



MSF Implementation Agreement for the LTE Access
Tile eNodeB to Security GW (<Zb-Reference>) and Inter
Operator Security GW (<Za-Reference>) Components

MSF-VoLTE-Sec-GW-001.FINAL

MultiService Forum Architectural Framework

Contribution Number: msf2011.151.00
Document Filename: **MSF-VoLTE-Sec-GW-001.FINAL**
Working Group: VoLTE
Title: **MSF Implementation Agreement for the LTE Access Tile eNodeB to Security GW (<Zb-Reference>) and Inter Operator Security GW (<Za-Reference>) Components**

Author: Russell Caton (Stoke)

Contact Information: rcaton@stoke.com

Last Uploaded: 10/17/2011

Abstract:

This document outlines the implementation agreement for the Za & Zb reference points in the LTE/EPC Architecture. Specifically, the Za reference point is an IpSec implementation between eNodeB to Aggregation Gateway and Zb reference point is between Aggregation Gateway to S-GW. The Za and Zb reference points are specified in 3GPP TS 33.210.

DISCLAIMER

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and the MultiService Forum is not responsible for any errors or omissions. The MultiService Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither the MultiService Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind whether based on theories of tort, contract, strict liability or otherwise, shall be assumed or incurred by the MultiService Forum, its member companies, or the publisher as a result of reliance or use by any party upon any information contained in this publication. All liability for any implied or express warranty of merchantability or fitness for a particular purpose is hereby disclaimed. The receipt or any use of this document or its contents does not in any way create by implication or otherwise: Any express or implied license or right to or under any MultiService Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor Any warranty or representation that any MultiService Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor Any commitment by a MultiService Forum company to purchase or otherwise procure any product(s) and/or service(s) that embody any or all of the ideas, technologies, or concepts contained herein; nor Any form of relationship between any MultiService Forum member companies and the recipient or user of this document. Implementation or use of specific MultiService Forum Implementation Agreements, Architectural Frameworks or recommendations and MultiService Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in the MultiService Forum.

For addition information contact:

MultiService Forum
48377 Fremont Blvd, Suite 117, Fremont, CA 94538
Phone: (510) 492-4050 Fax: (510) 492-4001
info@msforum.org WWW.MSFORUM.ORG
© MultiService Forum 2011

Table of Contents

1	Introduction.....	4
1.1	Scope	4
1.1	References	4
1.2	Definitions and Abbreviations	5
1.3	Definitions.....	5
1.4	Abbreviations	5
2	Context for use of Za & Zb Reference Points <<.....	7
3	General Description of Za & Zb reference points <.....	7
3.1	Zb	7
3.2	Za.....	7
4	Pre-Shared IKE v2.0 Key Configuration	8
5	Procedures over <Za and <Zb reference points	8
5.1	IKE v2.0 procedures.....	8
5.2	Tunnel (IKE) creation, including cookies.....	8
5.3	IKEv2 Tunnel Setup.....	9
5.4	IKEv2 Tunnel Setup with COOKIE.....	9
5.5	Tunnel (Child SA) creation	9
5.6	Example Message flow	10
5.7	SA Rekeying	10
5.8	Tunnel tear down.....	10
5.9	Example Message flow	11
5.10	Other procedures.....	11
6	Interface Profile	11
6.1	Zb reference point	11
6.2	Za reference point.....	11
6.3	IKEv2 (RFC 4306) Compliancy	12
7	IPSEC Parameters & Profiles	15
8	Core network elements	16

1 Introduction

1.1. Scope

This scope of this document covers the Za and Zb interfaces and an associated Security Gateway for use within an NDS/IP architecture as defined in 3GPP TS 33.210. The Za/Zb interfaces secure the S1 and X2 interfaces in an LTE network using standards compliant IPsec technology. Figure 1 shows the LTE/EPC architecture with an associated Security Gateway.

This document provides information to facilitate inter-operability with such a Security gateway when used in an LTE network in MSF inter-operability events.

