ATIS-1000060.2014(R2019)

Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services

AMERICAN NATIONAL STANDARD FOR TELECOMMUNICATIONS

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

AMERICAN NATIONAL STANDARD

Approval of an American National Standard requires review by ANSI that the requirements for due process, consensus, and other criteria for approval have been met by the standards developer.

Consensus is established when, in the judgment of the ANSI Board of Standards Review, substantial agreement has been reached by directly and materially affected interests. Substantial agreement means much more than a simple majority, but not necessarily unanimity. Consensus requires that all views and objections be considered, and that a concerted effort be made towards their resolution.

The use of American National Standards is completely voluntary; their existence does not in any respect preclude anyone, whether he has approved the standards or not, from manufacturing, marketing, purchasing, or using products, processes, or procedures not conforming to the standards.

The American National Standards Institute does not develop standards and will in no circumstances give an interpretation of any American National Standard. Moreover, no person shall have the right or authority to issue an interpretation of an American National Standard in the name of the American National Standards Institute. Requests for interpretations should be addressed to the secretariat or sponsor whose name appears on the title page of this standard.

CAUTION NOTICE: This American National Standard may be revised or withdrawn at any time. The procedures of the American National Standards Institute require that action be taken periodically to reaffirm, revise, or withdraw this standard. Purchasers of American National Standards may receive current information on all standards by calling or writing the American National Standards Institute.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000060.2014(R2019), *Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services*

Is an American National Standard developed by the ATIS **Packet Technologies and Systems Committee (PTSC)**.

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000060.2014(R2019)

American National Standard for Telecommunications

Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services

Alliance for Telecommunications Industry Solutions

Approved **November 10, 2014**

(Republished April 2022 with an administrative edit)

American National Standards Institute, Inc.

Abstract

The integrity, confidentiality, and availability of Emergency Telecommunication Service (ETS) in a multi-provider Next Generation Network (NGN) environment will depend on the security of each individual network involved in an end-to-end communication. To allow network-provided security of end-to-end ETS communications in a multi-provider environment, intra-network domain and inter-network domain security requirements for ETS protection are needed. This ATIS standard provides a minimum set of requirements for the security protection of NS/EP NGN-PS in LTE Access Networks.

Foreword

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair [AT&T]

V. Shaikh, PTSC Vice-Chair [Applied Communication Sciences]

M Geller, PTSC-CSEC Chair [Cisco]

R. Singh, PTSC-CSEC Vice-Chair [Applied Communication Sciences]

M. Ghassemzadeh, Technical Editor [Applied Communication Sciences]

R. Singh, Technical Editor [Applied Communication Sciences]

The Cybersecurity [CSEC] Subcommittee was responsible for the development of this document.

Table of Contents

Table of Figures

Table of Tables

American National Standard on –

Emergency Telecommunications Service (ETS): Long Term Evolution (LTE) Access Network Security Requirements for National Security/Emergency Preparedness (NS/EP) Next Generation Network (NGN) Priority Services

1 Scope, Purpose, & Application

This document defines a minimum set of security requirements for the National Security and Emergency Preparedness (NS/EP) Next Generation Network Priority Services (NGN-PS) within the context of Long Term Evolution (LTE) access networks. They include requirements on the LTE functional components and interfaces and their interworking with the Circuit Switched (CS) technologies that Service Providers expect to use for voice communications[1] in the initial LTE deployments.

The purpose of this document is to provide a minimum set of security requirements for the security protection of NS/EP NGN-PS in LTE Access Networks. The requirements address the protection of the LTE priority features, capabilities, and procedures. Specifically, they address the problem of securing the advance priority features and special priority handling (referred to here, collectively, simply as special handling) that NS/EP NGN-PS messages will require as they transit the LTE Access Network[2] in support of priority communications. Without protection of the LTE special handling to provide priority treatment for NS/EP NGN-PS, the needs of the NS/EP community to respond effectively to crises could be hampered. The requirements focus on security protection against attacks that would compromise the integrity and availability of the LTE Access Network advance priority and special handing features. The requirements also address confidentiality protection of the Service User's private and sensitive information. This information, which might include location information or data that could reveal the user's identity, must be protected while it is in transit across the network and while it is being stored on various network entities.

The scope of this document includes (1) integrity and availability protection of the LTE advance priority features and the special handling functions and capabilities, including the scheduling mechanisms, (2) integrity and availability of NS/EP communications on the LTE Access Network segment, and (3) confidentiality protection of sensitive and private Service User data. The scope includes secure state transitions and mobility within a LTE provider domain; and security for transport of signaling and user data over LTE interfaces, the Management Plane, Supporting IP Services, and Circuit Switch Fallback (CSFB) Signaling for interworking with Universal Mobile Telecommunications System (UMTS) and Code Division Multiple Access (CDMA) Single Carrier Radio Transmission Technology (1xRTT).

The scope is restricted to security of NS/EP NGN-PS (i.e., NGN Government Emergency Telecommunications Services and Wireless Priority Services, abbreviated as GETS and WPS, respectively) as defined in [ATIS-1000057] that are specific to the LTE access network. The scope of this document is limited to priority voice services for non-roaming scenarios.

Figure 1.1 illustrates the approach used to define and organize the security requirements that address protection of NS/EP NGN-PS for the LTE Access Network. In this document, the LTE Access Network as defined in [3GPP TS 23.002] consists of the:

---

[1] NGN Service Providers have elected to reuse CS technology rather than an IMS solution for their initial voice communications solution. The 3GPP specification [TS 23.272] covers circuit switch fallback (CS-FB).

[2] This refers specifically to traversal over various LTE interfaces in order to securely establish bearer channels needed for priority communications.

- air interface,
- backhaul network, and
- packet core (Evolved Packet Core [EPC]).

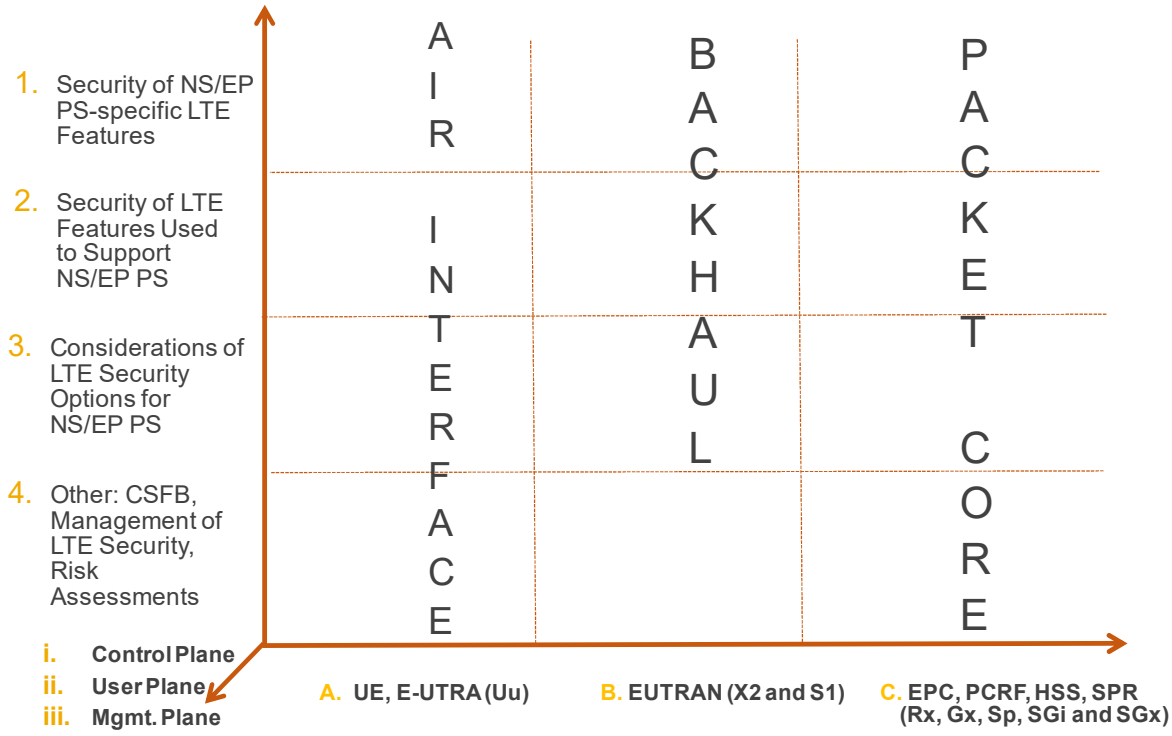

Figure 1. 1 - Approach

For each segment of the LTE Access Network Segments (A. Air Interface, B. Backhaul, and C. Packet Core) the security requirements cover the following four areas:

1. Security of LTE Features that are specific to NS/EP NGN-PS: confidentiality, integrity, and availability protection of features such as the advance priority features.
2. Security of LTE Features that support NS/EP NGN-PS: confidentiality, integrity, and availability protection of LTE functions and procedures used to support NS/EP NGN-PS (e.g., integrity protection of the special usage of call admission and other features that support NS/EP NGN-PS).
3. Consideration of LTE Security features critical to NS/EP NGN-PS: In cases where the LTE security specifications allow options, specific selections may be needed for NS/EP NGN-PS security.
4. Other: features and feature interworking, such as security of priority CSFB and management of LTE security and risk assessments that do not fit into the other categories.

For each of these four areas, the approach is extended through the user, management, and control planes, and when combined with the three network segments, constitutes three dimensions of coverage.

1.1 Relationship of Concepts & Terms

National Security/Emergency Preparedness Next Generation Network Priority Service (NS/EP NGN-PS), Legacy Government Emergency Telecommunication Service (GETS), and Wireless Priority Service (WPS)

are all facets of the U.S.A. instantiation of the international standard for ETS [E.107]. The relationship of the terms is portrayed in Figure 1.2. Refer to [ATIS-1000057] for more detail.

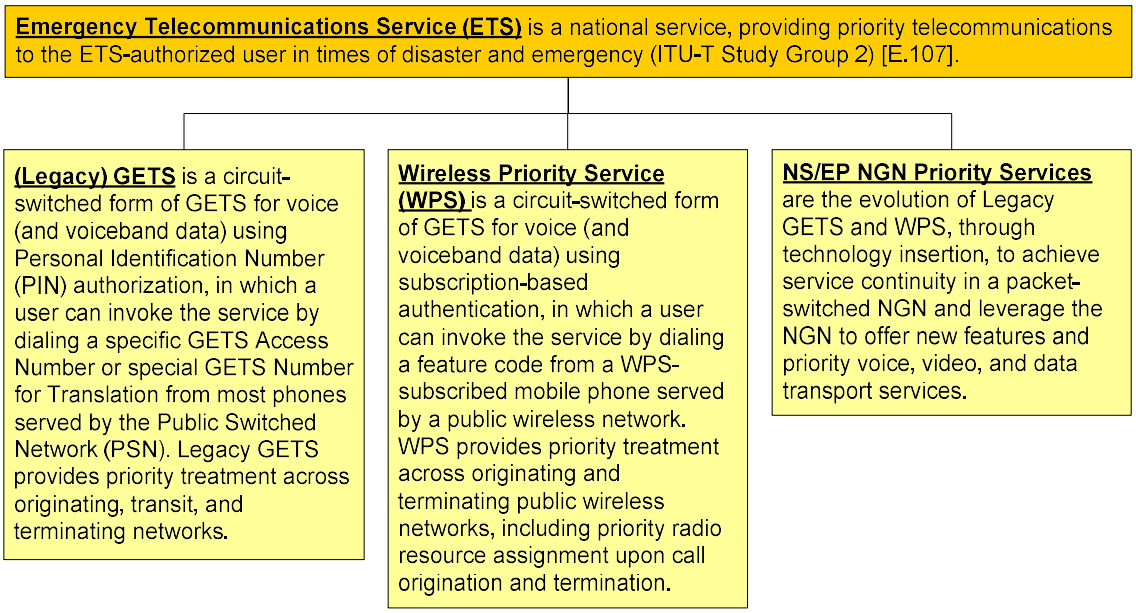

Figure 1. 2 - Relationship of Concepts and Terms

1.2 Requirement Labeling Conventions

This document distinguishes requirements and objectives from supporting text by the following convention:

- **Requirement** – Feature or function that is necessary to meet the needs of OEC/DHS. A Requirement contains the word “shall” and is identified by the letter “R”.
- **Conditional Requirement** – Feature or function that is necessary in specific applications to meet the needs of OEC/DHS . If OEC/DHS identifies a Conditional Requirement as necessary for a specific application, it shall be treated as a Requirement for the application. A Conditional Requirement contains the word “shall”, states the condition under which the defined capability applies, and is identified by the letters “CR”.
- **Objective** – Feature or function that is desirable and may be required by the OEC/DHS. An Objective contains the words “it is desirable” and is identified by letter “O”.

The intent of this presentation style is to improve the clarity, readability, and overall usefulness of the document.

1.3 Document Organization

This document is organized so that topics such as LTE infrastructure, LTE Intra E-UTRAN (Evolved UMTS Terrestrial Radio Access Network) mobility management, mobile-originating and mobile terminating call/session bearer priority treatments, and priority LTE Circuit-Switched Fallback to UMTS and to CDMA 1xRTT are given their own sections. The general layout is as follows:

- Introductory material, including the document scope, definitions of terms used throughout the document, and relevant technical descriptions and background.

- General security objectives that provide background and foundation for the requirements in this document.
- Topic-specific security requirements.
- Referenced documents and other source material.
- Acronyms used in this document.

1.4 Assumptions

It is assumed there are deployment scenarios where the LTE Access Network and the Core Network to which it is connected may be owned and operated by different service providers. This means the SGi interface may be intra-domain or inter-domain.

It is assumed that there might be deployment scenarios where the owner of the LTE access network equipment and facilities is different from the LTE wireless service provider (i.e., the wireless provider may lease LTE facilities from a facilities provider.)

It is assumed that the Service User has subscribed with a Service Provider for any combination of one or more of the NS/EP NGN-PS services, provided the Service User has a subscription with the Service Provider for the corresponding public services. Similarly, a Service User may access any NS/EP NGN-PS service for which he is authorized by the OEC/DHS from any normal public user device that is associated with a normal user subscription for the corresponding public service, even if there is no associated NS/EP NGN-PS subscription with the Service Provider, provided the Service User uses the proper OEC/DHS-assigned credentials when invoking the service.

It is assumed that the LTE-specific NS/EP NGN-PS features and capabilities for NS/EP NGN-PS subscribed UEs are within scope (e.g., LTE-specific Access Class Barring settings for NGN NS/EP NGN-PS configured in USIM are within scope).

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

2.1 ATIS References

[ATIS-1000057] ATIS-1000057, Service Requirements for Emergency Telecommunications Service (ETS) in Next Generation Network (NGN)[3]

[ATIS-0100523] ATIS-1000523, ATIS Telecom Glossary[4]

[ATIS-1000018] ATIS-1000018, NGN Architecture[5]

[3] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=28156 >

[4] http://www.atis.org/glossary/

[5] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=22964>

[ATIS-1000055] ATIS-1000055.2013, Emergency Telecommunications Service (ETS): Core Network Security Requirements[6]

[ATIS-0100009] ATIS-0100009.2006(R2011), Overview of Standards in Support of Emergency Telecommunications Service (ETS)[7]

2.2 ITU-T References[8]

[ITU-T X.800] ITU-T Recommendation 800, Security architecture for Open Systems Interconnection for CCITT applications

[ITU-T Y.2012] ITU Recommendation 2012, Functional Requirements and Architecture of Next Generation Networks

[ITU-T Y.2701] ITU-T Recommendation Y.2701, Security Requirements for NGN Release 1

2.3 IETF References[9]

[RFC 2401] RFC 2401, Security Architecture for the Internet Protocol

[RFC 2828] RFC 2828 Internet Security Glossary

2.4 3GPP References[10]

[TR 21.905] 3GPP TR 21.905 V10.2.0 (2010-03), Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 10). 3rd Generation Partnership Project

[TS 124 301] ETSI TS 124 301 V8.3.0 (2009-09), Universal Mobile Telecommunications System (UMTS); LTE; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301 version 8.3.0 Release 8). 3rd Generation Partnership Project.

[TS 22.011] 3GPP TS 22.153 V9.4.0 (2010-06), Technical Specification Group Services and System Aspects; Service accessibility (Release 9). 3rd Generation Partnership Project

[TS 23.002] 3GPP TS 23.002 V10.2.0 (2011-03), Technical Specification Group Services and System Aspects; Network architecture (Release 10). 3rd Generation Partnership Project

[TS 23.401] 3GPP TS 23.401 V10.7.0 (2012-03), Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) Access (Release 10). 3rd Generation Partnership Project

[TS 23.402] 3GPP TS 23.402 V10.7.0 (2012-03), Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP Accesses (Release 10). 3rd Generation Partnership Project

[TS 24.301] 3GPP TS 24.301 V8.1.0 (2009-03), Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (Release 8). 3rd Generation Partnership Project

---

[6] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=28147 >

[7] This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) at < https://www.atis.org/docstore/product.aspx?id=25486 >

[8] This document is available from the International Telecommunications Union. < http://www.itu.int/ITU-T/ >

[9] This document is available from the Internet Engineering Task Force (IETF). < http://www.ietf.org >

[10] This document is available from the Third Generation Partnership Project (3GPP) at < http://www.3gpp.org/specs/specs.htm >.

[TS 32.372] 3GPP TS 32.372 V9.0.0 (2009-12), Technical Specification Group Services and System Aspects; Telecommunication Management; Security services for Integration Reference Points (IRP); Information Service (IS) (Release 9). 3rd Generation Partnership Project

[TS 33.102] 3GPP TS 33.102 V10.0.0 (2010-12), Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 10). 3rd Generation Partnership Project.

[TS 33.210] 3GPP TS 33.210 V9.0.0 (2009-12). Technical Specification Group Services and System Aspects; 3G Security; Network Domain Security; IP Network Layer Security (Release 9). 3rd Generation Partnership Project

[TS 33.220] 3GPP TS 33.220 V10.1.0 (2012-03). Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); generic Bootstrapping Architecture (GBA) (Release 10). 3rd Generation Partnership Project

[TS 33.221] 3GPP TS 33.221 V10.0.0 (2011-03). Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates (Release 10). 3rd Generation Partnership Project

[TS 33.310] 3GPP TS 33.310 V11.1.0 (2012-09), Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF) (Release 11). 3rd Generation Partnership Project

[TS 33.401] 3GPP TS 33.401 V10.2.0 (2011-09), Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security Architecture (Release 10). 3rd Generation Partnership Project

[TS 36.331] 3GPP TS 36.331 V8.2.0 (2008-05), Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) Radio Resource Control (RRC); Protocol Specification (Release 8). 3rd Generation Partnership Project

[TS 36.423] 3GPP TS 36.423 V8.0.0 (2007-12), Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access Network (EUTRAN); X2 application protocol (X2AP) (Release 8). 3rd Generation Partnership Project

2.5 3GPP2 References[11]

[X.S0057-0] 3GPP2 X.S0057-0. April, 2009. E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects, Version 1.0.

3 Definitions, Acronyms, & Abbreviations

3.1 Definitions and Terminology

3.1.1 Security Services Definitions

3.1.1.1 Access control [RFC 2828]: Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy.

3.1.1.2 Authentication: The process of verifying the claimed identity of an entity (e.g., User Equipment, Service User, Service Provider, or other data source).

3.1.1.3 Authorization: A process of granting an authenticated entity (e.g., User Equipment, Service User, or Service Provider) access to a service or resource based on access rights and privileges.

3.1.1.4 Availability [RFC 2828]: The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the

system; i.e., a system is available if it provides services according to the system design whenever users request them.

3.1.1.5 Confidentiality [TS 33.210]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.1.6 Data Integrity [TS 33.210]: The property that data has not been altered in an unauthorized manner.

3.1.1.7 Integrity: See Data Integrity and System Integrity.

3.1.1.8 System Integrity [RFC 2828]: The quality that a system has when it can perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation.

3.1.2 Security Threats, Definitions, & Descriptions

3.1.2.1 Security: A term that refers to measures, procedures, processes, and tools that minimize the vulnerabilities and exploitation of weakness of assets and resources. An asset is anything of value.

3.1.2.2 Security compromise: Any action or event (intended or unintended) that alters the integrity or causes availability interruption of network element, system, function, procedure, protocol facility, or service as a result of exploitation of a security threat; or unauthorized disclosure of information.

3.1.2.3 Vulnerability: Any weakness that could be exploited to violate the integrity of a system or the information it contains.

3.1.2.4 Threat [ITU-T X.800]: A potential violation of security.

Example threats to a communication system include the following:

a) Destruction of information and/or other resources;
b) Corruption or modification of information;
c) Theft, removal, or loss of information and/or other resources;
d) Disclosure of information; and
e) Interruption of services.

3.1.3 Security Attack Descriptions

3.1.3.1 Masquerade [ITU-T X.800]: A masquerade is where an entity pretends to be a different entity. A masquerade is usually used with some other forms of active attack, especially replay and modification of messages. For instance, authentication sequences can be captured and replayed after a valid authentication sequence has taken place. An authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges.

3.1.3.2 Replay [ITU-T X.800]: A replay occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).

3.1.3.3 Rogue device: Term used to describe an unauthorized device connected to the network that poses security risks and threats. Rogue or misbehaving User Equipment (UE) attaching to the network could allow access-based threats.

3.1.3.4 Modification of messages [ITU-T X.800]: Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect, as when, for example, a message “Allow ‘John Smith’ to read confidential file ‘Accounts’” is changed to “Allow ‘Fred Brown’ to read confidential file ‘Accounts’”.

3.1.3.5 Denial of Service (DoS) [ITU-T X.800]: Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. The attack may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as the security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra

traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.

3.1.3.6 Insider attacks [ITU-T X.800]: Insider attacks occur when legitimate users of a system behave in unintended or unauthorized ways. Most known computer crime has involved insider attacks that compromised the security of the system.

> NOTE: For NS/EP NGN-PS, the term "legitimate users" in the definition applies to both the Service User (i.e., OEC/DHS employee or contractor responsible for operations procedures such as database updates) and the Service Provider employee (e.g., administrator).

3.1.3.7 Outsider attacks [ITU-T X.800]: Outsider attacks may use techniques such as:

a) Unauthorized wiretapping (active and passive);
b) Intercepting emissions;
c) Masquerading as authorized users of the system or as components of the system; and
d) Bypassing authentication or access control mechanisms.

3.1.3.8 Trapdoor [ITU-T X.800]: When an entity of a system is altered to allow an attacker to produce an unauthorized effect on command or at a predetermined event or sequence of events, the result is called a trapdoor. For example, a password validation could be modified so that, in addition to its normal effect, it also validates an attacker's password.

3.1.3.9 Trojan horse [ITU-T X.800]: When introduced to the system, a Trojan horse has an unauthorized function in addition to its authorized function. A relay that also copies messages to an unauthorized channel is a Trojan horse.

3.1.4 General NGN Definitions

3.1.4.1 Access Network: A set of equipment and facilities that connects a UE to a Core Network. An Access Network can include radio systems and controllers, Digital Subscriber Line (DSL), fiber and cable systems, loops, multiplexers, and routers.

3.1.4.2 Administrator: An individual (e.g., Service Provider employee, craft personnel, contractor, or other worker) authorized for accessing Network Elements (NEs) and support systems for Operations, Administration, and Maintenance (OA&M) purposes. Individual administrators are governed by the Service Provider privilege management policy assigning specific roles and access control privileges for OA&M purposes. "Administrator" is used in this document in place of the more common term, "user," to avoid confusion with service users; that is, callers, subscribers, Service Users, and any others who use the network in its capacity as a communications tool.

3.1.4.3 Core Network: A network infrastructure consisting of signaling and control elements, IP transport elements (such as high speed routers and border elements), and other network elements. The Core Network includes the policy and charging network element, e.g., a Policy and Charging Rules Function (PCRF). The Core Network provides connectivity to Access Networks of the same, or trusted, service provider and/or to other Core Networks of the same or other service providers. The Core Network does not include the Access Network.

3.1.4.4 Government Emergency Telecommunications Service (GETS): One facet of the U.S.A. instantiation of Emergency Telecommunications Service (ETS) using public telecommunications networks offered by OEC/DHS to authorized users for National Security and Emergency Preparedness (NS/EP) purposes. GETS is a circuit-switched form of ETS for voice (and voiceband data) using Personal Identification Number (PIN) authentication, in which a user can invoke the service by dialing a GETS-AN[11]

[11] GETS Access Number

or GETS-NT[12] from most phones served by the Public Switched Network (PSN). GETS provides priority treatment across originating, transit, and terminating networks.

3.1.4.5 Internet Protocol (IP) Multimedia Subsystem (IMS): An architecture specified by the Third Generation Partnership Project (3GPP) [TR 21.905] [TS 23.002] consisting of all Core Network elements to provide IP multimedia applications over IP.

3.1.4.6 IMS Core Network: The Core Network infrastructure of an IMS-based NGN consisting of all IMS elements, IP transport elements (such as high speed routers and border elements), and other network elements. An IMS Core Network supports various access technologies.

3.1.4.7 Network-to-Network Interface (NNI): The interface between two service provider networks or between two different technology domains within a service provider network, including all protocol levels.

3.1.4.8 Next Generation Network (NGN):A public telecommunications network based on Internet Protocol (IP) packet-switched technologies that is intended to augment and eventually replace the PSN. An NGN supports a broad mix of services including, but not limited to, voice services, video services, and data services.

3.1.4.9 NS/EP NGN Priority Services (NS/EP NGN-PS): The evolution of Legacy GETS and WPS to achieve service continuity in the packet-switched NGN and leverages the NGN to offer new features and priority multimedia services.

3.1.4.10 NS/EP NGN-PS call/session: A call/session related to NS/EP NGN-PS Voice, Video, or Guaranteed Bit Rate (GBR) Data service that traverses a Service Provider network.

3.1.4.11 Priority Treatment: Refers to mechanisms and features that support a greater probability of service success when NS/EP NGN-PS is invoked by a Service User.

3.1.4.12 Public Switched Network (PSN): A public telecommunications network (i.e., the Public Switched Telephone Network or a public wireless network) based on circuit-switched technologies that provides voice (and voiceband data) services.

3.1.4.13 Service: A telecommunications capability, provided to a user that can be accessed via a UE connected to a service provider's network. Examples of services include making a telephone call, or engaging in a video session, getting a map and directions from a server, or getting priority on establishment of a telephone call.

3.1.4.14 Service Provider (initial capital letters): A public telecommunications service provider authorized by OEC/DHS to provide NS/EP NGN-PS.

When "service provider" (without initial capital letters) is used, it refers to the normal provider of telecommunications services. For the purposes of this document, when Service Provider is used, it refers to an NS/EP NGN-PS Service Provider. When referring to offering Legacy GETS or WPS service, the term is modified as "Legacy GETS Service Provider" or "WPS Service Provider".

