ATIS STANDARD

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 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.

Published by

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

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

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

API	Application Program Interface
ASME	Access Security Management Entity
AuC	Authentication Center
CN	Core Network
CoAP	Constrained Applications Protocol
CPS	Cyber Physical Systems
D2D	Device to Device
DDS	Data Distribution Service
DNS	Domain Name System
DoS	Denial of Service
eMBB	Enhanced Mobile Broadband
eNodeB	evolved Node B
EU	European Union
eUICC	Embedded Universal Integrated Circuit Card
FCC	Federal Communications Commission
GBA	Generic Bootstrapping Architecture
GSM	Global System for Mobile communications
GSMA	GSM Association
HSS	Home Subscriber Server
IBE	Identity Based Encryption
ICCID	Integrated Circuit Card Identifier
ICT	Information and Communications Technology
IdAM	Identity Access Management
IdM	Identity Management
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIC	Industrial Internet Consortium
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPsec	Internet Protocol Security
Ki	Authentication Key
LoRa	Long Range
LTE	Long-Term Evolution
M2Mt	Machine to Machine trust
M2Ut	Machine to User trust
MQTT	Message Queuing Telemetry Transport

MME	Mobility Management Entity
MNO	Mobile Network Operator
NAS	Non-Access Stratum
NB-IoT	Narrowband Internet of Things
NFC	Near Field Communication
PDN	Packet Data Network
PIR	Private Information Retrieval
PKI	Public Key Infrastructure
RAN	Radio Access Network
RAT	Radio Access Technologies
RRC	Radio Resource Control
RSP	Remote SIM Provisioning
SDO	Standards Development Organization
SIM	Subscriber Identity Module
SM-DP	Subscription Manager – Data Preparation
SMS	Short Message Service
STIR	Secure Telephone Identity Revisited
TAC	Technological Advisory Council
UAV	Unmanned Aerial Vehicle
U2Mt	User to Machine trust
U2Ut	User to User trust
UE	User Equipment
UICC	Universal Integrated Circuit Card
U.S.	United States
USIM	Universal Subscriber Identity Module
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VoIP	Voice over Internet Protocol
WG	Working Group

3 Methodology

The FCC TAC Cybersecurity Working Group developed preliminary recommendations for a strategy, procedures, and steps necessary to help incorporate the concept of "security by design" into the very fabric of 5G. Specifically, this included recommendations for 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 initial recommendations were used as the starting point for additional analysis that included operational considerations, the latest developments in security best practices, and requirements work already underway in

3GPP. The objective of this analysis was to validate, refine, and enhance the initial recommendations to develop stage 1 (service) and stage 2 (architecture) 5G security requirements with broad support among service providers and suppliers.

4 Security in the 5G Environment

5G will enable a fully mobile and connected society. Drivers of 5G include Internet of Things (IoT), mobile broadband, and mission critical systems. This will require new service delivery models that involve new actors in the ecosystem. Cloud and virtualization technologies will be deployed to provide flexibility and the ability to deliver richer services quickly. Networks will provide greater Application Program Interface (API) access to users and third party service providers. This environment will generate many changes in the existing mobile networks and create new security challenges. We've identified four categories of security that warrant review and recommendations. These are not listed in any priority order.

- Denial of Service (DoS).
- Key management.
- Identity management.
- Isolation mechanisms.

While evaluating security requirements for 5G we identified three categories for how devices will attach to the network.

1) **3GPP direct network access** – In this category, the user equipment attaches directly to the 3GPP network. For example, a smart phone would attach to a carrier's network.
2) **Generic Access Network** – In this category, an API provides Internet Protocol (IP) access into a carrier's core network, usually tunneled over Internet Protocol Security (IPSec). Data from the API is fed into the phone network as if it were coming from an antenna or a tower. Carriers enable WiFi-calling for their customers using generic access network connectivity.
   In 3G/4G, IPSec is used to tunnel to the carrier's core network, and the device authenticates with the core network using Universal Integrated Circuit Card (UICC) Authentication and Key Agreement (AKA) credentials.
3) **Capillary network access** – In this category, the user equipment connects to a gateway that is on the 3GPP network. The device is authenticated by the gateway, not the 3GPP network. The gateway is connected to the 3GPP network as described in category 1 or 2. The gateway can thereby have its own identity and multiplex the user equipment traffic over one data connection, or it can have multiple identities that map to the devices on the capillary network. It is more common for the gateway to have one identity with the 3GPP network.