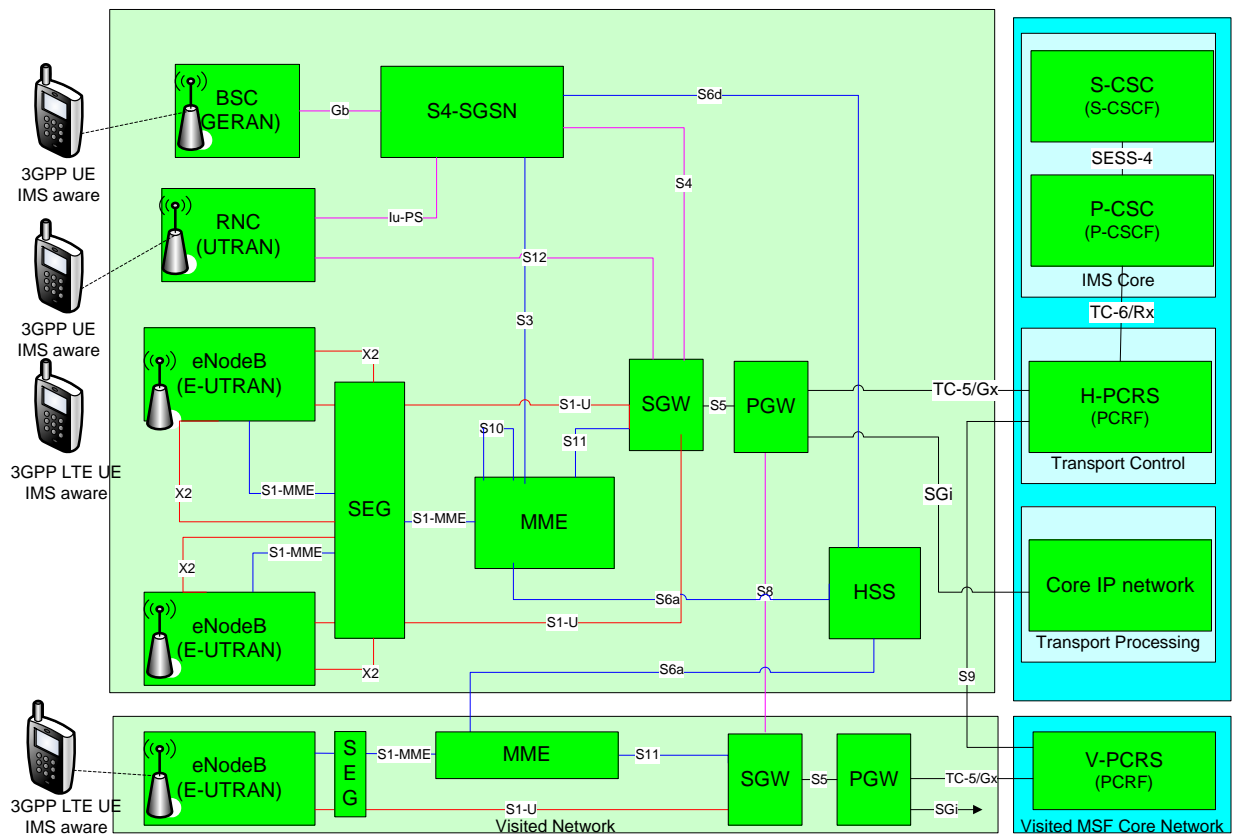


Figure 1. LTE/EPC Architecture with a Security Gateway

1.1 References

[1] RFC 4301: Security Architecture for the Internet Protocol

- [2] RFC 4303:IP Encapsulating Security Payload (ESP)
- [3] RFC 4306:Internet Key Exchange (IKEv2) Protocol
- [4] RFC 4307:Cryptographic Algorithms for Use in the IKEv2
- [5] RFC 4835:Cryptographic Algorithm Implementation Requirements for ESP and AH
- [6] 3GPP TS 33.210: Network Domain Security/IP Network Layer Security
- [7] RFC 2451:The ESP CBC-Mode Cipher Algorithms
- [8] RFC 3602:The AES-CBC Cipher Algorithm and Its Use with IPsec
- [9] RFC 3686:Using AES Counter Mode With IPsec ESP
- [10] RFC 3566:The AES-CBC-MAC-96 Algorithm and its Use With IPsec

1.2 Definitions and Abbreviations

1.3 Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", "OPTIONAL", "CONDITIONAL" and "IF" in this document are to be interpreted as described in the MSF Technical Committee Operating Procedures.

