5GMF White Paper

Cybersecurity in 5G Use Cases

Version1.1

March 29, 2024

The Fifth Generation Mobile Communications Promotion Forum

Table of Contents

1. Introduction (Report Overview)

This white paper originates from the increasing number of requests received in 2019 for studies into 5G security from many concerned individuals and organizations, which led to the 5GMF upgrading the Security AdHoc to the Security Study and Research Committee. The research on 5G security that the Committee has conducted since then has been compiled in this report.
In July 2020, the 5GMF White Paper "Security in 5G Use Cases Version 1.0" was released. After the publication of version 1.0, the results of research activities on each item of study (standardization, connected vehicle, and Fintech) were reflected in version 1.1.

2. Research Goals of the Security Study and Research Committee

The aim of the Committee's research was, as per the opinions of participating Committee members, to look at the specific fields of 1) IoT, 2) Connected Vehicles, and 3) Fintech to discover relevant security issues that related to overall trends in 5G security standards. Recruitment for committee members ended in September 2019, after which the 21 participants began their work.
Security issues in following use cases were chosen to be considered in this paper:

- IoT devices with limited computing devices, large numbers of IoT devices (authentication technology)
- Connected Vehicles, (self-driving vehicles, driver Assistance systems)
- FinTech related services (mobile commerce, etc.)

3. List of Acronyms

3GPP: Third Generation Partnership Project

5GAA: 5G Automotive Association

ACEA: European Automobile Manufacturers' Association

AECC: Automotive Edge Computing Consortium

AF: Application Function

AMF: Core Access and Mobility Management Function

AUSF: Authentication Server Function

CN: Core Network

CR: Compliance Rules

CRL: Certificate Revocation List

C-V2X: Cellular Vehicle-to-Everything

DDoS: Distributed Denial-of-Service

DoS: Denial-of-Service

DRM: Digital Rights Management

DSRC: Dedicated Short Range Communications

ECU: Electronic Control Unit

ENISA: The European Union Agency for Cybersecurity

eSIM: Embedded Subscriber Identification Module

ETSI: European Telecommunications Standards Institute

EVITA: E-Safety Vehicle Intrusion Protected Applications

GSMA: GSM Association

GUTI：Global Unique Temporary Identifier

HDCP: High-Bandwidth Digital Content Protection

HDMI: High-Definition Multimedia Interface

HIS: The Hersteller Initiative Software

IMSI: International Mobile Subscriber Identity

IRN: Infrastructure/Roadside Network

ITS-S: ITS Station

ITS-SCU: ITS Station Communication Unit

ITS-SU: ITS Station Unit

IVN: In-Vehicle Network

LDP: Local Dynamic Map

MEC: Mobile Edge Computing/Multi-Access Edge Computing

NAS: Non-Access Stratum

NESAS: Network Equipment Security Assurance Scheme

NEF: Network Exposure Function

NF: Network Function

NRF: Network Repository Function

NS: Network Slice

NSSAI: Network Slice Selection Assistance Information

NSSF: Network Slice Selection Function

OBU: Onboard Unit

OTA: Over-the-Air

PKI: Public Key Infrastructure

PVS: Probe Vehicle Systems

QoS: Quality of Service

RAN: Radio Access Network

RR: Robustness Rules

RSU: Roadside Unit

SAE International: Society of Automotive Engineers

SBA: Service Based Architecture

SCAS：Security Assurance Specifications

SCN: Sensor and Control Network

SMF: Session Management Function

SUCI: Subscription Concealed Identifier

TCG: Trusted Computing Group

TEE: Trusted Execution Environment

TFCS: Task Force on Cyber Security

TLS: Transport Layer Security

UE: User Equipment

UNECE: United Nations Economic Commission for Europe

UPF: User Plane Function

URLLC: Ultra-Reliable and Low Latency Communications

V2D: Vehicle-to-Nomadic Device

V2I: Vehicle-to-Infrastructure

V2N: Vehicle-to-Network

V2P: Vehicle-to-Pedestrian

V2V: Vehicle-to-Vehicle

V2X: Vehicle-to-Everything

4. Trends in Standards for 5G Security

4.1 Introduction

This chapter will provide an overview of standards trends as related to 5G security, focusing on the activities of the SA3 working group, which has been assigned by the 3GPP to discuss security and privacy standards. This overview will begin with a discussion on 5G standards and the schedule for its introduction, followed by a discussion on security in a 5G non-stand alone configuration, which will be used in 5G networks during the early stage of its deployment, then a discussion on the differences in security with LTE and 5G stand-alone configurations, then concluding with updates on security-related specifications after Release 16.

4.2 5G Standards and Introduction Schedule

The ITU and the 3GPP, which deal with international mobile telecommunications (IMT), have entered the final phase of standards activities with the planned realization of 5G (IMT-2020) in 2020. In order to realize 5G, studies on standards specifications include those for ultra-fast speeds (eMBB: Enhanced Mobile Broadband), ultra-low latency (URLLC: Ultra-Reliable and Low Latency Communication, and massive simultaneous connections (mMTC : massive Machine Type Communications).

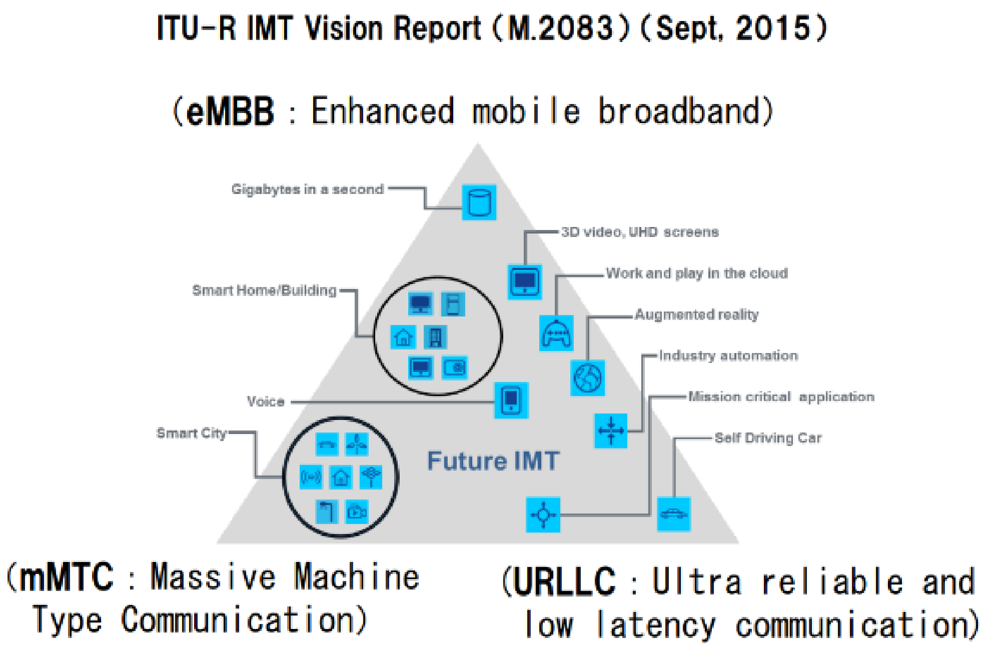


Figure 4.1 5G Use Cases as noted in the IMT-2020 Vision recommendations

eMBB services that use new frequency bands for 5G have been provided from 2020, which initiated the transition from 4G to 5G. In order to achieve this, base stations using New Radio (NR) technology operate non-stand-alone (NSA) configurations that cooperate with LTE core networks and LTE base stations. From 2021 to 2023, operators began to deploy 5G core networks with stand-alone (SA) configuration that support network slicing and other new 5G features, and NR began to utilize existing frequency bands. 5G SA can offer full-featured 5G services with ultra-high speeds, massive multiple simultaneous connections, high reliability, and ultra-low latency .

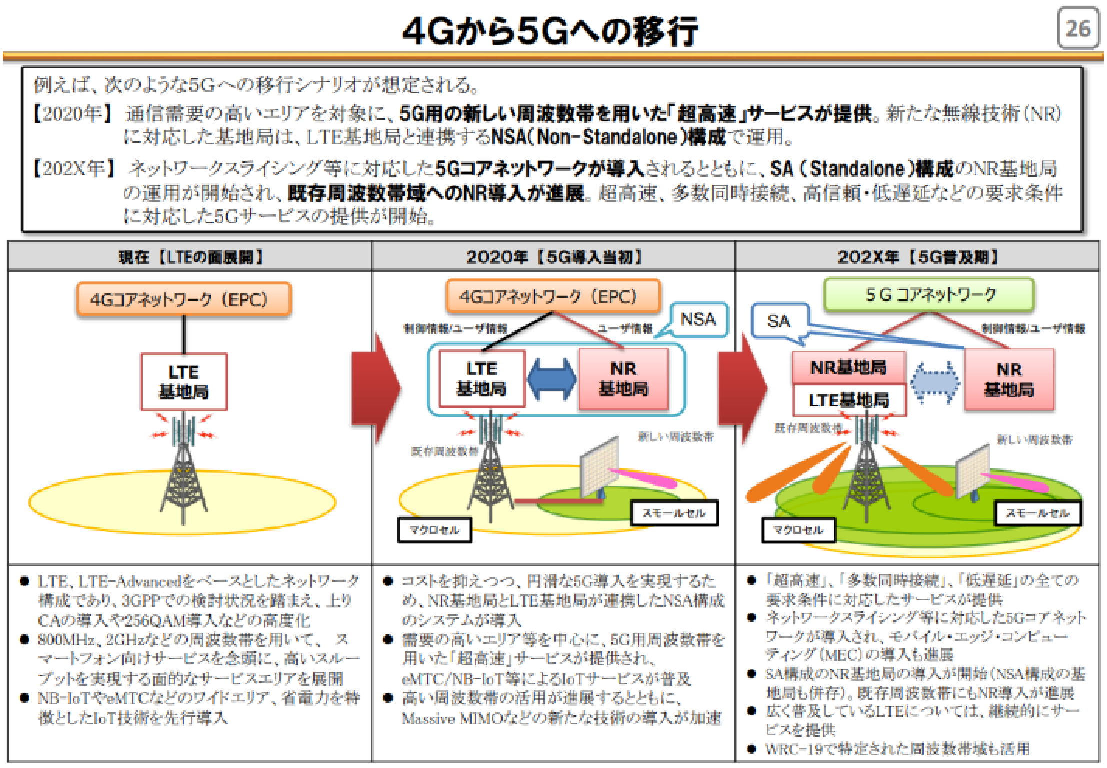


Figure 4.2 An excerpt from the MIC publication on the transition from 4G to 5G

Below is the past and future chronology of 3GPP SA3 security standards activities:

- June 2017 (Release 14)
  - 5G security studies
    - An outline of 17 fields with 5G security related issues and their solutions was produced
    - An outline for future studies was prepared.
- June 2019 (Release 15)
  - 5G phase 1 security
    - Trust model, key infrastructure, intercarrier security, privacy protection
    - Main use case was eMBB
- June 2020, Release 16
  - 5G phase 2 security

    - ✧ Developing and strengthening security specifications for new features supported by 5G phase 2, such as Cellular IoT, URLLC, Non-Public Networks
    - ✧ Integrity check for full rate User Plane traffic
    - ✧ Security for radio backhaul
- March2022 (Release 17)
  - Further evolution of 5G
    - ✧ Developing and strengthening security specifications for new use cases such as Proximity based Service and Industrial IoT.
    - ✧ Back porting user plane integrity check to LTE
- Q1 2024 (Release 18)
  - First release of 5G-Advanced
    - ✧ Further security enhancement including 5G core network

The specifications for 5G NR (New Radio) in the 5G radio system is in 3GPP Release 15, which specified that all 5G specialized equipment on the radio network, such as base stations and the core network, would use the SA to be built. Within 5G NR, the standards for NSA configurations which specifies the case of operating a combined LTE and NR network were finally decided in December 2017, and that during the early stages of offering 5G services from 2020 that this NSA configuration had been used. 5G phase 2 defined by Release 16 was the full 5G specification that covers not only eMBB but also mMTC and URLLC. In Release 16, 3GPP SA3 defined SCAS (Security Assurance Specification) for 5G core network functions, security specifications for network slicing, security enhancement for mMTC and URLLC, security for verticals and LAN services, etc. Also, integrity check for full-rate user plane traffic became mandatory, while it was optional for over 64kbps traffic in Release 15. In Release 17, integrity check for user plane traffic was back ported to LTE, so that LTE and NSA 5G services can support integrity check for user plane traffic. Following sections summarizes the basic security specifications defined in Release 15.

4.3 Non-stand Along (NSA) Security

NSA is the architecture which will be used to move forward the introduction of 5G using the LTE (4G) network core (EPC: Evolved Packet Core). Figure 4.3 shows that the device and the base station are the only pure 5G equipment, but high speeds and massive capacity is made possible through the use of 5G radio.

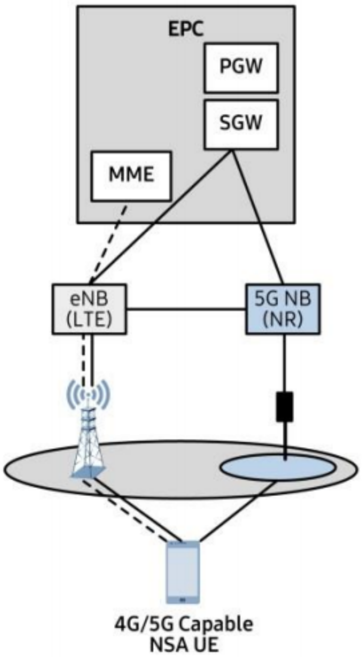


Figure 4.3 5G non-stand-alone configuration

NSA can extend LTE's high speeds and high capacity to 5G via dual connectivity as defined in TS 33.401 Annex E and the specifications for simultaneous transmission of LTE carriers between multiple base stations by using LTE base stations as primary base stations and using 5G base stations as secondary base stations. As security procedures are generally the same as those for LTE dual connectivity, the level of security in NSA will not be that different than for LTE. As described in the following sections, security for 5G will be strengthened when it moves to SA. Assuming that 5G and LTE will continue to exist side by side in this way means that it will be necessary to study the security issues in use cases in which there is a possibility of a downgrade attack when leaving a 5G area to connect to an LTE network.

4.4 5G phase 1 security

4.4.1 Changes to the Trust Model

5G security is designed around the idea that trust is decreasing when it is away from the core. One example of this is in terms of Radio Access Network (RAN), which at base stations is separated between distributed units (DU) and central units (CU). The DU does not retain cryptographic keys, and the U-Plane security is terminated at the CU, because DU will be deployed in an area where the level of physical security is lower. In addition, as shown in figure 4.4, during intercarrier roaming, Home Control is enhanced with the verification of the authentication process for the visiting roaming network (vPLMN) to be carried out by AUSF (Authentication Server Function) in the home network (hPLMN). As shown in Figure 4.5, Security Edge Protection Proxy (SEPP) is introduced in order to secure intercarrier communications.

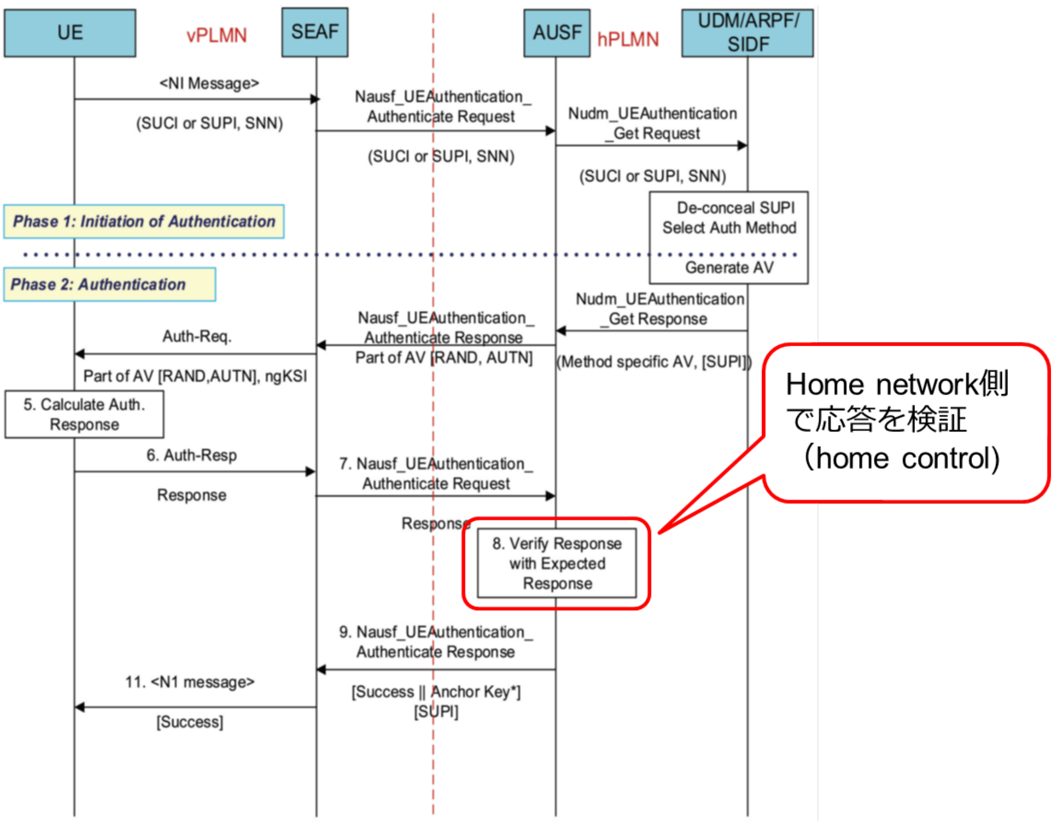


Figure 4.4 5G Authentication and Home Control

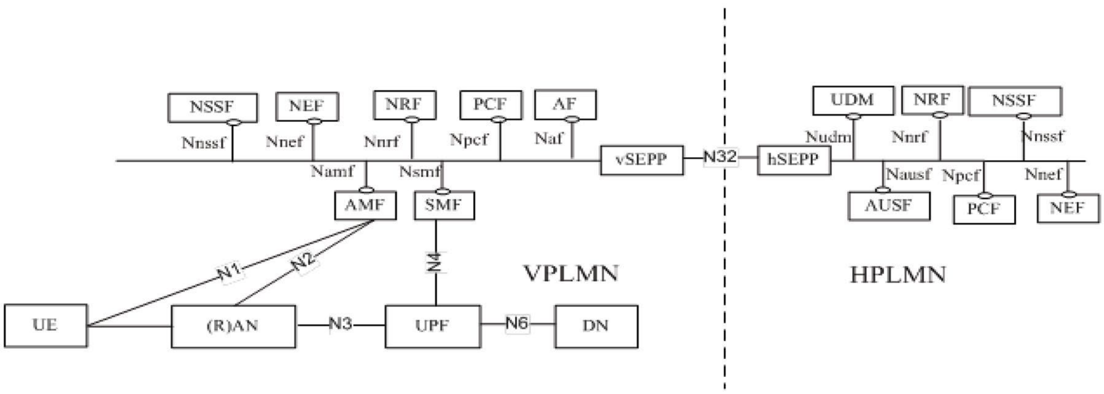


Figure 4.5 Roaming Architecture

4.4.2 Key Hierarchy Verification

The foundation of security in 5G, as it is with LTE, is the use of a long-term secret key (K) that is stored in the core network and the USIM. 5G has two types of authentications, Primary Authentication which is performed on all devices in order to access mobile network services and Secondary Authentication, which is optional and required when accessing a certain external data network (DN). After Primary Authentication successfully occurs between the core network and the User Equipment (UE), the serving network's unique anchor key (K_{SEAF}) is derived from K. From the anchor K the Cipher Key (CK) and the Integrity Key (IK) are derived. The key hierarchy beginning from the initial K is shown in figure 4.6.

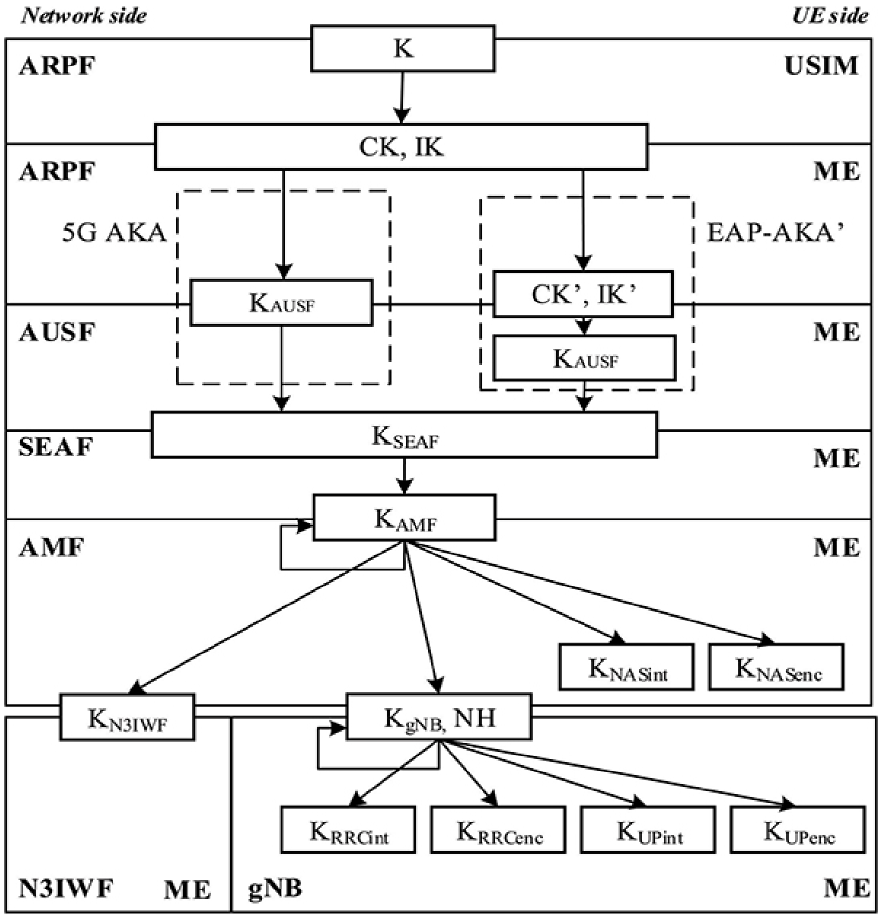


Figure 4.6 Key hierarchy

The key hierarchy includes: K、CK、IK、K_{AUSF}、K_{SEAF}、K_{AMF}、K_{NASint}、K_{NASenc}、K_{N3IWF}、K_{gNB}、 K_{RRCint}、K_{RRCenc}、K_{UPint}、and K_{UPenc}[1]。

---

1 AUSF: Authentication Server Function, SEAF: Security Anchor Function, AMF: Access Management Function, NAS: Non-Access Stratum, gNB: Next generation NodeB, RRC: Radio Resource Control, UP: User Plane

- K_{AUSF} is derived by both the device and ARPF from the CK as well as the IK during 5G AKA.

- K AUSF is derived from ME and AUSF in cases when using the 3GPP credential key to verify radio access that is supported by EAP.

- From K_{AUSF}, the AUSF and ME derive the anchor key K_{SEAF} which is then used to derive the K_{AMF} by ME and SEAF.

- K'_{AMF} key can be derived from the previous K_{AMf} via the ME and AMF when the UE moves from one AMF to another AMF.

- K_{NASint} と $K_{NASenc,}$ which protect NAS signaling, is derived from the K_{AMF} via the ME and AMF

- K_{gNB} is derived from the K_{AMF} via the ME and the AMF. The K_{gNB}, when moving, uses the intermediate key K_{gNB} * in which case it can be derived via the ME as well as the source gNB

- The AS integrity and confidentiality keys, which are called UP （K_{UPint} and K_{UPenc}） and RRC (K_{RRCint} and K_{RRCenc}), are derived from K_{gNB} via ME and gNB. The UP-confidentiality key is an extension for IoT services. The intermediate key NH, which will provide forward security during handovers, is derived via the ME and AMF.

