ATIS Standard:
5G Network Assured Supply Chain

ATIS-I-0000090
June 2022

ABSTRACT

As the deployment of 5G continues to expand in North America and across the globe, it is critical to secure 5G infrastructure. The scale of 5G is rapidly expanding across new vertical markets, broader industry sectors, and a massive number of new devices and applications. This new ATIS standard addresses the 5G supply chain (5G/SC) as a critical function in the design, build, deployment, and operation of 5G assured networks. We define the network to be the interconnecting fabric that enables endpoints (devices and clients) to exchange information with other endpoints or servers. The supply chain aspects associated with the endpoint (devices, clients, and servers) are not within the scope of this document.

This document focuses on the requirements and controls necessary to operationalize a set of agreeable levels of assurance associated with the lifecycle functions of high assurance 5G/SCs. This work is based on a flexible reference model and component flow through the complex 5G/SC to identify specific controls that can mitigate the identified threats and associated attacks. Attack classes are identified by using defined attributes. These attributes represent a defining quality of an asset (hardware component, module, system, software) and consequently reflects the asset's attackable characteristics.

Designating specific system components as "critical" as part of a 5G cybersecurity risk management effort is essential for managing supply chain risks within available or assigned resource constraints. Network operators and enterprises must select, shape, and scale their risk mitigation strategy according to business, operational and security needs. They also must prioritize a subset of "critical components" that warrants "extra attention" in the assurance assessment, testing, and monitoring activities.

The approach taken in this document is to leverage where possible techniques that can link back to a component's source to verify the authenticity and integrity of that component. The use of Software Bill of Materials (SBOM) and Hardware Root of Trust (HRoT) represents two methods that can effectively accomplish this goal. In addition, the application of security best practices helps secure each of the supply chain lifecycle functions identified.

The entity responsible for attesting the level of supply chain assurance for a network can use this specification with suppliers by providing:

- An assurance level that the supplier must comply with.
- A list of the identified critical components that apply to the supplier.
- This document and the set of requirements as listed in Section 8 as part of the purchase agreement, along with any desired exceptions and/or additions.

FORWARD

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global Information and Communications Technology (ICT) companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the all-Internet Protocol (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 Third 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 AND 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 [https://www.atis.org/policy/patent-assurances/] 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.

COPYRIGHT INFORMATION

ATIS-I-0000090

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

Table of Contents

1. Introduction

1.1 Scope

This document defines a flexible supply chain flow model and a comprehensive set of requirements that can be applied to any 5G supply chain (5G/SC) ecosystem. These requirements, associated controls, and metrics are applicable to a broad range of network use cases and can be utilized in most risk-management regimes associated with the selection and implementation of controls. The network is defined as the interconnecting fabric that enables endpoints (devices and clients) to exchange information with other endpoints or servers. The supply chain aspects associated with the endpoint (devices, clients, and servers) are not within the scope of this document.

This approach leverages the output of numerous Supply Chain Risk Management (SCRM) best practices, guidelines, and recommendations developed by other collaborative efforts between government and industry, which are referenced throughout this document.

1.2 Purpose

Although other standards venues have explored supply chain requirements, 5G mobile technology introduces an increasingly complex set of challenges due to the diverse application space and 5G's expanding global supply chain model. The goal of this standard is to provide entities operating networks and their suppliers with a flexible approach for assuring a 5G/SC at any level of component integration or product type. By applying these requirements and controls across the 5G/SC, customers can achieve a greater level of assurance that the 5G/SC is secure in light of a constantly changing and evolving threat environment.

1.3 Application

The 5G/SC model and requirements contained in this document have been developed for application in a broad range of high-assurance public and private networks. It is understood that the landscape of 5G/SC needs will continue to evolve with the ever-changing threat environment. Therefore, the approach described in this document is designed to be flexible across a wide range of 5G and beyond applications and solutions and be extensible into the future. Forward-looking use cases that are representative of real-world 5G deployments are selected and applied to the development of requirements in this document and can be translated to an implementable approach for delivering secure, resilient, and trustworthy 5G networks.