1.4 Abbreviations

3DES	Triple Data Encryption Standard
3GPP	3 rd Generation Partnership Project
ACA	Accounting-Answer
ACR	Accounting-Request
AES	Advanced Encryption Standard
AF	Application Function
AH	Authentication Header
AS	Application Server
ASN	Access Service Network
AVP	Application Value Pair
CBC	Cipher Block Chaining
CCF	Charging Collection Function
CDF	Charging Data Function
CDR	Charging Data Record
CDS	Charging Data Server
CGF	Charging Gateway Function
CGS	Charging Gateway Server
CSN	Connectivity Service Network
DH	Diffie-Helman
DNS	Domain Naming Service
ESP	Encapsulating Security Payload
FA	A mobile IP Foreign Agent entity
FQDN	Fully Qualifies Domain Name
HA	A mobile IP Home Agent entity
IA	Implementation Agreement
IKE	Internet Key Exchange
IMS	IP Multimedia System

IPsec	IP Security
MRFC	Multimedia Resource Function Controller
NDS/IP	Network Domain Security for IP protocols
PCRF	Policy and Charging Rules Function
P-CSC	Proxy – Call State Controller
OFCS	Offline Charging System
PDSN	Packet Data Serving Node
PEF	Policy Enforcement Function – enforces QoS assignments
PFS	Perfect Forward Secrecy
QoS	Quality of Service
MS	Mobile Station
RAA	Re-Auth Answer
RADIUS	Remote Authentication Dial-In User Service
RAN	Radio Access Network
SA	Security Association
SCTP	Stream Control Transmission Protocol
SFA	Service Flow Agent - Establishes the default service flows for a subscriber, ready for use when sessions are established
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol

2 Context for use of Za & Zb Reference Points <<

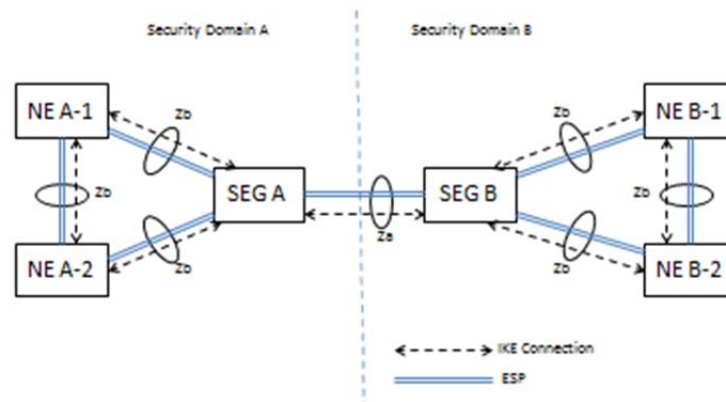


Figure 1: 3GPP R8 SEG Architecture showing Za and Zb

General Interface Areas

- eNodeB to EPC security association and aggregation, Za
- X2 mesh support, S-GW and MME load distribution and routing, Zb
- Standardization on IKE V2.0 for scalability and additional security features.

3 General Description of Za & Zb reference points <

3.1 Zb

This interface is implemented in order to allow for the secure separation of individual traffic flows, including O&M, signaling and user planes. By supporting multiple tunnels it is possible to specify individual QoS parameters for each traffic type, designed to meet the necessary KPIs, as an example treating signaling traffic with a higher priority and more robust security than the user plane

3.2 Za

This interface is implemented in order to allow for the secure transportation of data between network operators.

4 Pre-Shared IKE v2.0 Key Configuration

The pre-shared key information between the eNodeB and the SEG Gateway will be agreed between the IOT vendors and configured on the SEG and eNodeB (as required).

5 Procedures over <Za and <Zb reference points

5.1 IKE v2.0 procedures

The main procedures required for the SEG specification are:

- Tunnel (IKE) creation, including cookies.
- Tunnel (Child SA) creation
- SA Rekeying
- Child SA rekey
- Tunnel tear down