4.4.3 Strengthening privacy protections

Protection of international mobile subscriber identity (IMSI) has not been sufficient in networks historically, including 4G, and it has been possible to track subscribers through the use of an ISMI catcher. 5G strengthens the protection of subscriber ID by encrypting them using the home network public key.

The subscriber ID in 5G, called the Subscription Permanent Identifier (SUPI), is derived from the Mobile Country Code (MCC), Mobile Network Code (MNC), and the Mobile Subscriber Identification Number (MSIN). Devices, except when emergency registration, must use the Subscription Concealed Identifier (SUCI), which encrypts the MSIN part of the home network public key, to connect to the home network. The SUCI is put into the home network ARPF and the authentication proceeds by returning to the SUPI.

4.4.4 Primary / Secondary Authentication

As previously noted, in 5G there are two authentication processes: Primary Authentication performed by all devices in order to access mobile network services and Secondary Authentication that is optional and required when accessing a certain external data network (DN). Primary Authentication is independent of the access network and is also used to connect to non 3GPP access networks such as Wi-Fi. Authentication and key derivation use 5G-AKA as well as EAP-AKA. In order to strengthen Home Control, authentication results from the visiting roaming network are verified during the home network authentication procedure.

Secondary Authentication occurs using EAP in cases when authentication is requested from an external data network (DN). SMF behaves as an EAP Authenticator, using an external authentication server (DN-AAA). This presupposes the device needs to establish a security context with AMF via Primary Authentication.

4.4.5 On-demand Security

Since 5G will be used in a variety of field and services, devices and applications will require different security needs in addition to having different types of constraints. Due to this, it will be possible to select the type of strong encryption process desired, such as whether or not to have U-Plane encryption or tamper detection, gNB (base station) security policies that receive SMF via AMF, and algorithms that select gNB and UE based on capabilities as well as receiving notifications from UE.

4.4.6 Security Assurance

In order to ensure security of 5G networks and services, it is not sufficient to develop security specification. It is also important that all the 5G network equipment correctly implement security functions defined by the specifications. With this in mind, the 3GPP and GSMA collaborated to establish the Network Equipment Security Assurance Scheme (NESAS) in order to create a mechanism to conduct activities related to security related safety issues on network devices. The 3GPP is responsible for the Security Assurance Specification (SCAS) policy that is used by the NESAS.

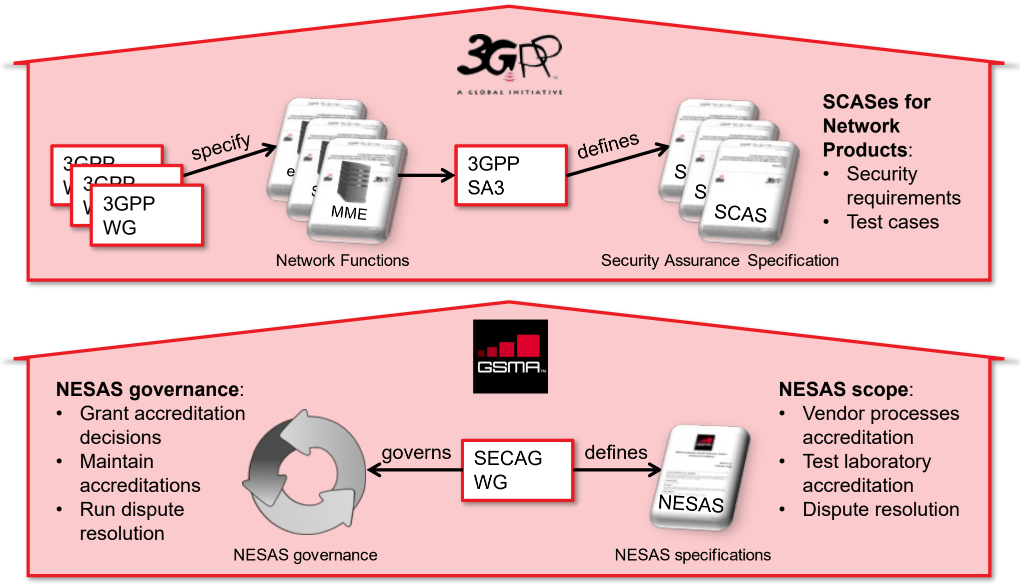


Figure 4.7 Network Equipment Security Assurance Scheme Overview – GSMA

4.5 5G security enhancement in Release 16 and later

The basic security specifications for 5G were defined in Release 15. In later releases, security specifications have been added and enhanced for supporting new use cases such as Cellular IoT, URLLC, Non-Public Network. For example, in Release 17, security specifications for Proximity base Services (ProSe) were defined for securing and protecting privacy in device discovery and device-to-device communication. User plane integrity check introduced in Release 15 was enhanced in Release 16 to support full-rate traffic and then back ported to LTE in Release 17.

Release 18, which will be the first release for 5G-Advanced system, further enhances 5G security in 5 key areas: Security Enablers for Verticals, 5G Core Network, Security Assurance, Security Function Evolution and RAN. Study items in Release 19 includes support for 256-bit cryptographic algorithms to prepare for post quantum cryptography.

4.6 Other organizations studying 5G security

In addition to the 3GPP, other standards bodies and industry groups studying 5G related security issues are introduced below:

- ITU-T
  - 5G related issues being studied include security related issues that are also being considered by Study Group 17. Discussion items on questions that were received are listed as follows, progressing towards offering 5G security recommendations on these issues, working with representatives from other standardization bodies. At time of December 2023, the following work items are discussed in Q2/17.

        - Guidelines of built-in security framework for telecommunications network
        - Security Requirements for the Operation of 5G Core Network to Support Vertical Services
        - Security capabilities of network layer for 5G edge computing
        - Guidelines and Technical Requirements for 5G Network Asset Security Risk Analysis
        - Security controls for operation and maintenance of IMT-2020/5G network systems

- GSMA
    - The NESAS was built following third-party testing and test equipment based on 3GPP TS33 series test specifications (SCAS: Security Assurance Specifications). The GSMA, working to guarantee 5G network security, has proposed NESAS to the European Union Agency for Cyber Security (ENISA). This will complement the EU Toolbox, the European Commission cyber security policy, with the ongoing implementation of cyber security policies in the individual nations of Europe.
    - The 5G Security Task Force (5GSTF) was established in November 2018 and it has held discussions on closing the standards gap from the point of view of implementation and operations. It published the following papers related to 5G security:
        - FS.34 Key Management for 4G and 5G Inter-PLMN Security
        - FS.35 Security Algorithm Deployment Guidance (メンバー外非公開)
        - FS.36 5G Interconnect Security (メンバー外非公開)
        - FS.39 5G Fraud Risks Guide (メンバー外非公開)
        - FS.40 5G Security Guide
        - IR.77 - Inter-operator IP Backbone Security Req. for Service and Inter-operator IP Backbone Providers (メンバー外非公開)
        - NG.113 - 5G Roaming Guidelines
        - NG.116 - Generic Network Slice Template
- NGMN
    - Three reports published on 5G security
        - 5G Security Recommendations Package #1: Access Network / DoS
        - 5G Security Recommendations Package #2: Network Slicing
        - 5G Security – Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience
        - NGMN 5G Network Security Capability Framework for Verticals
        - Security Considerations for 5G Network Operation
        - Security Aspects of Network Capabilities Exposure in 5G
        - 5G Mobile Network Sharing Security V1.02

4.7 Summary of 5G security standards trends

5G is specified to be a more secure network than LTE due to various security enhancements such as subscriber ID protection, integrity check in the user plane, enhanced Home Control, the introduction of SEPP, and the separation of DU-CU. However, there are concerns about security threats arising from new mechanisms introduced in 5G, such as SBA, virtualization, and network slicing. It is necessary to closely monitor discussions not only within 3GPP but also among industry groups such as the GSMA, from the perspectives of implementation and operation. Furthermore, since Release 16, additional specifications and enhancements have been made to accommodate various new use cases, it is essential to review the relevant specifications in more detail when considering security for applications and services in each use case.

5. Studies on 5G Security

This chapter discusses research related to three specific 5G use cases (IoT, Connected Vehicles, Fintech) from the general field of 5G security studies, summarizing the background and the results of a range of studies in each of the three use cases.

5.1 Use Case IoT Security

The 5GMF studied issues related to IoT security by examining research in IoT security papers published by both domestic and international organizations, beginning with a paper released by the 5GMF itself in October 2018 (1). Issues to be considered include topics related to 5G security that were found during the review of the research where improvements can be immediately provided, as well those topics, including development in specifications, where contribution of ideas may produce positive changes in future developments.

5.1.1. Glossary

(1) *Endpoint (EP):* A remote computing device that engages in two-way communications on a connected network, including but not limited to desktop or notebook PCs, smartphones, tablets, servers, workstations.
(2) *Peer:* In this context, a peer does not refer to an asymmetric relationship like with a client-server model, but terminals in a network model in which endpoints have equal relationships.

5.1.2. Overview of IoT Security Related Papers

In this section we will provide an overview of several papers related to IoT security.

5.1.2.1 IoT Security Guidelines (2)

The IoT Acceleration Consortium (IOTAC), the Ministry of Economy, Trade and Industry (METI), and the Ministry of Internal Affairs and Communication (MIC) in a paper published in July 2016 provided guidelines on the necessary security measures for IoT due to the unique characteristics of IoT and the basic principles of security by design as it relates to IoT devices, systems, and services in order to clarify the basic activities necessary from a security perspective.
The guidelines included the five guiding principles of policy, risk analysis, design, network connections and construction, and secure operations, as well as recommendations to the general public.

5.1.2.2 General Framework for Secure IoT Systems (3)

This paper was published by the National Center of Internet Readiness and Strategy for Cybersecurity (NISC) in August 2016. This paper discussed a two-step approach to the specific requirements of IoT security, based upon the perspective of the general requirements for all IoT systems as the unique characteristics of specific to individual sectors in which the system will be deployed. The overall general framework introduced is based upon the basic principles of security by design.

5.1.2.3 IoT Security Comprehensive Measures (4)

This paper was published by the MIC in October 2017 and based upon the NISC's general framework (3), it presents five concrete steps the nation can take to improve 5G security: vulnerability assessments, research and development, promotion of measures to the general public, human resource development, and international cooperation.

5.1.2.4 The Cyber/Physical Security Framework (Draft) (5)

This paper, published by METI in April 2018, provides a general framework for the private sector of the measures needed to be taken to ensure security when using IoT or AI in order to realize initiatives such as "Society 5.0" and "Connected Industries."
The necessary requirements and examples to counter security threats in the CPS are mapped to the definitions in the United States' National Institute of Standards and Technology (NIST) Cyber Security Framework.

5.1.2.5 IoT Safety/Security Development Guidelines (6)

The Information-Technology Promotion Agency, Japan (IPA) initially released this paper in May 2016 and published a revised version in April 2018. This paper focused on IoT system security design for software developers, providing IoT development security guidelines and discussing how to conduct threat analysis, different countermeasures, and how to detect vulnerabilities.

5.1.2.6 Security Guidelines for Product Categories: IoT Gateway (7)

The Connected Consumer Device Security Council (CCDS) released this paper in June 2017. Based upon security evaluations of smart home systems, it provides a concrete process via IoT security guidelines to conduct security evaluations as well as describing a process to evaluate security for all types of IoT devices.

5.1.2.7 IoT Security Guide Standards/Guideline Handbook (8)

The Japan Network Security Association (JNSA) released this paper in May 2018. It describes IoT security principals, norms, and standards that relevant domestic and international organizations have released to the public.

5.1.2.8 IoT Security Check sheet (9)

This check sheet was published for firms planning to introduce IoT devices, providing IoT security guidelines on security considerations from an end user perspective.

5.1.2.9 Draft NISTIR 8200 (10)

The US NIST released this paper in February 2018. This US government interagency report described the current state of international cyber security standards to close the gap between the current state of IoT and previous and ongoing research on security issues that has been already published.

In it, eleven core cyber security areas are discussed, along with related examples of standards, along with an overview of IoT applications generally as well as five specific IoT applications based on specific fields, focusing on the objectives, risks, and threats as they relate to IoT cyber security.

5.1.2.10 Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (11)

The European Union Agency for Cybersecurity (ENISA) released this paper in November 2017. The aim of the paper is to provide baseline recommendations for IoT security operations in Europe, including IoT paradigm, threat and risk analysis, security measures and good practices, gap analysis, and detailed recommendations.

5.1.2.11 Security Guidance for Early Adopters of the Internet of Things (12)

The Cloud Security Alliance, a non-profit organization that through international activities develops recommendations for best practices to realize cloud computing security, released this paper in February 2016. This paper's security guidelines are written for early adopters of IoT and discusses goals, threats to IoT towards individuals and organizations, challenges to providing secure IoT deployments, recommended security controls, and future efforts towards a secure IoT.

5.1.2.12 OWASP IoT Top 10 (13)

The Open Web Application Security Project (OWASP), an online community whose goal is to provide freely available technical articles and documents on web application security, published the original list in 2014 and updated it in December 2018. Listing the top 10 vulnerabilities of IoT devices, the original 2014 version focused on web applications generally, while revised 2018 list focused on IoT specific vulnerabilities.

5.1.2.13 Technical Specification TS-0003 Security Solutions (14)

The international organization OneM2M, which formulates policies for architecture as well as requirements for M2M and IoT technology, released document on technical specifications for security solutions based on global M2M standards. Specifications were defined for OneM2M security architecture, authentication, authorization, ID management and security framework, and privacy protection.

5.1.2.14 IoT Security Guidelines (15)

The GSMA, an industry organization which represents mobile operators and related businesses from over 200 countries, released these proposals in October 2017. It provides IoT security guidelines recommended by the GSMA and is made up of four documents, a summary and security guidelines for services, endpoints, and networks. The proposals provide mobile network solutions, including those related to IoT system availability, identification, and other privacy and security issues.

5.1.3 Topics Extracted

Many IoT security related papers have been released by international and domestic organizations and they have had different aims and complexity, as can be seen by those noted in section 5.1.1. For example, the NISC's General Framework for Secure IoT Systems (3) is written from a high-level perspective and provides a general framework necessary for an entire network, while the OneM2M Technical Specifications (14) provides specifications for security solutions for a specific type of IoT system, the OneM2M standard for M2M technology.

The 5GMF Security Studies Ad Hoc released its own principals that deeply considered the issues of 5G and its connections with IoT (16). Considering all the papers listed in 5.1.1 that discuss solutions to IoT system security issues as they relate to using mobile networks, the paper that is closest to the point of view of the 5GMF study is the GSMA IoT Security Guidelines. (15) Due to this, we want to discuss topics in the other papers we have considered as they relate to issues raised in the GSMA IoT Security Guidelines.

5.1.3.1 Issues listed in the GSMA IoT Security Guidelines

The GSMA IoT Security Guide CLP11-v2.0 overview document describes four challenges to IoT security:

- Availability
- Identity
- Privacy
- Security

5.1.3.2 Availability

The GSMA asks the following questions on the availability challenge in their IoT Security Guidelines:

1. How can Low Power Wide Area (LPWA) networks (e.g. NB-IoT and LTE-M) be deployed and operated with a similar level of security to traditional cellular systems?
2. How can multiple mobile operators support the same level of network security as IoT Endpoints migrate across network boundaries?
3. How can network trust be *forwarded* to capillary Endpoints that rely on Gateway Endpoints for communication?
4. How can the power constraints of Lightweight Endpoints be addressed in secure communications environments?

5.1.3.3 Identity

The GSMA asks the following questions on the identity challenge in their IoT Security Guidelines:

1. Can the user operating the Endpoint be strongly associated with the Endpoint's identity?
2. How can services and peers verify the identity of the end-user by verifying the identity of the Endpoint?
3. Will Endpoint security technology be capable of securely authenticating peers and services?
4. Can rogue services and peers impersonate authorized services and peers?
5. How is the identity of a device secured from tampering or manipulation?
6. How can the Endpoint and Network ensure that an IoT Service is permitted to access the Endpoint?

5.1.3.4 Privacy

The GSMA asks the following questions on the privacy challenge in their IoT Security Guidelines:

1. Is the identity of an Endpoint exposed to unauthorized users?

2. Can unique Endpoint or IoT Service identifiers allow an end-user or Endpoint to be physically monitored or tracked?
3. Is data emanating from an Endpoint or IoT Service indicative of or directly associated with physical end-user attributes such as location, action, or a state, such as *sleeping* or *awake*?
4. Is confidentiality and integrity employed with sufficient security to ensure that patterns in the resultant cipher-text cannot be observed?
5. How does the product or service store or handle user specific Personally Identifiable Information (PII)?
6. Can the end-user control the storage or use of PII in the IoT Service or product?
7. Can the security keys and security algorithms used to secure the data be refreshed?

5.1.3.5 Security

The GSMA asks the following questions on the security challenge in their IoT Security Guidelines:

1. Are security best practices incorporated into the product or service at the start of the project?
2. Is the security life cycle incorporated into the Software or Product Development Life Cycle?
3. Is application security being applied to both services and applications running on the embedded system?
4. Is a Trusted Computing Base (TCB) implemented in both the Endpoint and the Service Ecosystem?
5. How does the TCB enforce self-verification of application images and services?
6. Can the Endpoint or IoT Service detect if there is an anomaly in its configuration or application?
7. How are Endpoints monitored for anomalies indicative of malicious behavior?
8. How is authentication and identity tied to the product or service security process?
9. What incident response plan is defined for detected anomalies indicative of a compromise?
10. How are services and resources segmented to ensure a compromise can be contained quickly and effectively?
11. How are services and resources restored after a compromise?
12. Can an attack be spotted?
13. Can a compromised system component be spotted?
14. How can customers report security concerns?
15. Can Endpoints be updated or patched to remove vulnerabilities?

5.1.4. Overview of New Security Functions in 5G

Many new forms of security with arrive with the introduction of 5G as compared to previous mobile networks up to and including 4G-LTE. These are listed in a different section, however, to assist in clarifying the issues to be discussed, we want to briefly reintroduce the new security functions to be introduced with 5G, based upon “Key Points of 5G Security” by NEC’S Anand R. Prasad. (17)

5.1.4.1 Primary Authentication

Mutual authentication between UE and mobile networks occurred using a single mechanism, Authentication and Key Agreement (AKA), up to and including in 4G-LTE. However, as it is possible to customize this in 5G, an extension of the previously used AKA as well as the Extensible Authentication Protocol (EAP)-AKA, building upon the EAP framework, can be used. While previously it was necessary to support a different authentication mechanism to access non-3GPP technologies such as Wi-Fi, with 5G it will be possible to use the same mechanism when accessing 3GPP or non-3GPP technologies.
In addition, in special cases it is possible to use another EAP method besides EAP-AKA for authentication on private networks.

5.1.4.2 Credential Storage

In order to safely store credentials with high level of sensitivity such as private key K used in AKA it has been standard to use UICC, however with 5G it will be possible to offer an option of credential storage option using a secure hardware storage platform.

5.1.4.3 Secondary Authorization

Secondary Authorization is a mechanism offering authorization via data networks that exist outside the mobile network for UE that are authorized on a mobile network. Secondary authorization is realized by implementing an authorization flow from a different EAP method, such as EAP-AKA on the data network as an authenticator for UE functioning on the mobile network.

5.1.4.4 Inter-operator Security

Vulnerabilities have been found with SS7 and Diameter, which are currently used to facilitate inter-operator communication. In order to provide more secure inter-operator communications in 5G a new mechanism, called Secure Edge Protection Proxy (SEPP), will be introduced.

5.1.4.5 Privacy

Until 4G-LTE, mobile network subscribers' unique identifier, ISMI, was transmitted as plain text, leaving the chance that their privacy could be compromised via tracking. IMSI has been replaced in 5G with the randomly encrypted Subscription Concealed ID (SUCI), generated from the network operator public key Subscription Permanent ID (SUPI), making it possible to protect subscriber privacy.

5.1.4.6 Service Based Architecture (SBA)

5G will introduce adequate security with the adoption of an architecture based on various services used in the core network.

5.1.4.7 Central Unit (CU) - Distributed Unit (DU)

In 5G there will be the possibility in certain use cases that presumes a base station will be deployed in an unsafe location that the base station can be constituted as two entities, CU and DU, in which the flow of sensitive information will be retained in the CU.

5.1.4.8 Key Hierarchy

As previously stated, 5G will use a different key hierarchy as compared to the current mobile networks.

5.1.4.9 Mobility

Mobility itself will work the same as in 4G-LTE, however in 5G it is possible that the core network anchor is not in a secure environment, so secure mobility between anchor points is also necessarily provisioned in 5G.

5.1.4.10 Network Slicing

5G networks are split into different "slices" that will occupy different functions in order to meet the diverse trends in requirements for mobile networks, which therefore provides the opportunity to offer an appropriate security environment on one "slice" that does not influence other "slices" on the same network.

5.1.5. Addressing Issues Related to 5G Security Functions

In this section, the new security features in 5G used that were introduced in section 5.1.2.1 are considered as they relate to the GSMA security challenges introduced in section 5.1.3. Following section 5.1.2.1, the issues that have been extracted from the previously noted

research papers were considered to the related GSMA security guidelines to which they are related.
The IoT security issues discussed in this section should continue to be studied in relation to 5G networks in the future.

5.1.5.1 Availability

1. *How can Low Power Wide Area (LPWA) networks (e.g.NB-IoT and LTE-M) be deployed and operated with a similar level of security to traditional cellular systems?*
While up until 4G it was necessary for an entire mobile network to have the same security functions, in 5G due to the possibility of network slicing, it is possible to provide flexibility necessary low-end devices such as LPWA without influence from other parts of the network. [5.1.3.10]
2. *How can multiple mobile operators support the same level of network security as IoT Endpoints migrate across network boundaries?*
It is possible to be realized in 5G through inter-operator related constructions [5.1.3.4] [5.1.3.9]
3. *How can network trust be forwarded to capillary Endpoints that rely on Gateway Endpoints for communication?*
It is possible to provide direct access with 5G even low-end hardware with limited processing power. [5.1.3.10]
Supposing an EP that is dependent on GW still exists going forward, the issue of how to offer protective measures will continue to exist, however.
4. *How can the power constraints of Lightweight Endpoints be addressed in secure communications environments?*
In 5G, lightweight endpoint devices with power constraints will also be able to support network slicing. [5.1.3.10]

5.1.5.2 Authentication

1*. Can the user operating the Endpoint be strongly associated with the Endpoint's identity?*
In the case when the endpoint user ＝network subscriber, it is possible to associate the two on the network. [5.1.3.3]
However, especially in regard to IoT, it is thought that the endpoint user and network subscriber will not be the same and it will continue to be an issue if this is the case.
2. *How can services and peers verify the identity of the end-user by verifying the identity of the Endpoint?*
The answer to this question is the same as provided to question 1 above.
3. *Will Endpoint security technology be capable of securely authenticating peers and services?*

In 5G, it will be possible to use mutual authentication between the endpoint and authorized peers/services as secondary authentication. [5.1.3.3]

4. *Can rogue services and peers impersonate authorized services and peers?*

The answer to this question is the same as provided to question 3 above.