3.1.4.15 Service User (initial capital letters): An individual authorized by OEC/DHS to use ETS (Legacy GETS, WPS, or NS/EP NGN-PS) and to whom a user priority level assignment has been granted by OEC/DHS.

3.1.4.16 User Equipment (UE): A device allowing a user access to network services. For the purpose of this document, examples of a UE include a mobile station, a SIP phone, a notebook computer, a Personal Computer, an IP-based Private Branch eXchange (PBX), and an IP-based application server.

3.1.4.17 User-to-Network Interface (UNI): The interface between a UE and a service provider network, including all protocol levels.

[12] GETS Number Translation

3.1.5 LTE-Specific Definitions

3.1.5.1 Evolved Packet Core (EPC) [TR 21.905]: A framework for an evolution or migration of the 3GPP system to a higher-data-rate, lower-latency, packet-optimized system that supports multiple Radio Access Technologies.

3.1.5.2 Evolved Packet System (EPS) [TR 21.905]: An evolution of the 3G UMTS characterized by a higher-data-rate, lower-latency, packet-optimized system that supports multiple Radio Access Technologies. The Evolved Packet System comprises the Evolved Packet Core together with the evolved radio access network.

3.1.5.3 Evolved UTRAN (E-UTRAN) [TR 21.905]: An evolution of the 3G UMTS radio access network towards a high-data-rate, low-latency, and packet-optimized radio access network.

3.1.5.4 Globally Unique Temporary Identifier (GUTI): An identifier allocated to UE by the Mobility Management Entity (MME).

3.1.5.5 Non-Access Stratum (NAS) [TR 21.905]: Refers to protocols between UE and the core network that are not terminated in the UTRAN.

3.1.5.6 Universal Integrated Circuit Card (UICC) [TR 21.905]: A physically secure device, an integrated circuit card (or “smart card”), that can be inserted and removed from the terminal. It may contain one or more applications. One of the applications may be a Universal Subscriber Identity Module (USIM).

3.1.5.7 Universal Subscriber Identity Module (USIM) [TR 21.905]: An application residing on the UICC used for accessing services provided by mobile networks, which the application is able to register on with the appropriate security.

3.1.5.8 Za interface [TS 33.210]: The interface between Security Gateways (SEGs) belonging to different network/security domains.

3.1.5.9 Zb interface [TS 33.210]: The interface between SEGs and NEs and interface between NEs within the same network or security domain.

3.1.6 Other Descriptions

3.1.6.1 Application-to-Network Interface (ANI): An interface which provides a channel for interactions and exchanges between applications and network elements.

3.1.6.2 Authentication and Key Agreement (AKA): A security protocol that uses symmetric cryptography and a challenge-response procedure. A version known as EPS-AKA is used for 3GPP access (e.g., via an E-UTRAN).

3.1.6.3 Access Stratum: A sub-layer that is used for user plane and signaling exchanges between UE and the E-UTRAN. Access Stratum security mechanisms consist of integrity protection and ciphering of Radio Resource Control (RRC) signaling messages, and ciphering (but not integrity protection) of user data between the eNodeB and UE.

3.1.6.4 Evolved Node B (eNodeB): An LTE wireless communications station or base station.

3.1.6.5 evolved High Rate Packet Data (eHRPD) [X.S0057-0]: Network supports attachment to the EPC (evolved packet core) of 3GPP. The eHRPD network optionally supports seamless handoffs between E-UTRAN and evolved HRPD with single-radio terminals.

3.1.6.6 Extensible Authentication Protocol (EAP): A protocol that is used in a wide variety of applications, including (in LTE Access Networks) the bidirectional exchange of authentication messages between UE and the HRPD Serving Gateway (HSGW) for UE access to the EPC via an eHRPD network.

3.1.6.7 International Mobile Subscriber Identity (IMSI): A string of up to 15 decimal digits that identifies a unique mobile terminal or mobile subscriber. It consists of a 3-digit Mobile Country Code (MCC), a 2- or 3-digit Mobile Network Code (MNC), and a Mobile Subscriber Identification Number (MSIN) of up to 10 digits.

3.1.6.8 Long-Term Evolution (LTE): An industry term for one of the possible 4G wireless access technologies. An LTE Access Network (E-UTRAN) is all-IP and includes an air interface that is based on Orthogonal Frequency-Division Multiplexing. In addition, LTE interworks with a variety of other networks including IMS core, eHRPD (trusted non-3GPP access), and un-trusted non-3GPP IP access networks.

3.1.6.9 Message Authentication Code (MAC): A code computed by the serving network 3GPP Authentication, Authorization, and Accounting (AAA) server as part of the eHRPD authentication process.

3.1.6.10 Mobile Management Entity (MME): The primary signaling node in the evolved packet core. It is responsible for initiating paging and authentication of the mobile device, handling location information for each user, and choosing the right gateway during the initial registration process. The MME connects to eNodeBs through the S1-MME interface and connects to a Serving Gateway (S-GW) through the S11 interface.

3.1.6.11 Network Domain Security for IP-based protocols (NDS/IP) [TS 33.210]: A security architecture used for intra-domain and inter-domain communications in IP networks.

3.1.6.12 NS/EP NGN-PS Service: Provider is a Service Provider offering NGN Priority Services.

For purposes of this NS/EP NGN-PS security requirements document, an NS/EP NGN-PS Service Provider will be referred to as simply a Service Provider that offers at least one of the following services: NGN-PS Voice, NGN-PS Video, or NGN-PS Data Transport service.

3.1.6.13 Policy and Charging Control function encompasses the Policy and Charging Rule Function (PCRF), which makes policy decisions, and the Policy and Charging Enforcement Function (PCEF), which enforces policy decisions (under the control of the PCRF).

3.1.6.14 Packet Data Network Gateway (PDN-GW or P-GW or PGW): A Functional Element (FE) in the EPC that provides connectivity to/from external packet data networks and is responsible for anchoring the user plane for mobility between 3GPP and non-3GPP access networks.

3.1.6.15 Serving Gateway (S-GW): Routes and forwards user data packets. It serves as the mobility anchor for the user plane during inter-eNodeB handovers and between LTE and other 3GPP technologies. It manages and stores UE contexts and replicates the user traffic for lawful interception.

3.1.6.16 Serving Network Identifier (SN-ID): Required to be a Public Land Mobile Network (PLMN) ID (i.e., a combination of an MCC and an MNC).

3.1.6.17 Server-to-Network Interface (SNI): The instantiation of a reference point for interacting with service partners such as content providers, data information providers, and application service providers. SNI is used interchangeably with ANI when referencing a content provider partner.

3.2 Acronyms, Abbreviations, & Special Terms

1xRTT	Single Carrier Radio Transmission Technology
3GPP	3rd Generation Partnership Project
3GPP2	3rd Generation Partnership Project 2
AAA	Authentication, Authorization, and Accounting
ACB	Access Class Barring
ACL	Access Control List
AKA	Authentication and Key Agreement
ANI	Application Network Interface
AP	Application Protocol
ARP	Allocation and Retention Priority
AS	Access Stratum

AS	Application Server
ASME	Access Security Management Entity
AuC	Authentication Center
AVP	Attribute Value Pair
BS	Base Station
BSF	Bootstrapping Server Function
CDMA	Code Division Multiple Access
CK	Cipher Key
CM	Connection Management
COP	Committee of Principals
COW	Cell on Wheel
CS	Circuit Switched
CSCF	Call Session Control Function
CSD	Circuit-Switched Domain
DDoS	Distributed DoS
DHS	Department of Homeland Security
DiffServ	Differentiated Services
DN	Directory Number
DoS	Denial of Service
DPI	Deep Packet Inspection
DSCP	DiffServ Code Point
EAP	Extensible Authentication Protocol
ECM	EPS Connection Management
eCSCFB	evolved CSFB
eHRPD	evolved High Rate Packet Data
EMM	EPS Mobility Management
eNodeB	evolved NodeB
EPC	Evolved Packet Core
EPS	Evolved Packet System
ETS	Emergency Telecommunications Service
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
FE	Functional Element
GBR	Guaranteed Bit Rate
GETS	Government Emergency Telecommunication Service
GETS-AN	GETS-Access Number
GETS-FC	GETS-Feature Code
GETS-NT	GETS-Number Translation

GETS-PDN	GETS-Pseudo Destination Number
GIR	Government Industry Requirements
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
GTP-C	GPRS Tunneling Protocol for Control plane
GTP-U	GPRS Tunneling Protocol for User plane
GTPv1-U	GPRS Tunneling Protocol version 1 for User plane
GTPv2-C	GPRS Tunneling Protocol version 2 for Control plane
GUTI	Globally Unique Temporary Identity
HO	Handover
hPCRF	home Policy and Charging Rules Function
HRPD	High Rate Packet Data
HSGW	eHRPD Serving Gateway
HSS	Home Subscriber Server
IAM	Initial Address Message
IDS	Intrusion Detection System
IE	Information Element
IK	Integrity Key
IKE	Internet key Exchange
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	Internet Protocol security
IPv6	IP version 6
IR	Industry Requirements
IRP	Integration Reference Point
IS	Information Service
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
ITU	International Telecommunication Union
ITU-T	ITU – Telecommunication Standardization Sector
IWS	Interworking Solution

K	(Permanent Master) Key[13]
LMA	Local Mobility Anchor
LTE	Long Term Evolution
MAC	Medium Access Control
MAC	Message Authentication Code
MAG	Mobile Access Gateway
MCC	Mobile Country Code
MDM	Mobile Device Management
MME	Mobility Management Entity
MNC	Mobile Network Code
MO	Mobile Originating (call)
MPS-CS	Multimedia Priority Service - Circuit Switched
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
MT	Mobile Terminating (call)
NANP	North American Numbering Plan
NAS	Non Access Stratum
NCS	National Communications System
NDS	Network Domain Security
NE	Network Element
NGN	Next Generation Network
NNI	Network-to-Network Interface
NPA	Numbering Plan Area
NS/EP	National Security and Emergency Preparedness
OA&M	Operations, Administration, and Maintenance
OEC	Office of Emergency Communications
PBX	Private Branch Exchange
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PDCP	Packet Data Convergence Protocol
PDN	Packet Data Network
PDN-GW	PDN Gateway (also referred to in some documents as a P-GW or PGW)
PIN	Personal Identification Number

[13] The term Master can be interpreted to have unfortunate connotations in current usage. This terminology has been used in the approved IETF References and is being retained solely to assist the reader in understanding the principles and when referring to the referenced text.

PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PMIP	Proxy Mobile IP
PMIPv6	Proxy Mobile IPv6
PS	Priority Services
PSN	Public Switched Network
PSTN	Public Switched Telephone Network
PSWG	Priority Services Working Group
QCI	QoS Class Identifier
QoS	Quality of Service
RACF	Resource and Admission Control Functions
RACH	Random Access Channel
RAN	Radio Access Network
RFC	Request For Comment
RLC	Radio Link Control
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RRC	Radio Resource Control
SAE	System Architecture Evolution
SEG	Security Gateway
SGSN	Serving GPRS Support Node
S-GW	Serving Gateway
SIB	System Information Block
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SNI	Server-to-Network Interface
SN-ID	Serving Network Identifier
SN-MME	Serving Network MME
SP	Service Provider
SPR	Subscriber Profile Repository
SRAS	Special Routing Arrangement Service
SRB	Signaling Radio Bearer
SS7	Signaling System 7
S-TMSI	SAE-TMSI
TAU	Tracking Area Update
TMSI	Temporary Mobile Subscriber Identity

TS	Technical Specification
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
UNI	User-to-Network Interface
UP	User Plane
USIM	Universal Subscriber Identity Module
UTRAN	Universal Terrestrial Radio Access Network
VoIP	Voice over Internet Protocol
vPCRF	visited Policy and Charging Rules Function
WPS	Wireless Priority Service

4 Architecture & Procedures

4.1 Conceptual Access Network Functions within an NGN

Next Generation Networks support multiple fixed (e.g., xDSL, Cable, and Optical Fiber) and wireless (e.g., wireless local area networks, WiMax, 3G and 4G Radio Access Networks) access technologies.

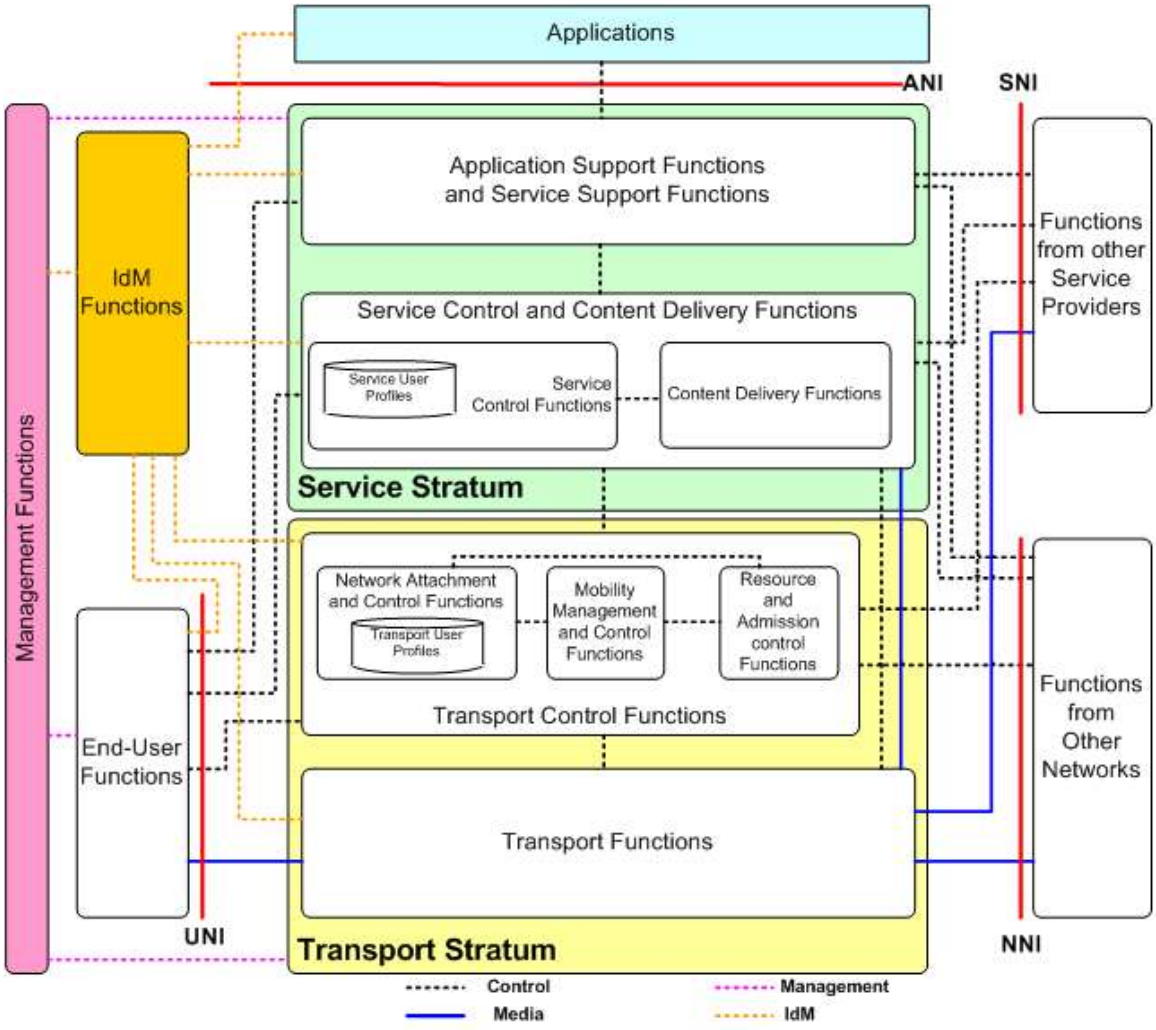

Figure 4. 1 - NGN Logical Architecture Overview (From Figure 1/ATIS-100018 and Figure 1 of ITU-T Y.2012)

Figure 4.1 shows the high-level NGN Logical Architecture as specified in [ATIS-100018] and [ITU-T Y.2012]. It illustrates that an NGN Architecture consists of three general purpose NGN reference points: the UNI, NNI, and the ANI; each of which can be mapped to specific physical and logical interfaces (e.g., the UNI is mapped to the EPS[14] LTE-Uu or IMS Core Gm interface). It also consists of two strata: a Transport stratum and a Service stratum.

The Transport stratum provides IP connectivity services to the NGN users (e.g., LTE bearer establishment) under the control of transport control functions (e.g., LTE Evolved Packet Core (EPC)) such as the network attachment control functions, the resource and admission control functions (RACF), and mobility management and control functions.

- The Resource and Admission Control Functions (RACFs) act as the arbitrators between service control functions and transport functions for admission control and Quality of Service (QoS). The RACFs (i.e., PCRF) perform policy-based transport resource control.
- The network attachment control functions provide registration at the access level and initialization of end-user functions for accessing NGN services. These functions provide transport stratum level

[14] Evolved Packet Systems

identification and authentication, manage the IP address space of the access network, and authenticate access sessions.

- The mobility management and control functions support IP-based mobility in the transport stratum (e.g., Intra E-UTRAN Handover).

The Service stratum provides functions that operate above the IP layer. This abstract representation of the functional grouping in the service stratum consists of the service control and content delivery functions including service user profile functions, and the application support functions and service support functions.

The Transport and Service strata are supported by management functions, shown at the left of Figure 4.1. Management Functions interact with the Service and Transport Strata directly and indirectly through End-User Functions (e.g., Over the Air Mobile Device Management for wireless devices) and Identity Management (IdM) functions.

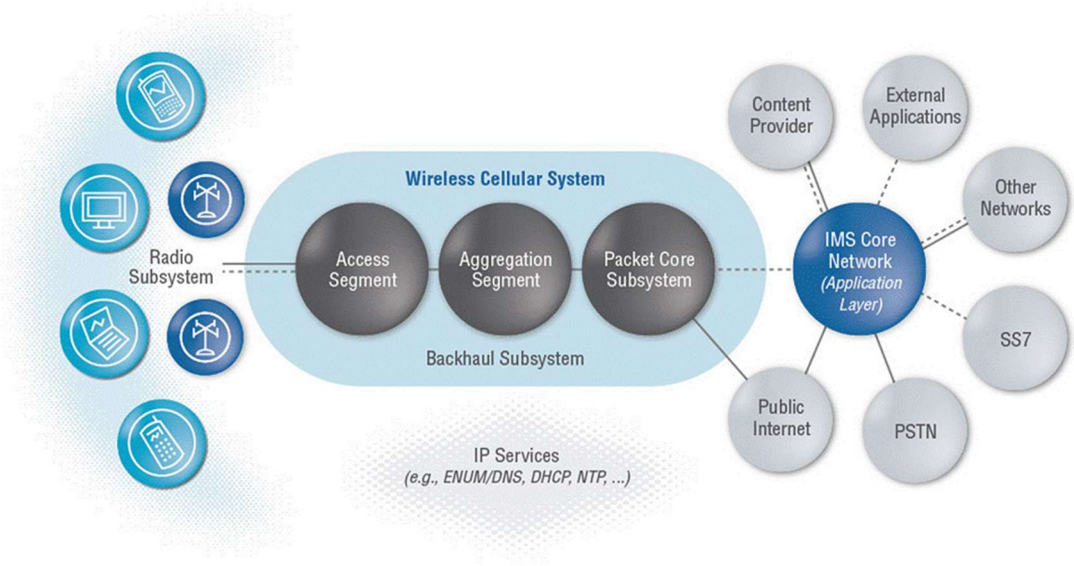

Figure 4. 2 - Generic Wireless Access Network Architecture and Interconnections

In context of the broader NGN from Figure 4.1, the Wireless Access Network has three main segments: a radio segment, a backhaul segment (which further consists of access segments and aggregation segments)[15], and a packet core segment, as shown in Figure 4.2.

Cellular radio traffic coming from cell phones and other UE enters the Access Segment of the Backhaul Subsystem at the cellular site. There, lower level traffic aggregation (multiplexing) is performed and then handed off to the access aggregation point. The traffic then enters the Aggregation Segment. Aggregated cellular traffic exits the Aggregation Segment and enters the Packet Core Subsystem at an access gateway (e.g., LTE S-GW). The generic cellular Wireless Access Network architecture shown in Figure 4.2 represents a generic architectural view independent of the specific wireless technology.

[15] Wireless Access Network backhaul segments may be administered by different service provider domains.

4.1.1 LTE Access Network Architecture

As stated in the Scope section, the discussion of the LTE Access Network architecture is restricted to the non-roaming reference architecture for 3GPP access. The Wireless Access network (Figure 4.2) specific to the LTE non-roaming reference architecture for 3GPP Access is shown in Figure 4.3. It shows endpoints and the specific set of Functional Entities (Fes) and FE interfaces that are considered for the NS/EP LTE Access Network security requirements of the NS/EP NGN-PS. These FEs and FE interfaces belong to the radio subsystem (UE's LTE-Uu termination), backhaul subsystem (eNodeBs), and packet core (LTE EPC) shown in Figure 4.2.

4.1.2 Non-Roaming Reference Architecture

The non-roaming reference architecture for 3GPP Access is shown in Figure 4.3. It is based on Figure 4.2.1-1 of [TS 23.401]. The Gxc[16] Interface is present only when S5 is Proxy Mobile Internet Protocol (PMIP)-based rather than General Packet Radio Service (GPRS) Tunneling Protocol (GTP)-based.

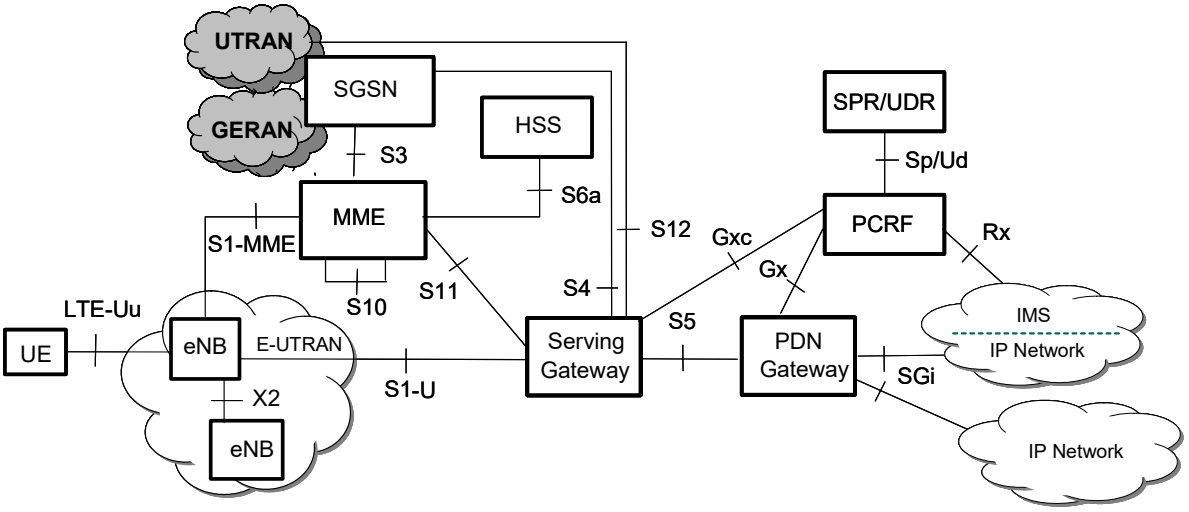

Figure 4. 3 - Non-Roaming Reference Architecture for 3GPP Access.

Figure 4.4 illustrates a more precise architecture diagram for the security requirement work which is based on Figure 4.3 but excludes S3, S4, and S12 interfaces to UTRAN because LTE interworking with other 3GPP access technologies is out of scope of this document.

[16] The LTE Architecture is rife with obscure-sounding interfaces with names such as Gxc, X2, SGi, and so on. Most of these interfaces are described briefly in Table 2 of this document.

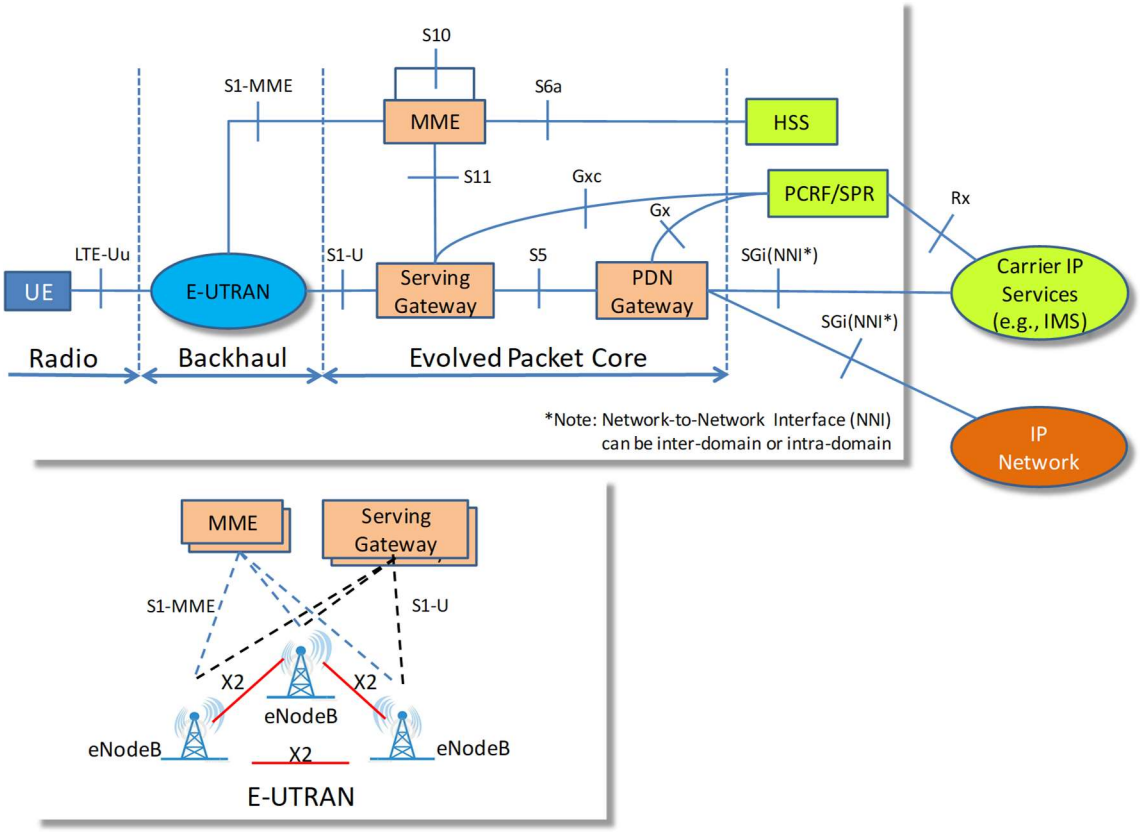

Figure 4. 4 - LTE Access Network Architecture

Table 4.1 provides a high-level description of the LTE-specific FEs and their specific LTE Access Network NS/EP NGN-PS priority functions and mechanisms including the FEs involved in CSFB. The purpose of Table 1 is to identify the priority services specific functions and mechanisms that have to be integrity and availability protected.