5 Denial of Service (DoS)

5G is expected to enable diverse services in the mobile operators' networks, which include enhanced mobile broadband (eMBB), Internet of Things (IoT) and mission critical services. Mission critical services for Unmanned Aerial Vehicle (UAVs) (e.g., drones), vehicular networks or industrial systems (e.g., factory automation, process automation) in particular require highly available, low-latency, and highly reliable communication systems. In addition, IoT will introduce a large number of devices that can be low cost and less sophisticated than current mobile devices. As more devices are connected to the cellular networks, the networks will be exposed to denial of service (DoS) targeting the limited resources of specific services, much like botnet-driven distributed denial of service attacks in the Internet. Limited resources on cellular networks will include spectrum bandwidth, processing capacity of control functions (e.g., Mobility Management Entity [MME]), processing capacity of user-plane functions (e.g., Packet Data Network [PDN] gateway), and network bandwidth. Each of those resources may be a target of DoS attacks. It should be noted that service outage due to DoS attacks would pose substantial threats to mission critical services. 5G systems should have mechanisms to identity DoS attacks and to limit or mitigate the impact of such attacks. Potential attack vectors are:

- **Packet injection attacks** – Compromised IoT devices are orchestrated to send packets simultaneously to overwhelm the network. Those devices may use radio resources allocated for other devices to inject bogus messages into the network. Such bogus packet injection cannot be effectively countered in the absence of an integrity check at the base station. Mobile-botnet driven DoS attacks may also become a significant threat.
- **External flooding attacks** – A high volume of unsolicited packets from the Internet may exhaust the bandwidth of mobile networks. Those packets may also be used to exhaust the battery of IoT devices. Such attacks may be launched by a botnet consisting of large number of bots (e.g., millions of malware infected devices) connected to the Internet.
- **Radio jamming attacks** – Devices emit jamming signals to disrupt communication between a device and a base station or between devices (e.g., Device to Device [D2D]). Jamming can be launched against control-plane signaling messages or user-plane data messages. Attackers may employ intelligent jamming in order to jam the radio spectrum persistently. For example, a presentation from this summer's Blackhat Conference[1] describes the use of a consumer UAV performing a jamming attack on stationary and moving targets.

5.1 Recommendations

#1: It is recommended that 5G standards be defined in such a way as to enable resource isolation techniques such as network slicing to confine the effects of DoS attacks.

Resources for different classes of traffic, services, and devices can be isolated based on:

- Message type: Control plane traffic, user plane traffic.
- QoS requirement: Delay, jitter, bandwidth, priority.
- Delivery requirement: Guaranteed delivery, best-effort traffic.
- Service type: Mission critical services (e.g., public safety, NS/EP NGN-GETS), eMBB services, IoT services, vehicular services (e.g., Vehicle to Everything [V2X], Vehicle to Infrastructure [V2I], Vehicle to Vehicle [V2V]).

Network slicing and path diversity should be deployed based on classes of traffic, services, and/or devices to limit the effects of DoS attacks.

#2: It is recommended that 5G networks be able to deauthorize an individual device (or multiple devices) in such a way as the device does not continue to utilize the control plane or media plane resources.

Deauthorization of devices essentially requires detection of DoS attacks and identification of devices used for the attacks. For DoS attack detection, the network should have an intrusion detection system that triggers alarms in the occurrence of attacks. Identification of devices used for the attack may require the following capabilities:

[1] Drone Attacks on Industrial Wireless a New Front in Cyber Security (PDF), available at: < https://www.blackhat.com/docs/us-16/materials/us-16-Melrose-Drone-Attacks-On-Industrial-Wireless-A-New-Front-In-Cyber-Security.pdf >.

