



H(e)NodeB Security

CONTACT INFORMATION:

phone: +1.301.527.1629

fax: +1.301.527.1690

email: whitepaper@hsc.com

web: www.hsc.com

PROPRIETARY NOTICE

All rights reserved. This publication and its contents are proprietary to Hughes Systique Corporation. No part of this publication may be reproduced in any form or by any means without the written permission of Hughes Systique Corporation, 15245 Shady Grove Road, Suite 330, Rockville, MD 20850.

Copyright © 2010 Hughes Systique Corporation

TABLE OF CONTENTS

<u>SECTION</u>	<u>PAGE</u>
1.0 HOME(E)NODEB SECURITY	4
1.1 ABSTRACT	4
1.2 H(E)NB SECURITY ARCHITECTURE	4
1.3 H(E)NB SECURITY CONCERNS	5
1.3.1 Compromise of H(e)NB credentials	5
1.3.2 Man-in-middle attacks	5
1.3.3 Replay attacks	5
1.3.4 Denial of service attacks	6
1.3.5 Eavesdropping	6
1.3.6 Masquerade	6
1.4 MITIGATION OF H(E)NB SECURITY CONCERNS/THREATS	6
1.5 H(E)NB SECURITY ASPECTS	7
1.5.1 Storage Environment.....	7
1.5.2 Device Integrity Check and Device validation.....	7
1.5.3 Mutual Authentication	7
1.5.4 IPSec tunnel establishment	10
1.5.5 Security between H(e)NB and H(e)MS	10
1.6 CONCLUSIONS	11
2.0 REFERENCES	12

1.0 HOME(E)NODEB SECURITY

1.1 Abstract

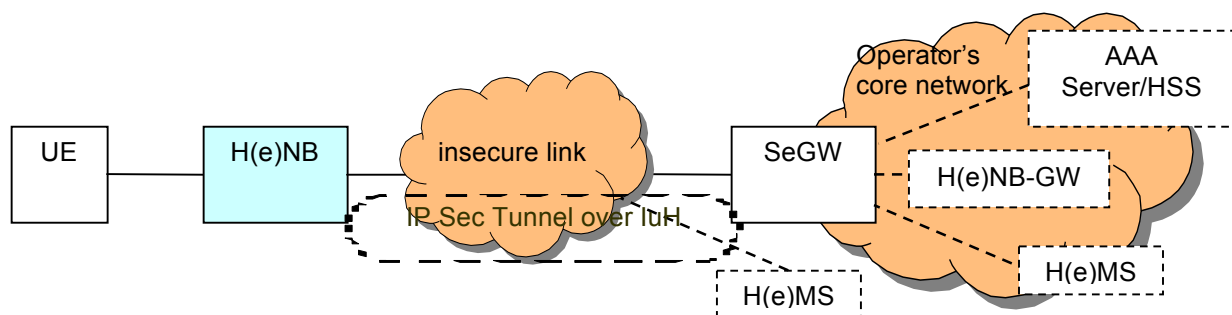
Femtocell access points (H(e)NBs) are close-range, limited-capacity base stations that utilize residential broadband connections to connect to carrier networks. The use of such distributed base station architecture improves reception and allows the operators to deliver fast, seamless, high-bandwidth cellular coverage into the homes and offices of their end customers.

The deployment of Femtocell solutions is attractive to mobile network operators as they successfully address coverage and mobile data bandwidth requirements by leveraging widely available broadband connections without the additional cost associated with the alternative macro-cell deployment.

Security is the most challenging area and critical aspect to prevent unauthorized access to important resources in any wireless communication network. Like all communications technologies, Femtocells also require robust security. To maintain the level of security that is expected of the telecommunications networks, Femtocell systems require that the authenticity of the communicating peers (access points and gateways) and the privacy and integrity of the data exchanged are guaranteed.

This paper summarizes various security concerns/threats on H(e)NB, mitigation of these security threats, security architecture and various security aspects to take care of the associated security issues.

1.2 H(e)NB Security Architecture



H(e)NB

A network element (typically deployed in customer premises) that connects User Equipment via its radio interface to the operator's core network. H(e)NB accesses operator's network via Security Gateway (SeGW).