Table 4. 1 - LTE Functional Entities

Functional Element	Subsystem	Description/Functions
UE	Device	A device that provides the interface between the user and the LTE Access Network (via the LTE air interface).
eNodeB	E-UTRAN	Is responsible for such functions as radio resource management, admission control, IP header compression, paging, MME selection, user plane ciphering, and priority marking of packets in the uplink (e.g., setting DSCP based on QCI[17]). eNodeB FE performs both UMTS Node-B and radio network controller (RNC) functions. Planned eNodeB-specific LTE Access Network NS/EP NGN-PS priority mechanisms may include dynamic control of Access Class Barring, initial radio layers (RRC Connection Establishment) special treatment for mobile initiated transmissions and for priority bearer establishment during intra E-UTRAN handover procedure, and priority paging.
MME	EPC	Performs mobility management and connection management functions for UE (e.g., generates temporary identifiers to UE and initiates paging messages to UEs via eNodeBs), authentication/authorization, NAS signaling security, NAS level congestion control, EPS bearer connection establishment, and S-GW and PDN-GW selection. Planned MME-specific LTE Access Network NS/EP NGN-PS priority mechanisms may include subscription-based priority handling when "highPriorityAccess" Establishment Cause is delivered to an MME from eNodeB, establishing paging priority, handling messages with priority, and exemptions to overload control.
S-GW	EPC	Supports user plane connectivity between the E-UTRAN and the EPC, routes and forwards user plane packets, and serves as the user plane mobility anchor for intra E-UTRAN handovers, the anchor for mobility between LTE and other 3GPP technologies, and the Mobile Access Gateway (MAG) for PMIPv6[18]. It performs dynamic policy PCEF function for PMIPv6. Planned S-GW-specific LTE Access Network NS/EP NGN-PS priority mechanisms may include delivery of NS/EP NGN-PS priority indication in the message triggering the Paging Procedure by inclusion of appropriate priority marking.
PDN-GW	EPC	Supports user plane connectivity between the EPC and external packet networks. UE may be connected to more than one PDN-GW. For PMIPv6 mobility management. It performs the Local Mobility Anchor (LMA) function and performs dynamic policy PCEF function for GTP-based S5/S8. Planned PDN-GW-specific LTE Access Network NS/EP NGN-PS priority mechanisms may include delivery of NS/EP NGN-PS priority indication during bearer establishment by inclusion of appropriate priority marking.

[17] Quality of Service (QoS) Class Identifier.

[18] Proxy Mobile IPv6.

Functional Element	Subsystem	Description/Functions
PCRF	EPC or IMS	Supports policy control decisions for the IP-Connectivity Access Network (IP-CAN) and data/media flow-based charging control functions. In addition to invocation-based dedicated bearer establishment and release with priority treatment to support application requests for mobile originated SIP call/sessions and for mobile terminated SIP call/sessions, planned PCRF-specific LTE Access Network NS/EP NGN-PS priority mechanisms may include subscription-based Advance Priority-SPR[19] for Default Bearer and IMS Signaling Bearers establishment. (Note that in roaming scenarios, the PCRF in the visited network is referred to as a "vPCRF" and the PCRF in the home network is referred to as an "hPCRF".)
HSS	EPC or IMS	Stores static and dynamic information about a subscriber, including a list of features and services associated with that subscriber, and the subscriber's location and means of access. In addition, a Home Subscriber Server (HSS) keeps information for registration and authentication of mobile devices. Planned HSS-specific LTE Access Network NS/EP NGN-PS priority subscription parameters may include the MPS-EPS-Priority.
P-CSCF[20]	IMS	Supports interfaces between the IMS core (visiting or home network) and various access networks (e.g., LTE Access Networks) (see Figure 4.3) for specific interfaces).
SEG	Any	An entity on the border of an IP security domain that will be used for securing native IP-based protocols.
SPR	EPC or IMS	Provides PCRF with subscription information related to the IP-CAN transport-level policies based on a subscriber ID (e.g., an IMSI), a PDN identifier and possible further IP-CAN session attributes, and notifies the PCRF when the subscription information has been changed (if the PCRF has requested such notifications).
UMTS MSC	UMTS CSD[21]	CSFB-capable Mobile Switching Center (MSC) that supports the SGs interface for exchange of CSFB signaling with MME in EPS. Mobility management is shared between UMTS MSC and MME across SGs using the SGs Application Part protocol.
UMTS SGSN	UMTS PSD	The UMTS SGSN (Serving GPRS Support Node), specifically the chosen S4 SGSN configuration, supports the S3 interface to MME for data session establishment and for handover signaling procedure. The 3GPP Release 8 SGSN provides signaling for mobility with E-UTRAN 3GPP and with other 3GPP access networks. S4 SGSN is relevant to the CSFB to UMTS for the PS Handover scenario.
UTRAN RNS	UMTS CSD	The Radio Network Subsystem (RNS) provides radio subsystem functions in the UMTS and includes one or more base stations (NodeBs) and a RNC. The RNS interfaces to the MSC using the Iu interface.
1x MSC	1xRTT CSD	1x Mobile Switching Center (MSC). The 1X circuit-switched MSC provides processing, control, and bearer path for calls and services. The MSC provides signaling capability via a Signaling System #7 (SS7)-based connection to the Base Station (BS) on the A1 interface and bearer paths via terrestrial circuits on the A2 and A5 interfaces.

[19] Subscriber Profile Repository.

[20] Proxy CSCF.

[21] Circuit-Switched Domain.

Functional Element	Subsystem	Description/Functions
1x IWS	1xRTT CSD	1x Interworking Solution (IWS) or the 3GPP2 IWS Function implements the necessary functionality needed in the cdma2000 network for signaling support to the eHRPD interworking solution and to the E-UTRAN to cdma2000 1x CSFB and Single Radio Voice Connection Continuity solutions.

Table 4.2 briefly describes the LTE interfaces that are considered in scope of this document. This table describes groups of interfaces sharing similar characteristics and profiles in terms of the user, control, and management planes; inter- and intra-domain connections; and protocol mechanisms.

The FE end-points and their communication interfaces provide integrity and availability protection to the processes and protocol mechanisms used to support priority treatment in the LTE Access Network; for example, integrity and availability protection of the process to identify priority traffic, generating the appropriate markings (e.g., Diffserv code points), and integrity protection during transport. The need for these functions depends on the interface profiles and message types (e.g., GTP-U messages) carried over a bearer designated with parameters (e.g., ARP[22]/QCI) for NS/EP NGN-PS.

[22] Allocation and Retention Priority

Table 4. 2 - LTE Interfaces (In Scope)

Interface	Domain	Plane	Protocols
S6a, Gx, Gxc, Rx, Sp, Ud	Intra	Control	Diameter/SCTP[23]/IP or Diameter/TCP[24]/IP (not yet specified, in the case of the Sp or Ud interfaces)
S6a, Rx	Inter	Control	Diameter/SCTP/IP or Diameter/TCP/IP
GTP-based S5	Intra	Control; User	GTP/UDP[25]/IP; (payload)/GTP[26]/UDP/IP
PMIP-based S5	Intra	Control; User	PMIPv6/IPv6/UDP/IPv4 or PMIPv6/IPv6; IP/GRE[27]/IP
GTP-based S8	Inter	Control; User	GTP/UDP/IP; (payload)/GTP/UDP/IP
PMIP-based S8	Inter	Control; User	PMIPv6/IPv6/UDP/IPv4 or PMIPv6/IPv6; IP/GRE/IP
S10	Intra/Inter	Control	GTP/UDP/IP
S11	Intra	Control	GTP/UDP/IP
S1-MME	Intra	Control	S1-AP/SCTP/IP
X2-C	Intra	Control	X2-AP/SCTP/IP
S1-M	Intra	Management	Not specified
X2-U, S1-U	Intra	User	Payload/GTP/UDP/IP
SGi	Intra/Inter	User	IP
LTE-Uu	Intra	Control	RRC/PDCP/RLC/MAC[28]/L1
LTE-Uu	Intra	User	Payload/IP/PDCP/RLC/MAC/L1
Sp	Intra	Control	Not yet defined, but likely to be Diameter/SCTP/IP or Diameter/TCP/IP
SGs	Intra	Control	SGsAP/SCTP/IP
S102	Intra	Control	GCSNA/UDP/IP
S3	Intra	Control	GTPv2-C/UDP/IP

4.1.3 LTE Procedures Relevant to NS/EP NGN-PS

LTE Access Network Mobile Originating (MO) and Mobile Terminating (MT) call/session flows are based on a collection of LTE procedures. The entire set of LTE procedures is described in [TS 23.401] and [TS 23.402]. Several major procedures that are used in the MO/MT flows are described briefly below and shown in Figure 4.5 and Figure 4.6. Note that in some cases a procedure may contain one or more other procedures.

[23] Stream Control Transmission Protocol.

[24] Transmission Control Protocol.

[25] User Datagram Protocol.

[26] GPRS Tunneling Protocol.

[27] Generic Routing Encapsulation.

[28] Radio Link Control and Medium Access Control.

- The PHYSICAL, Medium Access Control, and RRC Connection Establishment (or simply RRC Connection Establishment) procedure involves the establishment of radio bearers such as Signaling Radio Bearer 1 (SRB1), SRB2, and one or more Data Radio Bearers between a UE and an eNodeB. This process, which occurs when a UE switches on, transitions the UE from the RRC state of RRC-IDLE to RRC-CONNECTED. A subscribed NS/EP UE is given special treatment for mobile initiated transmissions to gain prioritized access to the radio resources at times of congestion during the RRC Connection Establishment procedure.
- The Attach procedure is a mobility management procedure that allows a UE to register with the network and receive services that require registration. This procedure is performed after UE switches on and the RRC Connection Establishment procedure is completed. The Attach procedure also establishes a default bearer between the UE and the network for always-on IP connectivity. Advance priority may be established during the Attach procedure to give priority access to the Core IMS signaling for subscribed NS/EP UEs.
- The Tracking Area Update (TAU) procedure is a mobility management procedure that allows the Serving Network MME (SN-MME) to locate a UE in a tracking area or set of tracking areas. When a TAU occurs in which the “TAU Request” message includes the “active flag” set, the bearers are activated by the eNodeB with the priority appropriate for the designated parameter (i.e., ARP) for NS/EP NGN-PS.
- The Service Request procedure involves transitioning the EPS Mobility Management (EMM) mode from the EMM-IDLE to EMM-CONNECTED in order to allow application layer data to be sent (following establishment of the appropriate bearers).
- The SIP Session Establishment procedure is used to establish a voice session between a UE and another device. The procedure involves many phases of MO/MT signaling, including radio bearer establishment, SIP signaling over an IMS bearer, policy control interactions, and end-to-end bearer set up. The SIP Session Establishment procedure, as part of the call/session origination procedure for establishing an NS/EP NGN-PS call, creates a dedicated media bearer or modifies an existing media bearer.
- The Paging procedure is used to page a UE in idle mode and to establish signaling and bearer connections (e.g., to support incoming voice calls). Paging is usually triggered by downlink packets arriving at the S-GW in an MT flow. The Paging procedure is initiated by the network to request the UE to invoke the Service Request procedure for the transport of NAS signaling or Application Layer data, or to prompt the UE to reattach as a result of a network failure. Paging procedure for the NS/EP NGN-PS priority treatment is conveyed from the S-GW to the MME with priority appropriate for the designated parameter (i.e., ARP) for NS/EP NGN-PS.
- The Handover procedure allows UEs in the ECM[29]-Connected states to modify their bearer connections when their location changes and their radio measurements indicate the need to change connection to a new cell. The LTE handover can occur internally within the same LTE network (which means handover happens between eNodeB FEs), between different LTE networks or between LTE and legacy 2G/3G networks (e.g., UMTS).
- The Detach procedure is used to remove bearers and clear states in the network when the UE is powered down or when requested by the network (e.g., due to the UE not responding to a TAU because it is out of coverage). From an NS/EP context, this procedure is important to free up resources.

The exact sequence of the above procedures used in an MO/MT call/sessions flow varies depending on the state of the UE and the network, and the services being invoked.

Figure 4.5 illustrates typical sequences of the LTE procedures occurring in support of SIP Mobile Originating Call/Sessions for a subscribed UE. When the user switches on the UE, RRC Connection Establishment procedure establishes RRC communication by performing RRC signaling between the UE and eNodeB. This is followed by the NAS Attach Request from the UE to the eNodeB, which the eNodeB forwards to the MME. The authentication procedure is performed between UE, MME, and HSS as part of the Attach

[29] EPS Connection Management

procedure unless a context between the UE and the network already exists. The LTE Attach procedure sets up a default bearer that is a user plane connection between the UE and the PDN-GW. As part of this procedure, the UE receives an IP address. The mobility management Tracking Area Update procedure signaling (not shown in Figure 5) occurs when there is physical movement of UEs between Tracking Areas. It could also occur periodically based on the operator policy for the network to keep track of the mobility of the UE. The Service Request procedure is needed when the UE transitions to EMM-IDLE after a period of bearer inactivity (i.e., UE transitions from EMM-CONNECTED to EMM-IDLE) – for example, when the UE has uplink NAS signaling pending. As the next step, the SIP Session Establishment Procedure is invoked for IMS Service by setting up SIP signaling between the UE and the Core IMS through the LTE access (i.e., E-UTRA termination, eNodeB, and EPC). At this time, the setting up of the voice service happens in the LTE user plane carrying application layer signaling (SIP). The major interacting role of LTE would be PCRF dynamic policy control and its interaction with EPC (PCEF) to offer bearer QoS differentiation. This means it is possible to dedicate a special bearer or bearers to provide messages with higher priority over others. NS/EP NGN-PS primarily uses the special handling of the LTE QoS differentiation capabilities.

Figure 4.6 illustrates typical sequences of the LTE procedures for a subscribed UE occurring in support of SIP Mobile Terminating Call/Sessions.

NOTE: Tracking Area Update procedure (not shown in Figure 4.5) may also occur during Mobile Terminating Call/Sessions.

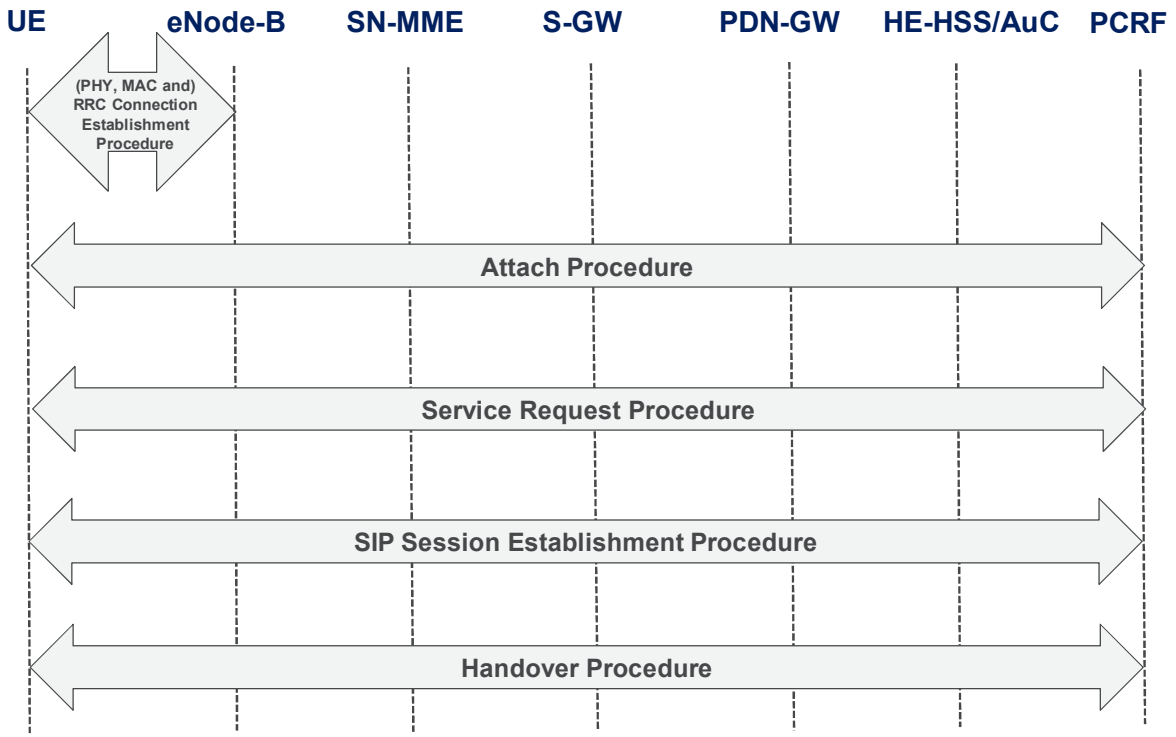

Figure 4. 5 - LTE Procedures Relevant to Mobile Originating Call/Sessions

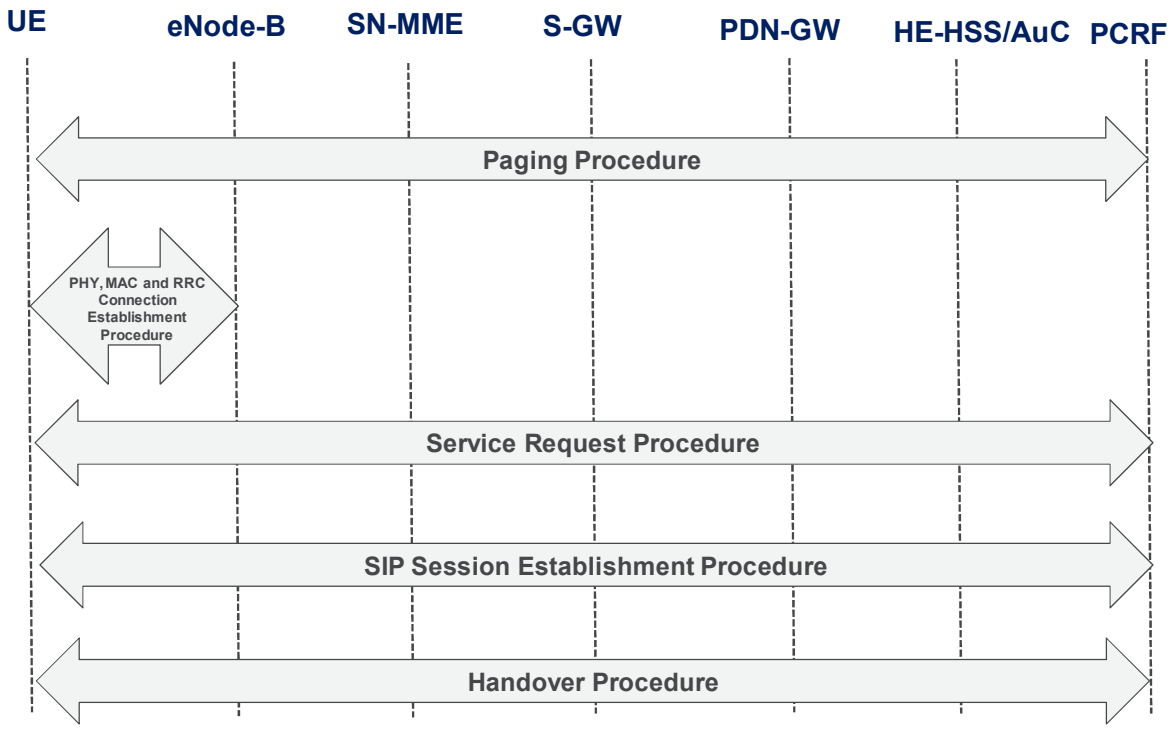

Figure 4. 6 - LTE Procedures Relevant to Mobile Terminating Call/Sessions

4.1.4 Conceptual View of LTE Access Network Security Architecture

The security architecture for the LTE radio access network and the EPC is defined in [TS 33.102] and [TS 33.401]. LTE supports five groups of security features shown in Figure 4.7:

- Network Access Security (I): The set of security features that provides users with secure access to services and protects against attacks on the radio access link. These security features include user and device confidentiality, data integrity and confidentiality, and user-network mutual authentication.
- Network Domain Security (II): The set of security features that enables nodes in the provider domain to securely exchange signaling data, and protects against attacks on the wireline network.
- User Domain Security (III): The set of security features that secures access to mobile stations.
- Application Domain Security (IV): The set of security features that enables applications in the user and provider domains to securely exchange messages.
- Visibility and Configurability of Security (V) (Not Shown in Figure 8): The set of features that enables the user to inform himself whether a security feature is in operation or not and whether the use and provision of services should depend on the security feature.

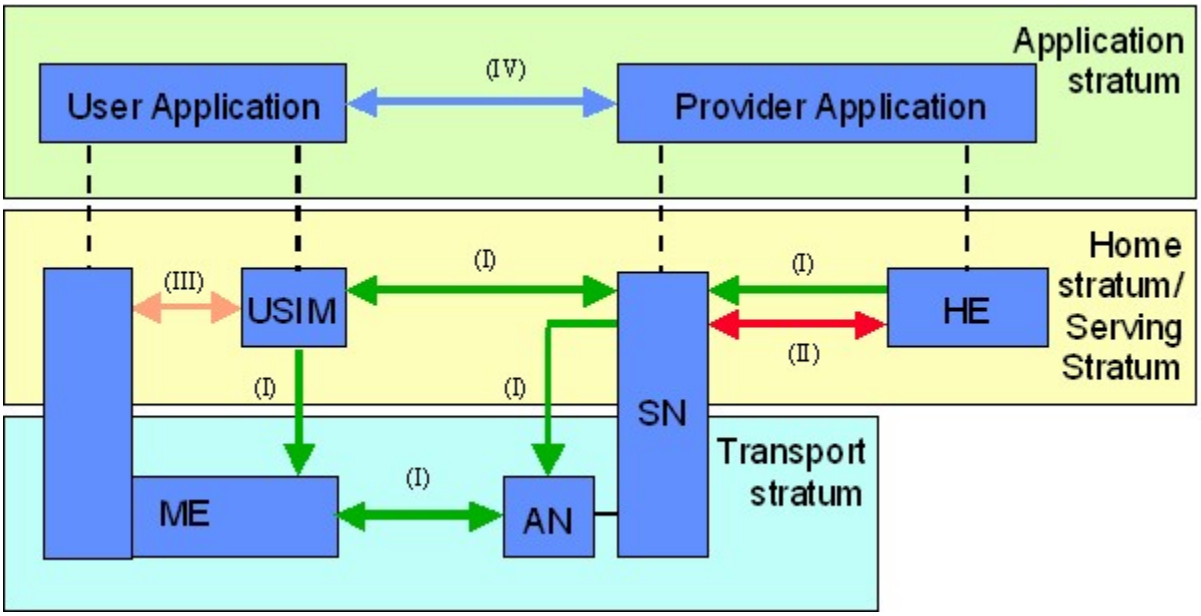

Figure 4. 7 - LTE security features

Figure 4.8 illustrates the general concepts of the LTE security architecture.

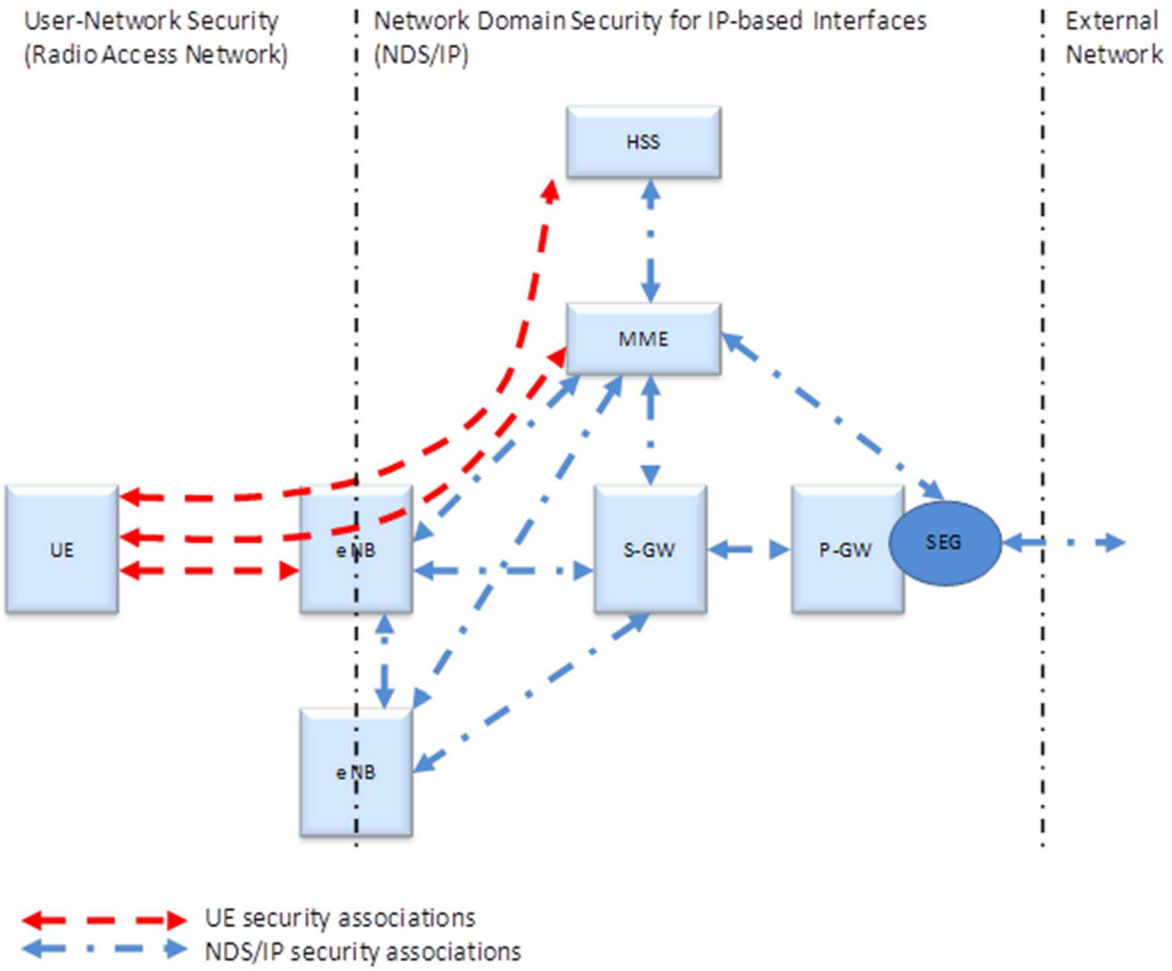

Figure 4. 8 -LTE Access Network Security Architecture

The Network Access Security architecture, defined in [TS 33.102] and [TS 33.401], protects users' access to LTE network using three layers of user-network security associations. The first layer security association is between the UE and the eNodeB to protect Access Stratum (AS) signaling and user data. The second layer is between the UE and the MME to protect Non-Access Stratum (NAS) signaling. The third layer is the long-term security association between the UE and its HSS (i.e., the home authentication server) for maintaining the long-term root security key and other security materials for authentication with the HSS.