- **Packet accountability** – Network should be able to identify the source of traffic. In the Internet, source address spoofing has been widely used for DoS attacks, e.g., DNS reflection/amplification attacks, to hide the origin of the traffic or concentrate the impact to the target. Countermeasures employed to mitigate the address spoofing attacks include ingress/egress filtering at routers. More recently, self-certifying network address (e.g., a device public key as a network address) has been proposed for the future Internet. A similar countermeasure needs to be considered for the cellular network to enhance packet/message accountability.
- **Device authentication/identification** – May be used as a way to prevent unauthorized malicious devices from accessing a network even if those devices have valid subscription and corresponding credentials, e.g., based on Universal Subscriber Identity Module (USIM) credentials, to attach to the network.
- **Device integrity** – It is desired for a network entity (e.g., a management entity) to verify device integrity, e.g., based on secure boot, to ensure that a device including hardware and software components are in trusted state.

#3: It is recommended that base stations have the ability to schedule the radio resource for each device in an unpredictable way.

In 5G, a base station should schedule the radio resource for each device in an unpredictable way by other devices. This would significantly reduce the risk of jamming attacks targeting a specific set of devices, e.g., mission critical devices.

#4: It is recommended that 5G network elements embed DoS detection and mitigation functions into the Radio Access Network (RAN) functions via key security indicators with related dynamic resolution.

DoS detection functions would include a set of measureable security indicators. Examples of key security indicators are: detect/identify excessive Attach Requests beyond a certain threshold from an anomalous pattern of devices, and detect/identify an anomalous pattern of devices continuously streaming Uplink data beyond a certain threshold (>x). Key security indicators can also be attributes of the functions that monitor and detect performance/threshold alarms.

The related dynamic resolution will be the mitigation aspect of these functions.

6 Key Management

Communication for the IoT is often constrained today to using short-range communication protocols such as Bluetooth-LE, Near Field Communication (NFC), 802.11 WiFi, ZigBee, ZWave, etc. A typical IoT implementation within a home or business environment is a wireless sensor network, where deployed sensors can communicate between themselves using mesh networking capabilities. This communication can take place directly or be proxied through a variety of external service gateways.

Typically, the nodes that participate in this meshed architecture are provisioned with cryptographic material that supports confidential, authenticated, and integrity-protected communications amongst themselves and to/through the gateway(s). The underlying cryptographic material and services required depends on the protocols that are being used (both communication and messaging) and the security objectives of each. For example, ZigBee-based communications require a network key (that is shared across nodes in the network, i.e., symmetric).

In addition to keys required for communication protocols, messaging protocols (e.g., Message Queuing Telemetry Transport [MQTT], Constrained Applications Protocol [CoAP], Data Distribution Service [DDS]) also levy cryptographic algorithms and key material. Although some messaging protocols only support username/password, many provide options for using symmetric keys, key pairs, and certificates to secure communication between devices.

With the introduction of 5G cellular technologies, IoT product developers will be able to redesign their products with broad, direct access to the cloud and reduced dependencies on local gateways. With the introduction of 5G cellular technologies, IoT product developers will be able to redesign their products with broad, direct access to the cloud and new capabilities for peer-to-peer communications. This requires flexible key management capabilities that support myriad use cases.

Today's key management methods for 4G/LTE networks are based on symmetric keys. The carrier loads a pre-shared symmetric key in the Authentication Center (AuC) (network-side) at subscribe time and the USIM (user-side) at manufacture time. The mutual authentication of user and network results in a derived key, Access Security Management Entity (ASME), which is then used to derive additional encryption and integrity keys for the Non-Access Stratum (NAS), Radio Resource Control (RRC) Signaling, and User Plane.