Security Gateway (SeGW)

A network element at the edge of the operator's core network terminating security association(s) for the backhaul link between H(e)NB and core network. SeGW represents operator's core network to perform mutual authentication with H(e)NB. After successful mutual authentication between the H(e)NB and the SeGW, the SeGW connects the H(e)NB to the operator's core network. Any connection between the H(e)NB and the core network is tunnelled through the SeGW.

H(e)NB Management System (H(e)MS)

This is a management server that configures the H(e)NB according to the operator's policy. H(e)MS is also capable of installing software updates on the H(e)NB. The H(e)MS server may be located inside the operator's core network (accessible on the MNO Intranet) or outside of it (accessible on the public Internet).

UE

Standard user equipment for UMTS (for HNB) or LTE (for HeNB)

H(e)NB Gateway (H(e)NB-GW) and MME

H(e)NB-GW serves as a concentrator for control plane traffic to/from multiple H(e)NBs over LuH interface. The H(e)NB-GW and the SeGW may be co-located. The HeNB-GW is optional, while the HNB-GW is mandatory. In the absence of a HeNB-GW, the HeNB is directly connected to the MME via the SeGW. HNB-GW is logically separate entities within operator's network.

AAA Server and HSS

HSS stores the subscription data and authentication information of the H(e)NBs. When hosting party authentication is required, AAA server authenticates the hosting party based on the authentication information retrieved from HSS

1.3 H(e)NB Security concerns

The threat model consists of attack threats from third parties that try to compromise the security of the communication links and from hosting parties that attack the H(e)NB devices themselves. The general security concerns/threats for any wireless network (node/device) and are also valid here for H(e)NB are listed below:

1.3.1 Compromise of H(e)NB credentials

The credentials used for securing the communication between H(e)NB and network can be compromised if the authentication algorithm/credentials used is weak which can be cracked by brute force attack OR through physical intrusion where H(e)NB authentication data is not stored in protected domain and can be read by the attacker through illegal means. Other possibility is if someone clones the authentication credentials and uses the same in illegal node (H(e)NB). This type of the attacks are avoided by using strong authentication algorithms/credentials (Refer mutual authentication chapter in the current paper) and storing authentication credentials/security data inside the secure domain (Refer Storage Environment chapter in the current paper where security data is stored in trusted environment TrE and Hosting party module)

1.3.2 Man-in-middle attacks

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

This kind of attack can happen when H(e)NB makes a first contact to the operator's network. During this contact, operator's endpoint cannot reliably identify the peer. An attacker on the internet can intercept all traffic from H(e)NB and later get access to all private information, impersonate the H(e)NB. These types of the attacks are avoided by using authentication credentials during the first point of contact with the network and these credentials shall be recognized by the operator. USIM or vendor certificates are used for this (Refer section Mutual authentication chapter in the current paper where certificate based device authentication and AKA based hosting party authentication is done to mitigate this risk).

1.3.3 Replay attacks

In this kind of attack, a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out by the attacker who intercepts the data and retransmits it. This is possible if the originator (H(e)NB) does not use unique authentication data and a session id which shall be incremented in every message communication with the peer. This kind of attacks are avoided by sending an incremental session id in the message/data communication so that receiver can know if this replayed or not (Refer Mutual

authentication chapter wherein the message exchange during device authentication or EAP-AKA based hosting party authentication involves the usage of incremental session id to avoid the replay attacks)

1.3.4 Denial of service attacks

This kind of attack is used by the attacker to deny the services to the genuine users. Attacker in this case keep on sending fake requests or data towards the destination forcing it to break down the link or to temporarily stop the service seeing the attack being planned. This kind of attack is avoided at H(e)NB by allowing only IKE negotiations and ESP-encrypted traffic using IKEv2 (Refer Mutual authentication chapter involving usage of IKEv2 protocol which is robust against the DoS attacks).

1.3.5 Eavesdropping

In case unprotected user data leaves the secure domain, this data is available for eavesdropping for the attacker. The same is the case of H(e)NB.