Network Access Security uses symmetric-key cryptographic algorithms and a symmetric key hierarchy shown in Figure 4.9.

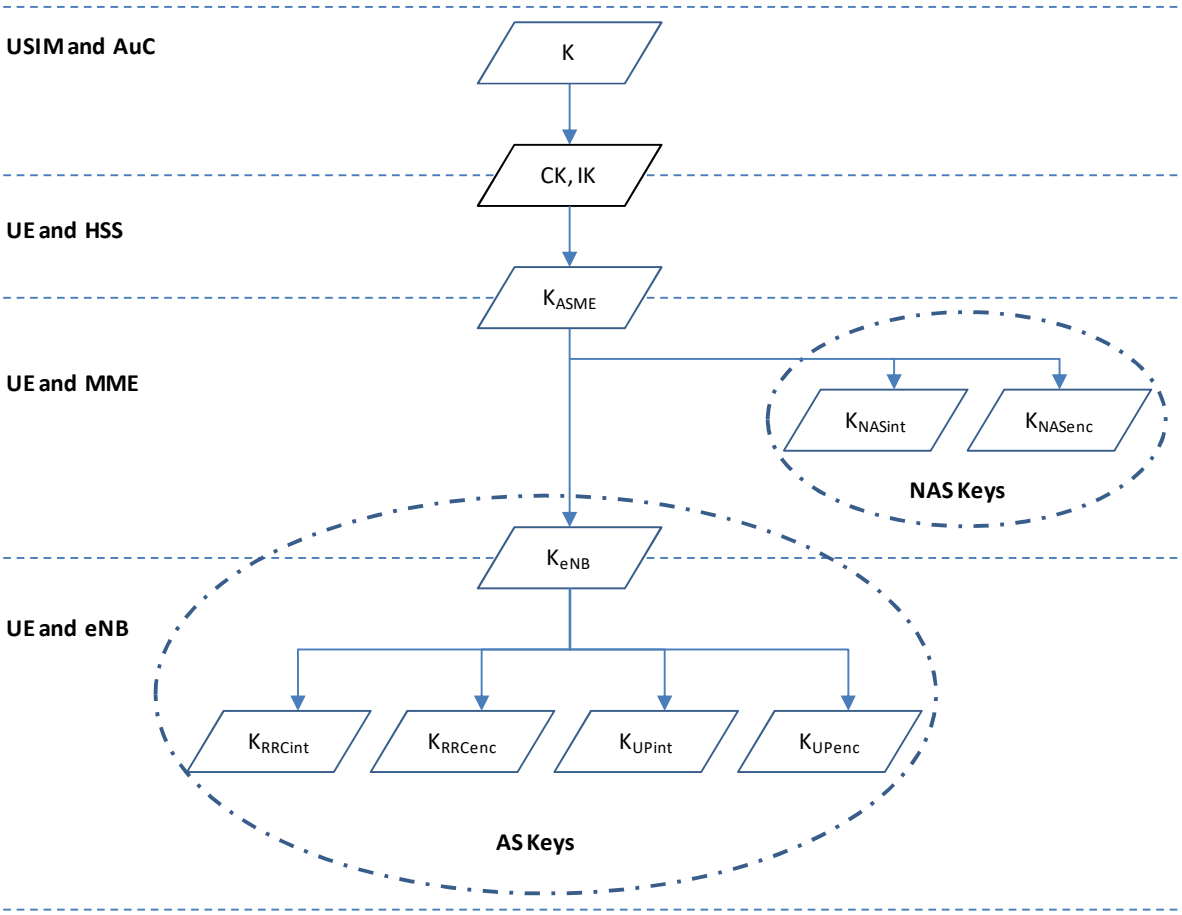

Figure 4. 9 - Key hierarchy for LTE Access Network

The purposes, users, and interdependences of the keys are shown in Table 4.3. All keys are 128-bit long (the ciphering and integrity keys for AS and NAS algorithms use only the 128 Least Significant Bits of the derived keys). This satisfies the 112-bit minimal symmetric key length required by the National Institute of Standards and Technology for US Government use after 2010 [SP 800-57].

Table 4. 3 - Security Keys for supporting LTE Network Access Security

Key	Purpose	Length (bits)	Used By	Derived From
K	Permanent master key	128	USIM and HSS/AuC[30]	
CK, IK	Cipher Key and Integrity Key	128	USIM and HSS/AuC	K
K_{ASME}	MME (ASME[31]) Intermediate Key	256	UE and HSS	CK, IK
K_{eNB}	eNB Base Key	256	UE and MME	K_{ASME}
K_{UPenc}, K_{UPint}	Encryption key and decryption key for user plane date	256 (128 LSB)	UE and eNodeB	K_{eNB}
K_{RRCenc}, K_{RRCint}	Encryption key and integrity key for RRC signaling	256*[32] (128 LSB)	UE, eNodeB	K_{eNB}
K_{NASenc}, K_{NASint}	Encryption key and integrity key for NAS signaling	256* (128 LSB)	UE and MME	K_{ASME}

3GPP LTE specifications require user-network mutual authentication at each connection setup (e.g., attach procedure or tracking area update). This Authentication and Key Agreement (AKA) procedure is also used for UE and network elements to establish shared secret keys that they will use to support Network Access Security. 3GPP LTE specifies the protection of user identity confidentiality over the air interface with three main measures: confidentiality of user's permanent identity, confidentiality of user's location, and non-traceability of user's services.

3GPP LTE specifications require that the user-network access signaling protocols, specifically the RRC and NAS protocols, be integrity protected, but allows such protections to be omitted for selected signaling messages and emergency calls under certain conditions.

3GPP LTE specification suggests that user data at the air interface not be integrity-protected based on two primary considerations. First, applications usually have their end-to-end integrity protection mechanisms, limiting the value of integrity protection at the air interface. Second, unnecessary security protection could impact radio network performance.

3GPP LTE specifications leave confidentiality protection for user-network access signaling and user data across the air interface optional, although it recommends such protections.

The Network Domain Security (NDS) architecture is defined in [TS 33.210] for securing IP-based signaling interfaces. IP-based interfaces are used between network elements in the core network, between eNodeBs, between eNodeB and core network, and between the core network and external networks. The collection of network elements and interfaces protected by the NDS architecture is referred to as the NDS/IP network. NDS/IP networks are divided into security domains. Each security domain is a set of networks managed by a single administrative authority. 3GPP specification of LTE [TS 33.210] mandates that integrity protection,

[30] Authentication Center.

[31] Access Security Management Entity.

[32] The asterisks (*) represent future work. The EPC and E-UTRAN shall allow for use of encryption and integrity protection algorithms for AS and NAS protection having keys of length 128 bits and for future use the network interfaces shall be prepared to support 256 bit keys.

message authentication, and replay protection be provided using Internet Protocol security (IPsec) [RFC 2401] over each IP-based signaling interface.

Security Gateways (SEGs) residing at the borders of each security domain are used to secure IP-based signaling between security domains using IPsec. SEGs are also used to secure IP-based signaling between network elements that are owned by the same operator in the same security domain, but are connected in a way that may lead to security breaches. For examples, some eNodeBs may be deployed in a trusted but vulnerable environment under the Service Provider's administrative control.

The Internet Key Exchange (IKE) protocol (version 1 or 2) is used to establish and manage IPsec security associations between SEGs, including establishing the security keys needed by the SEGs.

Integrity and confidentiality protections for user data over IP-based interfaces are not required by the current 3GPP LTE specifications.

Public key cryptography can be used to authorize and account for service usage in both home and visited networks [TS 33.221]. In this case, the UEs and the network elements in LTE Access Networks will need public-private key pairs and their digital certificates. A Public Key Infrastructure (PKI) needs to be used to issue and manage the digital certificates.

4.1.5 LTE Access Network Security-specific Flows and Security Context

To support security operations, UE and LTE network entities create and maintain EPS security contexts. An EPS security context contains the cryptographic keys, cryptographic algorithms, and other information needed to derive additional keys and support security operations. Each EPS security context consists of an EPS AS security context and an EPS NAS security context, each of which contains information to support security operations at the AS and the NAS levels respectively.

The major security-specific protocols and procedures include:

- Authentication and Key Agreement (AKA). The AKA supports user-network mutual authentication and establishes security keys and contexts on UEs and MMEs. It follows the same challenge-response protocol as the Global System for Mobile communications (GSM) with extended parameters [TS 33.401]. It is initiated by the MME and can be initiated as often as the network operator wishes. MME obtains the credentials related to each UE from the HSS and uses the information to create a challenge to the UE. If the UE answers the challenge correctly, the UE and MME will use their preconfigured shared secret to derive the additional secret keys necessary to support integrity and confidentiality protections.
- AS Security Mode Command. This procedure is used by the eNodeB to instruct the UE to start confidentiality and integrity protections for RRC signaling and, optionally, for user data at the air interface. The procedure also allows the UE and eNodeB to complete their AS security contexts by selecting the AS ciphering and integrity algorithms.
- NAS Security Mode Command. This procedure is used by the MME to instruct the UE to start performing integrity and confidentiality protections to NAS signaling and to allow UE and MME to complete their NAS security contexts by selecting the keys and algorithms for confidentiality and integrity protections. It is mandatory for the establishment of each new signaling connection between a UE and an MME.
- Internet Key Exchange (IKE) protocol. IKE is used to establish IPsec security associations for securing IP-based signaling interfaces between network elements in the core network, between eNodeBs, between an eNodeB and the core network, and between the core network and external networks.
- Security configurations. Operators need to configure initial security parameters and materials on eNodeBs, core network elements, and SEGs. These include the long-term shared root key on HSS, MME, and eNodeBs for supporting Network Access Security. They also include shared secrets for authentication of Diffie-Hellman algorithm parameters on eNodeBs, core network elements, and SEGs for establishing IPsec security associations to support Network Domain Security.
- Generic Bootstrapping Procedure [TS 33.220]. The bootstrapping procedure allows the UE and a Bootstrapping Server Function (BSF) in the LTE network to use the AKA procedure to establish the

shared security keys necessary for securing communications with the UE. A network application can then obtain these secret keys from the BSF to secure its communication with the UE without direct communications with the UE prior to establishing shared keys.

- Public Key Infrastructure (PKI). A PKI issues and manages digital certificates for the UEs and the network elements when public key cryptography is used to authorize an account for service usages.

5 General NS/EP LTE Security Requirements and Objectives

5.1 Functional Scope

According to the list of basic functional requirements documented and summarized in Table 1 of [ATIS-0100009], included here for convenience, NS/EP NGN-PS must be protected against unauthorized access.

The Service Provider is required to provide protection to prevent unauthorized access to NGN Priority Services.

This requirement is supported by a number of NS/EP Functional requirements shown in [ATIS-0100009]. The items directly related to Priority Services security are highlighted in blue. They include: Secure Networks, Anonymity, Restorability, Survivability/Endurability, and Reliability/Availability.

Table 5. 1 - Original Table of ETS Functional Requirements [ATIS-0100009]

NS/EP Telecommunication Services Functional Requirement	Description
a. Enhanced Priority Treatment	Services supporting NS/EP missions must be provided priority treatment over other traffic.
b. Secure Networks	Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
c. Non-Traceability	Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
d. Restorability	Should a disruption occur, services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
e. International Connectivity	Services must provide access to and egress from international carriers.
f. Interoperability	Services must interconnect and interoperate with other selected government or private facilities, systems, and networks.
g. Mobility	The communications infrastructure must support transportable, redeployable, or fully mobile communications (e.g., personal communications service, cellular, satellite, high frequency radio).
h. Ubiquitous Coverage	Services must be readily accessible to support the national security leadership and inter- and intra-agency emergency operations, wherever they are located.
i. Survivability/Endurability	Services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.

NS/EP Telecommunication Services Functional Requirement	Description
j. Voice-Band Service	The service must provide voice-band service in support of presidential and other communications.
k. Broadband Service	The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, and multimedia).
l. Scalable Bandwidth	NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
m. Affordability	Services must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf technologies, and services).
n. Reliability/Availability	Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

Mobility requirements mentioned above require securing LTE Access Network priority mechanisms and parameters, selection of the appropriate LTE Access Network security options (e.g., for securing the LTE air interface for carrying SIP signaling traffic), network management, and remote access security.

Other requirements deal with resiliency, availability, and survivability. They are required especially for securing FEs that are more exposed to external attacks and physical breaches.This document addresses all the applicable LTE Access Network interfaces, focusing on their FE endpoints' NS/EP functions and their priority transport security needs (as circumscribed by the Scope).

The detailed requirements that facilitate compliance to the security related NS/EP Telecommunication Services Functional Requirements in Table 5.1. are addressed in the subsequent sections of this document. The detailed requirements are organized in accordance with the reference models described in Section 4.

5.2 General LTE Security Objectives & Requirements

The Service Provider is required to protect NS/EP NGN-PS communications from security events (e.g., unauthorized access, interception, hijacking, and replay) that would compromise the security of NS/EP NGN-PS in accordance with commercially-available security best practices while the PS traffic is traversing the Service Provider's LTE Access Network domain.

The following are high-level general requirements:

R-1 (Required) The NS/EP NGN-PS Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the authenticity of NS/EP NGN-PS in accordance with commercially-available security best practices in the Service Provider's LTE Access Network domain.

R-2 (Required) The NS/EP NGN-PS Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the integrity of NS/EP NGN-PS in accordance with commercially-available security best practices in the Service Provider's LTE Access Network domain.

R-3 (Required) The NS/EP NGN-PS Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the confidentiality of NS/EP NGN-PS in accordance with commercially-available security best practices in the Service Provider's LTE Access Network domain.

R-4 (Required) The NS/EP NGN-PS Service Provider shall protect NS/EP NGN-PS communications from security events that would compromise the availability of NS/EP NGN-PS in

accordance with commercially-available security best practices in the Service Provider's LTE Access Network domain.

5.2.1 Common Objectives & Requirements

It is expected that Service Providers would be supporting and using a wide range of security tools and capabilities to protect the LTE Access Network itself and supported applications including NS/EP NGN-PS. It is important that appropriate measures be taken to ensure that the use of these security tools and capabilities in the LTE access do not negatively impact the performance of NS/EP NGN-PS or introduce any unintended security compromises to NS/EP NGN-PS.

R-5 (Required) NS/EP NGN-PS Service Provider use of security mechanisms (e.g., intrusion detection systems, deep packet inspection, and encryption) shall not interfere with the priority treatment mechanisms used to support NS/EP NGN-PS in the LTE Access Network domain.

O-1 (Optional) It is desirable that the NS/EP NGN-PS Service Provider use of security tools and capabilities in the LTE Access Network domain include appropriate measures to minimize impacts on NS/EP NGN-PS Quality of Service (QoS) (e.g., by introducing unnecessary delays).

5.2.2 Roles & Responsibilities in Multi-provider Arrangements

It is possible that not all LTE Access Network deployment scenarios will involve a single entity as the Service Provider. For example, it is possible that some deployment scenarios may involve multi-provider arrangements where the Service Provider (authorized by OEC/DHS through contract to provide NGN priority services) is using deployment arrangements where it is not the sole owner and operator of the LTE Access Network domain and the IMS Core Network to which the LTE Access Network is connected.

For multi-provider LTE Access Network arrangements, it is important that the roles and responsibilities for the security protection of NS/EP NGN-PS be established and enforced. Roles and responsibilities should be clearly defined for security policy enforcement, security risk assessment, security incident handling, and reporting, and defined in Service Level Agreements. It is also critical that designated organizational Single Points of Contact to coordinate NS/EP NGN-PS security issues be identified and documented.

CR-1 (Conditional Requirement) If the NS/EP NGN-PS Service Provider is using multi-provider arrangements where the Service Provider does not have sole responsibility for the operations or physical control of the LTE Access Network domain, the Service Provider shall establish, document, and enforce Service Level Agreements (SLAs) that describe the roles and responsibilities among the different entities that are involved in the security protection of NS/EP NGN-PS.

Examples of where CR-1 are applicable include, but are not limited to, scenarios in which:

- The LTE Access Network and the Core Network to which the LTE Access Network is connected are operated and controlled by different service providers.
- Business models in which the NS/EP NGN-PS Service Provider (SP) does not have sole responsibility for the operations and physical facility management control of the LTE Access domain (i.e., the LTE service provider may lease LTE facilities from a 3rd party facilities provider).
- The LTE service provider is using a 3rd party for backhaul services (i.e., transport services).

NOTE: It is recognized that in some cases the SP might not have a business relationship with the backhaul provider or even have any awareness of the identity of the backhaul provider (e.g., femtocell). Further study of these scenarios is needed to determine the security implications.

6 User-to-Network Interface (LTE-Uu) Security & UE Protection Specific to LTE

This section addresses protection of the LTE priority features, capabilities, and procedures that are specific to UE and LTE-Uu, the interface between UE and eNodeB. In particular, it addresses the problem of securing the NS/EP NGN-PS features that could be abused or manipulated in an unauthorized manner.

6.1 NS/EP NGN-PS Subscribed UE & LTE Air Interface Features

No NS/EP NGN-PS-specific security features are identified. As a result no security requirements are specified in this document related to this topic area.

6.2 NS/EP NGN-PS Special Handling of UE Features

6.2.1 Integrity of NS/EP LTE Access Class Procedures

The Access Class Barring (ACB) procedure [TS 22.011], [TS 36.331] that provides prioritized access for NS/EP NGN-PS depends on both NS/EP NGN-PS subscribed UEs and non-NS/EP NGN-PS subscribed UEs to honor and properly implement the barring procedures used for the LTE air interface contention management. This mechanism trusts the UE to honor a network indication (Access Class Barring information) that instructs it to determine whether it is allowed to request access. There are no means for the network to verify or enforce that the UE performs this test correctly or at all. Thus, while compliant UEs will honor ACB procedures and avoid use of the Random Access Channel (RACH) as intended, the mechanism does not prevent non-compliant UE from using the RACH, thereby consuming resources intended for NS/EP NGN-PS subscribed UE and for other priority use (e.g., emergency calling).

A UE that has been modified to omit the rules for RRC connection establishment can be used to congest the RACH that this mechanism is intended to protect. Intentional or accidental failure can result in a Service User UE facing greater than expected competition for the limited resources of the RACH, reducing the availability of radio resources to Service Users.

Rogue UEs bypassing contention-based RACH procedures (e.g., RRC connection establishment Procedure or ACB test) could cause RACH Overload for the uplink UE transmission. Therefore, LTE access class procedures must be integrity protected.

> **R-6 (Required)** The NS/EP NGN-PS Service Provider shall, as part of its UE vetting process, verify the integrity of the UE contention-based Random Access procedure.
>
> **R-7 (Required)** The NS/EP NGN-PS Service Provider shall, as part of its UE vetting process, verify the integrity of the Access Class Barring procedure.
>
> **R-8 (Required)** The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the contention-based RACH procedures to detect and report impacts on NS/EP NGN-PS availability.

R-8 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of received SIB2[33] IEs with NS/EP-specific AC Restrictions over Total number of received SIB2 IEs per Unit of Time. Refer to Appendix B for more information.

> NOTE: It is understood that this process of vetting the UE does not address the larger issue of integrity of UEs associated with other service providers.

[33] System Information Block

6.2.2 Integrity of USIM Provisioning for the NS/EP LTE Access Class & other Exempt Access Classes

The ACB mechanism controls access using access classes. The term access class refers to the method of controlling LTE access. There are 16 access classes. Class 14 is allocated to NS/EP Priority Services. Refer to [TS 22.011] for details on access classes values assignment.

Access control using access classes can be used to prevent UEs of commercial users from initiating an RRC connection through an action referred to as Access Class Barring (ACB). ACB can be invoked by the LTE network operator on some or all cells to suspend traffic during an overload situation (say, on a percentage basis). In LTE, each access class from 11 through 15 can be independently marked as exempt from Access Class Barring Test by the UE. ACB applies to transmissions initiated by a UE in RRC_IDLE[34] mode and is used to bar the UE from gaining access to the network's radio resources during network congestion.

UEs associated with NS/EP NGN-PS are provisioned with an Access Class value of 14 in their USIMs and with other private identifiers (e.g., Service User permanent master key – "K"). Thus, a Service User is given priority radio transmission for access during the RRC Connection Establishment procedure, which bypasses the normal random test procedure that is required for contention management of UEs requesting LTE access resources. (That is, if at least one of the Access Classes associated with a UE has been marked as exempt for the type of signaling the UE is requesting, the UE will have priority access by virtue of not having to perform the random test.) Thus, the ACB mechanism depends on the NGN Service Provider to provision appropriate access class values in the UEs' USIMs and for the network operators to exempt the access class from having to perform the random test.

Unauthorized access class provisioning in the USIM could impair availability of NS/EP NGN-PS by RACH overload for the uplink UE transmission. Therefore, the provisioning process must be integrity protected.

> **R-10 (Required)** The NS/EP NGN-PS Service Provider shall protect the integrity of the USIM provisioning process for configuring the NS/EP private identifiers (e.g., Access Classes) throughout the USIM provisioning life cycle by using access control, authentication, and authorization measures initiated from USIM provisioning systems and other remote access Over The Air mechanisms.

6.2.3 Integrity of NS/EP LTE Non-Contention Based Random Access for Priority Handover Procedures

Integrity is needed for non-contention based random access procedures because RACH Overload for the uplink UE transmission could be caused by rogue UEs initiating unauthorized RACH non-contention based procedures. A rogue UE, after performing an unauthorized non-contention based RACH procedure, could use a dedicated RACH preamble carried over the "RRC Connection Reconfiguration Complete" message to confirm with the target eNodeB its acceptance of an NS/EP NGN-PS handover with priority treatment.

The rogue UE that performs an unauthorized non-contention based RACH procedure would ignore whether dedicated RACH preambles are available in the target eNodeB and the fact that eNodeB needs to assign them to the UE based on service provider policy.

If public UEs could be modified to avoid performing the probabilistic ACB test, they could be used to congest the RACH that this mechanism is intended to protect. Such intentional or accidental actions can result in an NS/EP NGN-PS subscribed UE facing greater than expected competition for the limited resources of the RACH, reducing the availability of radio resources to Service Users.

[34] The Radio Resource Control (RRC) protocol is part of the LTE protocol stack. RRC handles the control plane signaling of Layer 3 between the UEs and the EUTRAN. There are two RRC states in LTE: RRC_IDLE and RRC_CONNECTED. In RRC_IDLE there is no signaling radio bearer established, so there is no RRC connection. In RRC_CONNECTED there is a signaling radio bearer established.

R-11 (Required) The NS/EP NGN-PS Service Provider shall, as part of its UE vetting process, verify the integrity of the UE Non-Contention based Random Access procedures (e.g., protection against tampering with dedicated preambles).

R-12 (Required) The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the non-contention based RACH procedures to detect and report impacts on NS/EP NGN-PS availability; i.e., ability to access the LTE network.

R-12 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example Statistics include: Number of Priority HO acknowledgements transmitted with dedicated RACH Preambles per Unit of Time over Total Number of Priority HO over Unit Time. Refer to Appendix B for more information.

6.2.4 Integrity of RRC Connection Establishment Procedure used for NS/EP LTE Priority Access

The availability of NS/EP NGN-PS could be compromised by manipulating rogue UEs to overload the RACH. The RACH overload for the uplink UE transmission could be caused by rogue UEs hardcoded with special cause code values that instruct the LTE network to assign them priority treatment in its allocation of bearer resources. Specifically, a rogue UE could tamper with the RRC Connection Request message to send an Establishment Cause (see Table 6.1 below) coded with a high Priority Access value. Therefore, the RRC Connection Establishment procedure must be integrity protected.

Table 6. 1 - RRC Connection Establishment Message Content

Information Elements	Options
UE Identity	S-TMSI
	Random Value
Establishment Cause	Emergency
	High Priority Access
	Mobile Terminating Access
	Mobile Originating Signaling
	Mobile Originating Data

R-13 (Required) The NS/EP NGN-PS Service Provider shall, as part of its UE vetting process, verify the integrity of the RRC Connection Establishment procedure.

R-14 (Required) The NS/EP NGN-PS Service Provider shall, as part of its UE vetting process, verify the integrity of UE Establishment Cause code assignments and default values.

NOTE: 3GPP LTE mandates integrity protection for NAS signaling messages such as the RRC Connection Request after the UE has obtained valid EPS security contexts. If the UE does not yet have valid security contexts, which is typically the case when the UE establishes its first RRC connection using the existing LTE specifications, the RRC Connection Request will not be integrity protected.

When RRC Connection Requests are not integrity protected, adversaries can intercept these messages, alter their contents, and then send the altered messages to the network. It will be difficult for the LTE network to distinguish these bogus messages from authentic RRC Connection Request messages. This can

severely interrupt the ability for NS/EP users to access the LTE network. This issue needs to be examined and solutions suggested.

6.3 NS/EP NGN-PS Considerations of LTE Air Interface Security Feature Options

6.3.1 LTE Air Interface Security

3GPP LTE air interface security focuses on protecting 1) Confidentiality of user identities, 2) Integrity of LTE signaling traffic across the air interface, and 3) Mutual authentication between the user and the LTE network. 3GPP LTE defines confidentiality protection procedures for signaling traffic and user data, but does not mandate such protections. See [TS 33.401] Section 5 for details.

Table 6.2 summarizes LTE air interface security protection features.

Table 6. 2 – LTE Air Interface Security Protection Features (3GPP Release 10 [TS 33.401])

	Features	LTE Protection
User Identity	Confidentiality	Required for IMSI
Signaling	Integrity	Required for RRC and NAS signaling
	Confidentiality	Recommended for RRC and NAS signaling
User Data	Integrity	Shall not be protected on the Uu interface
	Confidentiality	Recommended to be provided at Packet Data Convergence Protocol (PDCP) layer
Authentication	User-Network Mutual Authentication	Required

3GPP LTE uses three layers of security associations to support air interface security:

- UE to HSS security association for maintaining the long-term root security key used to derive other security keys and additional long-term security materials for authentication with the HSS.
- UE to MME security association for protecting NAS signaling.
- UE to eNodeB security association for protecting AS signaling and user data over the air interface.

6.3.1.1 User Data

With the current LTE standards, confidentiality protection for user data over the air interface is a service provider option. If confidentiality protection is to be provided for user data over the air interface, LTE requires that it be implemented at the Packet Data Convergence Protocol (PDCP) layer.