Symmetric keys typically suffer from a manage-ability problem as evidenced by the current processes' lack of flexibility in provisioning keys for the USIM. In order to support more flexible deployment models and the usage characteristics exhibited by IoT implementations, the following are recommended.

6.1 Recommendations

#5: It is recommended that industry standard encryption techniques be used to protect data during transport.

Proprietary encryption protocols should be excluded from industry standards.

Some of the key aspects that may be considered for encryption and authentication are listed below:

- Integrity of contents of communication or Secure 2-party communication.
  - Application Level encryption.
- Integrity of transport.
  - Ensuring industry standard encryption techniques are utilized to protect data during transport. Avoiding using proprietary encryption protocols and ensuring the message payload encryption and secure encryption key handshaking.
- Advanced packet filtering.
- Content detection in the presence of encryption.

#6: It is recommended that 5G networks provide options for using asymmetric key material to support diverse IoT Use Cases.

With 5G and the explosion of "things" connecting to it, we need to consider alternative security provisioning solutions such as device certificates and some form of certificate management solution to provide more scalable means of provisioning trust between devices, networks, and application domains. This requirement does not apply for 3GPP direct network access defined in Clause 5.

#7: It is recommended that 5G networks enable privacy protections to guard against using keys and certificates to identify and track consumers.

The IoT includes devices that can be bound to a particular person or property. The ability to identify a person or their actions through IoT devices must be protected. Strong protections against insiders within the key management systems and the cellular systems should also be put in place. For example, in the automobile industry connected vehicle design, certificate provisioning includes a pooling function for transaction signing to disallow tracking.

#8: It is recommended that 5G standards development consider alternative trust models that enable flexibility in establishing trust models across heterogeneous devices, access technologies, network domains, and communication modes.

Trust establishment is rigidly defined in 4G networks. 5G will require greater flexibility in being able to establish trust across heterogeneous devices, access technologies, network domains, and communication modes (e.g., human-to-device, device-to-device, device-to-infrastructure). Today's trust model solutions, e.g., Public Key Infrastructure (PKI), that support mobile devices, web browsers, and other applications may introduce difficult-to-scale trust management problems (via Trust Anchors) for 5G paradigms. Alternative, non-hierarchical, distributed trust models and technologies should be considered for 5G to maximize deployment model flexibility. Designing 5G capabilities such that relevant trust models can be "plugged and played" depending on the environment and use cases is ideal.

Greater communications flexibility is also needed. Device-to-device communications also calls for a means for devices to perform more dynamic peer-to-peer authentication with less dependency on the infrastructure. Such use cases require us to look beyond today's pre-provisioned symmetric key based solutions, and look toward other technologies such as PKI or Identity Based Encryption (IBE).

The use of alternative trust models also requires the ability to support flexible trust management features. IoT devices serviced by different telecommunication providers will have to interoperate. Some of these devices will establish trust relationships dynamically (e.g., a wearable health-monitoring device entering a hospital environment). This requires mechanisms for updating the trust stores that determine whether peer or infrastructure identities are trusted or not.

A relevant and timely example of alternative trust model considerations for 5G can be found in the recent efforts of the European Union's Horizon 2020 5G PPP 5G-ENSURE project[2]. Per the 5G-ENSURE website, their vision statement is as follows: "*The 5G-ENSURE project brings to the 5G PPP a consortium of telco and network operators, IT providers and cyber security experts addressing priorities for security and resilience in 5G networks…..5G-ENSURE will define a shared and agreed 5G Security Roadmap with various 5G stakeholders. The outcome will be a trustworthy 5G system offering reliable security services to customers with a "zero perceived" downtime for service provision*."

From a trust model perspective, the 5G-ENSURE project has examined high level technology enablers and published a preliminary roadmap document (dated March 2016)[3]. That document has defined several aspects of trust, all of which should be considered for 5G deployments[4]:

- Trust between automated systems (e.g., through advanced certificate and token based methods): that is Machine to Machine trust (M2Mt);
- Trust between human stakeholders holding responsibilities for different parts of 5G networks, between user and network operators and between users of the network (U2Ut);
- Trust that a human stakeholder has toward a system (U2Mt);

[2] Available at: < http://www.5gensure.eu/project-vision >.