5. *How is the identity of a device secured from tampering or manipulation?*

In 5G it is possible to use for secure storage a credential storage device other than UICC, which will ensure it is protected from tampering or manipulation. [5.1.3.2]

6. *How can the Endpoint and Network ensure that an IoT Service is permitted to access the Endpoint?*

In 5G, it will be possible to solve this through secondary authentication via mutual authentication between the UE and the IoT device that exists outside the Mobile Network [5.1.3.3]

5.1.5.3 Privacy

1. *Is the identity of an Endpoint exposed to unauthorized users?*

SUPI in 5G corresponds to IMSI in 4G-LTE as a way to differentiate subscribers, however it will be concealed and the use of SUCI that is created from the random encryption of the operator public key should ensure that the endpoint identity on the mobile network is not leaked. [5.1.3.5]

2. *Can unique Endpoint or IoT Service identifiers allow an end-user or Endpoint to be physically monitored or tracked?*

The answer is the same as provided in question 1 above. [5.1.3.5]

3. *Is data emanating from an Endpoint or IoT Service indicative of or directly associated with physical end-user attributes such as location, action, or a state, such as sleeping or awake?*

It is possible to achieve this in a 5G mobile network using an encryption process that takes into account the security of the entire mobile network.

4. *Is confidentiality and integrity employed with sufficient security to ensure that patterns in the resultant cipher-text cannot be observed?*

It is possible to achieve this in a 5G mobile network by using an encryption method that takes into account network security.

5. *How does the product or service store or handle user specific Personally Identifiable Information (PII)?*

This topic cannot be considered as it is not known whether or not the product or service is dependent on PII for processing or storage.

6. *Can the end-user control the storage or use of PII in the IoT Service or product?*

The answer is the same as provided in question 5 above.

7. *Can the security keys and security algorithms used to secure the data be refreshed?*

In 5G phase 2 studies are planned for a possible method to update the long-term valid key (The K shared by UICC and the core network) that would make this possible.

5.1.5.4 Security

1. *Are security best practices incorporated into the product or service at the start of the project?*
Services are outside the scope of this study. In addition, security best practices shared by different feature components offered as 5G core functions are discussed in the 3 GPP SCAS (Security Assurance Specification) framework.
2. *Is the security life cycle incorporated into the Software or Product Development Life Cycle?*
The answer to this question is the same as provided in question 1 above.
3. *Is application security being applied to both services and applications running on the embedded system?*
The answer to this question is the same as provided to question 1 above, however this may become an option with from studies on offering testing facilities on the state of application security on 5G networks.
4. I*s a Trusted Computing Base (TCB) implemented in both the Endpoint and the Service Ecosystem?*
The answer to this question is the same as provided to question 3 above.
5. *How does the TCB enforce self-verification of application images and services?*
The answer to this question is the same as provided to question 3 above.
6. *Can the Endpoint or IoT Service detect if there is an anomaly in its configuration or application?*
The answer to this question is the same as provided to question 3 above.
7. How are Endpoints monitored for anomalies indicative of malicious behavior?
The answer to this question is the same as provided to question 3 above.
8. *How is authentication and identity tied to the product or service security process?*
The answer to this question is the same as provided to question 1 above.
9. *What incident response plan is defined for detected anomalies indicative of a compromise?*
The answer to this question is the same as provided to question 1 above.
10. *How are services and resources segmented to ensure a compromise can be contained quickly and effectively*?
The answer to this question is the same as provided to question 1 above.
11. *How are services and resources restored after a compromise?*
The answer to this question is the same as provided to question 1 above.
12. *Can an attack be spotted?*
The answer to this question is the same as provided to question 1 above.

13. *Can a compromised system component be spotted?*

The answer to this question is the same as provided to question 1 above.

14. *How can customers report security concerns?*

The answer to this question is the same as provided to question 1 above.

15. *Can Endpoints be updated or patched to remove vulnerabilities?*

The answer to this question is the same as provided to question 1 above.

5.1.6 Results of the Survey of Concrete Solutions to problems with IoT

This section will discuss specific solutions to questions concerning IoT that were raised in the previous section.

5.1.6.1 Availability 1:　Safe deployment and operation of an LPWA network

Problem. How can Low Power Wide Area (LPWA) networks (e.g.NB-IoT and LTE-M) be deployed and operated with a similar level of security to traditional cellular systems?

Realizing a LPWA network will require a radio technology that can cover a range of many kilometers without consuming a lot of power. The requirements to deploy and operate such a network include being able to offer an accommodating telecommunications environment with a battery that can function for 15 years to meet the strong existing demand for such a low-level power system. To provide network security in such an environment it will be necessary to use lightweight encryption that uses an algorithm that does not consume a lot of power. However, up until 4G there has only been one kind of algorithm used to safeguard communication between the UE and the core network, which has made it difficult to provide such a low power consuming technology necessary for IoT.

Figure 5.1.1 Four Established Slice Achievement Value Targets for 5G

5.1.6.1.1 Measures for 5G

Network slicing has been introduced with 5G and as each separate “slice” acts independently of each other on the network such that they do not adversely affect each other it is now possible to change the algorithm that is used. Within the following four 5G use cases (as shown in figure 5.1.1) mMTC already has slice configurations that have been defined for use with LPWA networks:

1. eMBB
2. URLLC
3. mMTC
4. V2X

5.1.6.1.2 Considerations for IoT Platform Operators

IoT platform operators, regarding this topic, should confirm which existing slice configurations which are suitable for applications could be offered as well as which possible configurations are appropriate for their platforms.

5.1.6.1 Availability 2: Roaming security between multiple operators

Problem: How can multiple mobile operators support the same level of network security as IoT Endpoints migrate across network boundaries?

A vulnerability in the Diameter protocol was revealed in 2018, which has been utilized in in mobile networks through 4G to facilitate roaming, whereby subscriber information could be leaked. The possible attacks that could occur due to this vulnerability include:

- Subscriber information disclosure
- Network information disclosure
- Fraud
- Denial of service attacks on subscribers

5.1.6.2.1 Measures that can be taken in 5G

To counter this vulnerability a new network element has been introduced in 5G, called Secure Edge Protection Proxy (SEPP). SEPP, deployed at the individual operator’s network edge, offers the following functions:

- Ensures completely secure and confidential singling traffic during exchanges between different operators

- Topology hiding
- Filtering functions based on a firewall

In addition, the 5G primary authentication framework 5G-AKA/EAP-AKA', that supports both 3GPP access networks and non-3GPP access networks like Wi-Fi, also has the merit of preventing fraud in roaming scenarios with the establishment of a consistent authentication environment.

5.1.6.2.2 Considerations for IoT Platform Operators

Since this section is limited to actions between 3GPP operators, there is nothing that needs to concern IoT platform operators

5.1.6.2. Availability 3: Forwarding Trust to Capillary Endpoints.

Problem: How can network trust be forwarded to capillary Endpoints that rely on Gateway Endpoints for communication?

Capillary endpoints cannot directly communicate to the cloud but must have a device to act as a gateway. In this configuration, it is necessary to offer a solution as an attack can be made on the existing capillary network from the trusted gateway that is established on the cloud network

Since in 5G low performance, energy saving endpoints, such as a LPWA network device that can directly access the cloud as mentioned before, are being considered, basically this situation is not anticipated to be an issue.

However, the need for a solution to establishing trusted capillary endpoints remains.
as there are scenarios that exist that require a gateway that requires more than a low performance, energy saving device.

5.1.6.3.1 Issues for IoT Platform Operators to Consider

For scenarios in which gateways are needed for targeted applications, solutions are needed for extended gateways that can establish trust on the network side.

5.1.6.3 Availability 4: Power Constraint Measures for Lightweight Endpoints in Secure Communication Environments

Problem: How can the power constraints of Lightweight Endpoints be addressed in secure communications environments?

5.1.6.4.1 Power Constraint Measures for Lightweight Endpoints Considered by the 3GPP for General 5G Functions

The 3GPP is studying possible solutions (21) for the following major issues concerning Cellular IoT (CIoT) support in 5G that specifically relate to power constraints:

- 5.4 Key Issue 4: Power Saving Functions
- 5.5 Key Issue 5: UE TX Power Saving Functions

The following solutions to these problems are being considered:

- Solution 8: Enhancing MICO for Mobile terminated data/signaling
- Solution 9: Enhanced MICO mode with Active Time
- Solution 22: eDRX for CM-IDLE state in 5GS
- Solution 23: MICO Mode Management for Expected Application Behavior
- Solution 32: MO Data Buffering in the UE
- Solution 33: Delayed Paging Response
- Solution 34: Provisioning of UE TX power saving parameters
- Solution 38: eDRX RRC_INACTIVE STATE in 5GS
- Solution 41: Combining RRC-INACTIVE and 5G UP optimization

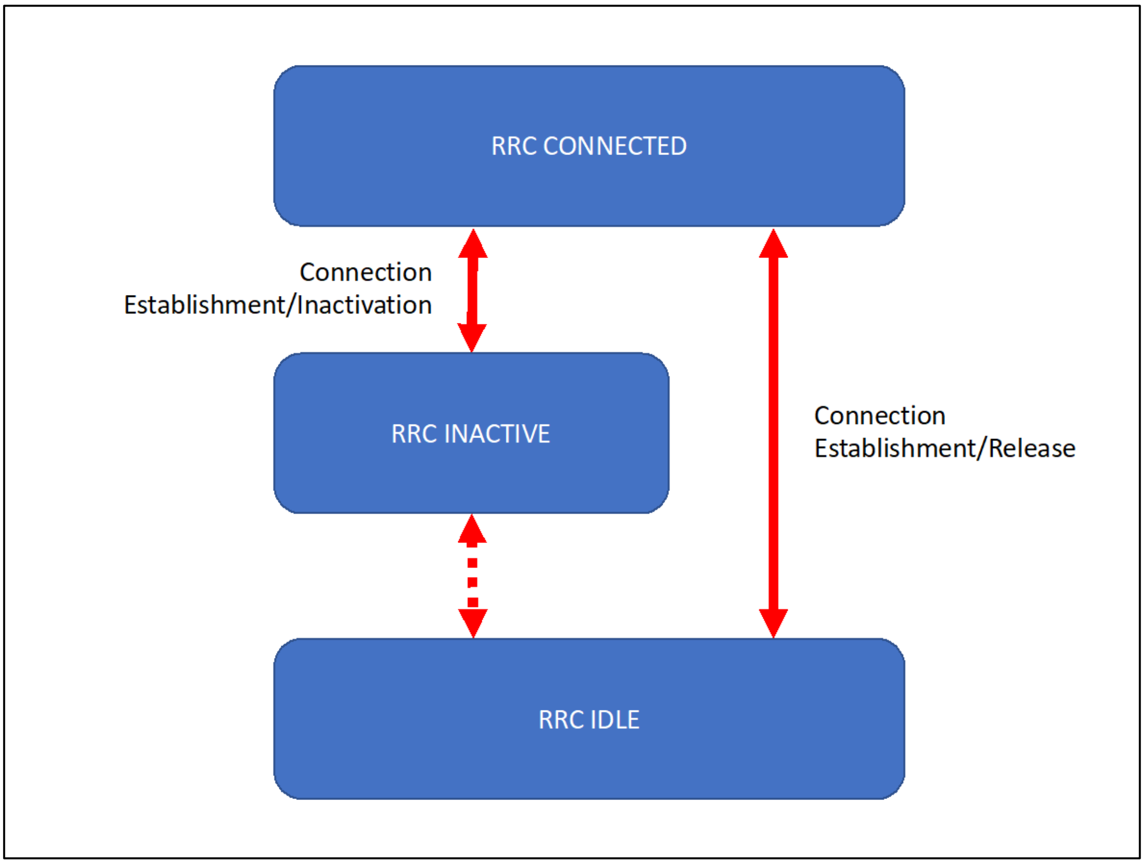


Figure 5.1.2 5G NR RRC Transition Diagram

In addition, in 5G a RCC INACTIVE status rule will be added to the existing RCC IDLE status and RCC CONNECTED status rules that have been in existence up until 4G (see figure 5.1.2). The RCC INACTIVE status is planned to retain the same power saving functions in the UE as the RCC IDLE status does while retaining the RRC and NAS context in the base station/CN and UE.

The 3GPP SA3, which oversees security studies for the aforementioned realization of regular 5G functions has defined the following security solutions:

1. Security handling in transitions between RRC INACTIVE and RRC CONNECTED (TS33.501 6.8.2.1)
    - The SC storage procedure during INACTIVE transitions and SC recovery method during CONNECTED transitions
        - Transition to gNB: same/different case
2. Key Handing during mobility in RRC INACTIVE state (TS33.501 6.8.2.2)
    - Realize notifications to the network UE when transitioning from the configured RNA

5.1.6.4.2 Issues for IoT Platform Operators to Consider

This section discusses the expectations for power saving methods in basic processing for communications between gNB/ng-ENB and the communication processor, however in order to realize the following UE operations the support of the application processor is necessary; therefore, AP specification definitions are necessary.
As transferring from RCC CONNECTED to RCC INACTIVE is to be implemented with gNB/ng-eNB, the transfer instruction at the UE, following 33.501 6.8.2.1.2, implements the RCC INACTIVE state transfer process

- In the case of transferring from the RCC INACTIVE to RCC CONNECTED, the UE, following 33.501 6.8.2.1.3, implements the transfer process

5.1.6.4. Identification/Authentication 1: The Possibility of Strongly Associating the User Operated Endpoint and the Endpoint Identity

Problem: Can the user operating the Endpoint be strongly associated with the Endpoint's identity?

The user operated endpoint is the use case where MNO offers subscriber services and the endpoint where operations are conducted is on an individual smartphone, making it possible for it to be associated with the DB (UDR functions in the 5G core) that the MNO utilizes.

In other cases, this is not offered currently by the 5G core, so it is necessary to provide a solution.

5.1.6.5.1 Solution example: Secondary Authentication Use

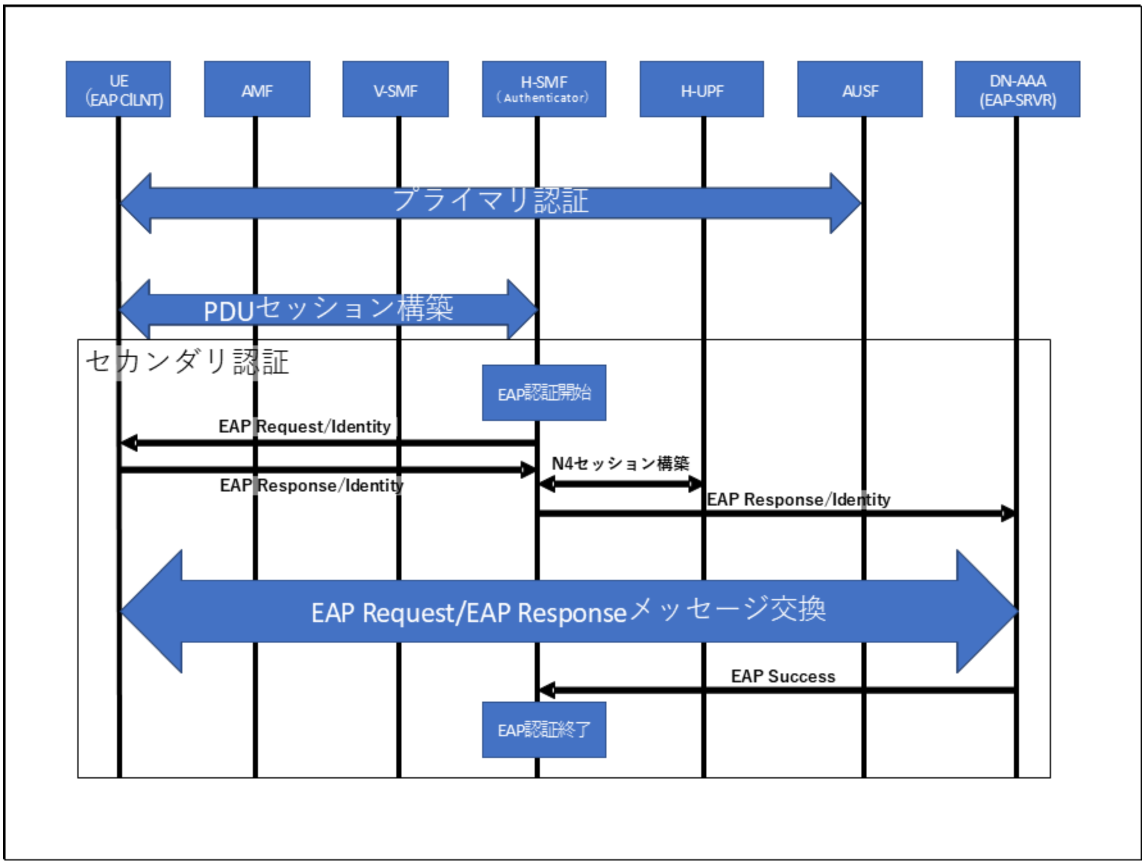


Figure 5.1.3　Outline of 5G Secondary Authentication

Secondary authentication in 5G, occurring after primary authentication of communications between the UE and 5GC, provides authentication between the UE and the AAA server operating on the DN.

The endpoint, utilizing the same function, can voluntarily conduct EAP authorization between the AAA server on the DN and the endpoint, making it possible to strengthen the association between the user and endpoint by requesting the appropriate authorization credential from the endpoint user during this EAP authorization process.

5.1.6.5.2 Considerations for IoT Platform Operators

IoT platform operators need to consider the following regarding solution discussed in 5.1.6.5.1.

- The authorization method for the user operated endpoint
- The EAP method to implement

5.1.6.5. Identification/Authentication 2: Is Secure Authentication for Peers and Services with Endpoint Security Technology Possible?

Problem: How can services and peers verify the identity of the end-user by verifying the identity of the Endpoint?

When considering the secure authentication of peers and services with endpoint security technology, it is important to consider what kind of endpoints with which the peers and services will be communicating.

IoT can be largely divided into the following two types of general uses. (Diagram 5.1.4)

1. Connections via a server
    - Communications received at the target EP via a temporary relay server
2. Direct connections to a local network
    - Communications between EP are directly handled on the local network via Wi-Fi/Bluetooth/ZigBee etc.

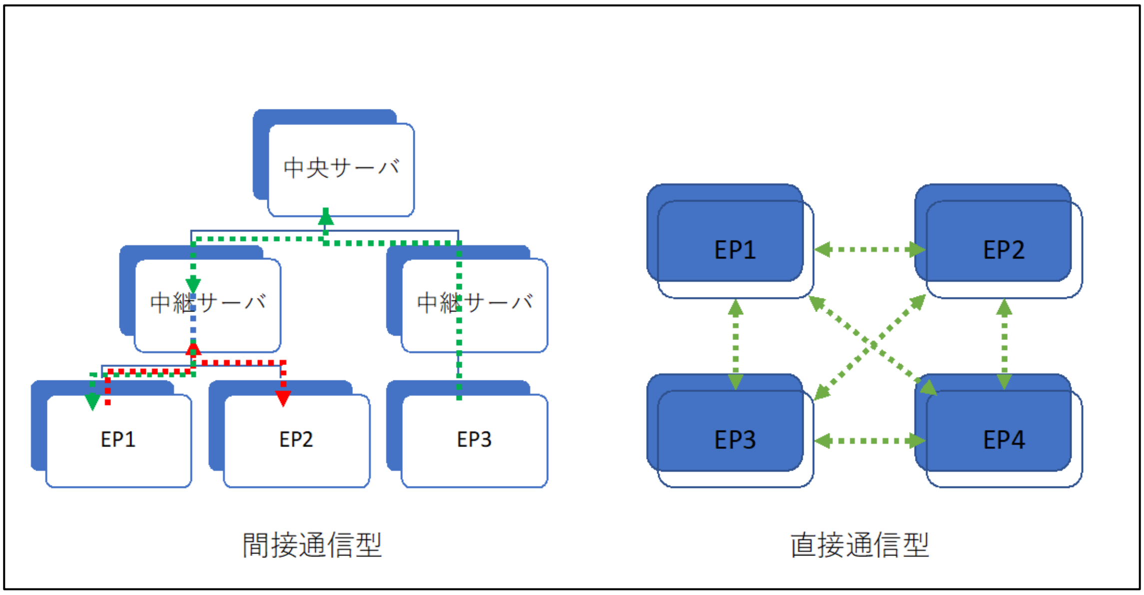


Figure 5.1.4 Typical forms of communication between endpoints

Case 1 is the standard form that IoT will take, in which communication is through a relay sever such as OneM2M.　IoT services offered through cloud providers such as AWS or Azure is also a standard method of providing communications between endpoints.

An example of IoT services is provided via direct connections is the IETF ACE (23). Weave, a standard developed by Alphabet's Nest Labs (24), also provides support for direct endpoint communications.

There are two ways to provide secure authentication between endpoints and peers and services: secondary authorization as offered in 5G and AKMA.

5.1.6.6.1 Secondary Authentication

As shown in figure 5.1.3, secondary authentication can be securely realized using a EAP protocol to provide secure authentication between a UE endpoint and a AAA server that is on a DN in the cloud

In addition, an IoT platform that connects via server such as OneM2M, the same AAA server can carry out the role of PEP/PDP through a central server or a designated relay server, which can provide a central control to determine whether to provide secure access based on the access control policy.

5.1.6.6.2 AKMA

AKMA (Authentication and Key Management for Application Functions), is an extension in 5G of the Generic Bootstrapping Architecture) that has existed in 4G, a function of standards provided by the 3GPP SA3.

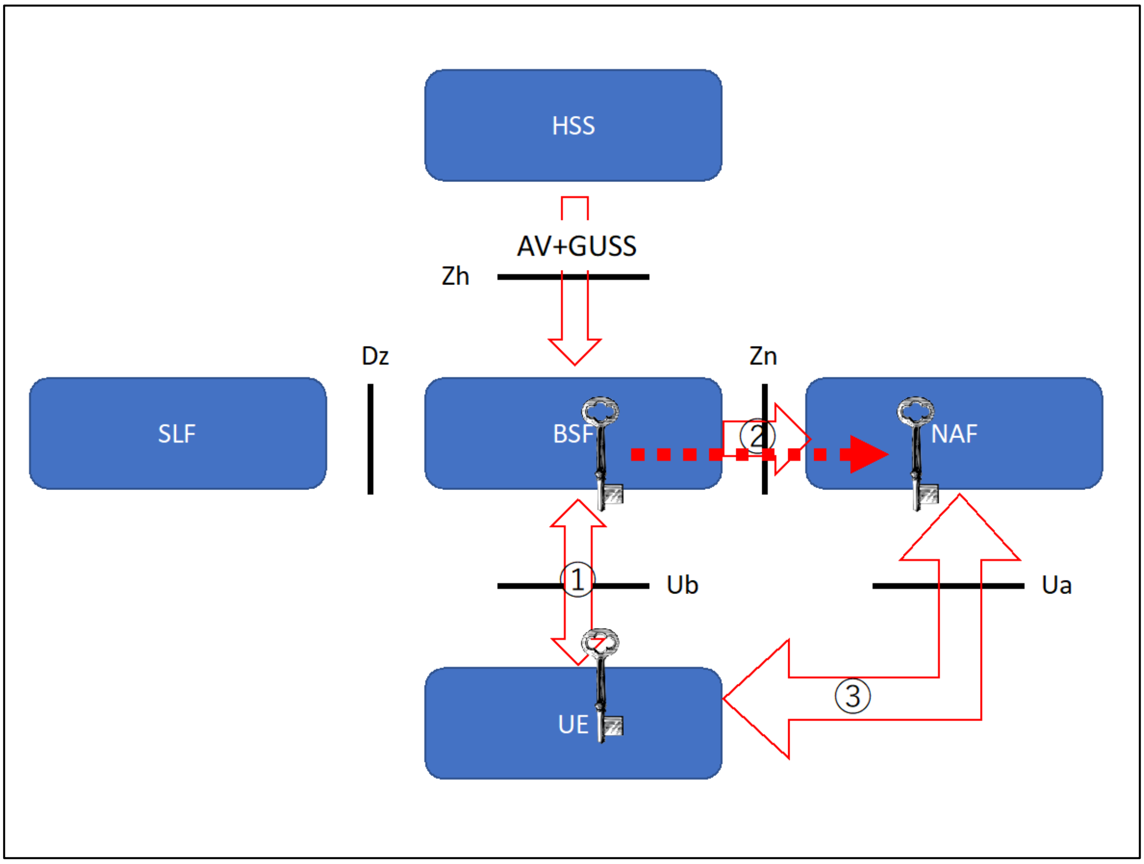


Figure 5.1.5 Overview of Key Sharing between NAF and UE via GBA

The process of secret key sharing between the Network Access Function (NAF) and the UA under GBA, which had the same value as AKMA until 5G, is shown in figure 5.1.5. Key sharing successfully occurs between the UE and the NAF after the UE generates a new shared key to provide authentication with the base of 4G AKA through the BootStrapping Function (BSF), and this shared key, newly generated by from the BSF, is offered to and received by the NAF.