R15 (Required) The NS/EP NGN-PS Service Provider shall be capable of providing confidentiality protection to user data (i.e., SIP signaling and voice media packets) across the LTE air interface for selected Service Users.

NOTE: Further study is needed to decide whether the aforementioned requirement can be explicitly applied to the IMS/SIP traffic carried over the LTE user plane air interface. It is understood that for selected UEs, the following LTE air interface user plane protection options are possible:

(a) Encrypt all information over the air (UE to eNodeB) including SIP signaling and user data.

(b) No encryption between UE and eNodeB, but IMS-based encryption between the UE and the P-CSCF for SIP signaling (after the initial IMS Registration message).
(c) Encryption over the air + IMS-based confidentiality (SIP encrypted twice).
(d) No encryption at all.
(e) Application layer encryption (for example encrypted voice) between the two end points (UE to UE) on top of (a), (b), (c) or (d).

6.3.2 Network Attachment Signaling

LTE UEs use the Network Attachment procedure to register with a LTE network [TS 23.401]. This procedure allows a UE to establish a default EPS bearer for supporting always-on IP connectivity and to trigger additional procedures to establish dedicated EPS bearers and to request IP addresses.

Security-related information exchanged between the UE and the LTE network during the Attach procedure is shown in Figure 7. Two such important information elements are:

- **"NAS signaling low access priority indicator**": The Attach Request carries a "NAS signaling low priority access indicator" to indicate the priority level of the request [TS 24.301] Section 4.3.17.4 [TS 124 301]. This indicator is configured in the USIM. To ensure service availability for Service Users, this indicator shall be set to "MS is not configured for NAS signaling low priority" on NS/EP NGN-PS Subscribed UEs. This is to ensure that NS/EP Subscribed UEs are not configured for low access priority indicator.
- **IMSI:** The IMSI will be in the Attach Request 1) during an initial attach to a network, or 2) when the UE does not have a valid temporary identifier such as a GUTI, or 3) when the UE is configured to perform Attach with IMSI when it accesses a new LTE network. If the Attach Request does not contain sufficient valid identification information, the MME will request the UE to send its IMSI or the International Mobile Equipment Identity (IMEI) in subsequent messages.

When Network Attachment signaling messages are not integrity protected, adversaries can intercept these messages, alter their contents, and then send the altered messages to the LTE network. Such attacks can make it difficult for Service Users to successfully complete their Network Attachment procedures. Therefore, the integrity of the Attach signaling messages for Service Users must be protected.

LTE mandates integrity protection for NAS signaling messages after the UE has established valid EPS security contexts. A UE will not have valid EPS security contexts before its initial network attachment.

NOTE: The Service Users need to be aware that the initial network attachment is not protected. Therefore, Service Users might need to take extra care to perform the initial Network Attachment procedures in a protected environment, where it is difficult for adversaries to capture LTE signaling messages, and then use the security contexts during the initial attachment later for protecting priority services.

UEs may also be configured to perform Attach with IMSI when accessing a new LTE network. Per LTE EPS-AKA procedure, there are specific cases where the MME may explicitly request the IMSI if it cannot establish a UE context and then the IMSI is sent in clear text from the UE to the MME. When the IMSI is sent in clear text there could be risk for disclosure of the Service User identity (i.e., identity/privacy issue) and unauthorized tracking.

O2 (Optional) It is desirable that the NS/EP NGN-PS Service Provider provide confidentiality protection of the IMSI in the initial UE identification message when the IMSI is requested by the LTE network and is sent in plain-text from the UE to the MME.

NOTE: It is recognized that standards development would be needed to allow practical solutions to meet O-2 because this impacts the UEs, network elements, and international roaming in a significant manner.

NOTE: The NS/EP NGN-PS Service Provider should minimize the exchange of IMSI in its Attach Procedures for NS/EP NGN-PS Subscribed UEs when accessing new LTE access networks (i.e., requiring initial attach).

6.4 UICC Security

UICC security is a matter that must be considered from the perspectives of the Service Provider and the Service Users.

From the Service Provider's point of view, the potential danger posed by the UE lies in its misuse to interrupt the network's ability to provide worry-free service to its users in the form of availability and call integrity. The UE is a network user in the sense of having its messages ferried across the network to their destinations, so the primary way that a UE can affect the availability of the network is by flooding the network with messages to an extent that other subscribers' calls cannot be completed. The UE can affect integrity by becoming party to fraudulent activity in which it appears to belong to a given user while performing actions on behalf of another (human or non-human) entity. It can also affect integrity by placing messages onto the network that cause network elements to misbehave.

While one or a small number of abused UEs can have a limited effect on either network availability or integrity, a cloned[35] UICC/USIM within the UE can in essence turn one phone into many that appear to be acting on behalf of the cloned phone's owner, affecting integrity since there is no way for the Service Provider to discern instantly which UEs are clones. Service Providers might be able to recognize the evidence of cloning by methods such as:

- Fingerprinting: Radio fingerprinting is a process used to identify a cellular phone or any other radio transmitter by the unique "fingerprint" that characterizes its signal transmission. Every wire-less device contains a radio fingerprint in its transmission signal that remains unique to that device despite changes to the device's IMEI or IMSI. The electronic radio fingerprint makes it possible to identify a wireless device by its unique radio transmission characteristics. Thus, cellular service providers are able to detect cloned devices by discrepancies between the radio fingerprint and the IMEI or IMSI. A cloned device will have the same numeric equipment identity but a different radio fingerprint.
- UE usage patterns: By noting deviations from the Service User's usage patterns, the service provider can move quickly to close down the Service User's account.

This vigilance means that the larger the number of clones of a given UICC/USIM, the greater the likelihood of rapid discovery, so cloning is a self-limiting exercise. This also suggests that a population of cloned UEs large enough to impede network availability could be discovered and the threat removed before an availability attack could reach its apex.

From the NS/EP NGN-PS perspective, UICC/USIM cloning might be chiefly harmful if the UEs containing the cloned UICC/USIMs are brought into play precisely during a crisis that affects the Service Providers' normal operations, including their capability to detect and respond to the cloned UEs. In such circumstances, loss of availability or integrity due to cloned UEs could be a distinct danger, although the amount of coordination among the attackers to activate their cloned UEs and initiate an attack under those circumstances would have to be extreme. It is possible that a crisis that hinders the Service Providers' ability to respond to clone-based attacks could itself be orchestrated by the attackers, but that would involve a multi-pronged assault on resources, infrastructure, or facilities and thus require much greater effort and coordination. While possible, it seems unlikely that a serious attack would be mounted using short-lived cloned UEs. Nevertheless, the Service Providers should be poised to detect and neutralize clone-based attacks on their networks.

It is recognized that LTE provides enhanced authentication and key management (EPS-AKA) capabilities; however, the possibility of attackers discovering methods to circumvent LTE protection against UICC/USIM cloning cannot be entirely ruled out. Therefore, the SP should maintain due diligence to protect against cloning.

[35] Mobile device cloning is the transfer of identity between one mobile device and another. Cloning the UICC/USIM in a UE allows the cloned UE to appear identical to the UE from which the identity was obtained.

R16 (Required) The NS/EP NGN-PS Service Provider shall establish and enforce security policies to minimize risks associated with NS/EP NGN-PS subscribed UE cloning in accordance with commercially-available security best practices.

R17 (Required) The NS/EP NGN-PS Service Provider shall be able to detect a cloned NS/EP NGN-PS subscribed UE.

R18 (Required) The NS/EP NGN-PS Service Provider shall be able to identify the Service User whose NS/EP NGN-PS subscribed UE has been cloned.

R19 (Required) The NS/EP NGN-PS Service Provider shall notify OEC/DHS and the affected Service User when it detects a cloned NS/EP NGN-PS subscribed UE.

R20 (Required) The NS/EP NGN-PS Service Provider shall have a capability to disable cloned NS/EP NGN-PS subscribed UEs.

7 E-UTRAN Security & E-UTRAN-to-EPC Interface Security

The requirements in this section address the security protection of the LTE priority features, capabilities, and procedures that are specific to eNodeBs, S1 (interfaces between the eNodeB and EPC components), and X2 (interfaces between eNodeBs). Specifically, they address the problem of securing the NS/EP NGN-PS-specific features from abuse or unauthorized manipulation (e.g., when considering compromised eNodeBs requesting unauthorized priority back-haul resources for public UEs).

7.1 NS/EP NGN- PS-specific E-UTRAN Features

This section describes securing NS/EP NGN-PS-specific features and procedures supported in eNodeB that need to be secured.

7.1.1 Protection of eNodeB Handling & Bypass of Machine Congestion Control Capabilities Used for Priority Resource Allocation of NS/EP NGN-PS: LTE-Uu, S1-MME, & S1-U

eNodeBs may use priority queuing (e.g., based on ARP/QCI values) or priority handling (e.g., for transmission of paging) in conjunction with Machine Congestion Control (MCC) bypass capabilities for NS/EP NGN-PS priority resource allocations during high-stress network traffic load conditions. These capabilities can be used for NS/EP NGN-PS during normal traffic congestion, during back-haul congestion (stemming from emergency conditions such as natural disaster), or during eNodeB partial equipment failures (i.e., eNodeB in a degraded state).

An example of priority treatment is exemption from MCC. If an eNodeB has an MCC function that discards traffic based on the traffic's priority (e.g., Ethernet Class Of Service value), the Service Provider can provision and configure the eNodeB so that NS/EP NGN-PS traffic has a higher priority than the corresponding public traffic and is therefore shed only after the public traffic is shed.

The eNodeB capabilities such as special queuing, scheduling, and MCC bypass capabilities that are used for priority resource allocation of NS/EP NGN-PS should be protected.

R21 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the eNodeB capabilities (e.g., MCC bypass) that are used for priority resource allocation for NS/EP NGN-PS during high traffic loads.

R22 (Required) The NS/EP NGN-PS Service Provider shall be able to verify integrity of eNodeB priority capabilities (e.g., MCC bypass) that are used for resource allocation for NS/EP NGN-PS during high traffic loads through data collection and analysis.

7.2 NS/EP NGN-PS Special Handling of E-UTRAN-Specific Features

This section describes securing NS/EP NGN-PS special handling features and procedures. These features and procedures are in need of integrity protection for reasons that vary with the individual features such as contention-based and non-contention-based random access, priority handover, and others. The subsections below provide examples of vulnerabilities associated with specific procedures along with consequences of exploitation. This provides the context for integrity requirements that can be stated generally as follows:

> **R23 (Required)** The NS/EP NGN-PS Service Provider shall protect the integrity of eNodeB features that are used to support NS/EP NGN-PS. The minimum set of eNodeB features to be integrity-protected are:
>
> 1. Access Class procedures.
> 2. Non-Contention-based Random Access procedures including protection against tampering with dedicated preambles.
> 3. Priority handover procedures, including protecting against tampering with ARP priority markings and their processing.
> 4. Handling of Establishment Cause codes.
> 5. Priority mechanisms that receive, store, analyze, and schedule events based on priority markings, and the data storage area where the priority marking data is stored.
> 6. Priority paging mechanisms.
> 7. Priority mechanisms that use priority markings for priority bearer establishment and modification, and the priority marking data itself.

The following subsections provide justification and context for protecting each of these features. Each subsection is laid out as follows: a brief statement of how abuse of the above features can lead to UE uplink overload conditions; a short discussion of the LTE mechanisms that could facilitate such abuse. In the event that monitoring a feature's activities for management purposes is needed, the requirement for such monitoring is provided.

7.2.1 Integrity of NS/EP LTE Access Class Procedures: LTE-Uu

RACH Overload for the uplink UE transmission can be initiated by a compromised eNodeB that orders UEs under its control to bypass RACH contention-based procedures.

The ACB mechanism [TS 22.011] [TS 36.331] that provides prioritized access for NS/EP NGN-PS services depends on both NS/EP NGN-PS subscribed UEs and non-NS/EP NGN-PS subscribed UEs to honor and properly implement the barring procedures used for the LTE air interface contention management. Specifically, the access class procedure trusts the UE to honor a network indication (Access Class Barring information) that instructs it to perform a test to determine whether it is allowed to request access; there is no way for the network to verify or enforce that the UE performs this test correctly or at all. Thus, a compromised eNodeB could instruct all the UEs under its control to honor ACB Test bypass procedures, preventing the use of RACH as intended, and consuming resources intended for NS/EP NGN-PS subscribed UE and for other priority use (e.g., emergency calling).

If an eNodeB could be modified to instruct UEs to bypass RACH contention-based procedures for the uplink UE transmission, then the devices under the eNodeB control could be used to congest the RACH that this mechanism is intended to protect. Intentional or accidental eNodeB actions could result in NS/EP NGN-PS subscribed UE facing greater than expected competition for the limited resources of the RACH, reducing the availability of radio resources to Service Users.

> **O-3 (Optional)** It is desirable that NS/EP NGN-PS Service Provider, for the eNodeB, establish and implement procedures to monitor the contention-based random access procedures to detect and report security impacts on the eNodeBs ability to handle NS/EP NGN-PS.

O-3 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example Statistics include: Number of received SIB2 IEs with NS/EP-specific AC Restrictions over Total number of received SIB2 IEs per Unit of Time. Refer to Appendix B for more information.

Note that NS/EP NGN-PS Service Providers cannot control how other Service Providers, including non-NGN-PS Service Providers, provision the ACs of their UEs; nor can they control whether the UEs of other Service Providers conform to the service access procedures [TS 22.011].

7.2.2 Integrity of NS/EP LTE Non-Contention Based Random Access Procedures for Priority Handover: LTE-Uu

A compromised eNodeB that tampers with its dedicated preamble settings that instruct UEs under its control to bypass contention-based random access procedures could cause radio resources to become unavailable for handovers at the eNodeB.

A compromised eNodeB could tamper with its pre-assigned dedicated preambles used in the intra E-UTRAN priority handover procedure. Service Users who have bearers that have been assigned an ARP chosen by the Service Provider for NS/EP NGN-PS use, and which are from the ARP block allocated for intra-domain operation, should be given priority access to the limited pool of dedicated RACH preambles in times of increased handover flow into a target eNodeB, which could exhaust the available pool of preambles.

Public UEs could be instructed by a compromised eNodeB to avoid performing the contention-based RACH probabilistic test. Such intentional or accidental actions could result in NS/EP NGN-PS subscribed UEs facing greater than expected competition for the RACH resources, reducing the availability of radio resources to Service Users.

> **O-4 (Optional)** It is desirable that the NS/EP NGN-PS Service Provider, for the eNodeB, establish and implement procedures to monitor the non-contention based random access procedures to detect and report security impacts on the ability of eNodeBs to handle Handovers for NS/EP NGN-PS.

O-4 may be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example Statistics include: Number of Handover Request Acknowledge messages with dedicated RACH preambles (for Non-Contention Based random access) requesting priority HO treatment per Unit of Time. Refer to Appendix B for more information.

7.2.3 Integrity of NS/EP LTE Priority Markings (Allocation and Retention Priority "ARP") for Priority Handover: X2-AP

Compromised eNodeBs could purposefully ignore ARP priority markings, resulting in the handover not receiving priority treatment or a failed handover.

ARP priority marking is used in the priority handover procedure by a target eNodeB to assign bearers for handover with priority [TS 36.423].

> **O-5 (Optional)** It is desirable that the NS/EP NGN-PS Service Provider establish and implement procedures to monitor the priority handover procedure to detect and report security impacts on the eNodeBs for NS/EP NGN-PS.

O-5 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of HO requests with NS/EP Priority ARP received at the target eNodeBs requesting Priority HO per Unit of Time. Refer to Appendix B for more information.

7.2.4 Integrity of RRC Connection Establishment Procedure used for NS/EP LTE Priority Resource Allocation: LTE-Uu/S1-MME

Compromised eNodeBs could:

- Prevent priority treatment or other special handling treatments requested by specific UEs by purposefully ignoring UE submitted Establishment Cause code values (see Table 5).
- Mark all UE messages with equal priority by assigning the same Establishment Cause code value (e.g., high Priority Access value reserved for Service Users priority access to the LTE network resources) over S1-MME such that MME cannot differentiate NS/EP-originated signaling messages from non-NS/EP-originated signaling messages.

Such intentional or accidental actions could cause an NS/EP NGN-PS subscribed UE to face greater than expected competition for the limited resources of the RACH, reducing the availability of radio resources to Service Users [TS 36.331].

> **O-6 (Optional)** It is desirable that the NS/EP NGN-PS Service Provider establish and implement procedures to monitor the RRC Connection Establishment Procedure to detect and report impacts on the ability of eNodeBs to request allocation of LTE priority resources.

O-6 may be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of RRC Establishment High Priority Access Cause Codes handled for NS/EP connections per Unit of Time. Refer to Appendix B for more information.

7.2.5 Integrity of NS/EP LTE Priority Markings (Allocation & Retention Priority "ARP"): S1-MME

Compromised eNodeBs could purposefully assign equal priority to received signaling messages having different ARP priority markings, causing depletion of LTE resources needed for the NS/EP NGN-PS use, and resulting in degraded service to Service Users.

ARP priority marking is used for priority bearer establishment and modification procedures at the eNodeB.

> **O-7 (Optional)** It is desirable that the NS/EP NGN-PS Service Provider establish and implement procedures to monitor the ARP priority marking within eNodeB to initiate priority bearer establishment and modification procedures to detect and report security impacts.

O-7 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics: Number of NS/EP-specific bearer establishment and modification requests (NS/EP-specific ARPs) per Unit of Time. Refer to Appendix B for more information.

7.2.6 Integrity of Paging Priority: S1-MME

Compromised eNodeBs could purposefully ignore paging priority indications received from MMEs, degrading or halting NS/EP NGN-PS call/session during network congestion.

Priority paging enables eNodeBs to send pages (indications) with priority for NS/EP NGN-PS call/sessions when the paging messages from the MME to the eNodeB are marked with paging priority.

> **O-8 (Optional)** It is desirable that the NS/EP NGN-PS Service Provider establish and implement procedures to monitor the processing of the priority paging within eNodeB to detect and report security impacts.

O-8 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of paging indications

processed with priority (NS/EP-specific ARPs) for NS/EP Mobile Termination establishments per Unit of Time. Refer to Appendix B for more information.

7.2.7 Integrity of NS/EP LTE Priority Markings (ARP/QCI)

Compromised eNodeBs could allow tampering with the ARP/QCI configuration settings to trigger unauthorized requests for the constrained bearer resources that are to be used for signaling (QCI=5) or dedicated media (e.g., QCI=4) instead of using a default bearer that is adequate for best effort data transport. This may cause depletion of LTE constrained resources needed for the NS/EP NGN-PS use.

> **R-24 (Required)** The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the processing of QCI priority marking used to establish signaling and dedicated media to detect and report security impacts.

R-24 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of QCI requests processed with QCI set for signaling and/or for dedicated media with NS/EP ARP set for priority handling per Unit of Time. Refer to Appendix B for more information.

7.3 LTE Security Features Critical to Service Users

The following LTE security features are crucial to Service Users:

- Authentication and Key Agreement (AKA) in support of user-network mutual authentication and the establishment of security keys and security contexts on UE and MME [TS 33.401].
- Generic Bootstrapping [TS 33.220] to allow a UE and a Bootstrapping Server Function (BSF) in the LTE network to use the AKA procedure to establish the shared security keys. A network application can then obtain these secret keys from the BSF to secure its communication with the UE without direct communications with the UE a priori to establishing shared keys.
- AS Security Mode Command used by an eNodeB to instruct a UE to start confidentiality and integrity protections for RRC signaling and optionally for user data at the air interface. This also allows the UE and eNodeB to complete their AS security contexts by selecting the AS ciphering and integrity algorithms.
- NAS Security Mode Command allows the MME to instruct a UE to start integrity and confidentiality protections to NAS signaling and to allow UE and MME to complete their NAS security contexts by selecting the keys and algorithms for confidentiality and integrity protections.
- UE-UICC (USIM) interface security.
- User and device identity confidentiality.

> NOTE: Further study is needed to explore issues that surround implementing requirements for EPS AKA, Generic Bootstrapping, AS, and NAS Security Mode Commands, to establish the shared keys for UE-UICC interface protection.
>
> NOTE: Further study is needed to determine whether NS/EP NGN-PS Service Provider policies should restrict the use of each temporary identifier particular to an NS/EP NGN-PS subscribed UE to a predefined period of time. Temporary identifiers strengthen confidentiality of user and device identity.

8 EPC Security & EPC (NNI) Interface Security including EPC-to-IMS Interface

The requirements in this section address the security protection of the EPC priority features, capabilities, and procedures which are specific to EPC components (i.e., MME, S-GW, PDN-GW, and optional HSS and PCRF/SPR) and for EPC-specific interfaces (e.g., S6a, S10, S11, S5/S8) within the scope of this document. They address other intra-domain and/or inter-domain (NNI) interfaces (e.g., SGi and Gx) where applicable. Specifically, the objective is to address the problem of securing the NS/EP NGN-PS specific features from abuse or unauthorized manipulation (e.g., when compromised EPC entities provide unauthorized priority access to LTE resources for public UEs or when NGN Service User UEs are denied access to the priority LTE resources).

8.1 NS/EP PS-specific EPC Features

This section describes NS/EP NGN-PS-specific features and procedures supported in EPC that need to be secured.

8.1.1 Advance Priority-SPR (Subscriber Profile Repository)

This section provides requirements to ensure the integrity of Advance Priority-SPR feature.

Advance Priority-SPR is a unique NS/EP NGN-PS feature which for its implementation requires that the NS/EP NGN-PS Service Provider network be configured with an SPR.

When the PCRF receives information from the SPR that the UE is subscribed to NS/EP, the PCRF modifies the ARP of the Default and IMS Signaling bearers to the highest priority level within the allocated ARPs for NS/EP.

PCRF Policy Charging Control tables use the NS/EP-specific Service User subscription data configured in the SPR for the PCRF to request priority bearer treatment during attach procedures. This is accomplished by setting the ARP value to the highest priority ARP within the ARP range assigned for NS/EP.

Advance Priority-SPR is enabled based on the “IMS Signaling Priority” information, “MPS EPS Priority” information, and the Service User’s priority level (“MPS Priority Level”) stored in the SPR and passed on to the PCRF at the time of Attach or PDN Connectivity Request to the APN used for IMS Signaling.

Insider attacks resulting in unauthorized manipulation of the configured NGN Service User subscription data in the NS/EP NGN-PS Service Provider provisioning and activation systems may result in this NS/EP advance priority EPC feature malfunctions. Advance priority EPC feature malfunctions may cause network congestion and denial of priority services to the NGN Service Users. Intentional or unintentional tampering with configuration of ARPs in PCRF or a compromised PCRF may cause policy rules appropriate for advance priority to be ignored. This can lead to NS/EP subscribed UEs not getting advance priority treatment or non-subscribed UEs getting advance priority treatments.

In summary, a compromised SPR Provisioning System, tampering with NGN Service User subscription and service profile data (e.g., IMS Signaling Priority information) within the SPR or erroneous policy table mapping and processing within the PCRF are examples of major vulnerability threats related to this NS/EP feature.

CR-1 (Conditional Requirement) The NS/EP NGN-PS Service Provider shall secure the provisioning, activation and processing of the Advanced Priority-SPR feature by protecting the integrity of its supporting systems and databases in which NS/EP data and data mapping are stored and processed. The key systems and databases include but are not limited to:

(a) SPR Provisioning System

(b) SPR
(c) PCRF.

[ATIS-1000055] Section 12.4.3, Requirements for Management of Insider Threats also applies.

8.1.2 Advance Priority-HSS (Home Subscriber Server)

This section provides requirements to ensure the integrity of Advance Priority-HSS feature.

Advance Priority-HSS is a form of Advance Priority, which unlike Advance Priority-SPR described above, may be provided in a network which does not include an SPR.

For Advance Priority-HSS, the HSS stores the highest priority ARP (within the ARP range assigned for NS/EP) for the NS/EP NGN-PS subscribed UE. During an Attach request from an NS/EP NGN-PS subscribed UE, the MME requests subscription and service profile data from the HSS which includes highest priority ARP among other data. The MME will initiate a priority attach treatment specific to the NS/EP NGN-PS subscribed UEs.

When the ARP received during the Attach procedure belongs to the set allocated for NS/EP, the PCRF sets the ARP of Default and IMS signaling bearers to the highest priority level within the allocated ARPs for NS/EP.

Intentional or unintentional tampering with configuration of ARPs in the PCRF or a compromised PCRF may cause policy rules appropriate for advance priority to be ignored. This can lead to NS/EP subscribed UEs not getting advance priority treatment or non-subscribed UEs getting advance priority treatments.

Insider attacks resulting in unauthorized manipulation of the configured NGN Service User subscription data in the NS/EP NGN-PS Service Provider provisioning and activation systems may result in the Advance Priority-HSS feature malfunction and in turn may cause network congestion and denial of priority services to the NGN Service Users.

Compromised HSS Provisioning System, tampering with NGN Service User subscription and service profile data (e.g., ARP) within the HSS or erroneous policy table mapping and processing within the MME are examples of major vulnerability threats related to the Advance Priority-HSS feature.

CR-2 (Conditional Requirement) The NS/EP NGN-PS Service Provider shall secure the provisioning and activation of the Advanced Priority-HSS feature by protecting the integrity of its supporting systems and databases in which NS/EP data is stored and processed. The key systems and databases include but are not limited to:

(a) HSS Provisioning System
(b) HSS
(c) MME

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats, also applies.

8.1.3 Protection of MME Handling & Bypass of Machine Congestion Control Capabilities Used for Priority Resource Allocation of NS/EP NGN-PS

This section provides requirements to ensure the integrity of MME Machine Congestion Control Capabilities Bypass for NS/EP NGN-PS mechanisms. Though congestion controls are necessary to minimize network instability and to increase the chance that normal public service is not severely degraded, such measures may impact NS/EP NGN-PS unless some exemptions are made to congestion controls. Compromised MMEs misconfiguration or lack of support for these exemptions (i.e., overload bypass actions) might cause denial of service to NS/EP traffic and Service Users.

R-25 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME-specific MCC Bypass actions that are applicable to NS/EP NGN-PS. The minimum set of overload bypass actions requiring protection includes:

(a) MME requesting from its interconnected eNodeBs to throttle traffic for new RRC connection establishment requests and only accept traffic from UEs with certain Establishment Causes (e.g., for emergency and high priority access).
(b) MME permitting RRC connection establishments with High Priority Access requests in addition to the ones currently allowed by "Permit Emergency Sessions and mobile terminated sessions-only" or to entirely forbid such an action to avoid impacting NS/EP NGN-PS[36].
(c) MME disallowing NAS level congestion control for mobile-initiated signaling with Establishment Cause set to "highPriorityAccess".
(d) MME exempting NAS level congestion control for EPS Session Management for mobile termination requests with an ARP for NS/EP NGN-PS use.
(e) MME exempting registered UE load rebalancing for the UE in an ECM-CONNECTED mode when it is handling an active NS/EP NGN-PS call/session as indicated by a bearer having an ARP associated with NS/EP NGN-PS use, except under critical conditions such as when required to perform an MME node restart.
(f) MME not ignoring "Downlink Data Notification" requests from an S-GW that are for an NS/EP NGN-PS call/session termination.