5.2 Tunnel (IKE) creation, including cookies.

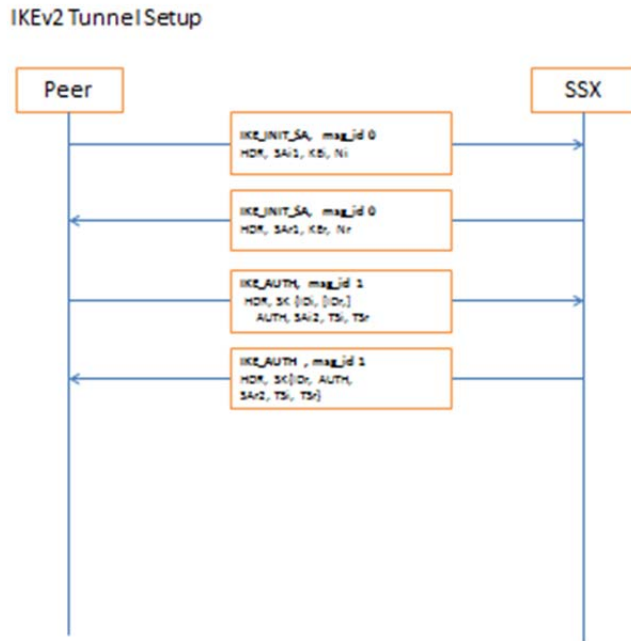
In order to establish a secure association and create a tunnel, either end point should be able to initiate and complete the creation of an IKEv2 tunnel with cookies disabled, allowed or required.

Peers should use Pre Shared Key for authentication of the remote gateway, detailed in section 4.

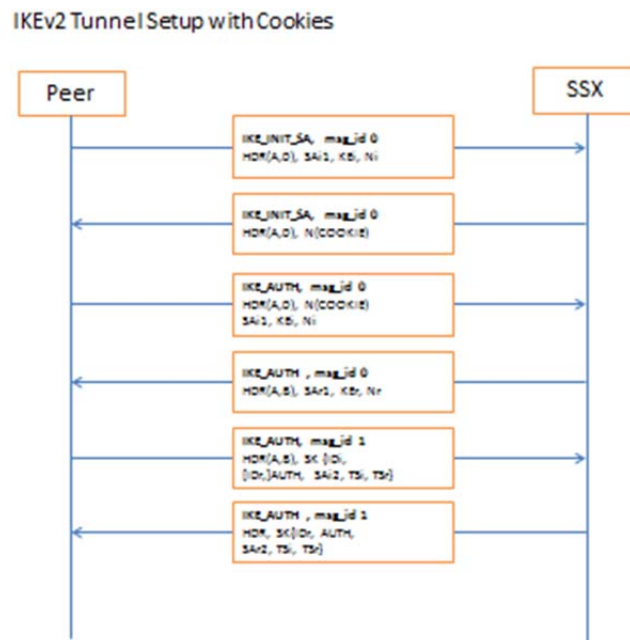
Example IKEv2 tunnel parameters :-

suite1	Select AES128, SHA-1, and DH-Group2
suite3	Select 3DES, SHA-1, and DH-Group2

5.3 IKEv2 Tunnel Setup



5.4 IKEv2 Tunnel Setup with COOKIE



5.5 Tunnel (Child SA) creation

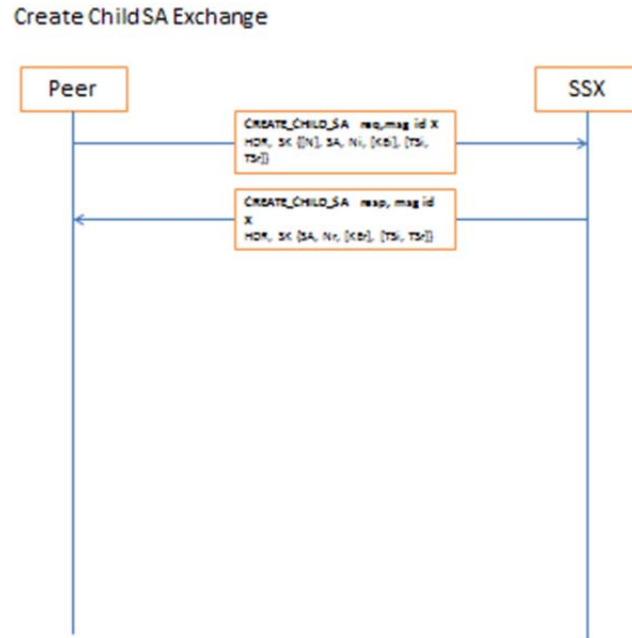
It should be demonstrated that either end point should be able to initiate and complete the creation of associated Child SA.

Suggested Child SA parameters :-

suite1 Select AES128, SHA-1, and PFS-Group2

suite3 Select 3DES, SHA-1, and PFS-Group2

5.6 Example Message flow



5.7 SA Rekeying

IKEv2 rekey

It should be demonstrated the either end point can successfully initiate and complete a re-keying of the IKEv2 tunnel. It is expected that this will be based on configurable timer settings.