[3] 5G-PPP Security Enablers Technical Roadmap (early vision) (PDF), available at: < http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf >.

[4] Available at: < http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.1-5G-PPPSecurityEnablersTechnicalRoadmap_early_vision.pdf >, Section 5.

- Trust that an automated system (machine) has in users that it interacts with, such as whether it believes the user is who they claim to be (M2Ut).

5G-ENSURE envisions defining a trust model ontology to enable the consistent encoding of the assets, threats, and controls in 5G systems. This will then be used for modeling the system and ensuring the system is designed to mitigate threats as they relate to the complex and dynamic nature of trust across 5G system providers, users, and automated systems.

While the 5G-ENSURE effort is still early in its development and its scope is focused on the EU, the security topics being matured and documented are clearly relevant to the FCC's communicated areas of interest. The TAC's perspective of the EU 5G efforts like 5G-ENSURE is that such efforts may serve as useful technical solution references for U.S.-based 5G security standards activities. The intent of highlighting the EU activities is not to imply a desire to influence them, but rather to learn from their progress on addressing common technical challenges such as 5G trust model development.

As a supporting element for the alternative trust models recommendation stated above, it is suggested that both the FCC and the TAC regularly monitor future 5G-ENSURE progress for potential reuse for U.S.-focused 5G security recommendations.

#9: It is recommended that 5G networks support new secure enrollment processes that allow entities other than carriers to provision enrollment certificates to devices.

This requirement does not apply for 3GPP direct network access defined in Clause 5.

Flexibility will be key when it comes to provisioning. For example, homeowners may need a simple but secure means of linking their smart home devices together into one home network. Provisioning will also need to be very scalable and adaptable to different network configurations, due to large numbers of devices interconnecting and forming collaborative networks. Solutions will also need to facilitate and streamline transfer of ownership when devices are bought and sold in secondary markets.

Flexible generation capabilities are also needed. Some IoT products will generate their own key material and initiate certificate signing requests. Other devices may be provisioned with centrally-generated key pairs and associated certificates. The ability for the infrastructure to handle both models will be important.

Some devices may also require multiple types of identities.   Flexibility in supporting multiple types of identities when the use cases warrant such support could aid end users in securing their devices (e.g., optional support for signature, encryption, key encipherment certificates). This is especially useful for some IoT protocols that allow multiple profiles to be used, all hosted on a single node.

Support for ownership changeover is also important. Many consumer IoT devices will be integrated directly into a home or a vehicle. This means that the devices will change hands over time, e.g., when a home or vehicle is sold. The ability to bind and unbind the device to a new network and a new identity quickly and easily is important. The ability to bind and unbind a batch of certificates is also important, e.g., a home being sold and the need to rekey all IoT devices in that home. Non-repudiation assurances of the cryptographic keys and the key provisioning designs are crucial for a variety of 5G-enabled IoT use cases.

#10: It is recommended that 5G networks support robust methods for identifying and responding to misbehavior.

Depending on their deployment environment, IoT device theft and other compromises may be common. Flexible methods for reporting device compromise and quickly cutting off authentication abilities for devices must be provided. Some devices will simply require an image update to restore to a non-compromised state, which means that the keys bound to a device would need to be revoked and then re-issued. The ability to efficiently perform this re-issuance online should also be explored for IoT devices that do not require higher levels of assurance.

#11: It is recommended that 5G networks support multiple devices that operate at multiple levels of sensitivity/assurance.

Not all IoT products require the same levels of security assurance. Some IoT devices (e.g., connected vehicles, other Cyber Physical Systems) require stringent security controls and any keys or certificates issued to those devices must go through a robust identity vetting process. Other consumer devices may require less stringent identity vetting, and could even include self-service capabilities. Security models for identity provisioning should offer flexible options for the levels of identity assurance (identity setup and vetting) prior to certificate issuance, and ideally include a level of assurance attribute embedded in the certificate. System owners can then use that attribute to make access control decisions.