8.1.4 Protection of S-GW Handling & Bypass of Machine Congestion Control Capabilities Used for Priority Resource Allocation of NS/EP NGN-PS

This section provides requirements to ensure the integrity of S-GW Machine Congestion Control Capabilities Bypass for NS/EP NGN-PS mechanisms. Though congestion controls are necessary to minimize network instability and to increase the chance that normal public service is not severely degraded, such measures may impact NS/EP NGN-PS unless some exemptions are made to congestion controls. Compromised S-GWs misconfiguration or not supporting these exemptions (i.e., overload bypass actions) may cause denial of service to NS/EP traffic and Service Users.

The S-GW has the ability to selectively throttle specific messages destined for MME (i.e., GTP-C over S11) based on the priority of the call/session as determined by the ARP associated with the request (e.g., discarding low priority Downlink Data Notification messages during congestion).

R-26 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the S-GW specific MCC Bypass actions that are applicable to NS/EP NGN-PS. The minimum overload bypass action requiring protection includes S-GW exempting from throttling action the following messages when these messages arrive on bearers with their ARP associated with NS/EP NGN-PS use:

(a) "Downlink Data Notification"
(b) "Create Bearer Request"
(c) "Update Bearer Request"

8.1.5 Protection of PDN-GW Handling & Bypass of Machine Congestion Control Capabilities Used for Priority Resource Allocation of NS/EP NGN-PS

This section provides requirements to ensure the integrity of PDN-GW Machine Control Capabilities Bypass for NS/EP NGN-PS mechanisms. Though congestion controls are necessary to minimize network instability and to increase the chance that normal public service is not severely degraded, such measures may impact

[36] 3GPP LTE Standards state that during MME congestion, specific messaging such as emergency sessions and mobile terminating sessions are allowed to be exempted from load shedding.

NS/EP NGN-PS unless some exemptions are made to congestion controls. Compromised PDN-GWs misconfiguration or not supporting these exemptions (i.e., overload bypass actions) may cause denial of service to NS/EP traffic and Service Users.

R-27 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the PDN-GW specific MCC Bypass actions that are applicable to NS/EP NGN-PS. The minimum overload bypass action includes PDN-GW priority handling of the NS/EP NGN-PS signaling over other signaling traffic by dropping packets associated with non NS/EP NGN-PS signaling first.

8.2 NS/EP Special Handling Specific to EPC Network Entities

The LTE EPC features and procedures that support special handling of NS/EP NGN-PS are in need of integrity and confidentiality protections. The subsections below provide a description of the feature and capability, particular vulnerabilities associated with specific procedures along with consequences of exploitation. This provides the context for their subsequent integrity and confidentiality requirements.

8.2.1 NS/EP NGN-PS Special Handling of MME Specific Features

This section describes securing the NS/EP NGN-PS Special Handling features and procedures for EPC's MME entity.

8.2.1.1 Integrity of MME Configuration Data for Mobile Termination Priority Paging: S1-MME

This section provides requirements to ensure the integrity of the NS/EP LTE Service User configuration data used by the MME to signal to the eNodeB the need for mobile termination priority paging initiated by a Service User.

The MME marks mobile termination requests from a Service User which are identified by an appropriate ARP level with the highest Priority Level in Paging Messages when sent to eNodeB. Intentional or unintentional configuration errors of ARP values in the MME or compromised MME misconfiguration or omission of Priority Levels in Paging messages may result in markings for non-NS/EP NGN-PS calls or all calls treated as NS/EP NGN-PS calls. This may result in congestion or cause priority handling to be ignored for NS/EP NGN-PS calls from Service Users.

R-28 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME provisioning process for configuring the NS/EP ARP and the corresponding Priority Level in the Paging message by means such as access control, authentication, and authorization.

R-29 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of stored NS/EP special handling data (i.e., Priority ARP) used for mobile termination establishments.

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats also applies.

8.2.1.2 Integrity of MME Configuration Data for Priority Handling of Bearer Establishment/Modification

This section provides requirements to ensure the integrity of the NS/EP LTE Service User configuration data used by the MME to request priority handling for bearer establishment and modification.

The MME handles bearer session establishment/modification messages (from and to eNodeB, the S-GW, or other MMEs) for NS/EP calls which are identified by NS/EP ARP (highest level ARP).

Intentional or unintentional configuration errors of ARP values in the MME or misconfigurations in compromised MME may result in NS/EP policy rules for priority treatment of the bearers to be ignored in turn this may delay processing of bearer handling messages which could result in poor performance for

NS/EP NGN-PS calls/sessions. Furthermore, as a result of the configuration errors, congestion or priority handling may be ignored for NS/EP NGN-PS calls/sessions from Service Users.

R-30 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME provisioning process for configuring the NS/EP ARP used to signal priority bearer handling by means such as access control, authentication, and authorization.

R-31 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of stored NS/EP special handling data (e.g., ARP) for bearer establishment/modification.

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats also applies.

8.2.1.3 Integrity of MME Incoming Messages Priority Processing: S1-MME, S6a, & S11

This section provides requirements to ensure the integrity of the special handling data processing in the MME for incoming priority messages from the HSS over S6a and from the S-GW over the S11 interface and from the eNodeB (S1-MME). This is to protect the appropriate Priority Level in the ARP for NS/EP use.

Insider attacks or a compromised MME may tamper with ARP values in the incoming messages received from the HSS, S-GW, and eNodeB which may result in NS/EP calls not receiving appropriate priority treatment.

R-32 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of LTE priority signaling to the MME from the eNodeB, HSS, and S-GW.

R-33 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME processing functions for the incoming MME priority messages.

R-34 (Required) The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the MMEs incoming message processing for NS/EP priority handling to detect and report security impacts.

R-34 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of incoming messages received from HSS, S-GWs and eNodeBs with NS/EP specific ARPs per Unit of Time. Refer to Appendix B for more information.

8.2.1.4 Integrity of MME Priority Handover Handling

This section provides requirements to ensure the integrity of the special handling data processing in MME for priority handover.

During handover, the MME encapsulates the NS/EP ARP in handover messages to request priority handling.

Insider attacks or a compromised MME may tamper with the NS/EP ARP values in the handover messages. This may result in ignoring priority handling policies causing failed or delayed handover for NS/EP Service User devices.

R-35 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of the MME outgoing priority messages that signal priority handover.

R-36 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME processing functions that support MME outgoing priority handover messages.

R-37 (Required) The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor outgoing priority handover messaging on the MMEs to detect and report security impacts.

R-37 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of outgoing messages with Priority HO that signal priority treatment per Unit of Time. Refer to Appendix B for more information.

8.2.1.5 Integrity of MME Configuration Data for Priority Transport

This section provides requirements to ensure the integrity of the priority transport initiated by MME:

- Priority Paging: The MME marks mobile call terminations from a Service User (identified by an NS/EP ARP) with appropriate DSCP in the S1-AP Paging message to be sent over the S1-MME interface to the eNodeB.
- Bearer establishment/modification requests: The MME marks bearer establishment/modification messages with appropriate DSCP values to be sent over the S1-MME, S6a, and S11 interfaces.
- TAU related messages: The MME marks TAU messages with appropriate DSCP values to be sent over the S1-MME interface.

Intentional or unintentional configuration errors in the NS/EP ARP, DSCP marking, and/or mapping errors in NS/EP ARP to the DSCP markings in the MME or caused by a compromised MME may result in erroneous priority handling for normal calls resulting in congestion or in denying priority calls to Service Users.

R-38 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME provisioning process for configuring the special handling NS/EP parameters (e.g., NS/EP ARP, appropriate DSCP marking and ARP to DSCP mapping per policy) by means such as access control, authentication, and authorization.

R-39 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of stored NS/EP special handling data in the MME (e.g., NS/EP ARP, DSCP marking and ARP to DSCP mapping per policy).

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats also applies.

8.2.2 NS/EP NGN-PS Special Handling of S-GW Specific Features

This section describes securing the NS/EP NGN-PS Special Handling features and procedures for EPC's S-GW entity.

8.2.2.1 Integrity of S-GW Incoming Messages Priority Processing: S5/S8 & S11

This section provides requirements to ensure the integrity of the special handling data processing in the S-GW for incoming priority messages from MME over S11 and from PDN-GW over the S5/S8 interface. The S-GW handles messages (from the MME or PDN-GW) for NS/EP calls (identified by appropriate ARP) with priority. Insider attacks or a compromised S-GW may tamper with ARP values in the incoming messages received from the MME or PDN-GW which may result in NS/EP calls not receiving appropriate priority treatment.

R-40 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of the LTE priority signaling to the S-GW from the MME and PDN-GW.

R-41 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the S-GW processing functions for the incoming S-GW priority messages.

R-42 (Required) The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the S-GWs incoming message processing for NS/EP priority handling to detect and report security impacts.

R-42 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of incoming messages received from MME and PDN-GW with NS/EP specific ARPs per Unit of Time. Refer to Appendix B for more information.

8.2.2.2 Integrity of S-GW Configuration Data for Priority Transport

This section provides requirements to ensure the integrity of the priority transport initiated by S-GW.

- GTP-U Messages Priority Marking: The S-GW marks GTP-U messages for NS/EP traffic (identified by NS/EP ARP) with appropriate DSCP over S1-U interface to the eNodeB.
- Priority Requests for Bearer Setup/Modification and Session Setup/Modification: The S-GW marks Bearer Setup/Modification Request and Session Setup/Modification Request for NS/EP session (identified by NS/EP ARP) with appropriate DSCP over S11 (to MME) and S5/S8 (to PDN-GW) interfaces.

Intentional or unintentional configuration error in the NS/EP ARP, DSCP marking, and/or mapping errors in NS/EP ARP to the DSCP markings in the S-GW or caused by a compromised S-GW may result in erroneous priority handling for normal calls resulting in congestion or in denying priority calls to Service Users.

R-43 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the S-GW provisioning process for configuring the special handling NS/EP parameters (e.g., NS/EP ARP, appropriate DSCP marking and ARP to DSCP mapping per policy) by means such as access control, authentication, and authorization.

R-44 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of stored NS/EP special handling data in the S-GW (e.g., NS/EP ARP, DSCP marking and ARP to DSCP mapping per policy).

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats also applies.

8.2.3 NS/EP NGN-PS Special Handling of PDN-GW Specific Features

This section describes securing the NS/EP NGN-PS Special Handling features and procedures for EPC's PDN-GW entity.

8.2.3.1 Integrity of PDN-GW Incoming Messages Priority Processing: S5/S8 & Gx

This section provides requirements to ensure the integrity of the special handling data processing in the PDN-GW for incoming priority messages from S-GW.

Insider attacks or a compromised PDN-GW could tamper with ARP values in the incoming messages received from the S-GW or PCRF, which could result in NS/EP calls not receiving appropriate priority treatment.

R-45 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of the LTE priority signaling to the PDN-GW from the S-GW.

R-46 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the PDN-GW processing functions for the incoming S-GW priority messages.

R-47 (Required) The NS/EP NGN-PS Service Provider shall monitor, gather statistics, and quantify the effects of the PDN-GWs incoming message processing for NS/EP priority handling.

R-47 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include the number of incoming messages received from S-GW with NS/EP specific ARPs per Unit of Time.

8.2.3.2 Integrity of PDN-GW Configuration Data for Priority Transport

This section provides requirements to ensure the integrity of the priority transport initiated by PDN-GW.

- Incoming priority messages from S-GW: The PDN-GW handles messages (from the S-GW) for NS/EP calls (identified by NS/EP ARP) with priority
- Priority Requests for Bearer Setup/Modification and Session Setup/Modification: The PDN-GW marks Bearer Setup/Modification Request and Session Setup/Modification Request for NS/EP session (identified by NS/EP ARP) with appropriate DSCP over S5/S8 (to S-GW) interface
- Outgoing priority messages to Core IMS: The PDN-GW marks packets for NS/EP sessions (identified by NS/EP ARP) with appropriate DSCP.

Intentional or unintentional configuration error in the NS/EP ARP, DSCP marking, and/or mapping errors in NS/EP ARP to the DSCP markings in the PDN-GW or caused by a compromised PDN-GW may result in erroneous priority handling for normal calls resulting in congestion or in denying priority calls to Service Users.

R-48 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the PDN-GW provisioning process for configuring the special handling NS/EP parameters (e.g., NS/EP ARP, appropriate DSCP marking and ARP to DSCP mapping per policy) by means such as access control, authentication, and authorization.

R-49 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of stored NS/EP special handling data in the PDN-GW (e.g., NS/EP ARP, DSCP marking and ARP to DSCP mapping per policy).

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats also applies.

8.2.4 NS/EP NGN-PS Special Handling of PCRF Specific Features

This section describes security protection for the NS/EP NGN-PS Special Handling features and procedures for EPC's optional PCRF entity[37].

8.2.4.1 Integrity of PCRF Outgoing Messages Priority Processing: Gx

This section provides requirements to ensure the integrity of the special handling data processing in the PCRF for outgoing priority messages to the PDN-GW.

Insider attacks or a compromised PCRF may tamper with ARP values. This may cause the policy rules appropriate for advance priority to be ignored in the outgoing messages transmitted to the PDN-GW which may result in NS/EP NGN-PS calls not receiving appropriate priority treatment or for non-subscribed UEs to receive advance priority treatment.

R-50 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of the LTE priority signaling to the PDN-GW from the PCRF.

R-51 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the PCRF processing functions for the outgoing PDN-GW priority messages.

[37] The PCRF entity may be collocated within Core IMS infrastructure and/or its LTE features and functions (e.g., LTE bearer management) may be integrated into the Core IMS PCRF entity.

R-52 (Required) The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the PCRF outgoing message processing for NS/EP advance priority handling to detect and report security impacts.

R-52 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of outgoing messages transmitted to the PDN-GW with NS/EP specific ARPs per Unit of Time. Refer to Appendix B for more information.

8.2.4.2 Integrity of Media Bearer Priority (ARP)

This section provides requirements to ensure the integrity of the special handling data stored and processed in the PCRF for the priority media resource allocation for NS/EP traffic.

When a bearer is assigned with an NS/EP specific ARP, the PCRF includes this ARP in the out-going messages on the signaling bearer to the PDN-GW (for GTP-based S5/S8) or to the S-GW for PMIP based S5/S8 to request establishment of the media bearer.

A compromised PCRF may tamper with the ARP populated in the signaling messages and transmitted over the Gx interface resulting in NS/EP traffic not receiving priority handling for the EPS media bearer establishment.

Requirements in Section 8.2.4.1 are applicable.

8.2.4.3 Integrity of Incoming Messages Priority Processing from Core IMS – (Rx)

This section provides requirements to ensure the integrity of the special handling data processing in PCRF for incoming priority messages from Core IMS.

During the establishment of Mobile Origination or Mobile Terminated calls/sessions, the Core IMS (P-CSCF) transmits an “AA-request” command to the PCRF including the “MPS-Identifier” Attribute Value Pair (AVP), and sets the session level “Reservation-Priority” AVP mapped from either the Service User’s priority level or a default priority level. Upon receipt of the above marking and mapping in the “AA-Request” command, the PCRF recognizes that this request is associated with an NS/EP NGN-PS call/session and should be given priority treatment consistent with the Service User’s priority level contained within the session level “Reservation-Priority” AVP.

Insider attacks or a compromised PCRF may tamper with marking, mapping, and processing within PCRF which may result in NS/EP NGN-PS calls not receiving appropriate priority treatment or for non-subscribed UEs to receive priority treatment.

R-53 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of the signaling messages which include priority marking to PCRF from the Core IMS (P-CSCF).

R-54 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the PCRF mapping and processing functions for the incoming messages with priority markings.

R-55 (Required) The NS/EP NGN-PS Service Provider shall establish and implement procedures to monitor the PCRF incoming message mapping and processing for NS/EP priority handling to detect and report security impacts.

R-55 can be achieved by data collection and statistical analysis. Specific measurement data to be collected for this purpose is not specified in this document. Example statistics include: Number of incoming messages received from Core IMS (P-CSCF) requiring NS/EP priority processing per Unit of Time. Refer to Appendix B for more information.

8.2.5 NS/EP NGN-PS Special Handling of HSS Specific Features

This section describes securing the NS/EP NGN-PS Special Handling features and procedures for EPC's optional HSS entity[38] .

8.2.5.1 Integrity of Priority Marking Data

Requirements in Section 8.1.2 are applicable.

8.3 EPC Security Features Critical to Service Users

This section provides requirements to ensure the integrity of EPC entities specific to their MCC Capabilities which indirectly impact NS/EP NGN-PS among other LTE application layer user plane data and applications. Congestion control functions are necessary to minimize network instability and to increase the chance that normal public service and NS/EP NGN-PS traffic are not severely degraded impacting the availability of NS/EP NGN-PS.

8.3.1 Protection of MME Machine Congestion Control Capabilities

Compromised MME, MME misconfigurations, or an MME that does not implement an MCC feature may cause denial of service to normal public services and to the NS/EP traffic (Security aspects of MME Congestion Control Bypass capabilities for NS/EP NGN-PS are covered in Section 8.1.3).

> **R-56 (Required)** The NS/EP NGN-PS Service Provider shall protect the integrity of the MME-specific NAS level congestion control for EPS Session Management and for Mobility Management to ensure network stability during congestion.

8.3.2 S-GW Machine Congestion Control Capabilities

Compromised S-GW, S-GW misconfigurations, or an S-GW that does not implement an MCC feature may cause denial of service to normal public services and to the NS/EP traffic (Security aspects of S-GW Congestion Control Bypass capabilities for NS/EP NGN-PS are covered in Section 8.1.4).

> **R-57 (Required)** The NS/EP NGN-PS Service Provider shall protect the integrity of the S-GW throttling function used to shed Downlink Data Notifications for low priority traffic to ensure network stability during congestion.

8.3.3 PDN-GW Machine Congestion Control Capabilities

Compromised PDN-GW, PDN-GW misconfigurations, or a PDN-GW that does not implement an MCC feature may cause denial of service to normal public services and to the NS/EP traffic (Security aspects of PDN-GW Congestion Control Bypass capabilities for NS/EP NGN-PS are covered in Section 8.1.5).

> **R-58 (Required)** The NS/EP NGN-PS Service Provider shall protect the integrity of the PDN-GW overload control functions used to shed packets on the IMS Signaling Bearers and Media Bearers to ensure network stability during congestion.

[38] The PCRF and/or HSS may be located within the Core IMS infrastructure and support LTE-specific features and functions (e.g., LTE bearer establishment) in an integrated manner with Core IMS PCRF and/or HSS respectively.

8.3.4 PCRF Machine Congestion Control Capabilities

Compromised PCRF, PCRF misconfigurations, or a PCRF that does not implement an MCC feature may cause denial of service to normal public services and to the NS/EP traffic

R-59 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the PCRF overload control functions to ensure network stability during congestion.

9 IP & Transport Security

9.1 Overview

This section discusses security of the underlying IP and transport network services of the LTE network segment, more specifically the LTE backhaul network. The general approach is that security compromises at the IP and transport services level could lead to security compromise of the NS/EP NGN-PS supported over the LTE backhaul network. The requirements and guidance provided in this section are not unique to NS/EP NGN-PS. It is expected that SP will need to implement security measures to protect the IP and transport network, and physical infrastructure for all supported services. However, because compromise to NS/EP NGN-PS could occur via the underlying IP, transport, and physical network infrastructure, this section provides requirements to minimize such security compromises.

9.2 Background

[TR 33.401] and the related documents [TS 33.102], [TS 33.210], and [TS 33.310] define the security architecture for LTE as well as the set of features and mechanisms to be implemented in the different network and service domains to obtain a level of security suitable for the support of the control and data plane of LTE by a backhaul network.

The 3GPP specifications recommend a model where IPsec tunnels are instantiated at the cell site to carry both bearer and signaling traffic across the backhaul network to a Security Gateway in the core network. However, the use of IPsec is not mandatory across the S1 and X2 interfaces. Basically, the 3GPP specifications allow for the usage of IPsec when the SP deems that its backhaul network is “un-trusted”. The use of IPsec in the backhaul network according to the 3GPP specifications is summarized in Table 9.1.

Table 9. 1 - Use of IPsec for LTE Backhaul Security

Planes	S1 Interface		X2 Interface	
	Trusted	**Un-Trusted**	**Trusted**	**Un-trusted**
Control	Optional	Mandatory (Tunnel or Transport Mode)	Optional	Mandatory (Tunnel or Transport Mode)
User	Optional	Mandatory (Tunnel or Transport Mode)	Optional	Mandatory (Tunnel or Transport Mode)
Management	Optional	Mandatory (Tunnel Mode)	X2: Interface does not carry management traffic	

9.3 Identification of “Un-trusted” Backhaul Network Segment

The concept of an “un-trusted” backhaul network is very open ended, and it is left to the SP to decide if the backhaul network is considered to be “un-trusted”. “Un-trusted” could mean many things. For example, it could mean that the backhaul network is provided by another entity (e.g., 3rd party or wholesale transport

provider), or the backhaul is shared by multiple entities. See related requirement in Section 5.2.2 on multi-provider arrangements.

Information on “trusted” and “un-trusted” network segment can also be found in ITU-T Recommendation [ITU-T Y.2701].

Given that security of the NS/EP NGN-PS will depend on the security of the underlying IP and transport network infrastructure, it is important that the SP have a method to determine when the backhaul network is “un-trusted”. More specifically, it is important to know when a particular communication flow (control, user, or management) will be traversing an “un-trusted” segment and IPsec should be used for security protection.

R-60 (Required): The NS/EP NGN-PS Service Provider shall establish and implement a documented plan describing the policies, management, and operational process to identify and distinguish “trusted” versus “un-trusted” IP and transport network segments in the LTE access network.

R-61 (Required): The NS/EP NGN-PS Service Provider documented plan shall have clear criteria as to the determination of “trusted” IP and transport network segments and the applicability of the 3GPP recommendations for use of IPsec in the LTE access network.

R-62 (Required): The NS/EP NGN-PS Service Provider shall establish and implement a management process to periodically review the LTE access network supporting NS/EP NGN-PS to detect if any changes in the underlying IP and transport has resulted in changes from “trusted” to “un-trusted” conditions and take appropriate actions.

R-63 (Required): The NS/EP NGN-PS Service Provider shall periodically update and monitor the plan for improvement.

9.4 Identification of LTE Network Assets

Identification of assets in the LTE access network is important because the identities of network elements are used in conjunction with authentication services to authenticate a requestor’s identity. Identification of assets in the LTE access network is important because the identities of network elements are used in conjunction with authentication services for authorization of network connectivity and access in the LTE access network segment. These assets should include any entity potentially connecting and gaining access to the LTE access network including entities such as Cell on Wheel (COW) used in disaster recovery.

R-64 (Required): The NS/EP NGN-PS Service Provider shall establish and implement a management process to register and uniquely identify assets (e.g., network elements) in the LTE access network.

R-65 (Required): The NS/EP NGN-PS Service Provider shall establish and implement a management process to register and uniquely identify external network entities (e.g., network elements) attaching to the LTE access network (e.g., network elements of other Service Providers).

9.5 Physical Security

Physical security protection of the assets (e.g., network elements and systems) of the LTE access network is very important. Physical security is primarily concerned with restricting physical access by unauthorized people (commonly interpreted as intruders) to facilities hosting LTE network elements and the network elements themselves.

R-66 (Required): The NS/EP NGN-PS Service Provider is required to establish and implement a documented plan in accordance with commercially-available security best practices for physical security protection of LTE access network assets supporting NS/EP NGN-PS.

A major challenge will be physical security protection of the network elements in “un-trusted” zones as described in [ITU-T Y.2701]. For example, wireless and shortrange wireless (femtocells) network systems placed in “un-trusted” zones or environment not controlled by the Service Provider.

For LTE network assets residing in “un-trusted” zones where physical security protection measures cannot be taken, it is desirable that the SP support and implement appropriate security solutions for perimeter monitoring and detect security events originating in the un-trusted zones (e.g., system tamper prevention and detection).

> **O-9 (Optional)** It is desirable that the NS/EP NGN-PS Service Provider implement appropriate security solutions for perimeter monitoring, and detection of security events originating in the LTE access network un-trusted zones.

Information sources for physical security include, but are not limited to:

- [b-GR-815-CORE], Generic Requirements for Network Element/Network System (NE/NS) Security.
- [b-GR-1332-CORE], Generic Requirements for Data Communications Network Security.
- [ITU-T Y.2701], Security requirements for NGN.
- [b-NRIC] Network Reliability and Interoperability Council (www.nric.org) Best Practices (items 6-6-5000 series).
- [b-SP800-53], Security and Privacy Controls for Federal Information Systems and Organizations.
- [b-ISO 27002], Information technology — Security techniques — Code of practice for information security management, Chapter 9 on Physical and Environmental Security with many controls and guidance.

9.6 Security Protection of Synchronization Mechanisms

The synchronization mechanisms of the LTE access network could be targeted for attacks because loss of synchronization could lead to radio link QoS and availability impacts. The synchronization features may also be applicable to security mechanisms that rely on the usage of timestamps (e.g., certificates).

It is possible that SP may choose to not encrypt synchronization traffic because of possible impact on the overall performance of synchronization protocols such as [b-IEEE 1588] and to avoid the operational burden. However, it is important that the synchronization mechanisms be protected against security compromise including internal attacks that enable, for example, delay insertions or cause quality of service degradation because it could lead to security impacts (e.g., integrity and availability) on the LTE access network and affect its ability to support NS/EP NGN-PS as intended.

> **R-67 (Required):** The NS/EP NGN-PS Service Provider shall protect the integrity of the synchronization mechanisms used within the LTE network.
>
> **R-68 (Required):** The NS/EP NGN-PS Service Provider shall protect the integrity of synchronization communications traffic (e.g., IEEE 1588v2 protocol) within the LTE network.
>
> **R-69 (Required):** The NS/EP NGN-PS Service Provider shall protect the availability of the synchronization mechanisms used within the LTE network.
>
> **R-70 (Required):** The NS/EP NGN-PS Service Provider shall protect the availability of synchronization communications traffic (e.g., IEEE 1588v2 protocol) within the LTE network.

9.7 Security Protection of IP Transport Routing Functions & Protocols

The requirements, objectives and conditional requirements defined in Section 11 (IP Transport Network Security) of the [ATIS-1000055] document are applicable to the LTE access network segment and should be supported.