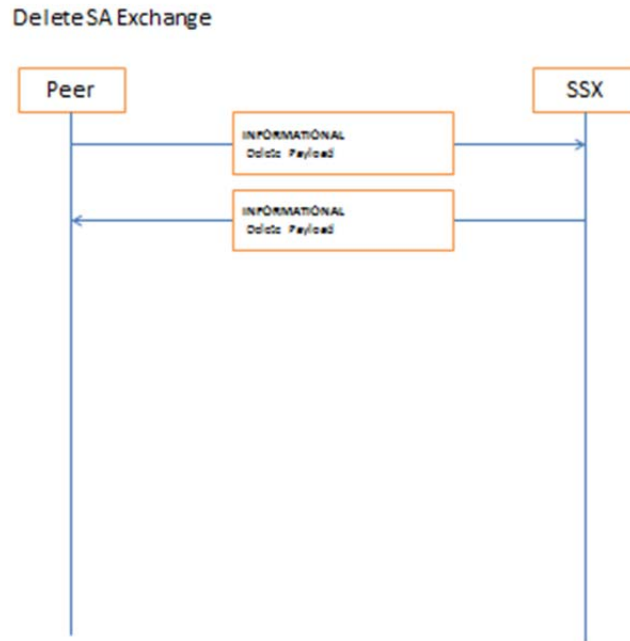
Child SA rekey

It should be demonstrated the either end point can successfully initiate and complete a re-keying of any associated Child SA. It is expected that this will be based on configurable timer settings.

5.8 Tunnel tear down

It should be demonstrated the either end point can successfully initiate and complete a tunnel tear down procedure.

5.9 Example Message flow



5.10 Other procedures

There are no other procedures.

6 Interface Profile

6.1 Zb reference point

The Zb reference point is between eNodeB/MME/SGW and SEG. It shall be implemented according to the definition in 3GPP TS33.210 (RFC 4306) unless stated otherwise.

6.2 Za reference point

The Za reference point is between SEGs (in different security domains). It shall be implemented according to the definition in 3GPP TS33.210 (RFC 4306) unless stated otherwise.

6.3 IKEv2 (RFC 4306) Compliancy

Stoke OS IKEv2 Gateway (RFC 4306) Compliancy Matrix			
Section Number	Section Name	Compliancy	Comments
1.1	Usage Scenarios	Full	
1.2	The Initial (IKE_INIT_SA and IKE_SA)	Full	
1.3	The CREATE_CHILD_SA Exchange	Full	
1.4	The Informational Exchange	Full	
1.5	Informational Messages outside of an IKE_SA	None	
2.1	Use of Retransmission Timers	Full	
2.2	Use of Sequence Numbers for Message ID	Full	
2.3	Window Size for Overlapping Requests	Partial	It is assumed the client's window size is always 1. Queries are not sent or processed
2.4	State Synchronization and Connection	Partial	
2.5	Version Numbers and Forward Compatibility	Full	
2.6	Cookies	Full	
2.7	Cryptographic Algorithm Negotiation	Full	
2.8	Rekeying	Full	
2.9	Traffic Selector Negotiation	Partial	The Tsi is sent with the value of the client's assigned IP address
2.1	Nonces	Full	
2.11	Address and Port Agility	Full	
2.12	Reuse of Diffie-Hellman Exponentials	None	Diffie-Hellman Exponentials are not re-used
2.13	Generating Keying	Full	
2.14	Generating Keying Material for the IKE_SA	Full	
2.15	Authentication of the IKE_SA	Full	
2.16	Extensible Authentication Protocol Methods	Full	
2.17	Generating Keying Material for CHILD_SAs	Full	