1.3.6 Masquerade

In this kind of attack, the attacker is able to configure the illegal H(e)NB such that users of a given CSG join it. The attacker buys an H(e)NB and configures it similar to that of an H(e)NB of a CSG. Having done that the attacker changes the setting in the H(e)NB to no encryption and integrity level or has access to the user keys in the H(e)NB. The attacker can do this by connecting the H(e)NB to the wired backbone of the H(e)NB provisioning company or use multi-hop solution to connect the H(e)NB to the valid one connected to the wired network. This kind of attack is avoided by hiding the CSG setting and other configuration. There should be binding between H(e)NBs and the users it can serve that should also be known by the network. The H(e)NB must be authenticated by the network.

1.4 Mitigation of H(e)NB security concerns/threats

The security concerns that are discussed in the previous chapter put certain requirements on the H(e)NB to mitigate the possible threats. These requirements can be summarized as below:

- Only algorithms of adequate cryptographic strength shall be used for authentication and protection of confidentiality and integrity
- Hosting Party controllable information shall be controlled by the operator
- IMSIs of users connected to H(e)NB shall not be revealed to the Hosting Party of the H(e)NB
- The integrity of the H(e)NB shall be validated before any connection into the core network is established.
- The H(e)NB shall be authenticated by the SeGW based on a globally unique and permanent H(e)NB identity (H(e)NB certificate)
- The H(e)NB shall authenticate the SeGW using SeGW certificate (signed by CA trusted by the operator)
- Optionally the hosting party of the H(e)NB may be authenticated by SeGW in co-operation with AAA server.
- The H(e)NB shall authenticate the H(e)MS, if the H(e)MS is accessed on the public Internet.
- The H(e)NB shall be authenticated by the H(e)MS using the same identity as for authentication to the SeGW, if the H(e)MS is accessed on the public Internet.
- The configuration and the software of the H(e)NB shall only be updated in a secure way, i.e. the integrity of the configuration data including the licensed radio parameters and the integrity of the software updates must be verified.
- Sensitive data including cryptographic keys, authentication credentials, user information, user plane data and control plane data shall not be accessible at the H(e)NB in plaintext to unauthorized access.
- The location of the H(e)NB shall be reliably transferred to the network.

- The H(e)NB shall be capable of filtering unauthenticated traffic received from the access network. Operator policy shall control which types of unauthenticated traffic are filtered.
- The H(e)NB shall authenticate the H(e)MS using H(e)MS certificate (signed by CA trusted by the operator) in case H(e)MS is accessible on MNO internet and vice versa.
- A secure backhaul link (between SeGW and core network) shall be established based on IKEv2 (with required authentications) and IPSec security based tunnel shall be used for the communication on the backhaul link.

1.5 H(e)NB Security Aspects

This chapter summarizes various security aspects that will be used at H(e)NB or on the interface between H(e)NB and SeGW/H(e)MS to take care of the security requirements listed above.

1.5.1 Storage Environment

Hosting Party Module (HPM -> similar to USIM for user authentication)

Hosting party is the party hosting the H(e)NB and having a contract with the PLMN operator. The Hosting Party authentication is based on a Hosting Party Module.

The Hosting Party Module (HPM) is a physical entity distinct from the H(e)NB physical equipment, dedicated to the identification and authentication of the Hosting Party towards the MNO (Mobile Network Operator). The HPM is a tamper resistant environment and contain the credentials used to authenticate the Hosting Party. The HPM is bound to the Hosting Party (e.g. by contractual agreement between Hosting Party and MNO) and supplied by the MNO to the Hosting Party. HPM is removable from the H(e)NB and this is possible for a Hosting Party to change the H(e)NB device by inserting the HPM in the new H(e)NB.

Trusted Environment (TrE)

The Trusted Environment (TrE) is a logical entity which provides a trustworthy environment for the execution of sensitive functions and the storage of sensitive security related data. All data produced through execution of functions within the TrE shall be unknowable to unauthorized external entities.

The TrE shall perform sensitive functions (such as storing private keys and providing cryptographic calculations using those private keys) needed for H(e)NB device authentication with the operator network

1.5.2 Device Integrity Check and Device validation

The H(e)NB and TrE performs a device integrity check upon booting and before connecting to the core network and/or to the H(e)MS. The device integrity check is performed based on one or more trusted reference value(s) and the TrE. The TrE should boot securely. The integrity of a component is verified by comparing the result of a measurement (typically a cryptographic hash) of the component to the trusted reference value. If these values agree, the component is successfully verified and can be started. For each of the component integrity checks, the TrE retrieves the corresponding trusted reference value from secure memory.

