ATIS-1000034.2010(S2020)

Next Generation Network (NGN): Security Mechanisms and Procedures

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-1000034.2010(S2020), *Next Generation Network (NGN): Security Mechanisms and Procedures*

Is an American National Standard developed by the **Cybersecurity (CSEC)** Subcommittee under 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-1000034.2010(S2020)

American National Standard for Telecommunications for

Next Generation Network (NGN): Security Mechanisms and Procedures

Alliance for Telecommunications Industry Solutions

Approved November 18, 2010

American National Standards Institute, Inc.

Abstract

ATIS-1000029.2008, *NGN Security Requirements*, provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs). This standard describes some security mechanisms that can be used to fulfill the requirements described in ATIS-1000029.2008 and specifies the suite of options for each selected mechanism. Specifically, this standard describes identification, authentication and authorization mechanisms; then discusses transport security for signalling and OAMP, and media security. It then describes audit-trail-related mechanisms and finally describes the provisioning. The security mechanisms described in this standard are based on use of the trust model defined in ATIS 100029.The list of security mechanisms described in this standard is not exhaustive. NGN providers are encouraged to support additional security tools, capabilities and operational measures as needed beyond the mechanisms specified in this standard for NGN security protection.

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 roster:

M. Dolly, PTSC Chair (AT&T)

W. Downum, Technical Editor (Telcordia)

C. Underkoffler, ATIS Chief Editor

The Signalling, Architecture, and Control (SAC) Subcommittee was responsible for the development of this document.

Table of Contents

1. Scope 1
   1.1 Assumptions 1
   1.2 Overview 1

2. Normative References 2
   2.1 ATIS references 2
   2.2 ITU-T references 3
   2.3 IETF references 3

3. Definitions 3
   3.1 Terms defined elsewhere 3
   3.2 Terms defined in this standard 5

4 Abbreviations and acronyms 5
   5 Conventions 7

6 Security risks and threats 8

7 Security trust model 8
   7.1 Single network trust model 8
   7.2 Peering network trust model 10

8 Identification, Authentication and Authorization 10
   8.1 Subscribers 11
   8.2 Network Element 11
   8.3 Credential usage in the NGN Security 11
   8.3.1 Device, Subscriber, and End-User Credentials 11
   8.3.2 X.509 public key certificates as credentials 12
   8.3.3 Shared keys as credentials 13
   8.3.4 Information provisioned in SUP/TUP-FEs for each set of credentials 14
   8.4 Identification and Authentication of Subscribers 15
   8.4.1 General Strategy 15
   8.4.2 Identification of the Subscriber through Network Source Address 16
   8.4.3 Identification of the Subscriber through TLS/IPsec Security Association 17
   8.4.4 Identification of the Subscriber through Challenge/Response 17
   8.4.5 Generic Bootstrapping Architecture (GBA) 19
   8.5 Identification and Authentication of End-Users 19
   8.5.1 General Strategy 19
   8.5.2 Identification of the End-User through TLS/IPsec Security Association 20
   8.6 Identification and Authentication by TE-BE 20

8.6.1 Use of X.509 Certificates ... 20

8.7 Authenticator-SAA/TAA-FEs Interface ... 21

8.7.1 Use of RADIUS and its extensions ... 21

8.7.2 Transport Signalling Security Association ... 22

8.8 Identification and Authentication of bearer traffic ... 22

9 Transport security for signalling and OAMP ... 24

9.1 TLS ... 24

9.1.1 Cipher suites ... 24

9.1.2 TLS Use of Certificates ... 27

9.1.3 Session Key Management ... 27

9.2 IPsec in Trusted and Trusted-but-Vulnerable Zones ... 28

9.2.1 AH and ESP ... 28

9.2.2 Transport and Tunnel Mode ... 28

9.2.3 Replay Protection ... 29

9.2.4 Key Management ... 29

9.3 Key agreement protocol between Untrusted and Trusted-but-Vulnerable Zone ... 31

9.4 IPsec between Untrusted and Trusted-but-Vulnerable Zone ... 31

10 Media Security ... 32

10.1 SRTP ... 33

10.1.1 Encryption and Authentication Algorithms ... 33

10.1.2 Cipher Suite Negotiation and Key Generation ... 33

10.1.3 Authentication interface between NGN Network Element and Secure Token Server ... 34

11 OAMP ... 34

11.1 Network Element interface to Logging Systems ... 35

11.2 Network Element Use of SNMP ... 35

11.3 Security Patch Management ... 35

11.4 Version management ... 35

11.5 Audit Trail, Trapping, and Logging at TE-BE ... 36

12 Provisioning of equipment in untrusted zone ... 36

APPENDIX A: Examples of Source-Address Assurance and its application to the mechanism of subscriber identification and authentication ... 38