10 Management Plane Security

10.1 Background: The S&P "Space"

See Section 10 of [ATIS-1000055]. For LTE access networks, the systems and platforms (S&P) of interest in this section are those involved in providing the E-UTRAN and the EPC.

10.2 Common Management Plane Security Requirements

All requirements found in Section 10.1of [ATIS-1000055] also apply to LTE access network Service Providers. In particular, further elaboration on the following requirements is provided in Section 7.3.

- **NGN Priority Services Data Integrity**: The Service Provider shall protect the integrity of NGN Priority Services provisioned data (see [ATIS-1000055], R-73). The Service Provider shall protect the integrity of any data distribution, transmission, updates or changes, and any offline data[39] associated with NGN Priority Service (see [ATIS-1000055], R-75).
- **Configurable Parameters and Default Values:** The Service Provider is required to establish and enforce rules for the administration of configurable parameters and default values in the context of supporting NGN Priority Services applications. Access control measures shall be implemented and enforced so that the execution of these functions is reserved only for the authorized administrator (i.e., all other users shall be denied this permission) (see [ATIS-1000055], R-86).
- **Data Confidentiality**: The Service Provider shall protect sensitive NGN Priority Services provisioned or stored data on S&Ps (e.g., subscription data) from unauthorized disclosure (e.g., protection from unauthorized insiders). This includes any sensitive offline data associated with NGN Priority Services. Sensitive data includes NGN Priority Services subscription information, usage records and other logged information (see [ATIS-1000055], R-88).

10.3 Specific Considerations for LTE Access Networks

10.3.1 E-UTRAN & E-UTRAN-to-EPC Interface

The requirements in this section address the security protection of management plane interactions which are specific to eNodeBs and to S1[40] (interface between the eNodeB and EPC components). For S1, a separate IPsec tunnel shall be used to carry management plane traffic (i.e., separate from control plane and data plane traffic). X2 (interface between eNodeBs) does not carry management plane traffic.

> **R-71 (Required)** For E-UTRAN used to support NS/EP NGN-PS, the NS/EP NGN-PS Service Provider shall enforce requirements pertaining to management plane interactions as specified in clause 13 of [TS 33.401].

10.3.1.1 eNodeB

10.3.1.1.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

[ATIS-1000055] R-75 applies to the NGN Priority Services offline data.

10.3.1.1.1.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data.

[39] Offline data resides in a system (e.g., an OSS) other than an FE.

[40] The discussion of S1 in this section applies to both S1-MME and S1-U.

[ATIS-1000055] R-88 applies to the NGN Priority Services offline data.

103.1.1.3 Security Features Critical to NS/EP NGN-PS

eNodeB security features for setup and configuration, key management, and secure environment, as specified by [TS 33.401], are foundational for LTE access networks. Although they should always be provided (regardless of the presence of NS/EP NGN-PS), they are discussed here since they are considered to be crucial for securing NS/EP NGN-PS Service Provider LTE Access Networks. Since they are expected to be present regardless of the presence of NS/EP NGN-PS, no new requirements (unique to NS/EP NGN-PS) are provided in this section.

Setting up and configuring eNodeBs shall be authenticated and authorized so that attackers shall not be able to modify the eNodeB settings and software configurations via local or remote access.

- The support of security associations is required between the EPC and the eNodeB and between adjacent eNodeBs, connected via X2. These security association establishments shall be used for user and control plane communication between the entities[41].
- Communication between the OA&M systems and the eNodeB shall be confidentiality- and integrity-protected from unauthorized parties.
- The support of security associations is required between the eNodeB and an entity in the EPC or in an OA&M domain trusted by the operator. These security association establishments shall be mutually authenticated.
- The eNodeB shall allow only authorized changes to its software and data.
- The eNodeB shall use authorized data and software.
- Sensitive parts of the boot-up process shall be executed with the help of the secure environment.
- Confidentiality of software transfer via the management plane towards the eNodeB shall be ensured.
- Integrity protection of software transfer via the management plane towards the eNodeB shall be ensured.

The EPC provides subscriber-specific session keying material for the eNodeBs, which also hold long-term keys, used for authentication and security association setup purposes. Protecting all these keys is important.

- Keys stored inside eNodeBs shall never leave a secure environment within the eNodeB except when done in accordance with 3GPP security specifications.

The secure environment is logically defined within the eNodeB and is a composition of functions for the support of sensitive operations.

- The secure environment shall support secure storage of sensitive data, e.g., long term crypto-graphic secrets and vital configuration data.
- The secure environment shall support the execution of sensitive functions, e.g., en/decryption of user data and the basic steps within protocols which use long term secrets (e.g., in authentication protocols).
- Sensitive data used within the secure environment shall not be exposed to external entities.
- The secure environment shall support the execution of sensitive parts of the boot process.
- The secure environment's integrity shall be assured.
- Only authorized access shall be granted to the secure environment, i.e., to data stored and used within, and to functions executed within.

[41] See Section 4 of this document for security requirements that pertain to the user and control plane communications.

10.3.1.2 S1 Interface (Management)

Clause 13 of [TS 33.401] includes security features for management plane protection over the S1 interface. The security features specified in clause 13 of [TS 33.401] are discussed here since they are crucial for securing NS/EP NGN-PS Service Provider E-UTRAN, but no additional requirements (beyond those in [TS 33.401]) are provided in this section. eNodeB security features for setup and configuration, key management, and secure environment, as specified by [TS 33.401], are foundational for LTE access networks. Although they should always be provided (regardless of the presence of NS/EP NGN-PS), they are discussed here since they are considered to be crucial for securing NS/EP NGN-PS Service Provider LTE Access Networks. Since they are expected to be present regardless of the presence of NS/EP NGN-PS, no new requirements (unique to NS/EP NGN-PS) are provided in this section.

- In order to achieve management plane protection over the S1 interface, IPsec Encapsulating Security Payload as profiled by TS 33.210, "3G security; Network Domain Security (NDS); IP network layer security", shall be implemented for all OA&M related traffic; i.e., the management plane, with confidentiality, integrity, and replay protection.
- Tunnel mode IPsec shall be implemented on the eNodeB for supporting the management plane. On the core network side, a Security Gateway may be used to terminate the IPsec tunnel. If no Security Gateway is used, the IPsec tunnel may be terminated in the Element Manager.
- If the sender of IPsec management plane[42] traffic uses DiffServ Code Points (DSCPs) to distinguish different QoS classes, either by copying DSCP from the inner IP header or directly setting the encapsulating IP header's DSCP, the resulting traffic may be reordered to the point where the receiving node's anti-replay check discards the packet. If different DSCPs are used on the encapsulating header, then to avoid packet discard under one Internet Key Exchange (IKE) Security Association and with the same set of traffic selectors, distinct Child-SAs should be established for each of the traffic classes (using the DSCPs as classifiers) as is specified in RFC 4301.
- For the management plane, IKEv2 with certificates based authentication shall be implemented on the eNodeB. The certificates shall be implemented according to the profile described by TS 33.310, "Network Domain Security (NDS); Authentication Framework (AF)". IKEv2 shall be implemented conforming to the IKEv2 profile described in TS 33.310.
- If management traffic is not carried over the same backhaul link as S1 traffic, then other security mechanisms and certificate profiles may be used. However, such other mechanisms must provide mutual authentication based on certificates, as well as confidentiality, integrity and replay protection. These functions shall have at least equal strength as that provided by the use of IKEv2/IPsec.
- If the S1 management plane interfaces are trusted (e.g., physically protected), then the use of protection based on IPsec/IKEv2 or equivalent mechanisms is not needed.

10.3.2 EPC

The requirements in this section address the security protection of management plane interactions which are specific to EPC FEs (MME, S-GW, PDN-GW, PCRF, and optionally HSS).

It is assumed that management plane traffic is not carried across NNI between two Service Providers.

It is assumed that the EPC-to-IMS interface (Gx) and the EPC inter-domain interface (SGi) within a single Service Provider network might carry management plane traffic.

Management plane interactions with EPC FEs occur via Integration Reference Point (IRP) Interfaces. 3GPP publishes a number of IRP specifications, each of which is related to a set of operations and notifications for a specific telecom management domain such as alarm management, configuration management, etc. For EPC FEs used to support NS/EP NGN-PS, secured IRPs must be used as defined in 3GPP TS 32.372, "Telecommunication management; Security services for Integration Reference Point (IRP); Information

[42] Note that in [ATIS-1000055], a similar consideration is discussed when IPsec tunnel mode encryption is used for signaling and media traffic.

Service (IS)". The management information (e.g., Management Information Base) unique to NS/EP NGN-PS that needs to be secured is discussed in Sections 7.3.2.1 through 7.3.2.4.

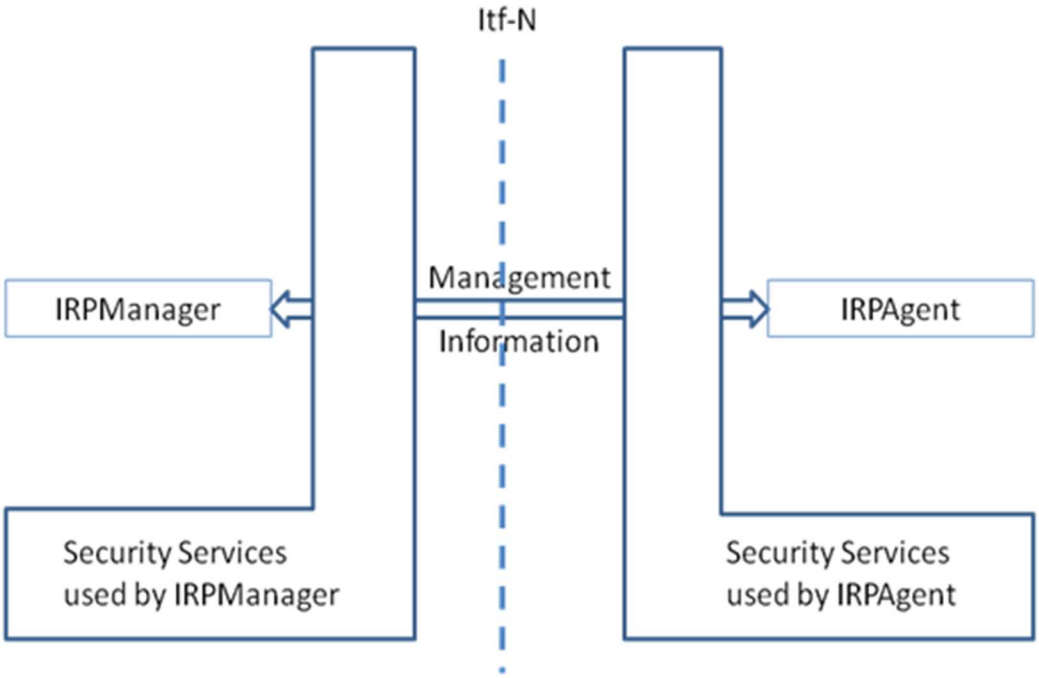

Figure 10. 1 - Security Architecture for a secured IRP

Figure 10.1 shows a view of the architecture of the IPRAgent (functions within EPC FEs) and IRP-Manager in the context of a Secured IRP. Secured communication between IRPManager and IRPAgent is realized by using one or more Security Services to address the specific identified threats. As specified in [TS 33.401], the underlying IP transport network for Itf-N may be protected using IPSec/IKEv2. However, if the Itf-N interfaces are trusted (e.g., physically protected), then the use of IPSec/IKEv2 or equivalent mechanisms is not needed.

The [ATIS-1000055] specifies the following requirements that are applicable to the EPC:

- **Authentication:** The Service Provider shall identify, **authenticate,** and authorize administrators and remote systems before giving them access to S&Ps supporting NGN Priority Services. Only authorized administrators and remote systems shall be granted system access (see [ATIS-1000055], R-68).
- **Authorization:** The Service Provider shall identify, authenticate, and **authorize** administrators and remote systems before giving them access to S&Ps supporting NGN Priority Services. Only authorized administrators and remote systems shall be granted system access (see [ATIS-1000055], R-68).
- **Integrity Protection:** The Service Provider shall **protect the integrity** of any data distribution, transmission, updates or changes, and any offline data[43] associated with NGN Priority Service (see [ATIS-1000055], R-75).
- **Activity Log:** The Service Provider shall generate and maintain **security logs** of successful and unsuccessful attempts to administratively access S&Ps supporting NGN Priority Service (see [ATIS-1000055], R-76). For administrative access to S&Ps supporting NGN Priority Services the Service Provider shall **capture and record** all activities (e.g., additions, changes, and removal of accounts, changes to the access authorizations of account holders) (see [ATIS-1000055], R-77).

[43] Offline data resides in a system (.e.g.,, an OSS) other than an FE.

The requirements given below provide mechanisms to achieve the requirements listed above:

R-72 (Required) For EPC FEs used to support NS/EP NGN-PS, the NS/EP NGN-PS Service Provider shall utilize the Authentication Security Service as specified in [TS 32.372] to realize the authentication security requirement for the management plane.

R-73 (Required) For EPC FEs used to support NS/EP NGN-PS, the NS/EP NGN-PS Service Provider shall utilize the Authorization Security Service as specified in [TS 32.372] to realize the authorization security requirement for the management plane.

R-74 (Required) For EPC FEs used to support NS/EP NGN-PS, the NS/EP NGN-PS Service Provider shall utilize the File Integrity Security Service as specified in [TS 32.372] to realize the integrity protection security requirement for the management plane.

R-75 (Required) For EPC FEs used to support NS/EP NGN-PS, the NS/EP NGN-PS Service Provider shall utilize the Activity Log Security Service as specified in [TS 32.372] to realize the activity log security requirement for the management plane.

10.3.2.1 MME

10.3.2.1.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

[ATIS-1000055] R-75 applies to the NGN Priority Services offline.

10.3.2.1.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data.

[ATIS-1000055] R-88 applies to the NGN Priority Services offline data.

10.3.2.2 S-GW

10.3.2.2.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

10.3.2.2.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data.

10.3.2.3 PDN-GW

10.3.2.3.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

10.3.2.3.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data.

10.3.2.4 PCRF

10.3.2.4.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

10.3.2.4.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data.

10.3.2.5 SPR

10.3.2.5.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

10.3.2.5.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data.

10.3.2.6 HSS

10.3.2.6.1 NGN Priority Services Data Integrity

[ATIS-1000055] R-73 and [ATIS-1000055] R-86 apply to the NGN Priority Services provisioned data.

10.3.2.6.2 NGN Priority Services Data Confidentiality

[ATIS-1000055] R-88 applies to the NGN Priority Services provisioned data identified.

10.4 Management of Security

According to Section 12 of [ATIS-1000055], Service Providers need a comprehensive process to manage the design, implementation, and operation of security solutions, measures, practices, tools, and capabilities that must be adopted and implemented to ensure the security of NGN Priority Services in the evolving NGN environment. The objectives and requirements that relate to the overall management of NGN Priority Services security found in that section need to be applied not only to core networks, but to LTE access networks as well. While all of these objectives and requirements will be impacted by the presence of LTE access networks, particular attention should be paid to those pertaining to risk assessment and management of supply chain issues.

11 Availability Protection

A distributed denial-of-service (DDoS) is a DoS attack in which large numbers of compromised systems (sometimes called a botnet) attack a single target.

NS/EP NGN-PS must be protected against DoS, DDoS, and other types of attacks in the LTE Access Network that could affect NS/EP NGN-PS availability. This includes protection against LTE Access Network attacks affecting NS/EP NGN-PS availability for individual Priority Services Users, a group of Priority Services Users, Priority Services Users in a specific location or site (e.g., Government Agency enterprise network site), Priority Services User in a targeted geographic or regional area, or NS/EP NGN-PS as a whole.

From an LTE Access Network perspective, E-UTRAN eNodeBs perform an access gateway function interfacing with the UEs and are vulnerable to DoS and DDoS attacks via radio frequency jamming or by launching distributed attacks from many UEs towards part of the network or attacks against other UEs. In addition, PDN Gateways, which are part of the EPC, perform an LTE network gateway function and may be exposed to trusted but vulnerable or un-trusted networks. Consequently, they are vulnerable to DoS and DDoS attacks launched from these networks.

11.1 eNodeB (D)DoS Attacks

The eNodeB acts as an access gateway for the LTE access network and is also the E-UTRAN network element that interfaces with UEs via LTE-Uu interfaces. eNodeB provides termination for major LTE security functions (e.g., RRC signaling) and is expected to be deployed in vulnerable locations, potentially exposed to insider and outsider attacks.

A variety of network infrastructure components such as Security gateways, Intrusion Detection Systems (IDSs) and network QoS monitoring tools, and firewalls with Access Control Lists (ACLs) that perform ingress IP packet filtering, ingress/egress rate limiting can protect against DoS attacks. In addition, policies may be defined for the eNodeB to protect against DoS attacks launched from many UEs towards part of the network or attacks against other UEs. Other related policies may include procedures to ensure eNodeB physical security and eNodeB authentication and access authorization with high assurances.

NS/EP NGN-PS should be highly available to the Service User which means NS/EP NGN-PS must be protected against DoS and DDoS threats potentially affecting NS/EP NGN-PS availability to the NS/EP NGN-PS Service User.

> **R-76 (Required)** The NS/EP NGN-PS Service Provider shall protect its EPS infrastructure against DoS, DDoS, and other types of attacks arising from the potential exposure of the eNodeBs to frequency jamming and UE-initiated attacks by applying industry best practices for mobile networks.

[ATIS-1000055] Section 12.4.3, Requirements for Management of Insider Threats, also applies.

11.2 PDN Gateway (D)DoS Attacks

The PDN-GW acts as a network gateway router for the LTE access network, and is also the EPC network element interfacing to each PDN via SGi interfaces, potentially including the Internet. As such, it bears responsibility to protect the UE and the LTE infrastructure from attacks originating in these networks.

A variety of network infrastructure components such as Border gateways and/or content-aware gateways with Deep Packet Inspection (DPI) capabilities, IDSs and network QoS monitoring tools, and firewalls with ACLs that perform IP packet filtering have been used to protect against DoS Attacks from un-trusted networks. In addition, policies may be defined at the PDN-GW to protect against DoS attacks. As SGi and Rx are inter-domain interfaces, these interfaces need to be secured.

NS/EP NGN-PS should be highly available to the Service User which means NS/EP NGN-PS must be protected against DoS and DDoS threats potentially affecting NS/EP NGN-PS availability to the NS/EP NGN-PS Service User.

> **R-77 (Required)** The NS/EP NGN-PS Service Provider shall protect its EPS infrastructure against DoS, DDoS, and other types of attacks arising from the potential exposure of the PDN-GW routers to the public Internet by applying industry best practices for protecting mobile networks.

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats, also apply.

11.3 Other Types of Attacks

11.3.1 Radio Access Network Frequency Jamming Attacks

In general there are some concerns that LTE access networks could be vulnerable to jamming attack techniques on the Radio Access Network (RAN). See [b-MIT] discussing a particular study of the issue. There are varying opinions as to whether such attacks are possible and what the effects of such attacks could be. The main concern is whether such attacks, if successful, could have implications on NS/EP NGN-PS availability. For example, sophisticated attackers targeting specific locations where first responders are expected or cell towers in a disaster region during a terrorist attack.

R-78 (Required) The NS/EP NGN-PS Service Provider shall protect its RAN infrastructure against frequency jamming or other types of attacks impacting NS/EP NGN-PS in accordance with commercially-available security tools and best practices.

R-79 (Required) The NS/EP NGN-PS Service Provider shall support and implement capabilities to detect location information (e.g., geographical and cell location information) of sources of frequency jamming attacks impacting NS/EP NGN-PS availability in accordance with commercially-available radio frequency monitoring and security tools and industry best practices.

Robust network design and implementation of appropriate network diversity practices is also important to counter these types of attacks (see Section 11.3.2).

11.3.2 Masquerading Attacks

It is expected that the LTE access network will have a number of different types of movable as-sets attaching and detaching to the network such as cell on wheel (COW). A COW is a mobile cell site that consists of a cellular antenna tower and electronic radio transceiver equipment on a truck or trailer. They are typically used to provide expanded cellular network coverage and/or capacity at special events (e.g., news and sporting events) and used in disaster areas where there is damage to the cellular infrastructure.

A security concern is the possibility that unauthorized entities could obtain equipment such as COW expressly to initiate attacks during a disaster already in progress. It is expected that such attacks are more likely to be initiated by insiders.

Refer to [ATIS-1000055] Section 12.4.3 for requirements on management of insider threats and Section 8.2.3 for requirements on authorization and privilege management.

11.3.3 Diversity & Redundancy for Survivability

The requirements R-125 through R-130 in Section 13.5 (Diversity and Redundancy for Survivability) of the [ATIS-1000055] document are also applicable to the LTE access network segment and should be supported accordingly.

12 NS/EP NGN-PS Special Handling for Priority Circuit-switched Fallback

The Evolved Packet System (EPS) is an all-IP packet switched domain unlike older 3GPP networks such as UMTS or non 3GPP networks such as CDMA2000, which support both circuit-switched domain and packet switched domain.

The requirements in this section address the security protection of the NS/EP priority circuit-switched fallback (CSFB) from EPS to specific circuit switched domains (i.e., UMTS or CDMA2000 1xRTT). The priority CSFB is a special handling case of the CSFB as documented in (3GPP TS 23.272) stage 2 specifications which describe CSFB system-wide functions. CSFB relies on reuse of the existing circuit

switched domain infrastructure until VoLTE with IMS as its core network and its supported UEs become available.

Section 12.1 provides an overview and security requirements for the priority CSFB to UMTS and Section 12.2 provides an overview and security requirements for priority CSFB to CDMA2000 1xRTT.

Both Sections 12.1 and 12.2 only consider non-roaming reference architectures.

12.1 Priority Circuit-switched Fallback to UMTS

NOTE: If the NS/EP NGN-PS Service Provider implements CSFB to UMTS, then the requirements in this section apply for the priority aspects of CSFB to UMTS.

CSFB in EPS enables the provisioning of voice services by reuse of Circuit-Switched (CS) infrastructure when the UE is served by E-UTRAN. A CSFB-enabled UE, attached to the E UTRAN may use 3GPP radio systems such as GERAN or UTRAN CS domain to establish an originating or terminating voice call. The non-roaming architecture for CSFB to UMTS is shown in Figure 12.1.

As illustrated in Figure 12.1, in addition to FEs in EPS, UMTS MSC, UMTS SGSN, and UTRAN RNS are involved in CSFB. CSFB uses many of the existing priority mechanisms used for supporting NS/EP NGN-PS in EPS.

The SGs interface between the MSC and the MME allows mobility management signaling and for the MSC to send the Paging Request to the MME for a terminating voice call. In UTRAN, the UE uses the UMTS-Uu interface to establish RRC connection as well as to establish voice calls in UMTS.

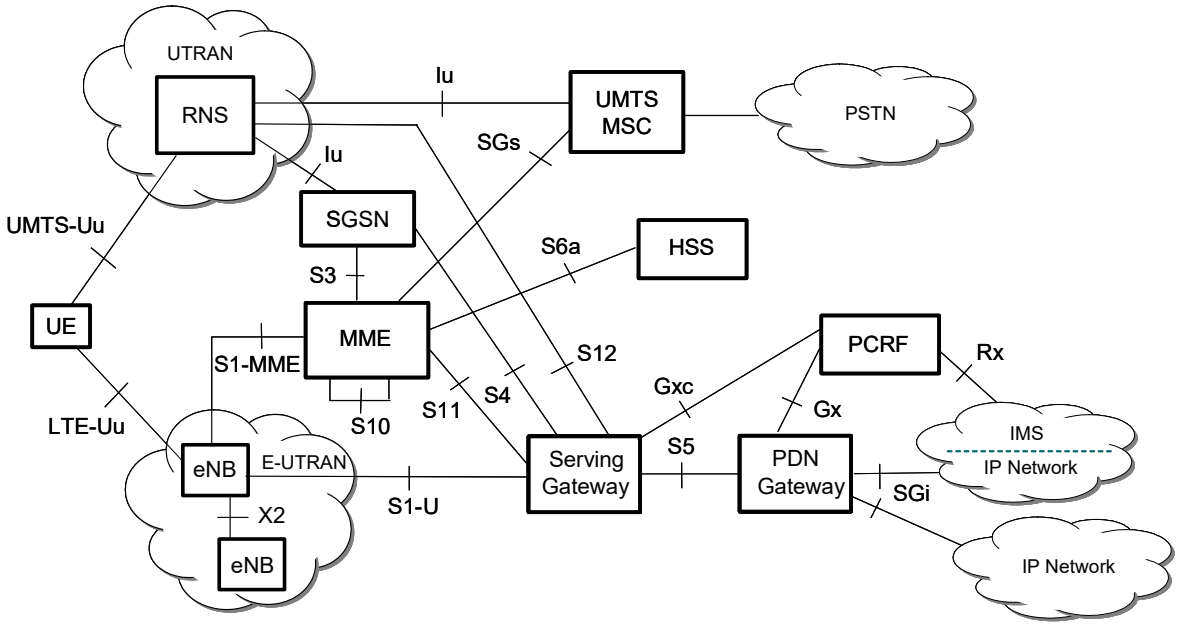

Figure 12. 1 - Non Roaming Architecture for CSFB to UMTS

CSFB is only available when the E UTRAN coverage is overlapped by the UTRAN coverage. For CSFB to occur, the UE has to be both IMSI attached (i.e., attached to UMTS CS domain) as well as attached to EPS. However, since a UE can receive and transmit in only one access network at any given time (unless it has dual Rx/Tx), the UE listens to only E-UTRAN while in E-UTRAN coverage area.

In order to support CSFB with priority, the HSS stores the MPS-CS-Priority bit in MPS-Priority AVP for the NS/EP NGN-PS subscribed UE. During Attach to the EPS, this indication is downloaded from the HSS to

the MME. For Mobile Originating CSFB calls, the MME uses this indication to handle requests from such UEs with priority and sets the “CSFB High Priority” value of the “CSFB Indicator” Information Element (IE) and sends it to the eNodeB. For Mobile Terminating CSFB calls, the UMTS MSC includes the priority indication in the Page Request message to the MME and the MME uses this indication to set the “CSFB High Priority” value of “CSFB indication” IE sent to the eNodeB.

The CSFB to UMTS solution relies on WPS in UMTS which provides for UE redirected handover from UMTS CS to GSM CS when capacity is not available in the RNS to support the call. See WPS UMTS IR for details.

There are four scenarios to consider for priority CSFB to UMTS. They are:

1. Mobile Origination with PS handover.
2. Mobile Origination without PS handover.
3. Mobile Termination with PS handover.
4. Mobile Termination without PS handover.

The following priority aspects are required to support CSFB in addition to what is already specified for NS/EP NGN-PS. These priority aspects need to be secured for CSFB.