The integrity of the device is verified if all components necessary for trusted operation of the device are verified. If the device integrity check according to failed, the TrE does not give access to the sensitive functions using the private key needed for H(e)NB device authentication with the SeGW

1.5.3 Mutual Authentication

H(e)NB and SeGW are mutually authenticated before H(e)NB is allowed the network access. Two types of authentications are executed: mandatory device authentication and/or optional hosting party authentication.

Mutual device authentication

The mutual device authentication is mandatory for H(e)NB wherein H(e)NB and SeGW both need to authenticate each other. Device mutual authentication is performed using IKEv2 with public key signature based authentication with certificates (Refer Reference 2). The H(e)NB's credentials and critical security functions for device authentication need to be protected inside a TrE.

The H(e)NB is provisioned with a device certificate. This device certificate allows the authentication of the H(e)NB by the SeGW (and thus the operator network). The device certificate is provided by the operator, manufacturer, vendor of the H(e)NB, or by another party trusted by the operator.

The SeGW is also configured with a certificate. This certificate allows the authentication of the SeGW by H(e)NB. Again SeGW certificate is provided by an operator trusted CA.

A Fully Qualified Domain Name (FQDN) formatted identifier is used for certificate based authentication of the H(e)NB and of the SeGW. For the H(e)NB this FQDN needs to be globally unique. If no DNS is available for resolution of the FQDN of the SeGW, then the IP address of SeGW shall be used as identifier.

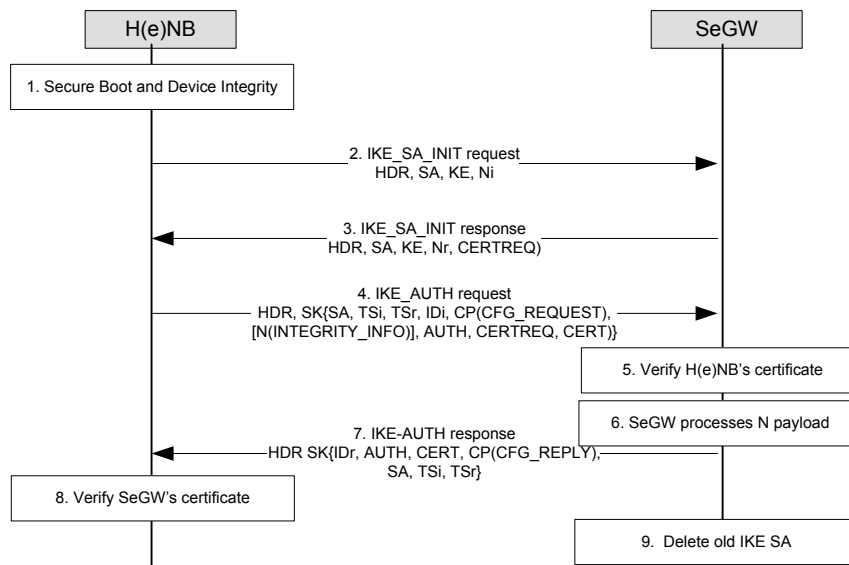
The H(e)NB may check the revocation status of certificates using OCSP (Refer Reference 7). The SeGW may check the revocation status of certificates using CRLs or OCSP.

The H(e)NB's TrE is used to provide the following critical security functions supporting the IKEv2 and certificate processes:

- The H(e)NB's identity stored in the TrE which shall not be modifiable
- The H(e)NB's private key stored in the TrE and shall not be exposed outside of the TrE
- The root certificate used to verify the signatures on the SeGW certificate stored in the H(e)NB's TrE and shall be writable by authorized access only. The verification process for signatures is performed by the H(e)NB's TrE
- The H(e)NB's TrE is used to compute the AUTH payload used during the IKE_AUTH request message exchanges

The H(e)NB needs to process SeGW certificate paths containing up to four certificates. The SeGW certificate and the intermediate CA certificates for the SeGW are obtained from the IKEv2 CERT payload. The certificates of the trusted root CA is obtained from the TrE of the H(e)NB. The H(e)NB checks the validity time of the SeGW certificates, and reject certificates that are either not yet valid or that are expired. In case the H(e)NB is configured to check the certificate revocation status of the SeGW certificate, and it receives no valid OCSP response, the H(e)NB aborts the IKEv2 protocol.