As shown in figure 5.1.5, the 5G core functions that are carried out by HSS and BSF represent a major change from 4G. The figure shows the possibility of a different architecture which these same functions can provide security authentication between the endpoint and peer/service that is planned to be offered by AKMA. This is suitable from the perspective of services provided by IoT platforms in which direct communication is not a centralized function of a central server.

Authentication and access management can be realized simultaneously via secondary authentication on the DN's AAA services conducted by PED/PDP. However, as shown in figure 5.1.5 with AKMA, it is possible to offer a shared key to a NAF using GUSS, making it possible it is possible to for the BSF to make access management decisions.

5.1.6.6.3. Considerations for IoT Platform Operators

More studies are needed for communications between endpoints on IoT platforms that operators will offer that will need to implement authentication processes between peers and services and endpoints.

5.1.6.6 Identification/Authentication 3: Preventing Tampering/Manipulation of Device Identity

Problem: How is the identity of a device secured from tampering or manipulation?

It is not possible to prevent physical tampering or manipulation to a device that is installed in a location that anyone can access where there is no physical security.

This type of physical attack was prevented in networks from GSM until 3G and 4G by secret key K that was used to connect mobile phone networks that was stored on a tamper resistant IC card. With 5G, a general security storage concept has been introduced with storage that is resistant to physical attacks.

The security storage on which contract credentials to be used on the 5G network access are kept as well as their processing requirements, as set out in TS33.501 5.24, are listed below:

- Subscription credentials shall be integrally protected using tamper resistant security hardware components
- The long-term key(s) of the subscription credential(s) (i.e.K) shall be confidentiality protected using a tamper resistant secure hardware component.
- The long-term key(s) of the subscription credential(s) shall never be available in the clear outside of the tamper resistant secure hardware component.
- The authentication algorithm(s) that make use of the subscription credentials shall always be executed within the tamper resistant secure hardware component.

5.1.6.7.1 Considerations for IoT Platform Operators

IoT devices offered by IoT platform operators that manage and operate their devices with their own unique credential information should have storage that is resistant to physical attack as in 5G. The following two candidates can be considered for implementing this kind of storage:

1. System on a Chip (SoC)
    - Cortex-M TrustZone
2. Independent encryption authentication device
    - Smartcards
    - ATECC508/608

5.1.6.7 Privacy 1: Is the Endpoint Identity Revealed to Unauthorized Users?

Problem: Is the identity of an Endpoint exposed to unauthorized users?

Although it had been considered up until 4G to replace the standard IMSI with the random value Temporary Mobile Subscriber Identity (TMSI) in order to prevent tracking via a permanent identifier, under certain circumstances ISMI was transmitted in plain text, making it possible that the endpoint identity could be revealed.

In 5G this has been rectified as the SUPI is never transmitted in plain text, rather only the randomly encrypted SUCI with the home network public key is transmitted, preventing the possibility that the endpoint identity could be revealed to an unauthorized user.

5.1.6.8.1 Points for IoT Platform Operators to Consider

In order to provide a solution in the case in which endpoints and services connected to an IoT platform have, unlike in 5G, independent identity assignments or uses, IoT operators need to implement the same considerations as in 5G.

1. Implement identity transmission only with secure encrypted transmissions with TLS.
2. Adopting the equivalent method as in 5G for protection in the case that the identity is transmitted in plain text

5.1.6.8 Privacy 2: Is It Possible for Location Data Released from the Endpoint or IoT Services be Associated with the End User?

Problem: Is data emanating from an Endpoint or IoT Service indicative of or directly associated with physical end-user attributes such as location, action, or a state, such as sleeping or awake?

This situation can be prevented from occurring by guaranteeing secure confidentiality and integral protection over the entire network. In 5G, the following confidential/integral algorithms to ensure confidentiality and integrity have been defined:

- *Ensuring confidentiality*

1. NEA0
   - Unencrypted (key stream is 0 and x or calculation in plain text)
2. 128-NEA1
   - Stream cipher snow 3G stream devised by Lund University's T. Johansson and P. Ekdahl
3. 128-NEA2
   - CTR128bit AES
4. 128-NEA3
   - 16 stage LFSR (Linear Feedback Shift Register) configuration stream cipher ZUC

- *Ensuring Integrity*

1. NIA0
   - Non integral protection (generated from 32bit Mac with message 0)
2. 128-NIA1
   - Generated from 32bit mac from SNOW 3G
3. 128-NIA2

- Generated from 32bit MAC from CMAC mode 128 bit

4. 128-NIA3
   - Generated from 32bit mac from ZUC

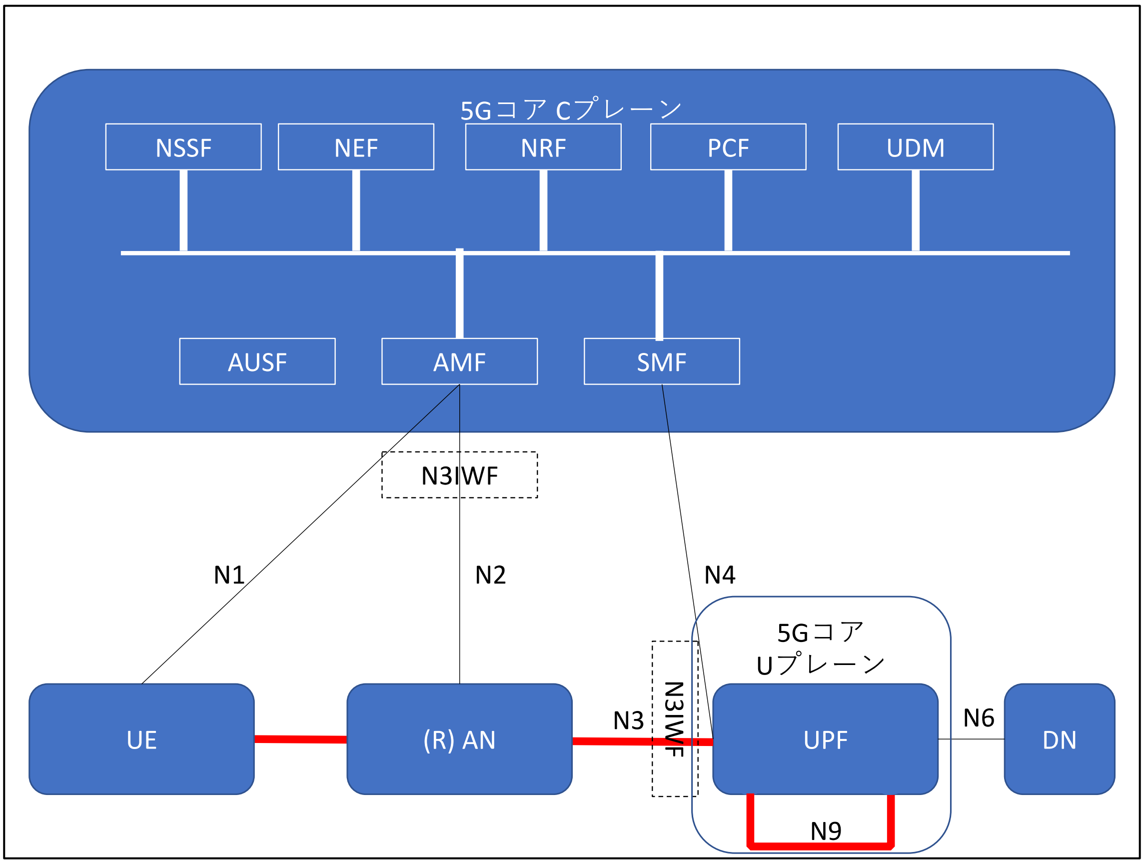


Figure 5.1.6 5G Core Conceptual Diagram

To solve this problem, algorithms of the above-mentioned option 2 must be used to ensure both confidentiality and integrity. It should be noted that these protections can only be applied in 5G, so user plane transmissions are only protected from the UE to the UPF (Fig. 5.1.6).

5.1.6.9.1 Points for IoT Platform Operators to Consider

As explained in the previous section, IoT platform operators will need to consider additional measures to ensure their network is secure when communicating with external data networks that connect to the user plane function through the N6 interface. Below is a list of options that can be considered.

- Secure end to end sessions between the UE and DN
  - IPsec, TLS
  - Use 5G's existing security functions
- Existing 5G security capabilities with extra support
  - Use secondary authentication or AKMA with an IKE or TLS HS shared key between UE and DN
- Secure communication between UPF and DN
  - Secure session infrastructure between UPF and DN
    - SSH Port Forwarding
- Physically deploy UPF and DN next to each other
  - Edge computing

5.1.6.10 Privacy 3: Is confidentiality and integrity completely and securely provided though the inability to detect any patterns in the cipher texts?

Problem: Is confidentiality and integrity employed with sufficient security to ensure that patterns in the resultant cipher-text cannot be observed?

This can be resolved by offering the second to fourth algorithms that are listed in section 5.1.6.9 to ensure confidentiality, or an equivalent algorithm, over the entire network.

5.1.6.10.1 Points for IoT Platform Operators to Consider

Same as in 5.1.6.9.1

5.1.6.11 Privacy 4: Can the security keys used to secure data as well as the security algorithm be refreshed?

Problem: Can the security keys and security algorithms used to secure the data be refreshed?

5.1.6.11.1 Refreshing Security keys

The 3GPP SA3 is considering this issue in the Study on Long Term Key Update Procedures and the following two candidate solutions have been released in TR 33.935-101

1. Diffe-Hellman based Key agreement over SIM OTA

2. Multiple sets of parameters on the USIM

5.1.6.11.2 Refreshing Security Algorithms

As stated above, the 3GPP SA3 has currently defined several different kinds of algorithms to ensure confidentiality and integrity.

- Integrity: NIA1～NIA3
- Confidentiality: NEA1～NEA3

Beginning with 3G, it has been possible for algorithms to be supplemented and refreshed multiple times, so the 3GPP foresees no problems occurring with the possibility of refreshing algorithms in 5G, as well.

5.1.6.11.3 Points for IoT Platform Operators to Consider

IoT platform operators need to consider the situation related to refreshing algorithms or encryption if they decided to use their own algorithm or encryption method on their platforms.

5.1.6.12 Security 1: Are security best practices included in products and services from the start of any project?

Problem: Are security best practices incorporated into the product or service at the start of the project?

The 3GPP, which oversees 5G standards, has been working on two frameworks, the Security Assurance Specification (SCAS) and the Security Assurance Methodology (SECAM), to provide network product security assurance for telecoms to use.

Work on SCAS and SECAM include the following:

- SCAS
  - Studies are being conducted on the special characteristics of 3GPP network products and the threat model towards those products along with studies into methodologies to provide network product security assurance.
- SECAM
  - Plan for SCAS in every network product
  - Network product security and network product R&D and compliance evaluation for managing the network product lifecycle.

The 3GPP, as seen in this process, is taking into consideration best security practices throughout the research and development stage for products that will be used in the 5G core network.

5.1.6.12.1 Points for IoT Platform Operators to Consider

Operators will need to consider equally the 3GPP's SCAS/SECAM with the products and services that use their platforms.

5.1.7 Overview of Related Work Items with the 3GPP

5.1.7.1AKMA

The research into the key issues related to AKMA in TR 33.835-200, which was sent to SA#86 for approval, has been completed. Work on the technical specifications (TS) are now planned to begin based on the conclusions of TR 33.835-200, which has been given the working title "Authentication and key management for applications based on 3GPP credential in 5G" (8). The aim of the TS based on the conclusions of the TR are as follows:

- Specify security architecture enhancements for 5G system to support AKMA
- Specify AKMA authentication procedures
- Specify AKMA key management procedures
- Specify the security related interfaces and corresponding protocols

5.1.7.2 LTKUP

Study points for Long Term Key Update Procedures (LTKUP) were still being considered as of the latest draft release of TR 33.935 in April 2019.

5.1.7.3 SCAS

Security Assurance Specification (SCAS) was a study item at the 3GPP SA3 from December 20, 2012, to December 20, 2013, during which the special characteristics and threat models of 3GPP network products were studied. The following two methodologies to ensure network product security were considered:

1. Common Criteria (ISO 15408) Standards
2. Proprietary method
    - Create an overall list of special characteristics and functions following an evaluation of the specified product and then determine the suitability with the security requirements based on the results of the threat analysis.
    - Prepare the SCAS based on each (class of) network products.

Option 2, a proprietary method, was adopted, although during the evaluation process the CC methodology was also utilized when deemed appropriate.

5.1.7.4 SECAM

Security Assurance Methodology (SECAM) was allocated the following two tasks

- SCAS formulations for security standards as well as test specifications
- Network product security and network product R&D and compliance evaluation for managing the network product lifecycle.

The 3GPP is providing assistance with formulating, governing, and maintaining SECAM, but the organization currently responsible for SECAM is the GSM Association (GSMA) This body has formulated the following requirements and procedures for SECAM.

- Certification for vendor network products as well as the network product lifecycle management process
- Certification for test labs (for authorized vendors and third parties)
- Dispute resolution

5.1.8 Review of IoT Security Use Cases

IoT security papers from domestic and international sources were studied and issues were extracted, focusing on GSMA documents, in which further studies are necessary as related to issues concerning 5G. Through this analysis, the following applications that have been newly added to 5G were found to be able to solve issues related to IoT security.

- Network Slicing
- Secondary Authentication
- Privacy Considerations

Based on the results of this, measures to counter the specific, representative issues are collected in Table 5.1 below:

Table 5.1: Representative Problems and Answers

Problem	Answers
Can LPWA networks operate with the same level of security as traditional cellular networks?	Yes, with the flexible support of mMTC slice using 5G's network slicing functionality.
Can the same level of network security be offered with IoT devices used across several mobile operators?	Yes, security can be ensured with inter-operator mobility using SEPP (Secure Edge Protection Proxy).
Can network trust be forwarded to endpoints that rely on communications with gateway endpoints?	This is not a concern as lightweight endpoints can communicate directly with each other.

Can lightweight endpoint power limits that can be used in secure communication environments be avoided?	This will be possible with the adoption of proposed solutions for issues related to lightweight endpoints that have power limits
Can the identity of an endpoint be strongly associated with users who operate the endpoints?	Yes, users can be associated with endpoints through the use of 5G secondary authentication.
Can endpoint security technology safely authenticate peers and services?	Yes, services can be safely authenticated through functions such as 5G secondary authentication and AKMA.
Can device identity be secured from tampering or manipulation?	Yes, it is possible to ensure this as secure storage other than the UICC can be used with 5G's credential storage functionality.
Can endpoint identity be revealed to unauthorized users?	No, as endpoint identity leakage in 5G networks can be avoided because 5G networks use the more anonymous SUCI rather than IMSI, which can be developed to be used by services, as well.
Can data released from endpoints and IoT services, such as physical end user attributes (location, behaviors such as one is asleep or awake) be directly displayed or implied?	In 5G networks, encryption is utilized across the entire mobile network to take account of security. This can also be built into services, as well.
Does the encryption process provide a sufficient level of protection to confidentially and integrity, such that the pattern in the existing cypher-text cannot be observed.	In 5G networks, encryption is utilized across the entire mobile network to take account of security. This can also be built into services, as well.
Can the security keys used to secure data as well as the security algorithms be refreshed?	The ability to refresh long term keys (K shared between UICC and core networks) in 5G is being considered and the ability to build this functionality into services is also being considered
Are security best practices incorporated into the product or service at the start of the project?	Activities have been conducted using 3GPP SCAS (Security Assurance Specification) framework for 5G core products. This can also be considered when building services, as well.

5.2 Use Case Connected Vehicle Security

5.2.1 Overview

Automobiles that are equipped with the ability to connect via a network to the larger transportation infrastructure, such as other vehicles or traffic signals, is one service that will be realized in the age of 5G. Connected vehicles are expected to bring about more efficient traffic patterns, safer streets, and new services. These new services are expected to be developed and introduced out of a variety of related fields, such as infrastructure and safety. However, networking capabilities also comes with the reality of unknown threats, therefore it is necessary to prepare countermeasures to ensure the security of the network.
With this in mind, the 5GMF Planning Committee established the Security Research Adhoc in July 2018, followed after further preparations by the establishment of the Security Research Committee in July 2019. These activities were carried out to perform studies to better understand security issues from the services expected in the age of 5G, specifically targeting security issues that were related to the fields of IoT, Connected Vehicles, and Fintech. In July 2020, the 5GMF White Paper "Security in 5G Use Cases, Version 1.0" summarizing the results of these investigations was released. This report reflects the latest status of research activities in the Connected Vehicle field since the release of Version 1.0 as Version 1.1. Concretely, this section reports on the results of research in the field of Connected Vehicles, including services that are to be realized with the development of Connected Vehicles, listing the different security issues that are related to the services that will be realized with Connected Vehicles and specifying what issues need further study in regards to 5G (see Fig 5.2.1). This chapter is organized as follows: this introduction to the chapter; section 5.2.2, which lists the results of research by standards organizations in regards to connected vehicle security, a summary of the results of studies from industry organization that are provided in standards reports and guidelines, and a list of other relevant reports; section 5.2.3, which, following the security requirements that were outlined from the reports from relevant organizations listed in 5.2.2, lists some technical components used by 5G networks to realize Connected Vehicles and the security issues that arise from their use.

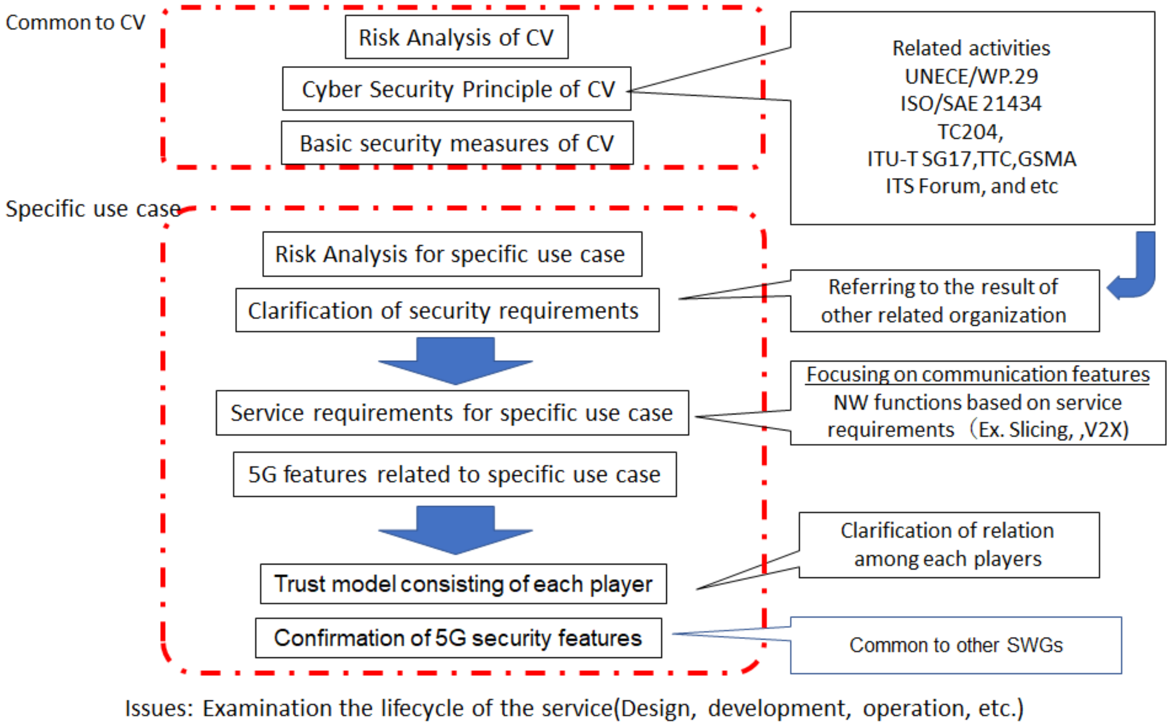


Figure 5.2.1 Study Background of this Report

5.2.2. Standards Related to Connected Vehicle Security

5.2.2.1. UNECE/WP.29

The United Nations Economic Commission for Europe (UNECE) World Forum for Harmonization of Vehicle Regulations on Intelligent Transport Systems and Automated Driving (ITS/AD) established the Task Force on Cyber security and Over the Air (OTA), which began working in December 2016.

This task force formulated guidelines for cyber security as well as data protection. Guidelines, following general principals, were provided for data protection for personal data, safety for failsafe devices and functionality, and security related to unauthorized access and wiretapping and falsification of data, as shown in table 5.2.1, with guidelines provided for high level requirements [1]. In addition to the above-mentioned guidelines, specific studies were held focusing on cyber security and software updates, out of which the following two guidelines were positioned as draft regulations. (2018, revised in 2019)

Table 5.2.1 Overview of Guidelines for Cyber Security and Data Protection.

category	measures ensuring cybersecurity and data protection
Data protection	The principle of lawful, fair and transparent processing of personal data means in particular
	The means of anonymization and pseudonymization techniques shall be used.
	The collection and processing of personal data shall be limited to data that is relevant in the context of collection
	Introducing the concept of “privacy by design” or “privacy by default”
Safety	Standards for the functional safety of critical electric and electronic components or systems in vehicles such as ISO 26262 shall be applied
	Failsafe that does not affect the data in the CV or CV when connecting or communicating with the CV or a vehicle with autonomous driving technology.
	Prevention of unauthorized access to circuit infrastructure information and unauthorized alteration of software by cyber attacks via wireless communication and diagnostic ports
	Equipment with safe mode in the case of emergency
Security	The protection of connected vehicles and vehicles with autonomous driving technology requires verifiable security measures according security standards (e.g. ISO 27000 series, ISO/IEC 15408)
	Connected vehicles and vehicles with autonomous driving technology shall be equipped with integrity protection and managing cryptographic keys
	Mutual authentication in communication between control devices in connected vehicle or vehicle with autonomous driving technology to prevent from cyber attack to circuit infrastructure information by via wireless communication and diagnostic port
	Online Services for remote access into connected vehicles and vehicles with autonomous driving technology should have a strong mutual authentication and assure secure communication (confidential and integrity protected) between the entities.

5.2.2.1.1. Proposal for a Recommendation on Cyber Security [2]

Previous guidelines, targeting vehicle manufactures, provided basic policies for overall security for vehicle systems as well as networks and the cloud, threats and countermeasures and security management methodology in research and development, commercialization, and when manufacturing is discontinued. Within these guidelines, Annex A contains the draft for cyber security regulation for the UN.

Here is an overview of the basic principles listed in chapter 3 and the threats to vehicles systems in chapter 4. The basic principles listed in chapter three provides comprehensive principles on topics including: guidance for the management top layer, supply chains, thinking about defense in depth, defense, detection, and analysis of attacks, and security evaluation, as shown in table 5.2.2: Basic rules in the Cyber Security Report) Threats are listed in terms of the related vehicle components, as shown in see table 5.2.3 as well as table 5.2.4 to table 5.2.9. Especially in terms of threats related to software updates and connections to external components, awareness of the vehicle structure is essential. Among these, items related to communications and networks include threats related to communications channels and external connections, as shown in tables 5.2.5 and 5.2.8. Countermeasures including anonymity, authentication and authorization, tamper proofing, and non-repudiation can ensure basic security if implemented.