Differentiating between IoT devices can also be supported by embedding attributes of the device within a certificate. Within the IoT, the ability to differentiate between different types or classes of devices will be important within and across industries. In addition to understanding the levels of assurance provided by a particular certificate and its host device or application, it would also be useful to provide system owners with the ability to embed additional attribute information within identity certificates. For example, the ability to cryptographically bind the identity of an emergency services vehicle within a certificate used for authentication would be useful in allowing transportation infrastructures to make appropriate decisions (this is the current design of the IEEE 1609.2 certificate format).

The threat environment for different types of IoT devices will also drive the need to support flexibility in the lifetimes configured for keys and certificates used within the IoT. Just as with different levels of assurance associated with IoT device types, different types of IoT devices will have different product and usability lifetimes. Generally, higher assurance certificates (i.e., more rigorous vetting process) will be given shorter lifetimes, however privacy impact assessments performed by IoT device vendors and system owners may also drive the need for shorter lifetimes (e.g., automobiles).

7 Identity Management

Identity Management (IdM) is a broad administrative area that deals with identifying individuals, entities, or general “principals” (e.g., humans, services, communication endpoints, or devices) in a system (e.g., a country, a network, a compute cloud, or an enterprise). Their established identity is typically the basis to accomplish further security goals, such as policy-based access control decisions to resources within that system (e.g., granting access to licensed spectrum for communication based on the proper authentication of a post-paid International Mobile Subscriber Identity [IMSI]) or recording of actions mapped to their actors to establish a non-repudiable transaction history (e.g., through blockchain-based transaction integrity preservation). The term “identity” is the relation each entity bears just to itself, while the term “identifier” is a name that labels the identity of a unique entity.

7.1 Recommendations

#12: It is recommended that the 5G network that provides access to a device be able to uniquely identify, authenticate, and authorize each individual device that accesses the network either directly or indirectly (e.g., via a gateway, virtual network).

User Equipment devices (UEs) are the subscriber entry points into the 5G network and are perhaps the weakest element on the architecture as the Mobile Network Operator (MNO) has little control over its security parameters. UEs can be the gateway for various security vulnerabilities into the 5G service. On the network side, issues such as Rogue eNodeBs or Eavesdropping/Man in the middle attack must still be considered.

Attackers can take advantage of a known weakness wherein the user identity transference occurs unencrypted, in clear text between the UE and the eNodeB, during the initial attach procedure. This allows an eavesdropper to track the user cell-location or launch a man in the middle attack by user IMSI impersonation and relay of user messages.

#13: It is recommended that an equipment or subscriber identity that is transported across networks and presented to a terminating device be authenticated and authorized.

Phone number spoofing has become a significant problem with the proliferation of VoIP networks. It is used to violate regulatory rules, such as those related to robocalling, and even to evade law enforcement when committing a crime, such as SWATing. The Internet Engineering Task Force (IETF) has been working on solutions to provide authentication of an originating phone number in the Secure Telephone Identity Revisited (STIR) working group[5]. 5G networks should ensure that phone numbers and any other identifying information that is transported across networks and presented to a device can be authenticated and authorized. ATIS has developed the SHAKEN framework using the IETF STIR protocols for phone number verification.

#14: It is recommended that UE be able to authenticate the network before attaching.

5G networks must have the ability for devices to reliably authenticate the network they are communicating with. 3GPP specifies access security in TS 33.203 that includes authentication-related mechanisms and traffic protection between the UE and core networks. Strong encryption in the attach phase and UE authentication to the eNodeB will deter both rogue elements and man in the middle attacks. Adopting PKI with the public key of the MNO being stored in the USIM allowing the UE to encrypt privacy related information such as the IMSI transmitted to the eNodeB will enable confidentiality. Encryption should be implemented between the UE and eNodeB to thwart attackers leveraging IMSI paging and location identification vulnerabilities thus protecting subscriber privacy and security.