A.1. Subscriber identification and authentication linked to access-line authentication ... 38

A.2. Subscriber identification and authentication linked to explicit access authentication at IP Connectivity Establishment ... 40

APPENDIX B - Emergency Telecommunications Service (ETS) Interconnection Security ... 43

B.1 Background ... 43

B.2 Scope/purpose ... 43

B.3 Security Objectives and Guidelines for Interconnection of ETS ... 43

B.4 Authentication and Authorization 43
B.5 Transport Security for Signaling and OAMP 44
B.6 Media Traffic 44
B.7 Support of Calling Number ID and Calling Name ID Restriction Features 44
B.8 Non-traceability 44
B.9 End-to-End Peer-to-Peer Encryption 44

APPENDIX C - Security Best Practices 45
C.1 Introduction 45
C.2 Firewalls 45
C.3 Operating System Hardening 46
C.4 Vulnerability Assessment 46

APPENDIX D – Bibliography [Informative] 48

Table of Figures

Figure 1 Security trust model/[ATIS-1000029] 8
Figure 2 – Peering trust model/[ATIS-1000029] 10
Figure 3 - NGN Entities involved in authentication procedure – UNI example. 23
Figure 4 - The relationship of media encryption, BE's capabilities, and originator/destination's desire 33
Figure A. 1 - High-level message flows of example 1 38
Figure A. 2 - High-level message flows of example 2 41

Table of Tables

Table 1– Some basic and extensions fields of an X.509 public key certificate 13
Table 2 – Authenticator's actions for each authentication result 16
Table 3 - Candidate cipher suites for NGN 25
Table 4 - Candidate cipher suites (optional) for NGN 26

American National Standard for Telecommunications –

Next Generation Network (NGN): Security Mechanisms and Procedures

1. Scope

ATIS-1000029 (NGN Security Requirements) [ATIS-100029], provides security requirements for next generation networks (NGNs) and its interfaces (e.g., UNIs, NNIs and ANIs), including a trust model. The security mechanisms selected to implement these requirements will contain options, and mismatched options are undesirable because they tend to introduce security vulnerabilities and make it more difficult to achieve interoperability.

This standard therefore highlights some important security mechanisms that can be used to realize the requirements in [ATIS-100029] and specifies the suite of options to be used for each selected mechanism to reduce interoperability and mismatch problems. The list of mechanisms described in this standard is not exhaustive. NGN providers are encouraged to support additional security tools, capabilities and operational measures as needed beyond the mechanisms specified in this standard for NGN security protection.

This standard is intended to be used with [ATIS-1000029] and [ITU-T Y.2701] to provide a base for NGN security. It should be used with other security related standards and other specifications as appropriate for specific security areas.

> Note: The mechanisms described in this standard for identification and authentication are part of the broader topic generally known as IdM ("identity management").

1.1 Assumptions

This standard is based on the following assumptions:

1. The bundling of functional entities, as defined in [ATIS-1000018] and [ITU-T Y.2012], to a given network element will vary, depending on the vendor.
2. Each NGN provider has specific responsibilities within its domain for security. For example, implementing applicable security services and practices to a) to protect itself, b) to assure end-to-end security is not compromised within its network, and c) to assure high availability and integrity of NGN communications.
3. Each network domain will establish and enforce policies of service level agreements (SLAs) to assure the security of its domain and the security of the network interconnections. It is assumed that the SLAs would specify security services, mechanisms and practices to protect the interconnected networks and the communications (signalling/control traffic, bearer traffic and management traffic) across UNIs, ANIs and NNIs.
4. This standard addresses network-based security, which is achieved by applying a layered architecture, consisting of perimeter security to trusted domains, physical security of provider equipment, and potentially the use of encryption

1.2 Overview

This standard is organized as follows:

- Clause 2 (References) – This clause provides normative references.