1. Introduction
    1.1. Preamble
    1.2. Scope
    1.3. Approach
2. Definitions (and abbreviations)
3. Cyber security principles
4. Threats to vehicle systems and ecosystem
5. Mitigations
6. Requirements for cyber security processes and how to evidence their application
7. Conclusion and Recommendation for further proceedings

Annexes

A Draft proposal to introduce a UN Regulation on Cyber Security

B List of threats and corresponding mitigation

C List of Security Controls related to mitigations incl. examples

D List of reference documents

Figure 5.2.2 Cyber Security Report Contents

Table 5.2.2 Basic Cyber Security Principles

section	cyber security principles
3.3.1	Organizational security should be owned, governed and promoted at the highest organizational level
3.3.2	Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain
3.3.3	Organizations should implement cyber security monitoring and incident response to ensure vehicle types are secure over their lifecycle;
3.3.4	All organizations, including sub-contractors, suppliers and potential 3rd parties, should work together to enhance the security of the system
3.3.5	The vehicle should be designed using a defense-in-depth approach. The vehicle manufacturer should design the vehicle architecture to reduce the likelihood that compromise of assets within one architectural element would result in propagation of the attack to other architectural elements;
3.3.6	The security of software and hardware should be managed throughout the lifetime of the vehicle
3.3.7	The storage and transmission of data should be secure and should be controlled
3.3.8	The vehicle manufacturer should assess security functions with testing procedures
3.3.9	The vehicle should be designed to be resilient to cyber attacks
3.3.10	The vehicle should be designed with the capability to detect cyber attacks and respond appropriately
3.3.11	Access to vehicle services and functions should be controlled, in accordance with access control mechanisms and allocation of roles established in compliance with national or regional legislation, and available only to authorized parties
3.3.12	Vehicles should log relevant access data, which can be used for post incident analysis and forensics

Table 5.2.3 Threats to Vehicles

section	Threats to vehicles	Relationship with communication
4.3.1	Threats regarding back-end servers	
4,3,2	Threats to vehicles regarding their communication channels	◎
4.3.3	Threats to vehicles regarding their update procedures	
4.3.4	Threats to vehicles regarding unintended human actions	
4.3.5	Threats to vehicles regarding their external connectivity and connections	○
4.3.6	Potential targets of, or motivations for, an attack	

Table5.2.4 Threats to Backend Services

section	Threats to back-end services
4.3.1(a)	Use of back-end servers to attack vehicles and external data(1)
4.3.1(b)	Impact on vehicle operation due to backend server destruction(2)
4.3.1(c)	Loss or leakage of data stored in the backend server(3)

Table 5.2.5 Threats to Communication Channels

Section	Threats to vehicles regarding their communication channels	5 G
4.3.2(a)	Spoofing of messages or data received by the vehicle	○
4,3,2(b)	Communication channels used to conduct unauthorized manipulation, deletion or other amendments to vehicle held code/data	○
4.3.2(c)	Communication channels permit untrusted/unreliable messages to be accepted or are vulnerable to session hijacking/replay attacks	○
4.3.2(d)	Information can be readily disclosed. For example through eavesdropping on communications or through allowing unauthorized access to sensitive files or folders	○
4.3.2(e)	Denial of service attacks via communication channels to disrupt vehicle functions	○
4.3.2(f)	An unprivileged user is able to gain privileged access to vehicle systems	○
4.3.2(g)	Viruses embedded in communication media are able to infect vehicle systems	○
4.3.2(h)	Messages received by the vehicle, or transmitted within it, contain malicious content	○

Table 5.2.6 Threats during Software Updates

section	Threats to vehicles regarding their update procedures
4.3.3(a)	Misuse or compromise of update procedures(12)
4.3.3(b)	It is possible to deny legitimate updates (13)

Table 5.2.7 Threats from Unintended Human Actions

section	Threats to vehicles regarding unintended human actions
4.3.4(a)	Misconfiguration of equipment or systems by legitimate actor, e.g. owner or maintenance community (14)
4.3.4(b)	Legitimate actors are able to take actions that would unwittingly facilitate a cyber-attack(15)

Table 5.2.8　Threats from External Connections

section	Threats to vehicles regarding their external connectivity and connections	5G
4.3.5(a)	Manipulation of the connectivity of vehicle functions enables a cyber-attack, this can include telematics; systems that permit remote operations; and systems using short range wireless communications(16)	○
4,3.5(b)	Hosted third party software, e.g. entertainment applications, used as a means to attack vehicle systems(17)	
4.3.5(c)	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	

Table 5.2.9 Potential vulnerabilities that could be exploited if not sufficiently protected or hardened

section	Potential vulnerabilities that could be exploited if not sufficiently protected or hardened
4.3.6(a)	Cryptographic technologies can be compromised or are insufficiently applied(26)
4.3.6(b)	Component parts or supplies could be compromised to permit vehicles to be attacked(27)
4.3.6(c)	Software or hardware development permits vulnerabilities(28)
4.3.6(d)	Network design introduces vulnerabilities(29)
4.3.6(e)	Physical loss of data can occur(30)
4.3.6(f)	Unintended transfer of data can occur (31)
4.3.6(g)	Physical manipulation of systems can enable an attack(32)

5.2.2.1.2 Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues [3]

As the electrification of vehicles progresses, the importance of software updates increases due to the need to add new functions, provide performance improvements, and correct imperfections via updates. Due to this, the cyber security task force studied for vehicle manufacturers guidelines and regulations for software updates.

The overall structure is shown in figure 5.2.3. In this section, guidance is provided for overall software update procedures as well as safety and security regulations and identifying software to be updated.　In addition, in the annex, a draft regulation was provided to define the Regulation X Software Identification Number (RXSWIN) for vehicle manufacturers and software updates.

In Chapter 5, safety and security regulations were provided, which included, as shown in table 5.2.10, falsification of updated software and protection from attacks when updating the system.　In addition, the ability to authenticate authority and the information (documents) needed to authenticate authority was also proscribed.

In response to the study of this regulation, domestically, the law that implements software updates (which includes rules on cyber security), the Road Transport Vehicle Act, Section 99, Clause 3 (revised), was amended in May 2019[4].

1. Introduction
   1.1.Preamble
   1.2.Scope
2. Definitions
3. Document structure
4. Process for software updates
5. Safety and security requirements for software updates
6. Identification of the installed software
7. Conclusion and Recommendation for further proceedings

Annexes

A Draft proposal to introduce a UN Regulation on uniform provisions concerning the approval of software updates processes

B Draft proposal to amend existing UN Regulations to introduce software identification numbers (RXSWIN)

Figure 5.2.3 Contents of Software Update Guideline

Table 5.2.10 Security Requirements for Software Updates

section	Requirements
5.2.1	The location and movement of the vehicle should not be restricted during the download portion of a software update unless safety implications result from the download process.
5.2.2	・Recovery from a failed or interrupted update ・The vehicle manufacturer shall ensure that the vehicle user is able to be informed about the update before the update is executed ・the vehicle manufacturer shall demonstrate how the update will be executed safely and shall ensure that software updates can only be executed when the vehicle has enough power to complete the update process
5.2.3	the vehicle manufacturer shall ensure that the vehicle cannot be driven during the execution of the update and that the driver cannot use any functionality of the vehicle that would affect the safety of the vehicle or the successful execution of the update
5.5 Requirements for evidencing that updates and the update process is safe and secure.	To support any certification process for permitting software updates, particularly those over the air, the authority shall be competent and able to assess the processes and procedures of a vehicle manufacturer with respect to the above safety and security requirements
	To enable an assessment of the vehicle manufacturer's processes and procedures with regard to conducting software updates safely and securely the vehicle manufacturer shall be able to provide to the authority: ・documentation describing how the update will be performed securely. ・documentation describing how the update will be performed safely ・documentation describing any interaction/requirements of the vehicle user (if any) in the update process

5.2.2.1.3. UNR155[5], UNR156[6]

The ITS/AD (Automated Driving Subcommittee) of WP.29 adopted UNR155 "Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber update and software updates management system" (2020.06). Both require automotive

OEMs and suppliers to ensure a business management system to ensure the adequacy of cyber security and software updates.

5.2.2.1.3.1. UNR155

Figure 5.2.4 shows the structure and outline of UNR 155, which obliges automotive OEMs and suppliers to establish security processes and implement security measures based on a cyber security management system (CSMS) throughout the entire product life cycle, including the development phase, manufacturing phase, and operational phase. and security measures based on the Cyber Security Management System (CSMS) throughout the development, manufacturing, and operational phases of the product lifecycle, and provides a framework for applying for type certification of vehicles based on compliance with the CSMS. Section 7 of UNR 155 specifies specific CSMS requirements, cybersecurity requirements for vehicles developed and operated within the CSMS framework and reporting requirements.
The following processes are required to put the above CSMS into practice.
The process by which the organization manages cybersecurity,
The process of identifying risks to the vehicle,
The process of classifying and evaluating the identified risks,
The process for verifying that identified risks are properly managed,
The process of verifying that risk assessments are up to date,
Processes to monitor, detect, and respond to threats, vulnerabilities, and cyberattacks against the vehicle.
Processes to verify that countermeasures are effective against new threats.
The process by which data is provided to analyze cyber-attacks and attempts at cyber-attacks.
In addition, Annex 5 provides examples of cybersecurity threats and corresponding countermeasures that are necessary to implement the CSMS.

5.2.2.1.3.2. UNR156

The structure and outline of UNR 156 are shown in Figure 5.2.5. UNR 156 specifies the requirements for process approval and vehicle type approval as general specifications for the purpose of safely updating the software of the Electronic Control Unit (ECU) installed in a vehicle. In particular, Section 7 describes the 12 processes required to implement a Software Update Management System (SUMS), the information to be recorded and stored when updating software for a specific vehicle, the security measures for software updates, and the requirements for OTA. The requirements for software updates, including security measures for software updates and OTAs, are specified in the SUMS. The processes involved in implementing a Software Update Management System (SUMS) include, for example, information on initial and updated software versions, and a process for uniquely identifying the hardware components associated with a type-approved system, processes that enable vehicle manufacturers to identify vehicles for software updates, and processes that evaluate, identify, and record whether software updates affect type-approved systems.

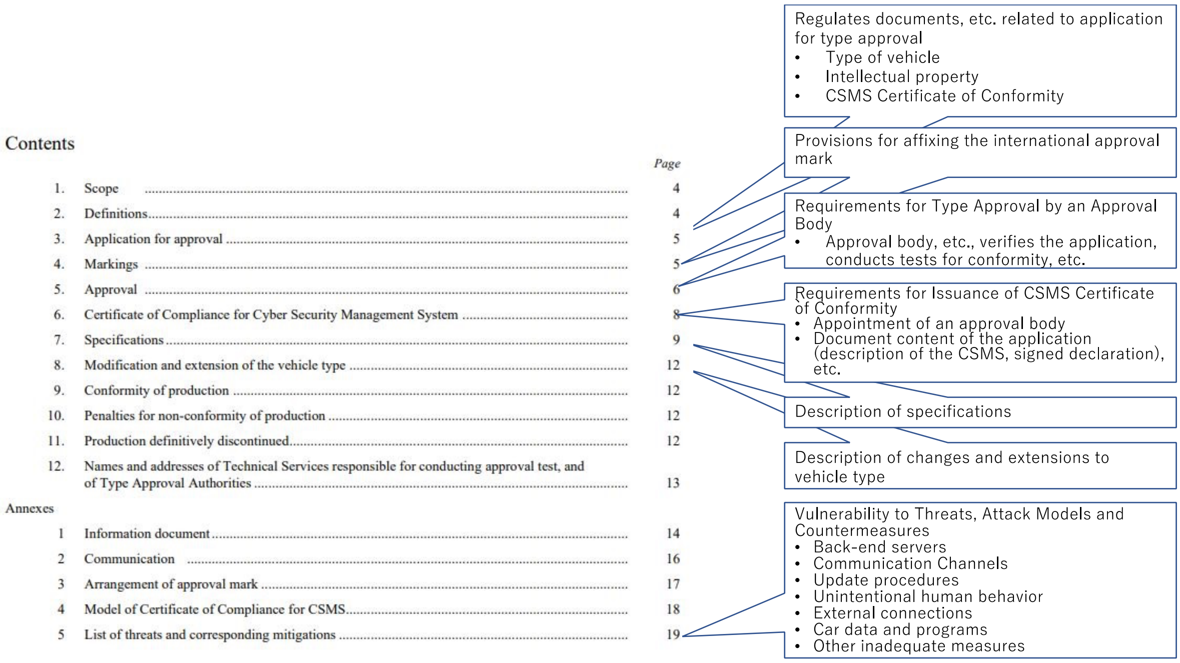


Figure 5.2.4 Structure and Overview of UNR 155

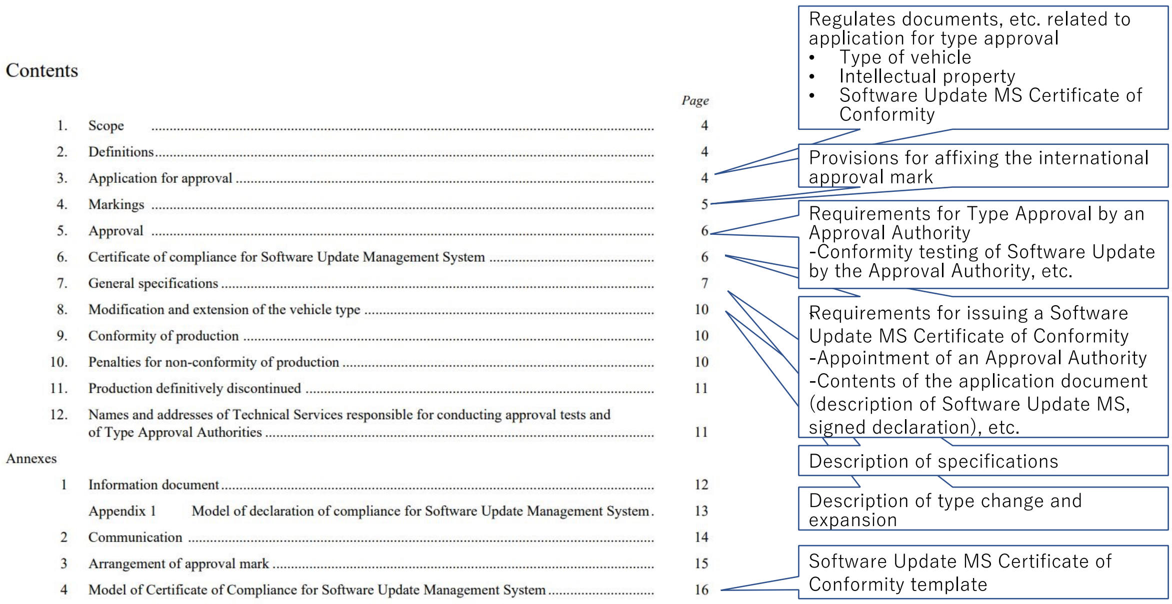


Figure 5.2.5 Structure and Overview of UNR 156

5.2.2.2. ISO TC 22 (Road vehicles)

In ISO/TC22, the ISO/SAE21414(Road Vehicles-Cybersecurity engineering) is standardized in 2021. These standards regulate the requirements for interface security risk management as well as the entire lifecycle of a vehicle, from initial engineering (concept, design, development), production, operation, and maintenance up until the vehicle is no longer being operated. In addition, these standards also define the vocabulary for a shared framework and process in regard to the transmission and operation of cyber security risks between shareholders. The defined process offers clear countermeasures to reduce possible successful attacks, reduce losses, and against constantly changing threats. Global firms are provided consistency and can hasten decision making. These standards are expected to be reflected in the WP29 cyber security principals [7].

These standards are outlined in figure 5.2.6 and overall structure is shown in figure 5.2.7. The overall structure is summarized below from [8].

Chapter 6, Risk Assessment Methods and Treatment includes the definitions for the requirements on conducting risk management as well as implementations of asset analysis, risk analysis, and risk evaluation. Chapter 8, Product Development, defines the requirements for necessary cyber security activities for vehicles, from production and operation until the end of development. It especially targets the unique horizontal division of labor for vehicles, including concept, system, hardware, and software. Chapter 9, Production, Operations, and Maintenance, defines requirements for necessary cyber security activities from the end of development until the vehicle is scrapped, including the collection of vulnerability data, incident responses, incident measures, and the specific requirements to follow when the vehicle is scrapped. Chapter 10 on Cybersecurity Management defines the process requirements and specific rules for the structure of a cyber security strategy organization and the cyber security management requirements for a vehicle's entire lifecycle.

A summary of cyber security activities is shown below in figure 5.2.8. This process, which is defined in ISO 26262 for functional safety standards, is called a triple v process. The three component parts of the triple v are the system, the software, and the hardware. These standards are related to the requirements of cyber security activities, process definitions, and methodologies, so does not include the following:

- Applications of concrete cyber security technology and solutions
- Requirements for specific improvement measures
- Requirements for the communication systems
- Back-office requirements
- EV charging requirements
- Autonomous vehicle requirements

As mentioned above, ISO/SAE 21434 is characterized by providing requirements for cyber security management for the entire vehicle management process, from design and development to operation and scrapping.

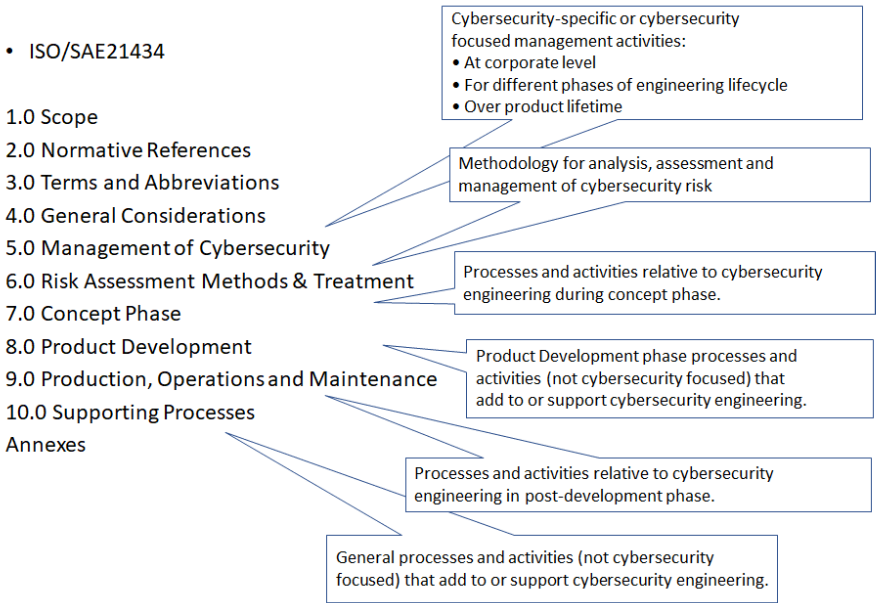


Figure 5.2.6 Table of Contents and Overview of ISO/SAE21434

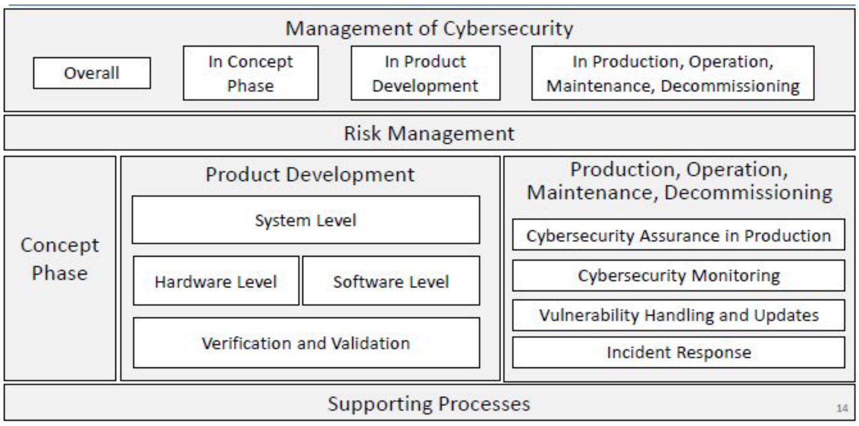


Figure 5.2.7 Structure of ISO/SAE21434

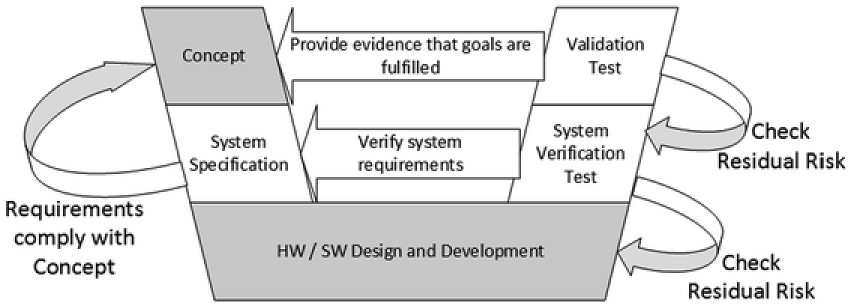


Figure 5.2.8 Overview of the Cyber Security during the Development Process

5.2.2.3. ISO TC204（Intelligent Transport Systems）

TC204 has different committees that focus on standards for ITS, including data for transportation, communications, and control systems [9]. The communications subcommittee ISO TC204/WG16 covers communication standards for ITS [10]. The committee's work on security related standards is in ISO21217 [11] and ISO16461 [12].　The cooperative system subcommittee ISO TC204/WG18 released their standards for security in ISO/TS21177 [13] and ISO/TS21185 [14] (Table 5.2.11).

Table 5.2.11 Related Security Standards in TC204

Standards	Title	Overview
ISO21217	CALM(Communications access for Land mobile) Architecture	Define security features in the protocol stack
ISO16461	ITS – Criteria for privacy and integrity protection prove vehicle information systems	Evaluation criteria for privacy of probe information
TS21177	ITS- ITS station security services for secure session establishment and authentication between trusted devices	A system that quickly authenticates and establishes secure communication between ITS base stations
TS21185	ITS- Communication profiles for secure connections between trusted devices	Profile standard for lower layer communication for secure communication between ITS base stations and vehicles

ISO21217 specified the type of node communication reference architecture referred to as ITS station units that are planned for an ITS communication network. It defines the communication node necessary for node-to-node communications between nodes on various ISO networks. An overview of the requirements is shown in diagram 5.2.9 and a diagram of the reference architecture is shown in diagram 5.2.10. The infrastructure components defined are firewalls that can detect intrusions, authentication, authorization, profile management, network security management with SMIB, and hardware security modules.