Future Considerations:

- Homomorphic Encryption, allowing operations on encrypted data.
  - Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result that, when decrypted, matches the result of operations performed on the plaintext.
- Private Information Retrieval (PIR).
  - PIR protocol allows a user to retrieve an item from a source without revealing which item is retrieved. PIR is a weaker version of 1-out-of-n oblivious transfer, where it is also required that the user should not get information about other items in possession of the source.

#15: It is recommended that Soft SIMs deploy rigorous cybersecurity measures that can protect against attacks aimed at software applications.

[5] Available at: < https://datatracker.ietf.org/wg/stir/charter/ >.

Traditional SIMs have the benefit of combined hardware and software security. SIMs stored as a software application will be attractive to hackers. To protect identity and credentials in Soft SIMs would require more extensive security measures than exist today.

8 Isolation Mechanisms

In 5G, to achieve authorized access to the base station may require different trusted access mechanisms to SIMs – especially for off-loads. A method may be required not only to identify a network user, but also their location, mobility tracking, and data usage attribution.

An ideal approach would leverage network slicing combined with cognitive computing in each base station, local storage in each base station, local networking in every base station, plus random number-based encryption coding and recoding during transmission that can only be decoded by the intended recipients.

Taking user plane security as an example, some applications may not want to rely on security provided by the network, but may rather use end-to-end application level security. Underlying network-terminated security would not provide a higher degree of security to the applications, but may have an impact on delay or resources on the terminal. Other applications, however, may want to rely on user plane security supported by the network, and may even need user plane integrity protection in addition to encryption.

The energy cost of encrypting one bit is one or two orders of magnitude less than transmitting one bit. However, for the most constrained battery-dependent devices with a long target life time, there may be a need to consider even more lightweight solutions, as every micro joule consumed could be of importance.

8.1 Recommendations

#16: It is recommended that 5G standards be defined in such a way as to enable resource isolation techniques such as network slicing to enable different levels of security among different resources.

Network slicing can be an important tool to handle the very diverse requirements of different applications and user groups. By having a properly implemented, high-assurance isolation mechanism to support slicing, it is possible to confine the impact of security requirements to single slices, rather than the whole network. The cost of high assurance and certification can therefore be concentrated onto an infrastructure virtualization/isolation layer.

Another option worth considering is simply putting the responsibility in the endpoints, i.e., in connected devices or organization data centers. Data security is an example of a service that could be handled this way. Besides the isolation/slicing itself, many other examples of network-enabled security as a service can be attractive to multiple user groups, including network enforced security policies, authentication, key management, and data security services.

#17: It is recommended that there be access to the control plane and media plane at the base station to enable security monitoring of traffic.

Anomaly detection will be an important tool to identify potential attacks. The closer the monitoring is to the source, i.e., base station, the greater the opportunity is to limit the attack to a smaller part of the network.

9 Summary

The recommendations and related text included in this report originated from a report of the FCC's Technological Advisory Council (TAC) 5G Cybersecurity Subcommittee of the Cybersecurity Working Group. The 5G Subcommittee submitted that report to the ATIS PTSC to seek broader industry input and feedback. The 5G Subcommittee document was modified based on input from the ATIS PTSC as provided in this ATIS TR.

The recommendations in this document will be used as a source for further joint efforts of the ATIS PTSC and the 5G Subcommittee to submit input to 3GPP SA3. The FCC would like to get broad industry support for input to 3GPP.

While creating input for 3GPP we expect the group to modify the text as needed, modify the text to be consistent with 3GPP SA3 Stage 1 and Stage 2 requirements, identify whether a requirement is redundant with existing requirements (and therefore not necessary), and add new requirements if any are identified.

It is possible that the FCC will extend the work of the 5G Subcommittee with ATIS PTSC to continue to monitor 5G security requirements and suggest more input to 3GPP SA3 if necessary.