12.1.1 Priority CSFB Configuration Data – HSS

HSS stores the MPS-CS-Priority bit in MPS-Priority AVP for the NS/EP NGN-PS subscribed UE.

Compromised HSS Provisioning System and tampering with the NS/EP NGN-PS subscribed UE information within the HSS are examples of major vulnerability threats related to the Priority CSFB.

> **R-80 (Required)** The NS/EP NGN-PS Service Provider shall secure the configuration of the priority CSFB by protecting the integrity of HSS Provisioning Process in which NS/EP data is stored and processed.

[ATIS-1000055] Section 12.4.3, Requirement for Management of Insider Threats also applies.

12.1.2 Confidentiality of MME Incoming Message Handling for Priority CSFB - MME

For an NS/EP NGN-PS subscribed UE, the MME receives a priority indication (MPS-CS-Priority bit of MPS-Priority AVP) in the Update Location Answer message during Attach procedure. This is received from the HSS over S6a. This information is used in MME for later priority processing during Mobile Originated CSFB to UMTS.

Insider attacks or a compromised MME may allow tampering with MPS-CS-Priority bit of MPS-Priority AVP in the Update Location Answer received from the HSS which may result in priority Mobile Originated CSFB calls not receiving appropriate priority treatment.

> **R-81 (Required)** The NS/EP NGN-PS Service Provider shall protect the confidentiality of CSFB Priority indication sent from the HSS to the MME.

12.1.3 Integrity of NS/EP LTE Access Class Procedures for Priority CSFB: LTE-Uu

Access Class Barring parameter for CSFB is a parameter broadcast in E-UTRAN SIB Type 2 to inform the UE if CSFB origination is subject to ACB or not. CSFB relies on an extended service request which includes the “highPriorityAccess” Establishment Cause

A UE that has been modified to omit the rules for RRC connection establishment can gain unfair access to RACH that this mechanism is intended to protect. Intentional or accidental failure can result in an NS/EP NGN-PS subscribed UE facing greater than expected competition for the limited resources of the RACH, reducing the availability of radio resources to NS/EP NGN-PS subscribed UEs.

R-7, R-8, and R-9 are applicable to CSFB to UMTS.

12.1.4 Integrity of Paging Messages for CSFB & Priority Processing - MME

Priority indication in the “Paging Request” message from the UMTS MSC to the MME is received over SGs for Mobile Terminating CSFB to UMTS.

Insider attacks or a compromised MME may allow tampering with priority indication in the paging request received from UMTS MSC which may result in priority Mobile Terminating CSFB calls not receiving appropriate priority treatment.

R-82 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of CSFB priority indication to the MME in the Paging Request from UMTS MSC.

R-83 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the MME processing functions for the incoming MME messages with CSFB priority indication.

12.1.5 Integrity of CSFB Priority Messages & Processing - eNodeB

Priority indication “CSFB High Priority” is received in the Initial Context Setup Request from the MME to eNodeB. This is for both priority CSFB terminating call or for CSFB originating calls (by an NS/EP subscribed UE) over S1-MME. For CSFB without PS Handover, the eNodeB includes “csFallbackHighPriority” Release Cause value in RRC Connection Release message to the UE.

Insider attacks or a compromised eNodeB may allow tampering with priority indication in the Initial Context Setup Request received from MME or RRC Connection Release sent to the UE which may result in Mobile Originating CSFB or Mobile Terminating CSFB calls not receiving appropriate priority treatment.

R-84 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of CSFB priority indication sent by MME to eNodeB and from eNodeB to UE.

R-85 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the eNodeB processing functions for both incoming and outgoing messages with CSFB priority indication.

12.1.6 Integrity of Priority Indication sent by E-UTRAN to UTRAN during Priority CSFB with PS Handover

CSFB with PS Handover requires transfer of “CSFB High Priority” indication sent by eNodeB to RNS in a transparent container via the MME and UMTS SGSN.

Insider attacks or compromised E-UTRAN and/or UTRAN FEs may allow tampering with priority indication in the transparent container carried from eNodeB to RNS via MME and UMTS SGSN which may result in priority CSFB calls not receiving appropriate priority treatment.

R-86 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of CSFB High Priority indication transferred between E-UTRAN and UTRAN during CSFB.

R-87 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the E-UTRAN and UTRAN FE processing functions transferring “CSFB High Priority” indication.

12.1.7 Integrity of RRC Connection Request Procedure to UTRAN for CSFB via Release with Redirection to UMTS - UE

When PS handover is not supported for Mobile originated or Mobile terminated calls, UE sends “Originating High Priority Signaling” or “Terminating High Priority Signaling” Establishment Cause to the RNS.

The availability of NS/EP NGN-PS CSFB could be compromised by rogue UEs manipulating the “Establishment Cause” to request priority for all CSFB calls that may result in eNodeB not having resources to provide priority for priority CSFB calls.

R-88 (Required) The NS/EP NGN-PS Service Provider shall, as part of its UE vetting process, verify the integrity of the RRC Connection Request procedure specific to UMTS.

12.1.8 Integrity of Priority CSFB Processing – UMTS MSC

UMTS MSC needs to recognize priority indication in the "CM[44] Service Request" message from UE via RNS for priority mobile originated calls and in the ISDN User Part (ISUP) Initial Address Message (IAM) message from the Public Switched telephone Network (PSTN) for priority terminated calls.

Insider attacks or a compromised UMTS MSC may allow tampering with priority indication in the CM Service Request received from the RNS or priority indication in the IAM which may result in Mobile Originated CSFB calls or priority Mobile Terminating CSFB calls not receiving appropriate priority treatment.

R-89 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the UMTS MSC processing functions based on priority indication received in IAM and CM Service Request.

NOTE: The rest of the call set up procedure is based on the UMTS WPS which includes recognition of WPS invocation (e.g., *272 dialed digit prefix) and authorization procedures. Security associated with WPS aspects of MSC is for further study.

12.2 Priority Circuit-switched Fallback to CDMA 1xRTT

NOTE: If the NS/EP NGN-PS Service Provider implements CSFB to CDMA2000 1xRTT, then the requirements in this section apply for the priority aspects of CSFB to 1xRTT.

A CSFB-enabled UE, attached to the E UTRAN may use a non-3GPP trusted network such as CDMA2000 1xRTT Circuit-Switched Domain (CSD) to establish an originating or terminating voice call.

The non-roaming architecture for CSFB to CDMA 2000 1xRTT is shown in Figure 12.2. The 1x Interworking Solution (IWS) function may be collocated at the 1x BS location (as shown in Figure 12.2) or it may be standalone. When the IWS provides support for High Rate Packet Data (HRPD) interworking, the IWS will be collocated at the HRPD access network location. Figure 12.2 shows the case where the A1 interface connects the 1x MSC with a collocated IWS to the 1x BS.

[44] Connection Management

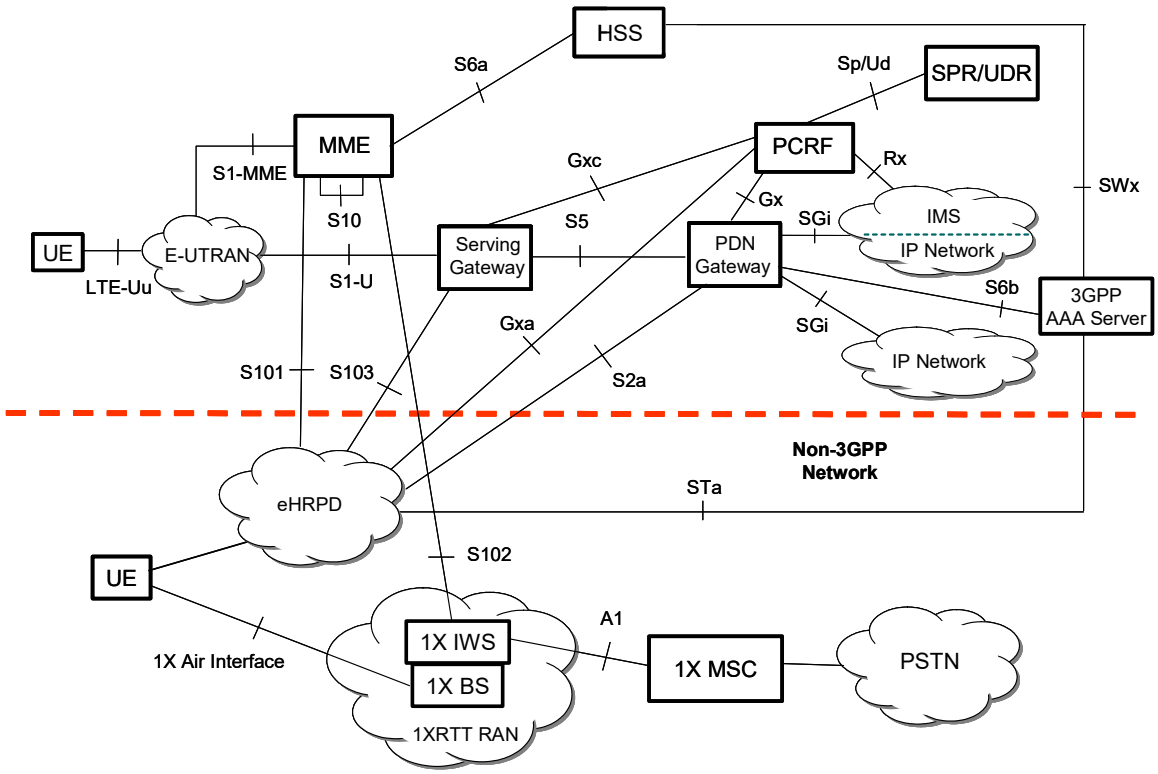

Figure 12. 2 – Non-Roaming Architecture for CSFB to CDMA 2000 1xRTT

As illustrated in Figure 12.2, in addition to FEs in EPS, a 3GPP2 1x Interworking Solution (IWS) and 1x Mobile Switching Center (MSC) are involved in CSFB. The S102 interface provides a tunnel between the 1x IWS and the MME. It is used to signal the MME to page the UE in E-UTRAN for a Mobile Terminating (MT) voice call and also to carry an "A21-1X Air Interface Signaling" message between the 1xIWS and the MME. The "A21-1X Air Interface Signaling" message encapsulates either the CDMA2000 1xRTT "Origination" message originating from a UE or the "Universal Handover Direction Message" message originating from CDMA2000 1xRTT network for evolved CSFB (eCSFB).

CSFB or eCSFB to 1xRTT is only available when the E UTRAN coverage is overlapped by the CDMA2000 1xRTT radio coverage. For CSFB to occur, the UE has to be attached in the E-UTRAN and pre-registered with 1xRTT CS domain service in CDMA2000 1xRTT. However, since a UE can receive and transmit in only one access network at any given time (unless it has dual Rx/Tx), the UE listens only to E-UTRAN.

As described in Section 12.1 and similar to CSFB to UMTS, in order to support CSFB with priority, the HSS stores the MPS-CS-Priority bit in MPS-Priority AVP for the NS/EP NGN-PS subscribed UE. At the time of Attach, the "MPS-Priority" AVP is downloaded from the HSS to the MME. For Mobile Originated CSFB calls, the MME uses this indication to handle requests from such UEs with priority and sets the "CSFB Indicator" IE value to "CSFB High Priority" and sends it to the eNodeB in the Initial Context Setup Request. For Mobile Terminated CSFB calls, the 1x MSC includes the priority indication in the Page Request message ("Call Priority" bits of the "Generic Circuit Services Notification Application (GCSNA) Status" IE) to the MME and the MME uses this indication to set the "CSFB Indicator" value to "CSFB High Priority" and sends it to the eNodeB.

Two types of procedures are supported: denoted CSFB and eCSFB. CSFB is based on RRC Connection Release with UE redirection, while eCSFB provides for allocation of resources at the 1xBS prior to signaling the UE to retune its transceiver to 1xRTT. CSFB is not suited for NS/EP NGN-PS as it does not provide for continuation of PS services during a CS call. The eCSFB approach is therefore preferred. The eCSFB uses a handover mechanism over the S102 interface which is available to signal the 1xIWS prior to releasing the RRC connection in the E-UTRAN.

Based on the two types mentioned above, there are four different scenarios to consider for CSFB to CDMA2000 1xRTT. They are:

1. Mobile Originated CSFB
2. Mobile Terminated CSFB
3. Mobile Originated eCSFB
4. Mobile Terminated eCSFB

The following priority aspects are required to support CSFB to 1xRTT in addition to the common EPS special handling aspects already discussed in Priority CSFB to UMTS (Section 12.1) and those already specified for NS/EP NGN-PS. The priority aspects that need to be secured for CSFB to 1xRTT are described in the following sections.

12.2.1 Priority CSFB Configuration Data – HSS

This is considered as common EPS priority aspects for CSFB to UMTS and CSFB to 1xRTT which is already discussed in Priority CSFB to UMTS Section 12.1.1.

R-80 and [ATIS-1000055] Section 10.4.3, “Requirements for Management of Insider Threats,” apply.

12.2.2 Confidentiality of MME Incoming Message Handling for Priority CSFB - MME

This is considered as common EPS priority aspects for CSFB to UMTS and CSFB to 1xRTT which is already discussed in Priority CSFB to UMTS Section 12.1.2.

R-81 applies.

12.2.3 Integrity of Paging Messages for CSFB & Priority Processing - MME

The MME needs to detect Priority indication in the Paging Request message from 1x IWS for priority terminated CSFB calls.

Insider attacks or a compromised MME may allow tampering with priority indication in the Paging Request which may result in priority Mobile Terminating CSFB calls not receiving appropriate priority treatment.

> **R-90 (Required)** The NS/EP NGN-PS Service Provider shall protect the confidentiality of CSFB Priority indication to the MME in the Paging Request from 1x IWS.
>
> **R-91 (Required)** The NS/EP NGN-PS Service Provider shall protect the integrity of the MME processing functions for the incoming MME messages with CSFB priority indication from 1x IWS.

12.2.4 Integrity of NS/EP LTE Access Class Procedures for Priority CSFB: LTE-Uu

This is considered as common EPS priority aspects for CSFB to UMTS and CSFB to 1xRTT which is already discussed in Priority CSFB to UMTS Section 12.1.3.

R-7, R-8, and R-9 apply.

12.2.5 Integrity of Paging Messages for CSFB & Priority Processing – 1x Interworking Solution

Priority indication in the “Paging Request” message from the 1x MSC to the 1x IWS is received over A1 for Mobile Terminating CSFB to 1xRTT.

Insider attacks or a compromised 1x IWS may allow tampering with priority indication in the paging request received from 1x MSC which may result in priority Mobile Terminating CSFB calls not receiving appropriate priority treatment.

R-92 (Required) The NS/EP NGN-PS Service Provider shall protect the confidentiality of CSFB priority indication in the Paging Request to the 1x IWS from 1x MSC.

R-93 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the 1x IWS processing functions based on priority indication received in the Paging Request from the 1x MSC.

For both Mobile Originated and Mobile Terminated CSFB calls to 1xRTT (cdma2000) which use the "eCSFB" variant to support redirection of PS domain services to eHRPD, the following requirement specifies the security protection for the 1x IWS processing functions including PS handover functions.

Insider attacks or a compromised 1x IWS may allow tampering with priority treatment sent to 1x BS which may result in priority CSFB calls not receiving appropriate priority treatment.

R-94 (Required) The NS/EP NGN-PS Service Provider for "eCSFB" shall protect the integrity of the 1x IWS processing including PS handover functions based on priority indication received in the Assignment Request from 1x MSC.

12.2.6 Integrity of CSFB Priority Messages & Processing - eNodeB

This is considered as common EPS priority aspects for CSFB to UMTS and CSFB to 1xRTT which is already discussed in Priority CSFB to UMTS Section 12.1.5.

R-84 and R-85 apply.

12.2.7 Integrity of Priority CSFB Processing – 1x MSC

1x MSC needs to recognize priority indication in the ISUP IAM message from PSTN for the calling party for Mobile Terminated CSFB to 1xRTT (cdma2000) call. It should further provide priority handling of this request in times of congestion.

Insider attacks or a compromised 1x MSC may allow tampering with priority indication in the IAM messages sent over the A1 interface, which may result in priority Mobile Terminating CSFB calls not receiving appropriate priority treatment.

R-95 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the 1x MSC processing functions based on priority indication received in IAM message from a calling party from CSD and the Priority Indication received in the CM Service Request.

R-96 (Required) The NS/EP NGN-PS Service Provider shall protect the integrity of the 1x MSC processing functions for the priority indication sent over A1 interface to IWS for UE paging.

For both Mobile Originated and Mobile Terminated CSFB calls to 1xRTT (cdma2000) which use the "eCSFB" variant to support redirection of PS domain services to eHRPD, the following requirement specifies protecting the integrity of 1x MSC processing that provides Priority indication to the 1x IWS/1x BS.

Insider attacks or a compromised 1x MSC may allow tampering with priority indication in which may result in priority Mobile Originating or Mobile Terminating CSFB calls not receiving appropriate priority treatment.

R-97 (Required) The NS/EP NGN-PS Service Provider for "eCSFB" shall protect the integrity of the 1x MSC processing functions that provide Priority indication to the 1x IWS/1x BS to support redirection of PS domain services to eHRPD.

13 Bibliography

At the time of publication, the editions indicated were valid. All standards are subject to revision, and users of this document are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

[b-GR-1332-CORE] Telcordia Technologies, Inc. March 2002. Generic Requirements for Data Communications Network Security. GR-1332 CORE.[45]

[b-GR-815-CORE] Telcordia Technologies, Inc. March 2002. Generic Requirements for Network Element/Network System (NE/NS) Security, Issue 2. GR-815 CORE.[46]

[b-IEEE 1588] IEEE 1588-2008 (2008), Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.[46]

[b-ISO 27002] ISO/IEC 27002:2005(E) (June 15, 2005), Information technology — Security Techniques — Code of Practice for Information Security Management.[47]

[b-MIT] Talbot, David, "One Simple Trick Could Disable a City's 4G Phone Network," November 14, 2012. MIT Technology Review. Web Reference> [48]

[b-NRIC] Network Reliability and Interoperability Council. (2005), Best Practices for Telecommunications Network Reliability.

[b-SP 800-53] National Institute for Standards and technology (February 2012), Security and Privacy Controls for Federal Information Systems and Organizations Revision 4. NIST Special Publication 800-53. National Institute of Standards and Technology Gaithersburg, MD.[49]

[b-SP 800-57] United States Department of Commerce, National Institute of Standards and Technology (NIST) "Special Publication 800-57 Recommendation for Key Management – Part 1: General (Revised)", 2007.[50]

[45] Telcordia documents are available from Telcordia at < http://telecom-info.telcordia.com >.

[46] This document is available from the Institute of Electrical and Electronics Engineers (IEEE). < http://shop.ieee.org/store/ >

[47] This document is available from the International Organization for Standardization. < http://www.iso.ch/iso/en/prods-services/ISOstore/store.html >

[48] http://www.technologyreview.com/news/507381/one-simple-trick-could-disable-a-citys-4g-phone-network/

[49] This document is available at the National Institute of Standards and Technology (NIST) at < http://www.itl.nist.gov/fipspubs/ >.

Annex A: Integration Reference Points: Background Information

(informative)

For the purpose of management interface development 3GPP has developed an interface concept known as Integration Reference Point (IRP) to promote the wider adoption of standardized management interfaces in telecommunication networks. The IRP concept and associated methodology employs protocol and technology neutral modeling methods as well as protocol specific solution sets to achieve its goals (see Figure A.1).

The three cornerstones of the IRP concept are:

- **Top-down, process-driven modeling approach:** The purpose of each IRP is automation of one specific task, related to the TeleManagement Forum Telecom Operations Map. This allows taking a “one step at a time” approach with a focus on the most important tasks.
- **Technology-independent modeling:** To create from the requirements an interface technology independent model. This is specified in the IRP Information Service.
- **Standards-based technology-dependent modeling:** To create one or more interface technology dependent models from the technology independent model. This is specified in the IRP Solution Sets.

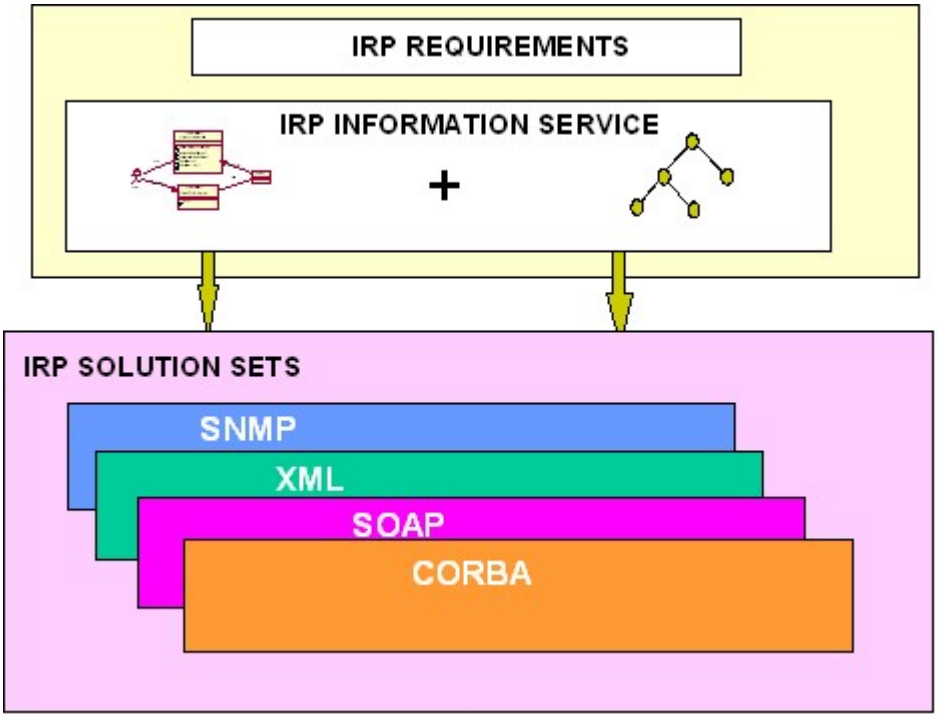

Figure A. 1 - IRP components (with example Solution Sets)

Annex B: Requirement Categories Mapping

(Informative)

Figure 1.1 describes the approach that has been taken to derive the requirements, conditional requirements, and objectives in this document. This appendix shows how each of those requirements, conditional requirements, and objectives aligns with the four categories that comprise the vertical axis in that figure; namely:

- Security of NS/EP-specific LTE features
- Security of LTE Priority Processing features
- LTE Security feature options for NS/EP considerations
- Critical LTE foundational features

Categories 1 and 2 are specific to NS/EP NGN-PS.

Each row in the tables contains a checkmark that indicates to which of the above four categories that requirement, conditional requirement, or objective aligns.

The purpose of this mapping is to give OEC/DHS a clear perspective on how each requirement, etc. relates to its mission.

Table B. 1 – Objectives

OBJECTIVES				
Objective Number	**Security of NS/EP PS specific LTE Features**	**Security of LTE Features Used to Support NS/EP PS**	**Considerations of LTE Security Options for NS/EP PS**	**Other Critical to NS/EP: Management of LTE Security**
O-1.	✓			
O-2.				✓
O-3.		✓		
O-4.		✓		
O-5		✓		
O-6.		✓		
O-7.		✓		
O-8.		✓		
O-9.				✓

Table B. 2 - Conditional Requirements

CONDITIONAL REQUIREMENTS				
Conditional Requirement Number	**Security of NS/EP PS specific LTE Features**	**Security of LTE Features Used to Support NS/EP PS**	**Considerations of LTE Security Options for NS/EP PS**	**Other Critical to NS/EP: Management of LTE Security**
CR-1.	✓			
CR-2.	✓			
CR-3.	✓			

Table B. 3 - Requirements

REQUIREMENTS				
Requirement Number	**Security of NS/EP PS specific LTE Features**	**Security of LTE Features Used to Support NS/EP PS**	**Considerations of LTE Security Options for NS/EP PS**	**Other Critical to NS/EP: Management of LTE Security**
R-1.	✓			
R-2.	✓			
R-3.	✓			
R-4.	✓			
R-5.				✓
R-6.		✓		
R-7.		✓		
R-8.		✓		
R-9.		✓		
R-10.		✓		
R-11.		✓		
R-12.		✓		
R-13.		✓		
R-14.		✓		
R-15.			✓	
R-16.				✓
R-17.				✓

REQUIREMENTS				
Requirement Number	**Security of NS/EP PS specific LTE Features**	**Security of LTE Features Used to Support NS/EP PS**	**Considerations of LTE Security Options for NS/EP PS**	**Other Critical to NS/EP: Management of LTE Security**
R-18.				✓
R-19.				✓
R-20.				✓
R-21.	✓			
R-22.	✓			
R-23.		✓		
R-24.		✓		
R-25.	✓			
R-26.	✓			
R-27.	✓			
R-28.		✓		
R-29.		✓		
R-30.		✓		
R-31.		✓		
R-32.		✓		
R-33.		✓		
R-34.		✓		
R-35.		✓		
R-36.		✓		
R-37.		✓		
R-38.		✓		
R-39.		✓		
R-40.		✓		
R-41.		✓		
R-42.		✓		
R-43.		✓		
R-44.		✓		
R-45.		✓		

REQUIREMENTS				
Requirement Number	**Security of NS/EP PS specific LTE Features**	**Security of LTE Features Used to Support NS/EP PS**	**Considerations of LTE Security Options for NS/EP PS**	**Other Critical to NS/EP: Management of LTE Security**
R-46.		✓		
R-47.		✓		
R-48.		✓		
R-49.		✓		
R-50.		✓		
R-51.		✓		
R-52.		✓		
R-53.		✓		
R-54.		✓		
R-55.		✓		
R-56.				✓
R-57.				✓
R-58.				✓
R-59.				✓
R-60.				✓
R-61.				✓
R-62.				✓
R-63.				✓
R-64.				✓
R-65.				✓
R-66.				✓
R-67.				✓
R-68.				✓
R-69.				✓
R-70.				✓
R-71.				✓
R-72.				✓
R-73.				✓

REQUIREMENTS				
Requirement Number	**Security of NS/EP PS specific LTE Features**	**Security of LTE Features Used to Support NS/EP PS**	**Considerations of LTE Security Options for NS/EP PS**	**Other Critical to NS/EP: Management of LTE Security**
R-74.				✓
R-75.				✓
R-76.				✓
R-77.				✓
R-78.				✓
R-79.				✓
R-80.		✓		
R-81.		✓		
R-82.		✓		
R-83.		✓		
R-84.		✓		
R-85.		✓		
R-86.		✓		
R-87.		✓		
R-88.		✓		
R-89.		✓		
R-90.		✓		
R-91.		✓		
R-92.		✓		
R-93.		✓		
R-94.		✓		
R-95.		✓		
R-96.		✓		
R-97.		✓		