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 Requirements
6 Overview of ITS communications
7 ITS station overview
8 Details of elements of ITS-S reference architecture
9 Typical implementations of ITS station units
Annex A Illustration of typical ITS-SU implementations
Annex B ITS-S configurations

Figure 5.2.9 Table of Contents on ISO21217

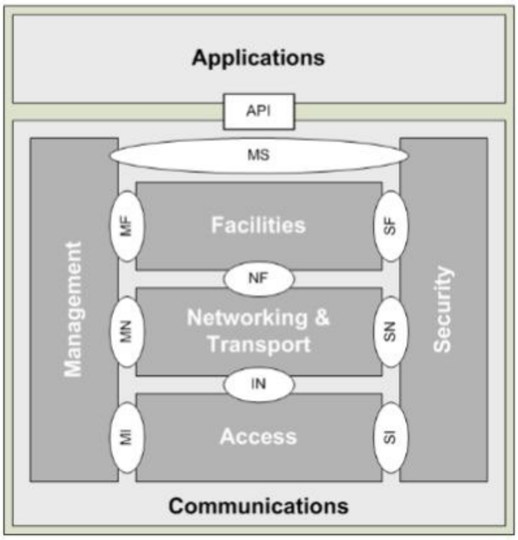


Figure 5.2.10 ISO21217 CALM reference architecture

ISO16461 provides the evaluation criteria in regard to probe vehicle data service privacy for those firms that plan to offer these services, as shown in diagram 5.2.11. ISO16461 includes the following contents for standards related to probe vehicle systems (PVS). PVS is a system in which valuable data is offered to users from statistical analysis conducted on probe data that is collected from individual vehicles. The standards include the following:

- Integral protection of data from PVS and an anonymity protecting architecture
- Security evaluation criteria and requirements that protect the privacy and integrity of PVS data
- Requirements for the generation and handling of appropriate probe data via data anonymization

1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 Reference architecture
6 Basic framework
7 Criteria for privacy protection

Figure 5.2.11 Table of Contents on ISO16461

ISO/TS21177 specifies, as shown in diagram 5.2.13, the protection of data integrity, anonymity, and authentication between trusted devices in regard to ITS stations. As shown in diagram 5.2.12, when two devices are cooperating through a trusted relationship infrastructure, data is protected during mutual communication. The standards in ISO 21217 state that ITS station units (ITS-SU) that have the physical implementation of the ITS station (ITS-S) functionality are trusted devices. In addition, an ITS-SU is constructed from many ITS station communication units (ITS-SCU) that are paired with an ITS internal network. In other words, the ITS-SCU is the smallest entity that can be called a trusted device, as shown in diagram 5.2.14. In this situation, the ITS station needs access to secure data from infrastructure/road networks (IRN) and inter-vehicle networks (IVN), as shown in diagram 5.2.15 and 5.2.16. Therefore, the following requirements for ITU-S security services for establishing trusted relationships between ITS applications have been established. Trusted relationships can be established with the following three ITS application cases:

- Communication between different ITS-SCU within an individual ITS-SU
- Communication between ITS-SCU in different ITS-SU
- Communication between an ITS-SU and a sensor and control network (SCN)

As shown in diagram 5.2.17, services that offer ITS applications will provide, beyond the TLS protocols that offer secure sessions, a security adapter layer that includes authentication and authorization, anonymity and privacy, data integrity, and secure services preventing unauthorized access.

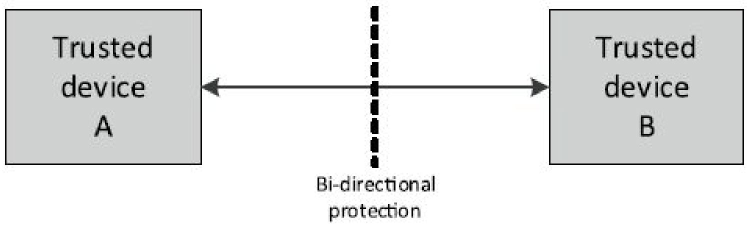


Figure 5.2.12 Basic structure of TS21177

1 Scope
2 Normative
3 Terms and
4 Symbols and abbreviated
5 Overview
6 Process flows and sequence diagrams
7 Security Subsystem: interfaces and data types
8 Adaptor Layer: Interfaces and data types
9 Secure Session services
Annex A (informative) Usage scenarios
Annex B (normative) ASN.1 module

Figure 5.2.13 Table of Contents on TS21177

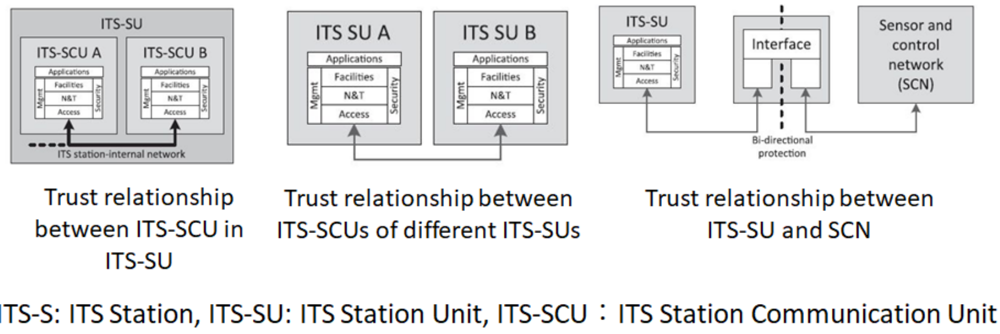


Figure 5.2.14 Trusted relationships in ITS Services

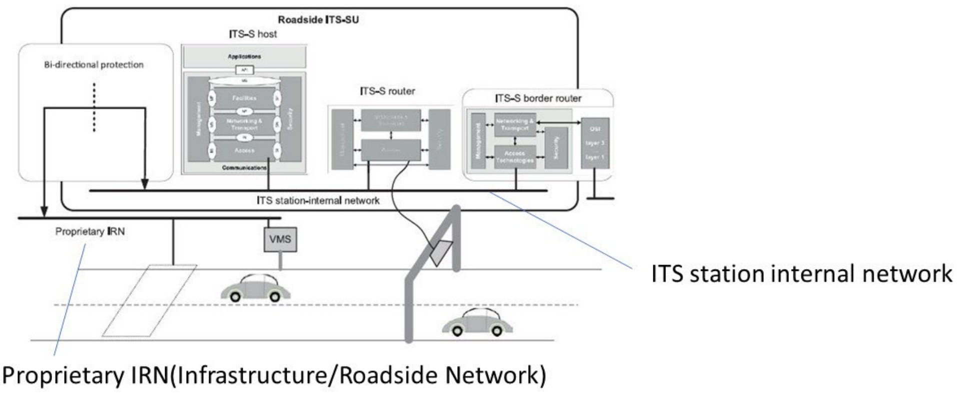


Figure 5.2.15 Example of a roadside ITS-SU connected with proprietary IRN

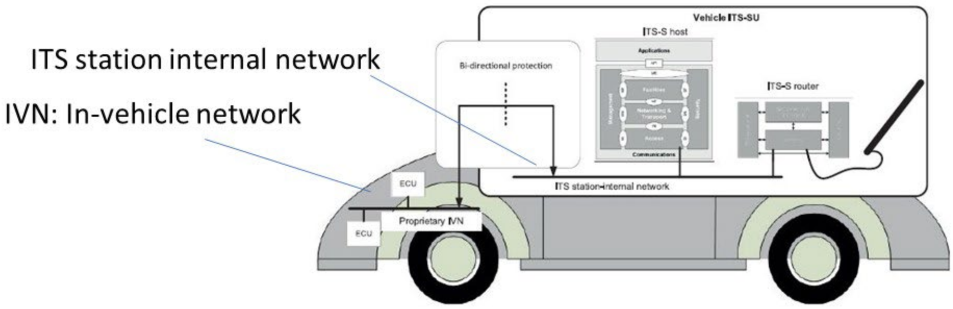


Figure 5.2.16 Example of an ITS-SU connected to a proprietary IVN

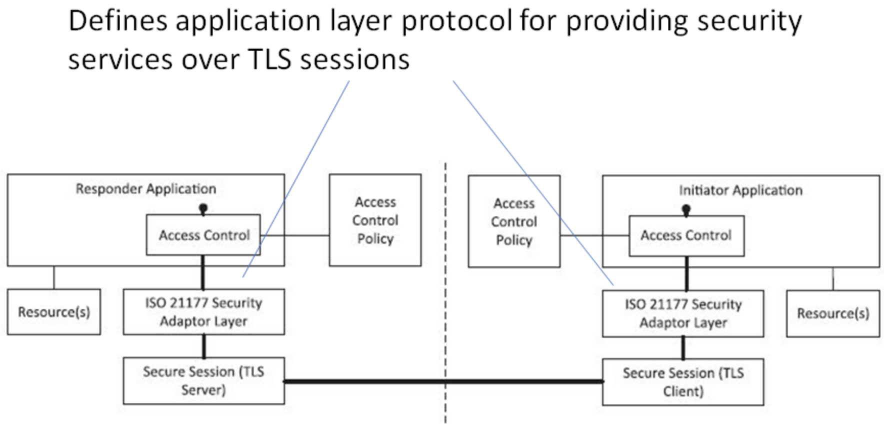


Figure 5.2.17 Logical architecture in TS21177

ISO/TS21185 specifies the methodology to define ITS-S communication protocols between standardized trusted devices, as shown in diagram 5.2.18. The specified protocol provides the capability to securely exchange data with a low latency between devices using a different configuration.

1 Scope.
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 OID conventions
6 Architecture
7 Communication profiles and protocol
8 ITS communication protocols
9 ITS-S communication protocol stacks
10 ITS-S communication
Annex A (normative) ASN.1 module

Figure 5.2.18 Table Contents on TS21185

5.2.2.4. ITS Forum

ITS Forum are domestic organizations whose purpose is to promote the spread of ITS information communication systems by carrying out research of R&D and standardization on ITS information communication systems, liaison and coordination with related organizations, information collection, and enlightenment activities. In addition, various guidelines have been formulated and made public in order to popularize and promote ITS. Regarding the security of Connected Vehicles, "ITS Forum RC-009 Security Guidelines for Driving Support Communication Systems" (2011) [15], which specifies security guidelines for vehicle-to-vehicle and road-to-vehicle communication information, and " Survey Report for the Advancement of ITS and Autonomous Driving Using Cellular Communication

Technology" (2019, revised in 2021) [16] jointly prepared by the Cellular System TG and the 5GMF Connected Vehicle Ad Hoc Meeting are formulated.

5.2.2.4.1. ITS Forum RC-009 Security Guidelines for Driving support Communication Systems

Figure 5.2.19 shows the structure of the above guidelines.

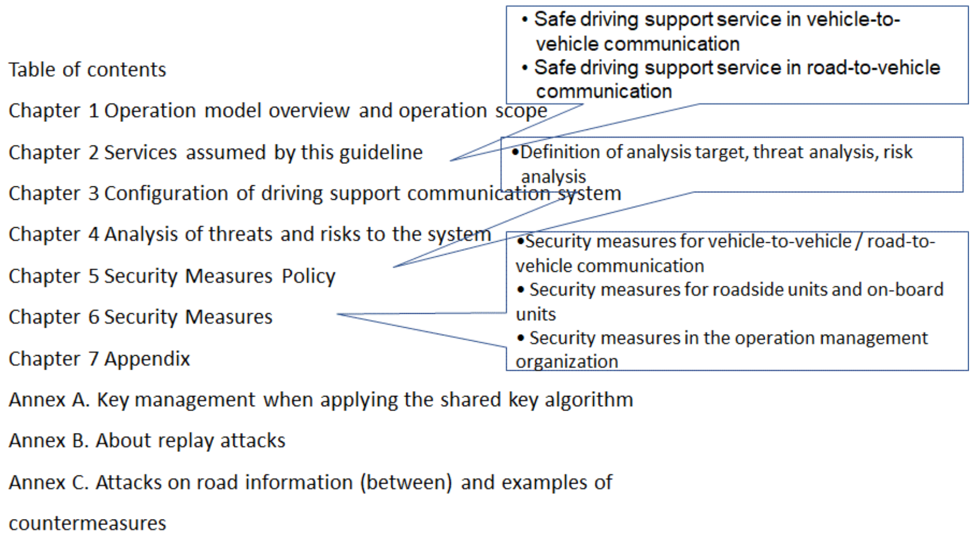


Figure 5.2.19 ITS Forum RC-009 Security Guidelines for Driving Assistance Communication Systems

Figure 5.2.20 shows the scope of this guideline. The broadcast communication between vehicles and roads is a target to be analyzed. Here, security measures are stipulated assuming threats associated with services, such as vehicles illegally delivering information on fake priority vehicles and impersonating priority vehicles, and fake roadside devices delivering fake information.

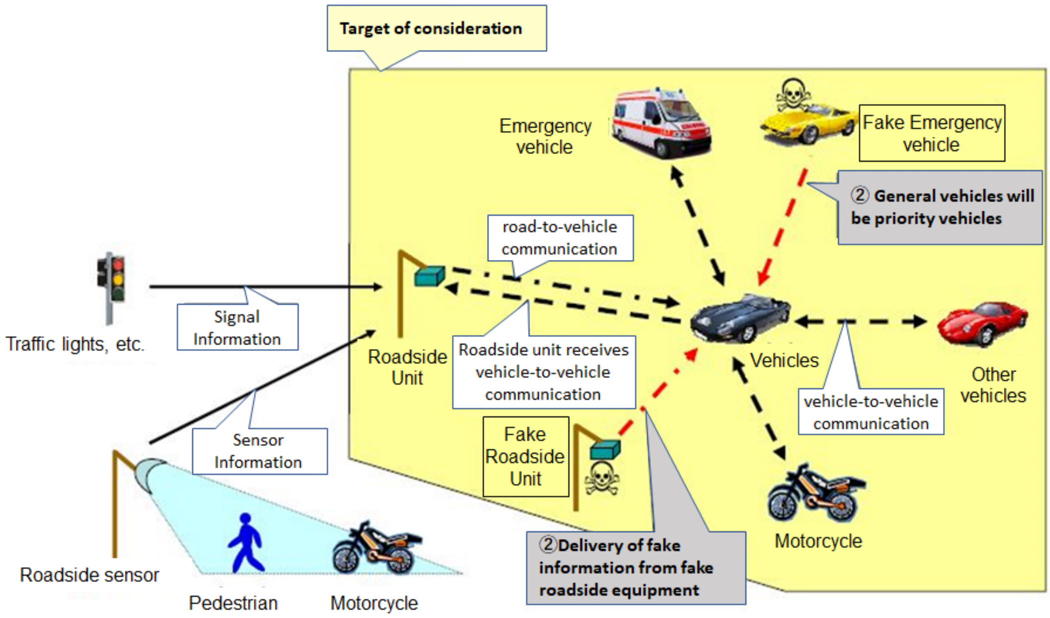


Figure 5.2.20 ITS Forum RC-009 Guidelines to be considered

Table 5.2.12 shows examples of risk analysis. As concrete security measures based on this risk analysis, The following cryptographic mechanisms are stipulated; message integrity using message authentication code for communication information between vehicles and road vehicles, and sender's message origin authentication using digital signatures.

Table 5.2.12 Examples of risk analysis

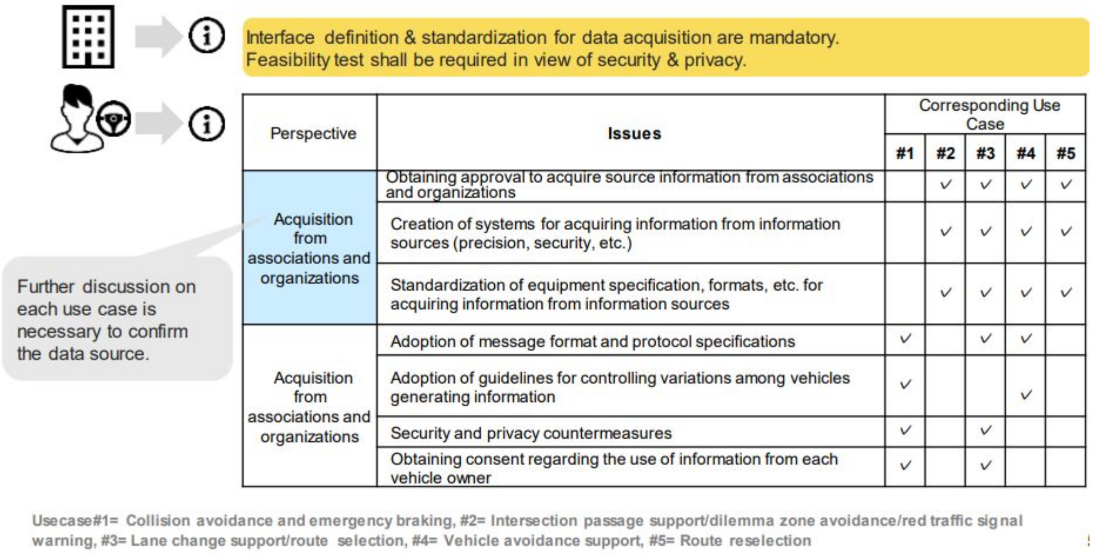
ID	Threats	Items	Level	Reason
N	Spoofing of Vehicle, Transmission of fake driving information	Motivation	Moderate	Purpose of confusion
		Difficulty	Solvable	Theoretically possible to attack
		Impact	Medium	Limited impact at the location where it was sent
O	Spoofing of Vehicle, Transmission of fake general purpose information	Motivation	Moderate	Purpose of confusion
		Difficulty	Solvable	Theoretically possible to attack
		Impact	Medium	Limited impact at the location where it was sent
P	Spoofing of Vehicle, Replay Attacks	Motivation	Moderate	Purpose of confusion
		Difficulty	None	There are attack examples
		Impact	Medium	Limited impact at the location of the attack
Q	Location Tracking	Motivation	High	There is a clear purpose such as profiling of a specific individual and There is great profit
		Difficulty	Solvable	Theoretically possible to attack
		Impact	Low	It is the same as stalking because it affects a specific individual and needs to be tracked within the communication distance.

5.2.2.6.2. Problem investigation report for the advancement of ITS / autonomous driving using cellular communication technology

The purpose of this report is to clarify the domestic issues for the advancement of ITS / autonomous driving using cellular V2X, and to accelerate the verification of the effectiveness of cellular V2X and the implementation and consideration of countermeasures.

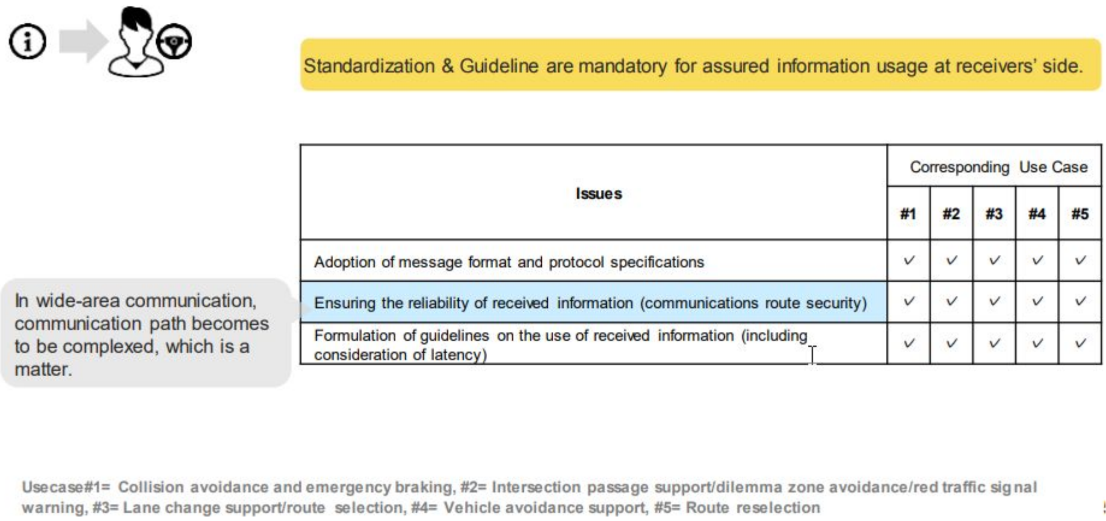
This report summarizes the security and privacy issues related to information distribution in cellular V2X.

Regarding five use cases of V2X (1: collision avoidance / emergency braking, 2: intersection passage support / dilemma zone avoidance / red light alert, 3: lane change support / route selection, 4: vehicle evacuation support, 5: Route re-search), the issues on sending and receiving information are organized in 2019 version (see Fig. 5.2.21 and Fig. 5.2.22).



Perspective	Issues	Corresponding Use Case				
		#1	#2	#3	#4	#5
Acquisition from associations and organizations	Obtaining approval to acquire source information from associations and organizations		✓	✓	✓	✓
	Creation of systems for acquiring information from information sources (precision, security, etc.)		✓	✓	✓	✓
	Standardization of equipment specification, formats, etc. for acquiring information from information sources		✓	✓	✓	✓
Acquisition from associations and organizations	Adoption of message format and protocol specifications	✓		✓	✓	
	Adoption of guidelines for controlling variations among vehicles generating information	✓			✓	
	Security and privacy countermeasures	✓		✓		
	Obtaining consent regarding the use of information from each vehicle owner	✓		✓		

Figure. 5.2.21 Issues on Communication Sharing (Information Acquisition)



Issues	Corresponding Use Case				
	#1	#2	#3	#4	#5
Adoption of message format and protocol specifications	✓	✓	✓	✓	✓
Ensuring the reliability of received information (communications route security)	✓	✓	✓	✓	✓
Formulation of guidelines on the use of received information (including consideration of latency)	✓	✓	✓	✓	✓

Figure. 5.2.22 Issues on Communication Sharing (Information Usage at Vehicles)

With regard to narrowband (V 2V/V2I/V2P) and wideband (V2N) communications, the former refers to the possibilities and challenges of ensuring security and privacy using PKI, while the latter refers to security and privacy issues based on the availability of encryption and TLS in the wireless segment.

5.2.2.5. ITU-T

In ITU-T, Question 27 (Vehicle gateway platform for telecommunication / ITS services and applications) in Study Group 16 (SG16: Multimedia) is standardizing the communication of Connected Vehicles. In Question 13 (Security aspects for Intelligent Transport System) of Study Group 17 (SG17: Security), the security related to Connected Vehicles and their communication systems are standardized. This section describes the activity status of SG17 Question 13 and the contents of the standard to be published as Recommendations. In particular, since the publication of the 5GMF White Paper "Cybersecurity in 5G Use Cases Version 1.0", a very wide variety of recommendations and draft recommendations have been developed for connected vehicles, as shown in this section. This section provides an overview, focusing on X.1371 and X.1373, which are closely related to UNR155 and UNR156, as well as X.1372, which is positioned as a comprehensive security guideline for V2X communication systems.

5.2.2.5.1. Recommendation issued in SG17 Question 13 and work items under discussion

Table 5.2.13 The list of recommendations shows the documents issued as recommendations in SG13 Question 13.

Table 5.2.13 List of recommendations

Number	Title	Overview
X.1373	Secure software update capability for intelligent transportation system communication devices	Recommendation ITU-T X.1373 provides secure software update procedures between a software update server and vehicles with appropriate security controls. This Recommendation can be practically utilized by car manufacturers and ITS-related industries as a set of standard capabilities for best practices. Approved in 2020-05-29
X.1372	Security guidelines for Vehicle-to-Everything (V2X) communication systems	This Recommendation identifies threats in V2X communication environments and specifies security requirements for V2X communication to mitigate these threats. This Recommendation also provides description of

		possible implementation of V2X communication with security. Approved in 2020-03-26
X.1374	Security requirements for external device with vehicle access capability	Recommendation ITU-T X.1374 analyses security threats to connected vehicles in two parts: threats against interfaces which are used to communicate between a vehicle and its external devices, and threats against external devices which communicate with the vehicle. Approved on 2020-10-29
X.1375	Methodologies for intrusion detection system on in-vehicle system	Recommendation ITU-T X.1375 establishes guidelines for an intrusion detection system (IDS) for in-vehicle networks (IVNs). Recommendation ITU-T X.1375 mainly focuses on how to detect intrusion and malicious activities on IVNs such as those using a controller area network (CAN) that cannot be supported by general IDSs currently deployed on the Internet. Approved on 2020-10-29
X.1371	Security threats to connected vehicles	Recommendation ITU-T X.1371 describes security threats to connected vehicles and the vehicle eco-system. Approved on 2020-05-29
X.1376	Security-related misbehavior detection mechanism based on big data analysis for connected vehicles	Recommendation X.1376 describes a security-related misbehavior detection mechanism for connected vehicles to help stakeholders to utilize automotive data to improve vehicle security. Approved on 2021-01-07
X.1383	Security requirements for categorized data in V2X communication	This Recommendation categorizes the data used in V2X communication into several types such as object attribute data, vehicle status data, environmental perception data, vehicle control data, application service data and user personal data, and assigns three security levels for the categorized data types. Based on these categorized data types and assigned data

		security levels, this Recommendation provides security requirements for categorized data in V2X communication. Approved on 2023-03-03
X.1380	Security guidelines for cloud-based data recorders in automotive environment	Recommendation ITU-T X.1380 provides security guidelines for cloud-based data recorders in automotive environments. It describes threats, vulnerabilities, security requirements, and use cases for cloud-based data recorders in automotive environments. Approved on 2023-03-03
X.1381	Security guideline for Ethernet-based in-vehicle networks	this Recommendation provides security guidelines for automotive Ethernet technology. This Recommendation includes a reference model of automotive Ethernet and analysis of threat and vulnerability for Ethernet-based IVNs. In addition, this Recommendation provides security requirements and use cases of Ethernet-based IVNs. Approved on 2023-03-03
X.1373rev	Secure software update capability for intelligent transportation system communication devices	Revision of X.1373 to reflect the results of discussions at UNECE WP29 and input from OEM vendors on implementation. Target Date 2024.4
X.1377	Guidelines for an intrusion prevention system for connected vehicles	This Recommendation provides methodologies for both intrusion detection and intrusion prevention. The proposed IPS consists of the intrusion detection plane – an external component with intrusion detection algorithms – and the data plane – in-vehicle networks (IVNs) where traffic monitoring and active response happen. This Recommendation aims to protect (automotive) Ethernet-based IVNs. Approved on 2022-10-14
X.1382	Guidelines for sharing security threat information on connected vehicles	This Recommendation is intended to help organizations stay in touch with the connected vehicles sharing community and to contribute threat information which would support the

		practices of connected vehicles safety protection. Overall, this Recommendation aims to enhance security threat information sharing and mitigate the potential impact of cybersecurity attacks on connected vehicles Approved on 2023-03-03
X.1379	Security requirements for roadside units in intelligent transportation systems	This Recommendation will help to guide vendors and operators of RSUs to adopt the appropriate security schemes to fulfil security requirements specified to protect RSUs from security risks and attacks from cyberspace thus to ensure the security of ITS. Approved in 2022-07-14

Table 5.2.14 shows the work items under discussion in SG13 Question 13 (as of December 2023).

