



ATIS-1000077

ATIS Standard on -

5G Security Requirements



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 and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

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 OF MERCHANTABILITY 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.

Published by

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

Copyright © 2017 by Alliance for Telecommunications Industry Solutions
All rights reserved.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher. For information contact ATIS at 202.628.6380. ATIS is online at < <http://www.atis.org> >.

ATIS-1000077

ATIS Standard on

5G Security Requirements

Alliance for Telecommunications Industry Solutions

Approved January 11, 2017

Abstract

This document contains draft security-related recommendations intended for 5th Generation mobile network (5G) standards development activities.

Foreword

The Alliance for Telecommunications Industry Solutions (ATIS) serves the public through improved understanding between carriers, 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. International Telecommunication Union – Telecommunications Sector (ITU-T) and U.S. International Telecommunication Union – Radiocommunication Sector (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.

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. The word *may* denotes a optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

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 Communications Sciences)

Table of Contents

1	Scope, Purpose, & Application	1
1.1	Scope.....	1
1.2	Purpose	1
2	Definitions, Acronyms, & Abbreviations.....	1
2.1	Acronyms & Abbreviations.....	1
3	Methodology	3
4	Security in the 5G Environment.....	4
5	Denial of Service (DoS)	4
5.1	Requirements	5
6	Key Management	6
6.1	Requirements	7
7	Identity Management	10
7.1	Requirements	10
8	Isolation Mechanisms	12
8.1	Requirements	12
9	Summary	13

ATIS Standard on –

5G Security Requirements

1 Scope, Purpose, & Application

1.1 Scope

This report identifies stage 1 and stage 2 security requirements for 5th Generation (5G) mobile networks to ensure “security by design” in 5G networks.

1.2 Purpose

The Federal Communications Commission (FCC) asked the FCC’s Technological Advisory Council (TAC) Cybersecurity Working Group “... to recommend to the FCC the strategy, procedures and steps necessary to help incorporate the concept of ‘security by design’ into the very fabric of 5G ...”. The FCC also asked, “What are the tools and security controls that should be built into 5G design specifications in order to make 5G networks and devices sufficiently secure from the onset?”

The Cybersecurity Working Group created a 5G Subcommittee to address the FCC’s requests. The 5G Subcommittee created the following work plan:

- Develop a list of tools and security controls that should be built into 5G specifications in the form of recommendations.
- Collaborate with ATIS to review and refine the document, including revising or removing existing recommendations and text and adding new recommendations and text.
- Create an ATIS document that would be used to influence the 3rd Generation Partnership Project (3GPP) 5G standards development process to incorporate security by design.

The 5G Subcommittee has created a document of security recommendations. This ATIS Technical Report (TR) provides technical analysis and further input on the 5G Subcommittee document and recommendations.

2 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at: < <http://www.atis.org/glossary> >.

2.1 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
3GPP	3rd Generation Partnership Project
2G	2nd Generation mobile network
3G	3rd Generation mobile network
4G	4th Generation mobile network
5G	5th Generation mobile network
AKA	Authentication and Key Agreement