2.18	Rekeying IKE_SAs Using a CREATE_CHILD_SA exchange	Full	
2.19	Requesting an Internal Address on a Remote Network	Full	
2.2	Requesting the Peer's Version	None	The clients version is not queried nor are queries
2.21	Error Handling	Full	
2.22	IPComp	None	
2.23	NAT Traversal	Full	
2.24	Explicit Congestion Notification (ECN)	None	Outside scope of this document
3.1	The IKE Header	Full	
3.2	Generic Payload Header	Full	
3.3	Security Association Payload	Full	
3.4	Key Exchange Payload	Full	
3.5	Identification Payloads	Partial	supported: ID_IPV4_ADDR, ID_FQDN, ID_RFC822_ADDR
3.6	Certificate Payload	Partial	As per scenario 1.3 (above), Certificate authentication is supported.
3.7	Certificate Request Payload	Partial	As per scenario 1.3 (above), Certificate authentication is supported.
3.8	Authentication Payload	Full	
3.9	Nonce Payload	Full	
3.1	Notify Payload	Partial	Not supported: INITIAL_CONTACT
3.11	Delete Payload	Full	
3.12	Vendor ID Payload	Partial	
3.13	Traffic Selector Payload	Partial	
3.14	Encrypted Payload	Full	
3.15	Configuration Payload	Partial	See 2.19 above.
3.16	Extensible Authentication Protocol (EAP)	Full	
4	Conformance Requirements	Full	
5	Security Considerations	Full	
6	IANA Considerations		
7	Acknowledgements		
8	References		
A	Summary of Changes from IKEv1	Full	

B.1	Group 1 – 768 Bit MODP	Full	See Notes on supported
B.2	Group 2 – 1024 Bit MODP	Full	See Notes on supported

Supported Cryptographic Algorithms

IKE_SA

Five Cryptographic suites are supported. Suite1, Suite2, Suite3, Suite4 and custom (a customizable one).

Suite1: ENCR_AES_CBC(128-bit), AUTH_HMAC_SHA1_96, PRF_HMAC_SHA1, and Diffie-Hellman Group 2 (1024 Bit MODP).

Suite2: ENCR_AES_CBC(128-bit), AUTH_HMAC_SHA1_96, PRF_HMAC_SHA1, and Diffie-Hellman Group 5 (1536 Bit MODP).

Suite3: ENCR_3DES, AUTH_HMAC_SHA1_96, PRF_HMAC_SHA1, and Diffie-Hellman Group 2 (1024 Bit MODP).

Suite4: ENCR_3DES, AUTH_HMAC_SHA1_96, PRF_HMAC_SHA1, and Diffie-Hellman Group 2 (1024 Bit MODP).

Custom: Choose one of five encryption algorithms,

AES128, AES128-CTR (counter-mode), AES192, AES256 and 3DES.

Choose one of two hash algorithms,
MD5 and SHA-1.

Choose one of three PRF algorithms,
PRF_HMAC_MD5, PRF_HMAC_SHA1, and PRF_AES128_XCBC.

Choose one of two Diffie-Hellman algorithms,
Group 2 (1024 Bit MODP) and Group 5 (1536 Bit MODP).

CHILD_SA

Five Cryptographic suites are supported. Suite1, Suite2, Suite3, Suite4 and custom (a customizable one).

Suite1: ENCR_AES_CBC(128-bit), SHA-1 hash, SHA-1 PRF, and PFS Group 2 (1024 Bit MODP).

Suite2: ENCR_AES_CBC(128-bit), SHA-1 hash, SHA-1 PRF, and no PFS.

Suite3: 3DES encryption, SHA-1 hash, SHA-1 PRF, and PFS Group 2 (1024 Bit MODP).

Suite4: 3DES encryption, SHA-1 hash, SHA-1 PRF, and no PFS.

Custom: Choose one of five encryption algorithms,
ENCR_AES_CBC(128-bit), ENCR_AES_CTR(128-bit), ENCR_AES_CBC(192-bit), ENCR_AES_CBC(256-bit) and ENCR_3DES.

Choose one of three Integrity(hash) algorithms,

AUTH_HMAC_MD5_96, AUTH_HMAC_SHA1_96, and AUTH_AES96_XCBC_96.

Choose one of three PFS algorithms,
None, Group 2 (1024 Bit MODP) and Group 5 (1536 Bit MODP).

Supported Authentication Methods

~~IKE_SA~~
The ~~SSX~~ and the peer need to authenticate each other using one of two schemes,
preshared-key (secret) and PKCS12 certificate

7 IPSEC Parameters & Profiles

Vendors should be able to support the following IPsec profiles :-

Attribute	Profile 1	Profile 2
PH1 – Encryption	AES128	3DES
PH1 – Hash	SHA-1	SHA-1
PH1 – DH group	DH2	DH2

Attribute	Profile 1	Profile 2
PH2 Encryption	AES128	3DES
PH2 Hash	SHA-1	SHA-1
PH2 PFS	Group 2	Group 2

8 Core network elements

A common NTP (SyncE/IEEE 1588v2.0?) server is required to ensure each vendor eNodeB and each vendor SEG elements are synchronized.

--- End of Document ---