Table 5.2.14 the work items under discussion in SG13 Question 13 (as of December 2023)

Number	Title	Overview
X.itssec-5	Security guidelines for vehicular edge computing	Security guidelines for vehicles to use edge computing capabilities. In addition to analyzing threats, it also shows security requirements for responding to threats and security precautions in three use cases. Target Date 2023.9
X.af-sec	Evaluation methodologies for anonymization techniques using face images in autonomous vehicles	This draft Recommendation provides an overview of anonymization techniques using face images in autonomous vehicles and an evaluation method to improve the maturity of anonymization Target Date. 2026-09
X.evpnc-sec	Security guidelines for electric vehicle plug and charge (PnC) services using vehicle identity (VID)	This draft Recommendation briefly describes the security guidelines for the electric vehicle plug and charge service using vehicle identity. It identifies threats to the model and provides security requirements. Target Date. 2024-09
X.evtol-sec	Security guidelines for electric vertical take-off	This draft Recommendation provides an overview of eVTOL system, security threat and security

	and landing (eVTOL) vehicle in an urban air mobility environment	requirements for eVTOL system equipped with various connectivity. Target Date. 2024-03
X.fod-sec	Security guidelines for a feature on demand (FoD) service in a connected vehicle environment	A FoD service means subscription-based services that users can selectively download and install the features they need into their connected vehicles online. This draft Recommendation provides a security threat analysis and specifies security requirements including mitigation methods such as authentication of a subscriber. Furthermore, this Recommendation provides how to implement the mitigation methods to fulfill the security requirements. Target Date. 2026-09
X.idse	Evaluation methodology for in-vehicle intrusion detection systems	This draft Recommendation provides a methodology for evaluating IVIDSs (in-vehicle intrusion detection systems) in views of its performance, effectiveness, etc. Target IVIDSs in this Recommendation are mainly identified in Recommendation X.1375. Target Date. 2024-09
X.ota-sec	Implementation and evaluation of security functions to support over-the-air (OTA) update capability in connected vehicles	This draft Recommendation provides how to implement the security functions and how to evaluate these functions. Moreover, this draft Recommendation additionally provides security threat analysis and security requirements for OTA update capability based on X.1373, X.1373rev and X.1371. Target Date. 2025-09
X.sup-cv2x-sec	Supplement to X.1813 - Security deployment scenarios for cellular vehicle -to-everything (C-V2X) services supporting ultra-reliable and low latency communication (URLLC)	This Supplement is to highlight and share the security deployment scenarios for C-V2X services supporting URLLC based on the context of X.1813. Target Date. 2024-09

5.2.2.5.2. X.1371: Security threats to connected vehicles [17]

The structure and overview of this Recommendation is shown in Figure 5.2.23. Section 6 defines the model of the connected car (see Figure 5.2.24), and Section 7 lists the security threats in that model. The threats are listed in terms of threats to the connected vehicle and the entire ecosystem including the connected vehicle, the targets and motivations of the attacks, and the potential vulnerabilities associated with those threats. Specific threats are categorized into back-end servers, communication channels, software updates, unintended acts by humans, and external connections, consistent with UNR 155. The Appendix also lists examples of attack methods against vulnerabilities and threats, which are also reconstructed with reference to UNR 155 to ensure consistency with UNR 155.

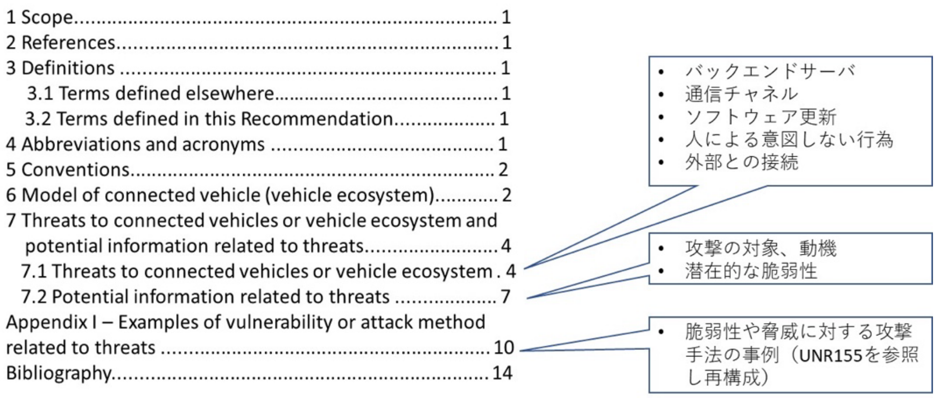


Figure 5.2.23 Structure and Overview of X.1371

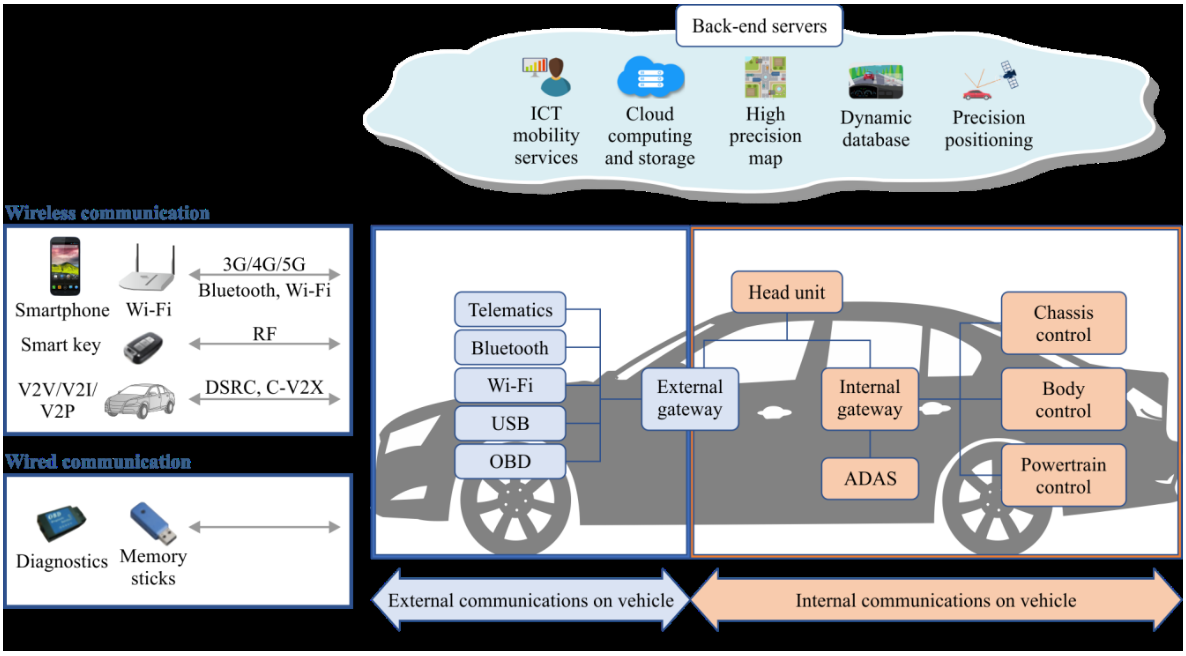


Figure 5.2.24 Concept of Connected Vehicle (Vehicle ecosystem)

5.2.2.5.3. X.1373: Secure software update capability for intelligent transportation system communication devices [18]

This recommendation aims to provide a secure software update procedure for ITS (intelligent transportation system) communication equipment. It also includes the basic model of software updates, security controls for software updates, and abstract data format specifications for update software modules.

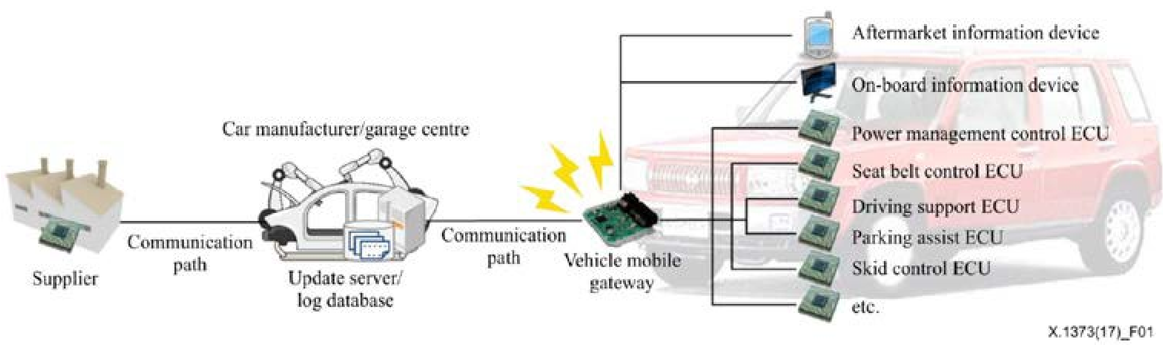


Figure 5.2.25 Basic modules built into the vehicle (from X.1373 recommendation)

Figure 5.2.25 shows the connection between a module such as an ECU built into the vehicle and a supplier who provides update software. The update software will be passed to the vehicle manufacturer, from which it will be sent to equipment such as the ECU that needs to be updated via the gateway built into each vehicle.

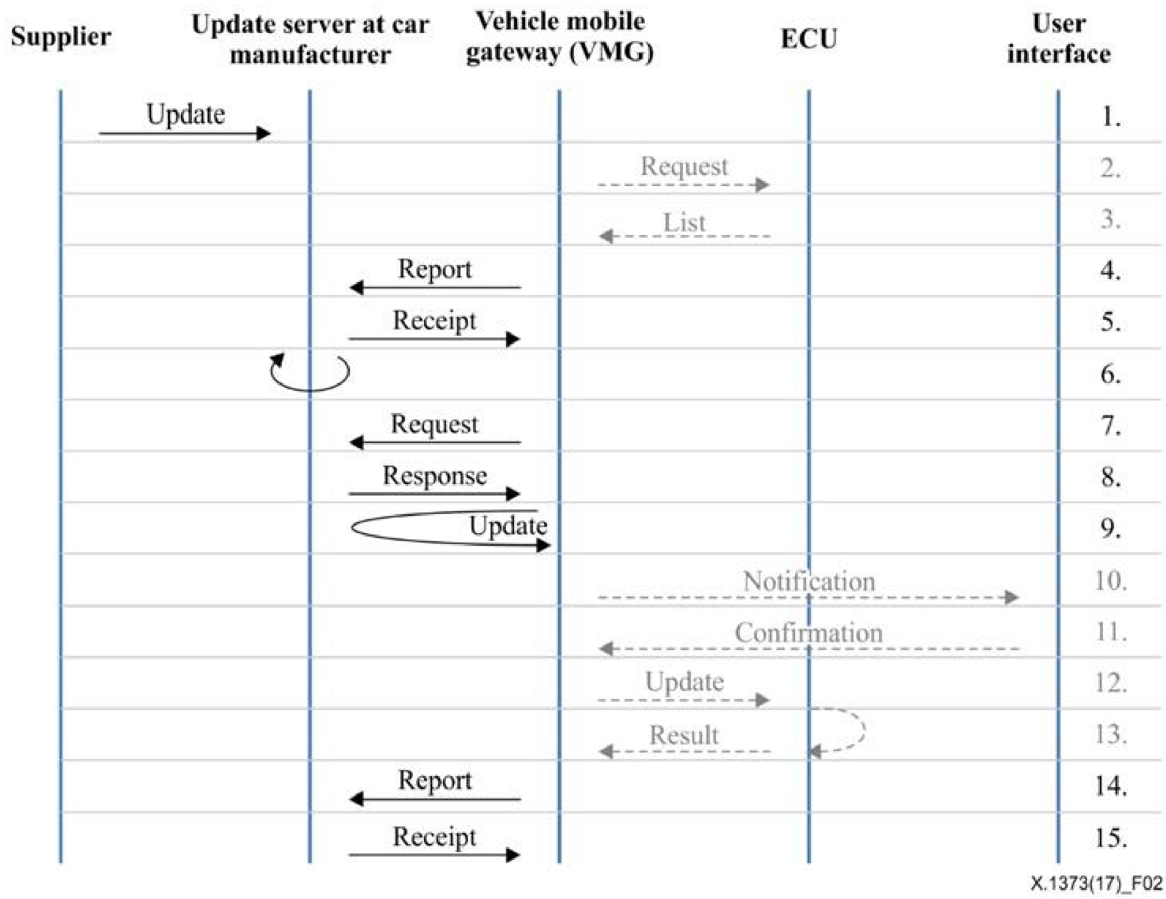


Figure 5.2.26 Model of software update process

Figure 5.2.26 is a model of the basic software update procedure. Software update procedure specifications and message formats are specified according to this model.

5.2.2.5.4 X.1372: Security guidelines for Vehicle-to-Everything (V2X) communication systems

This is a security guideline for V2X (Vehicle-to-Everything ") communication, where V2V (Vehicle-to-Vehicle), V2I (Vehicle-to-infrastructure), V2D (Vehicle-to) -nomadic Devices), and V2P (Vehicle-to-Pedestrian) are included. This recommendation also specifies V2X security threats, security requirements, and the implementation of V2X communication with security features.

Threats are categorized in terms of confidentiality, integrity, availability, denial, authenticity, accountability, and authentication, and threats are listed for each item.

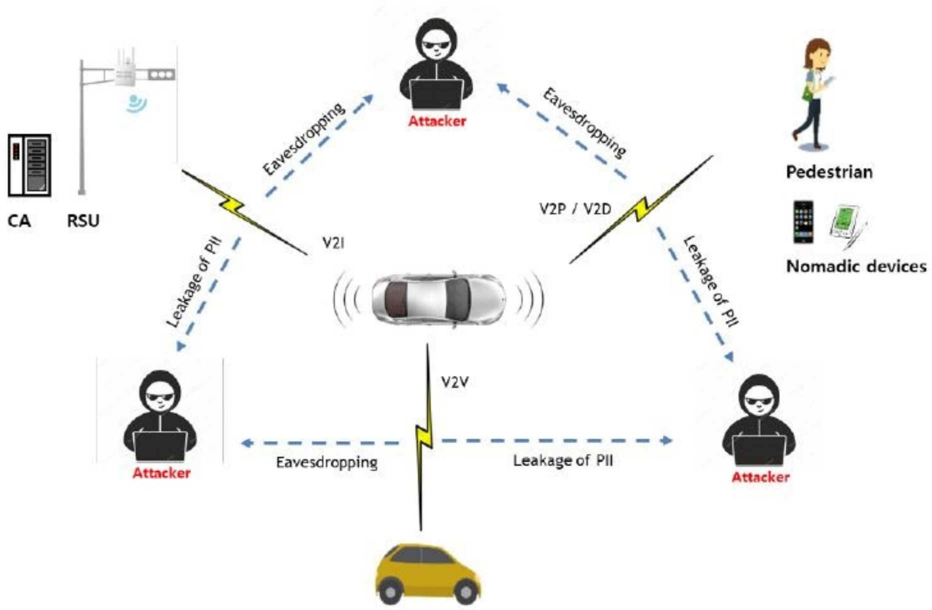


Figure 5.2.27 Threats of Confidentiality

Figure 5.2.27 shows threats to confidentiality, which are eavesdropping and personal information breaches.

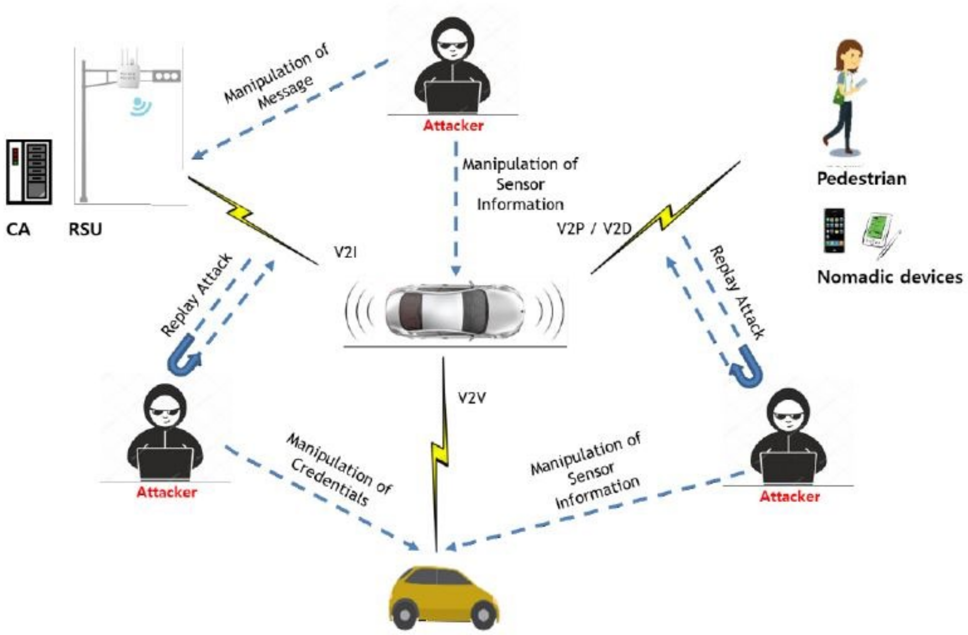


Figure 5.2.28 Threats to Integrity

Figure 5.2.28 shows the threats to integrity, which are tampering with routing messages, tampering with credentials, tampering with sensor information, and tampering with applications on devices.

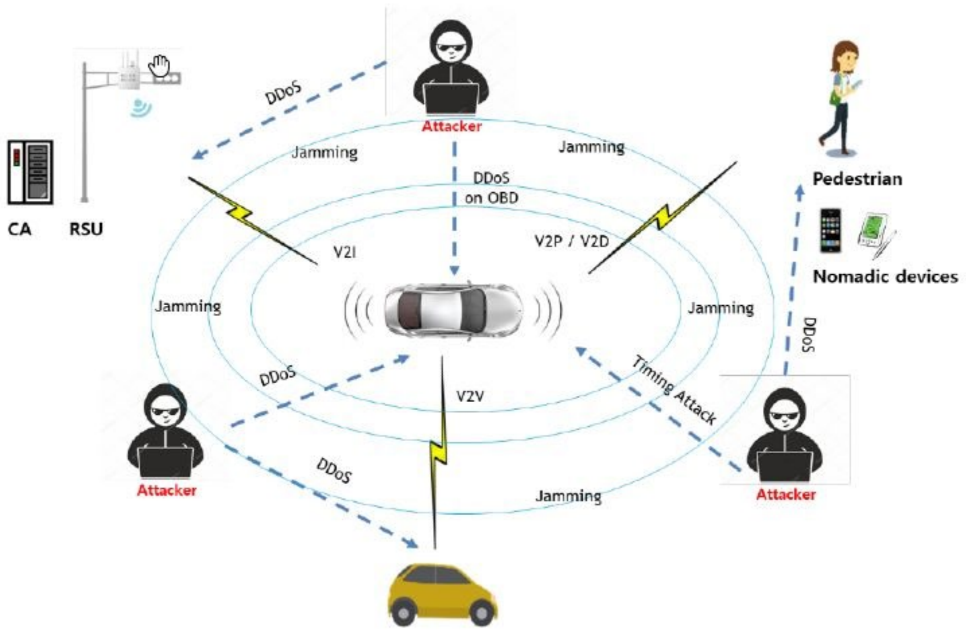


Figure 5.2.29 Threats to availability

Figure 5.2.29 shows threats to availability, which are interference/ DDoS attacks on V2X communication channels, DDoS attacks on OBU, timing attacks, and sensor hacking.

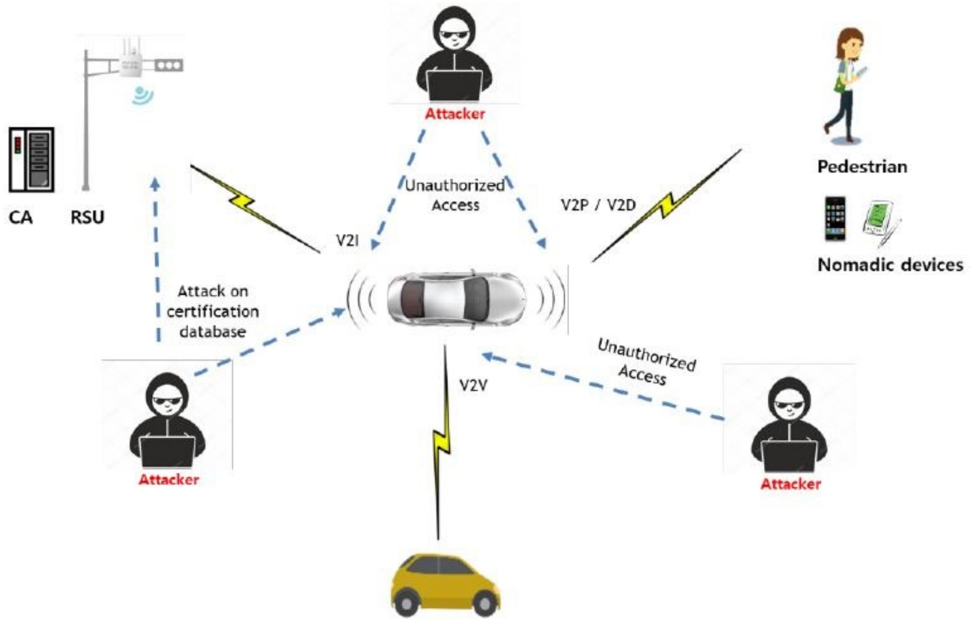


Figure 5.2.30 Threats to non-repudiation

Figure 5.2.30 shows the threat to non-repudiation, which are tampering with the certificate database and unauthorized access to credentials.