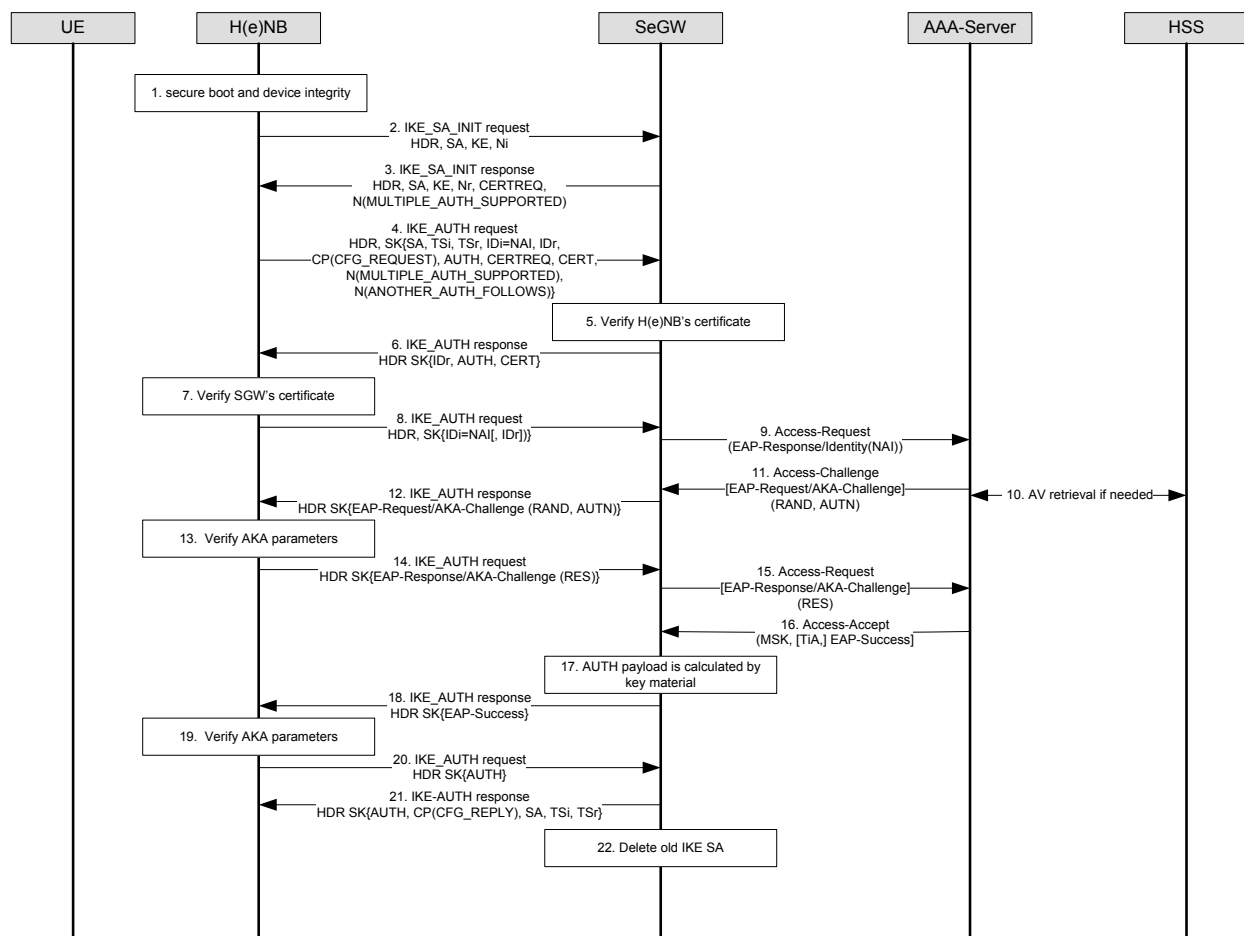
The SeGW need to process H(e)NB certificate in similar way as H(e)NB does. The SeGW checks the certificate revocation status if configured by local policy.



Mutual hosting party authentication

The hosting party mutual authentication is optionally performed by the operator's network following successful device mutual authentication.

