [22] RFC-2411: "IP Security Document Roadmap".
- [23] RFC-2412: "The OAKLEY Key Determination Protocol".
- [24] RFC-2451: "The ESP CBC-Mode Cipher Algorithms".
- [25] RFC-2521: "ICMP Security Failures Messages".
- [26] RFC-3554: "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec".
- [27] RFC-1750: "Randomness Recommendations for Security".
- [28] 3GPP TS 25.412: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signalling transport".
- [29] [RFC-3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec"](#)

***** **Second change** *****

5.3.3 Support of ESP encryption transforms

IPsec offers a fairly wide set of confidentiality transforms. The transforms that compliant IPsec implementations are required to support are the ESP_NULL and the ESP_DES transforms. However, the Data Encryption Standard (DES) transform is no longer considered to be sufficiently strong in terms of cryptographic strength. This is also noted by IESG in a note in RFC-2407 [18] to the effect that the ESP_DES transform is likely to be deprecated as a mandatory transform in the near future.

It is therefore explicitly noted that for use in NDS/IP, the ESP_DES transform shall not be used and instead it shall be mandatory to support the ESP_3DES transform.

[Support for the AES-CBC cipher algorithm \[29\] is mandatory. It is noted that the AES-CBC key length for use with this specification shall be 128 bits.](#)

***** **Third change** *****

5.4 Profiling of IKE

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following additional requirement on IKE is made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of pre-shared secrets for authentication shall be supported;
- Only Main Mode shall be used;
- IP addresses and Fully Qualified Domain Names (FQDN) shall be supported for identification;
- Support of 3DES in CBC mode shall be mandatory for confidentiality;
- [Support of AES in CBC mode \[29\] shall be mandatory for confidentiality;](#)
- Support of SHA-1 shall be mandatory for integrity/message authentication.

Phase-1 IKE SAs shall be persistent with respect to the IPsec SAs is derived from it. That is, IKE SAs shall have a lifetime for at least the same duration as does the derived IPsec SAs.

The IPsec SAs should be re-keyed proactively, i.e. a new SA should be established before the old SA expires. The elapsed time between the new SA establishment and the cancellation of the old SA shall be sufficient to avoid losing any data being transmitted within the old SA.

For IKE phase-2 (IPsec SA):

- Perfect Forward Secrecy is optional;
- Only IP addresses or subnet identity types shall be mandatory address types;
- Support of Notifications shall be mandatory.

[Key Length and support of AES transform:](#)

[Since the AES-CBC allows variable key lengths, the Key Length attribute must be specified in both a Phase 1 exchange \[20\] and a Phase 2 exchange \[18\]. It is noted that the key length for use with this specification shall be 128 bits.](#)