An EAP-AKA based method is used for hosting party authentication. When Hosting Party Authentication is used, both device and hosting party authentication must be completed successfully before a secure tunnel to the operator network can be established. The authentication of the hosting party is based on credentials contained in a separate Hosting Party Module (HPM) in H(e)NB, and in the MNO HLR/HSS. An AKA credentials is stored in HPM enabling to use EAP-AKA. EAP authentication executes between H(e)NB and AAA server and the SeGW acts as EAP authenticator and forwards the EAP protocol messages to the AAA server to retrieve an authentication vector from AuC via HSS/HLR. A globally unique identifier in the format of an IMSI is used for EAP-AKA based authentication. These IMSIs are marked in HLR/HSS as used for H(e)NBs, e.g. by allocating dedicated ranges or by adding specific attributes to avoid misuse of these IMSIs for ordinary UEs.



1.5.4 IPsec tunnel establishment

The H(e)NB uses IKEv2 protocol to set up at least one IPsec tunnel to protect the traffic with SeGW, i.e. a pair of unidirectional SAs (Security Associations) between H(e)NB and SeGW. All signalling, user, and management plane traffic over the interface between H(e)NB and SeGW is sent through an IPsec ESP tunnel (with NAT-T UDP encapsulation as necessary) that is established as a result of the authentication procedure.

The H(e)NB initiates the creation of the SA i.e. it acts as initiator in the Traffic Selector negotiation. Upon H(e)NB's request, the SeGW allocates IP address to the H(e)NB after successful authentication. The H(e)NB and SeGW uses the IKEv2 mechanisms for detection of NAT, UDP encapsulation for NAT Traversal, H(e)NB initiated NAT keep-alive, IKEv2 SA and IPsec SA rekeying, and Dead Peer Detection (DPD).

During setup of the tunnel, the H(e)NB includes a list of supported ESP authentication transforms and ESP encryption transforms as part of the IKEv2 signalling. The SeGW selects an ESP authentication transform and an ESP encryption transform and signal this to the H(e)NB.

1.5.5 Security between H(e)NB and H(e)MS

In case that the H(e)MS is accessible on MNO Intranet, H(e)MS traffic can be protected through the support of one of the two security mechanisms determined by the Network Operator's Security Policies:

- H(e)MS traffic is protected in hop-by-hop way. H(e)MS traffic is protected by IPsec tunnel between H(e)NB and SeGW.

- H(e)MS traffic is protected end-to-end between the H(e)NB and the H(e)MS by utilizing TLS tunnel inside the IPsec Tunnel for additional end-to-end security. When TLS is performed between H(e)NB and H(e)MS, mutual authentication between H(e)NB and H(e)MS will be based on device certificate for the H(e)NB and network certificate for the H(e)MS. H(e)NB and H(e)MS may check the validity of the certificates.

In case that the H(e)MS is accessible on the public Internet, the H(e)MS is exposed to attackers located in insecure network. H(e)MS traffic is protected by TLS tunnel established between H(e)NB and H(e)MS. In this case, mutual authentication between H(e)NB and H(e)MS will be based on device certificate for the H(e)NB and network certificate for the H(e)MS. The H(e)NB verifies the H(e)MS identity by checking the subjectAltName field of the H(e)MS certificate against the name of the H(e)MS. The H(e)NB may check the revocation status of the H(e)MS certificate using OCSP. Support for OCSP is optional for the operator network. The H(e)NB should support OCSP

For the management of the H(e)NB by the H(e)MS, the CPE WAN Management Protocol TR-069 is used. H(e)NB utilizes this TR-069 method to download software from H(e)MS or a server.

1.6 Conclusions

The usage of security mechanisms including usage of Trusted Environment (to store all critical security related data), device integrity check, mutual authentication between H(e)NB and SeGW (certificate based using IKEv2 for device authentication and EAP-AKA based mutual hosting party authentication), mutual authentication between H(e)NB and H(e)MS (certificate based using TLS) and creation of secure IPsec based tunnel between H(e)NB and SeGW for transforming backhaul traffic has mitigated/avoided various security concerns /threats discussed in this paper.

2.0 REFERENCES

IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol"

IETF RFC 4739: "Multiple Authentication Exchanges in the Internet Key Exchange (IKEv2 Protocol", Nov 2006.

IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)"

3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

GPP TS 25.467: "UTRAN architecture for 3G Home Node B (HNB); Stage 2".

IETF RFC 2560: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP"

IETF RFC 4806: "Online Certificate Status Protocol (OCSP) Extensions to IKEv2"

IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

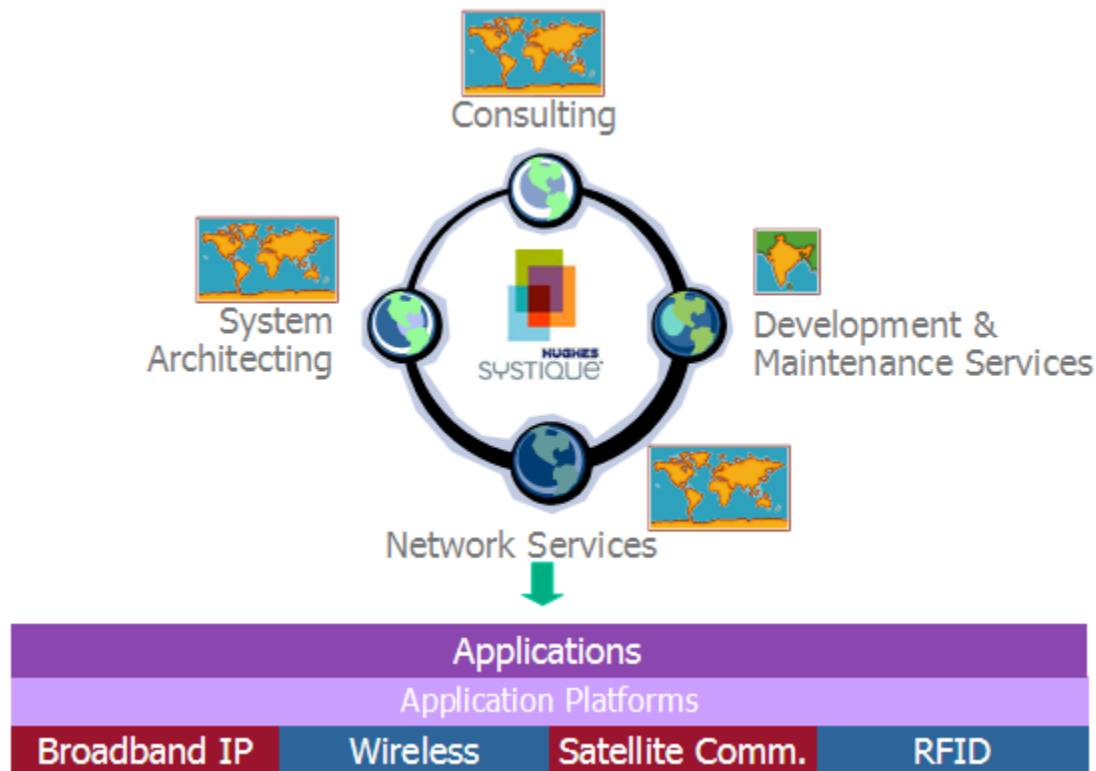
3GPP TS 33.102: "3G security; Security architecture"

3GPP TS 33.320: "Security of Home Node B (HNB)/Home evolved NodeB (HeNB) – Release 9"
The Broadband Forum TR-069: "CPE WAN Management Protocol v1.1", Issue 1 Amendment 2, December 2007

APPENDIX A ABOUT HUGHES SYSTIQUE CORPORATION

HUGHES Systique Corporation, part of the HUGHES group of companies, is a leading communications Consulting and Software company. We provide Consulting, Systems Architecture, and Software Engineering services to complement our client's in-house capabilities. Our "Best Shore" model coupled with an experienced management and technical team is capable of delivering a total solution to our clients, from development to deployment of complex systems, thus reducing time, risk and cost

HSC Solution Space:



CONTACT INFORMATION:

phone: +1.301.527.1629

fax: +1.301.527.1690

email: whitepaper@hsc.com

web: www.hsc.com

HSC Expertise Areas in Brief:



CONTACT INFORMATION:
 phone: +1.301.527.1629
 fax: +1.301.527.1690
 email: whitepaper@hsc.com
 web: www.hsc.com