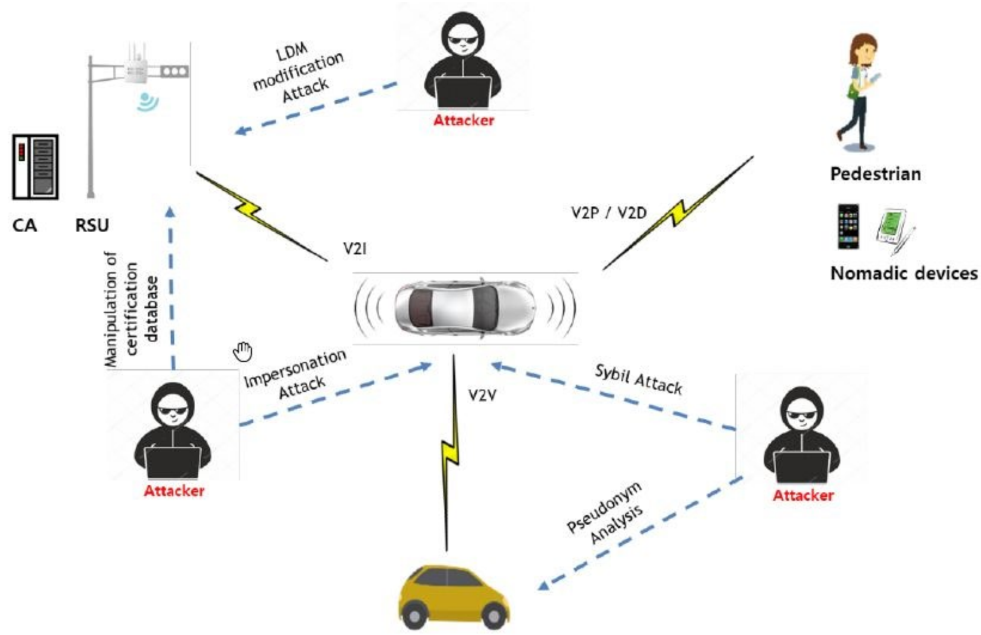


Figure 5.2.31 Threats to Authenticity

Figure 5.2.31 shows the threat to authenticity, which are tampering attacks on the routing table / LDP (Local Dynamic Map), spoofing attacks, Sybil attacks (multiple ID attacks), pseudonym analysis attacks, and tampering with the certificate database.

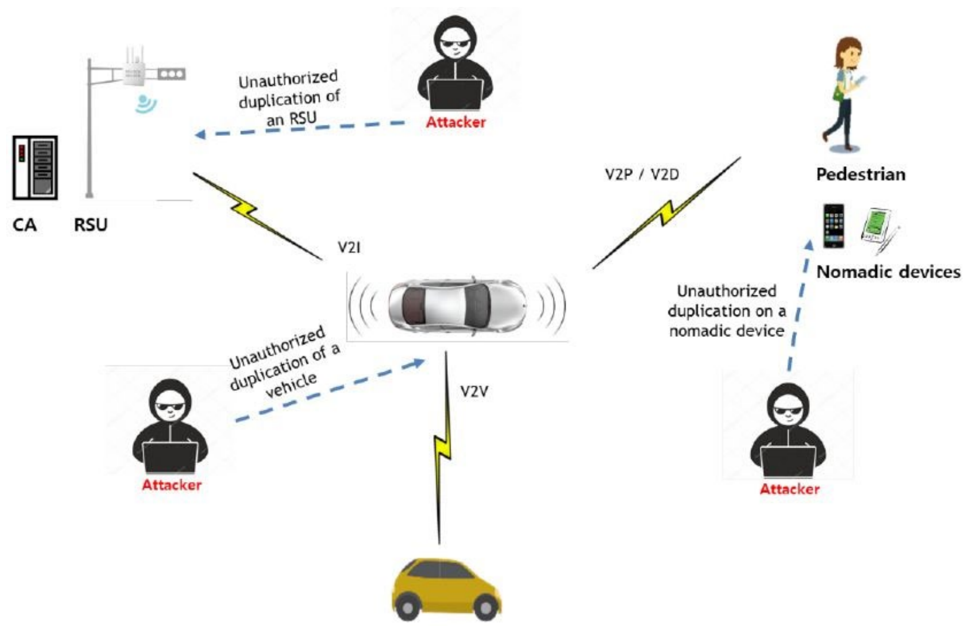


Figure 5.2.32 Threats to Accountability

Figure 5.2.32 shows the threat to Accountability, which are unauthorized duplication of devices and vehicles / RSUs.

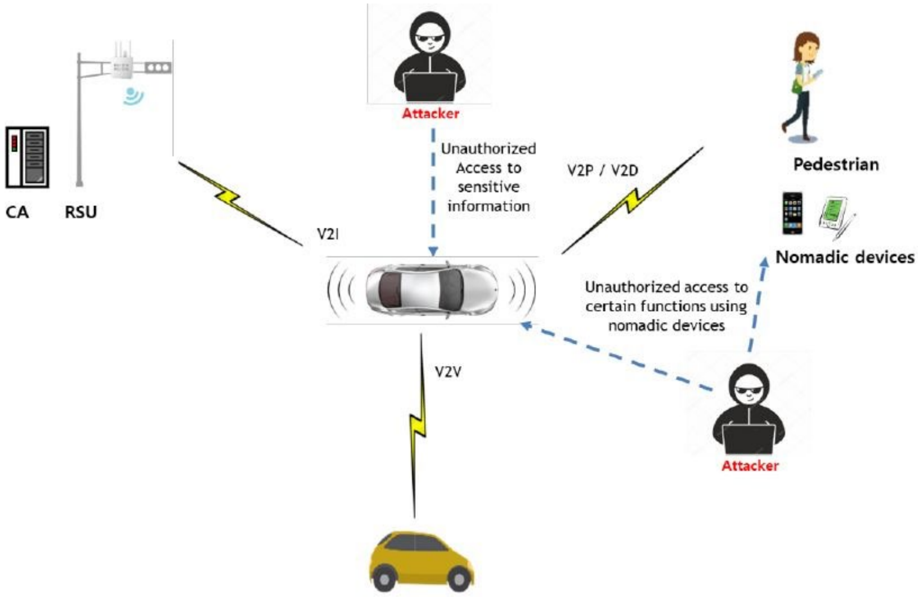


Figure 5.2.33 Threats to Authentication

Figure 5.2.33 shows the threats to authentication, which are unauthorized access to information on safety in the vehicle and unauthorized access to functions built into the vehicle.

The recommendation stipulates the security requirements corresponding to each of the above items and indicates which security requirements should be addressed for the use cases related to V2X communication. In addition, as examples for implementation in line with security requirements, use of encryption for entity authentication and confidentiality, verification of the integrity of emergency information, entity authentication in platooning, use of PKI, etc. are contained.

5.2.2.6. TTC (Telecommunication Technology Committee)

As for TTC, the Security Expert Committee and the Connected Car Expert Committee handle vehicle-related security, and related members of the Security Expert Committee participate in the Connected Car Expert Committee and carry out collaborative activities. This section describes the documents being prepared by the Connected Car Expert Committee.

5.2.2.6.1. Standardization and practical application issues of remote update technology for automobiles

A document issued in December 2017 as a technical report explains the status of studies on remote software update technology by various organizations and the status of creating standardized documents at this time. In October 2019, information on UNECE WP.29 was added and updated, and it was published as the second edition. This document is open to the public and can be downloaded from web page of TTC.

Conventionally, the software installed in the device such as the ECU was updated by the work vehicle using the diagnostic tool by wired connection. In recent years, remote software update (OTA reprogramming), which updates software remotely (without the intervention of a specialized worker) via a network, has been paid attention. This document focuses on the use cases of this software update, and investigates both domestically and internationally the status of activities at government agencies, academic societies, industry groups, NPOs, etc.

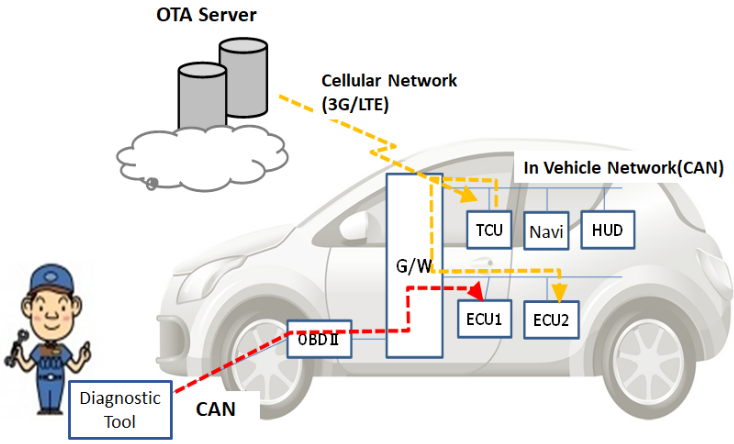


Figure 5.2.34 Examples of Reprogramming
(Red: conventional wired reprogramming, yellow: OTA reprogramming)

The related organizations surveyed are as follows.

- 5GAA (5G Automotive Association)
- ACEA (European Automobile Manufacturers Association)
- SAE International (Society of Automotive Engineers)
- UNECE WP.29 GRVA TFCS
- Bluetooth SIG
- IEEE 802
- ISO TC22 (Road vehicles)
- ISO TC204 (Intelligent transport systems)
- ITS Info-communication Forum
- ITU-T FG-VM (ITU-T Focus Group on Vehicular Multimedia)
- ITU-T SG16 (Multimedia)
- ITU-T SG17 (Security)
- OneM2M
- W3C
- Wi-Fi Alliance
- The Fifth Generation Mobile Communications Promotion Forum (5GMF)
- EVITA (E-safety vehicle intrusion protected applications)
- HIS (The Herstellerinitiative Software)
- TCG (Trusted Computing Group)

5.2.2.6.2. Others

The Connected Car Expert Committee has decided to start writing a new report on the security of autonomous driving. In connection with this, on January 31, 2020, a workshop entitled “Security Issues Related to Autonomous Driving” was held by inviting speakers from outside.

5.2.2.7. GSMA

The GSMA, an industry group related to mobile communications, has created the following IoT security guidelines and made them available to the public through its website. It has been translated into languages other than English, and there is also a Japanese version.

- IoT Security Guidelines: Overview Document
- IoT Security Guidelines for Service Ecosystems
- IoT Security Guidelines for Endpoint Ecosystems
- IoT Security Guidelines for Network Operators
- IoT Security Assessment

The GSMA began to study Automotive IoT Security as series of IoT security guidelines but ended without moving to full-scale activities due to difficulty in collaborating with the automotive industry and lack of supporters.
The GSMA's IoT security project has undertaken various efforts, including the creation of the above IoT security guidelines, but was suspended in March 2020. As a vehicle-related activity, the use of eSIM in automobiles is being considered in eSIM activities, and the necessity of establishing a new group is being considered (as of March 2020). In addition, the GSMA has built the NESAS (Network Equipment Security Scheme) [19] as a security certification framework for communication devices. NESAS consists of equipment tests based on the 3GPP TS33 series test specifications (SCAS: Security Assurance Specifications) and third-party audits.

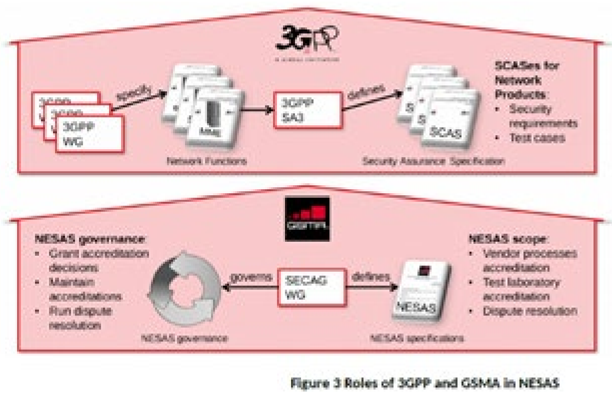
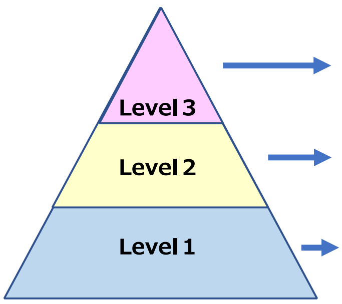


Figure 5.2.35 Relationship between the GSMA NESAS and 3GPP SCAS

To ensure the security of 5G networks, the GSMA is proposing NESAS to the European Union Agency for Cybersecurity (ENISA). [20] This complements the European Commission's 5G cybersecurity measures "EU Toolbox" [21], and European countries are currently implementing security measures for 5G networks.

5.2.2.8 Japan Automobile Manufacturers Association, Inc. (JAMA)/ Japan Auto Parts Industries Association (JAPIA)

The Japan Automobile Manufacturers Association, Inc. (JAMA) and the Japan Auto Parts Industries Association, Inc. (JAPIA) released Cybersecurity Guidelines V2.1 (2023.09.01) [22] with the aim of promoting the improvement of cyber security measures and efficient inspection of the level of measures in the entire automotive industry by specifying a framework for measures to be taken over the next three year and stating self-assessment criteria common to automobile industry.
Based on the items to be achieved by each company involved in the automotive industry, this guideline defines the levels into Level 3, which is a group of items to be aimed as a final destination, Level 2, which is a standard group of items, and Level 1, which is a minimum group of items to be implemented, and defines a total of 153 check items based on 24 classified labels (See Figure 5.2.36 and Table 5.2.15).



Level	Definition
Lv3	Items that the automotive industry should be aiming for at this point.* * April 2022
Lv2	Items that the automotive industry should be aiming for as standard
Lv1	The minimum what should be implemented in the automobile indusry

Based on security levels and definitions in the Automotive Industry Cyber Security Guidelines

Figure 5.2.36 Security Levels Defined in Cybersecurity Guidelines

Table 5.2.15 Examples of Requirements and Conditions of Achievement (selected items)

Label	Objective	Requirement	No.	Level	Condition(s) for Achievement	Achievemnt Criteria
17 Communication Control	Prevention information leakage, unauthorized modifications, and system stoppages due to unauthorized operation of critical equipment such as servers	Communication control to information systems, IT equipment/devices, and malicious websites to prevent cyberattacks and internal information leaks	103	Lv2	A firewall is installed at the boundary between the internet and internal company network to restrict communication	【Rules】 ・A system shall be to restrict internal and external network communication [Introduction Location] -Boundaries between internal and external networks [Items to be restricted] -The IP addresses of connection sources and connection destinations -Communication Ports
			104	Lv2	Firewall filtering settings (communication permissions/blocking settings) are recorded, with regular checks for unnecessary settings	【Rules】 ・Filtering setting for internal and external network communication shall be recorded ・Periodically check for unnecessary filtering settings ・Delete unnecessary filtering settings 【Item to be recorded】 ・Applicant name, IP addresses of connection source and destination communication direction, protocol, port number, registration date, expiration date

						【Confirmation frequency】 ・Once a year
			105	Lv2	Remote access IDs are managed with regular checks for unnecessary IDs	【Rule(s)】 ・The issuing, changing and deleting of remote access IDs are carried out through an application/approval system ・There shall be regular checks for unnecessary IDs ・Unnecessary IDs are deleted 【Confirmation frequency】 ・Once a year

As shown in Table 5.2.15, 24 labels such as "communication control" are defined as major items of classification, 153 functions such as "installation of firewalls" are defined as conditions for achievement as middle items, and achievement criteria such as rules, targets, and frequency of confirmation are defined as minor items. From a broad perspective, labels (major items) related to communication include "monitoring of external connections (14)," "internal connection rules (15)," "communication control (17)," "authentication and authorization (18)," and "detection of unauthorized access (23). Here, the numbers in parentheses represent label numbers.
Currently, each member company is required to conduct a self-check on the JAMA website.

5.2.2.8. Summary

In this section, we summarize each group introduced in Sections 5.2.2.1 to 5.2.2.8 and their activities and clarify their relationships (Table 5.2.16).
The UNECE / WP.29 Cyber Security Task Force provides basic cyber security policies throughout the life cycle of systems, which are development, commercialization, and product termination. The systems consist of vehicle, network and clouds. As an example of use case, it provides procedures for remote software updates (remote reprogramming, OTA), its safety and security requirements, guidance on identifying software to be updated, and its underlying Regulations. The basic policy of cyber security stipulated in UNECE / WP.29 is in the form of referring to ISO / SAE 21434, which is jointly developed by ISO and SAE. In

accordance with the basic policy specified in UNECE / WP.29, it defines cybersecurity risk management requirements, processes for communicating and managing cybersecurity risks, and a common language framework throughout the life cycle of a car. By complying with ISO / SAE 21434, car manufacturers and suppliers prove that they comply with the UNECE / WP.29 cybersecurity regulations. Regarding software updates, ISO / SAE 24089 will be positioned as a standard according to Regulation, but consideration has just begun.
TC204 is a standardization body related to ITS, and in particular, WG16 (Communication Subcommittee) and / WG18 (Cooperative Systems Subcommittee) standardize communications between base stations and vehicles in ITS. TC204 also stipulates security measures such as authentication and confidentiality that should be realized between communication devices and measures related to privacy protection of probe information.
In order to promote the spread of ITS information communication systems, the ITS Forum aims to following activities, namely research and development of ITS information communication systems, research on standardization, liaison and coordination with related organizations, collecting relating information, enlightenment activities, etc. As for security, it has published guidelines for vehicle driving support communication systems.
In ITU-T, SG16 Question 27 standardizes the communication of connected vehicles. SG17 Question 13 standardizes the security of connected vehicles and their communication systems. So far, the procedure for secure remote software updates and security guidelines for V2X have been standardized.
As for TTC, the Security Expert Committee and the Connected Car Expert Committee handle vehicle-related security, and related members of the Security Expert Committee participate in the Connected Car Expert Committee and carry out collaborative activities.
The GSMA began to study Automotive IoT Security as series of IoT security guidelines but ended without moving to full-scale activities due to difficulty in collaborating with the automotive industry and lack of supporters. As a vehicle-related activity, the use of eSIM in automobiles is being considered in eSIM activities, and the necessity of establishing a new group is being considered (as of March 2020).
JAMA and JAPIA are studying a framework for cybersecurity measures in the automotive industry and self-assessment criteria.

Table 5.2.16 Relationship between each standard

Abbreviation	Organizations	Overview
UNECE/WP.29	World Forum for Harmonization of Vehicle Regulations (WP.29) under the United Nations (UN) /	International standards such as international harmonization of automobile safety and environmental standards and international mutual

	Economic Commission for Europe (ECE)	recognition of automobile certification by the government [5]
ISO TC22	Joint organization by the International Standard Organization (ISO) and the Society of Automotive Engineers (SAE) in the United States	ISO / SAE jointly developed ISO / SAE 21434 from September 2016 [5] Expected to be referred to by WP.29 International Regulation for Vehicle Cyber Security
ISO TC204	Technical Committee under the International Standard Organization (ISO) (TC204)	Responsible for international standards related to ITS ISO / SAE 21434 takes initiative in the content related to autonomous driving [23]
ITS Forum	ITS Info-communications Forum	A domestic organization whose purpose is to promote the spread of ITS information and communication systems. Formulated and published various guidelines to popularize and promote ITS.
ITU-T SG17	Study Group (SG17) under the International Telecommunication Union (ITU) Telecommunications Standardization Division (T)	International standardization of telecommunications. ITS security is standardized in Question 13, SG17
TTC	Telecommunication Technology Committee	Standardization of Information and communication network in Japan Conducted trend surveys and reports on automobile-related security
GSMA	GSM Association ; An international Organization consisting of mobile carriers and related companies	Established NESAS, authentication framework of a device security [24] Currently no activity on automotive IoT security
JAMA	Japan Automobile Manufacturers Association, Inc. (JAMA) A domestic industry organization consisting of	Together with JAPIA, study a framework for cyber security measures and self-assessment criteria in the automotive industry

	manufacturers that produce automobiles	
JAPIA	Japan Auto Parts Industries Association (JAPIA) Japan's leading trade association for automotive parts	Together with JAMA, study a framework for cyber security measures and self-assessment criteria for the automotive industry

5.2.3. Security on connected vehicle

5.2.3.1. Security requirements for connected vehicles

In Chapter 5.2.2, the standardization activities related to connected vehicle were surveyed, and the relationship between each standard were clarified. Then, the common security requirements for connected vehicle were clarified. These standards specify not only security requirements inside the vehicle but also security requirements in the ecosystem, including roadside devices and the cloud. In other words, these standards specify wider security requirements which cover from policy for security measures, methodologies for security management, to secure communication services and protocols between ITS base stations, which are components of the connected vehicle systems.
Services related to connected vehicle are expected to have various use cases such as autonomous driving support, infotainment, car life support, agents, etc. In order to ensure the security of these services, it is also necessary to consider the security requirements for stakeholders such as service providers, cloud providers, telecommunications providers, and so on. For example, by conforming to ISO27011 (ITU-T X.1051) [25] for telecommunications carriers and ISO27017 (ITU-T X.1601) [26] for cloud carriers, the security of communication or cloud services is guaranteed.
In this chapter, we will clarify the target services (use cases) of connected vehicle and the system requirements to realize safe and secure services. Next, assuming that 5G is used as a public network of connected vehicle, we will focus on the functions of the 5G network to satisfy the above system requirements. Furthermore, in the next chapter, we will discuss the security issues related to the above focused 5G network functions.

5.2.3.1.1. Connected Vehicle Use Case Overview

As widely penetration of connected vehicles, not only achieve efficiency and sophistication of transportation, but also create new industries and services in various fields that were not directly related to automobiles are also expected. Therefore, it is important to first clarify security issues in the connected vehicle that are expected in the 5G era.

In this report, we will focus on the four services defined by the "Study Group for the Realization of a Connected Car Society" [27] sponsored by the Ministry of Internal Affairs and Communications The four services are summarized below.

-Safety service

A service that supports safe driving by informing road conditions and traffic conditions to vehicles and drivers and issuing warnings as necessary.

-Car life support service

A service tailored to the situation of the vehicle and driver by transmitting and analyzing information such as the condition and position of the vehicle and the driving characteristics of the driver to the outside.

Infotainment service

A service that provides various entertainment in the vehicle such as watching videos and VR (virtual reality) by connecting to the Internet.

Agent service

Useful services in emergencies such as traffic accidents and disasters.

In addition, in order to clarify the security requirements without loss of generality, the following use cases in the above report will be used.

UC-1: Driving support (safe driving support, autonomous driving support, driver monitor, elderly driver support) for the safety service,

UC-2: Vehicle management, operation management, Infrastructure management / automobile insurance service for the car life support service,

UC-3: Online entertainment service for the infotainment service,

UC-4: Emergency call / road assistant service for the agent service.

The communication requirements and communication modes for each use case are as follows.

Service overview (main features)	
Use case	Safe driving support, autonomous driving support, driver monitor, elderly driver support
Content of Information	Surrounding vehicle driving status, vehicle control information, dynamic map, driver status
Requirements of communication	High reliability, low latency
Communication Type	Short range communication, Wide range communication
Issues	Study of highly reliable and low-latency communication methods regardless of manufacturer (including cooperation with overseas manufacturer) Securing a dedicated band

Schedule	Image of service advancement	Required Technology
Current	Providing drivers with driving support information that will help prevent accidents at intersections, accident-prone points, etc.	・Communication means (V2I) that detects / distributes the status of vehicles and pedestrians on real time basis in a specific area such as an intersection ・Communication technology (V2V) that collects the running conditions of surrounding vehicles in real time
Short term	Advanced safe driving support by information providing -Expansion to pedestrians, automobiles, etc. -Response to driver in emergency -Support for elderly drivers Level 2-3 automatic driving support -Providing information for facilitating autonomous driving -Exchange of Vehicle control information during platooning	・Communication between pedestrian and vehicle, Improved accuracy of positioning ・Driver monitoring, ・Cooperative system communication for autonomous driving, ・Advancement of infrastructure sensor (system support for vehicles without communication equipment), ・Utilization of communication for automatic driving monitoring / control
Middle term	Autonomous driving support for level 4 or higher Traffic control of autonomous driving vehicles	・Communication for automatic driving monitoring / control ・Advanced traffic control for autonomous driving vehicles

Figure 5.2.37 UC-1: Overview of safe driving support, autonomous driving support, driver monitoring, and elderly driver support services [27]

Service overview (main features)	
Use case	-Vehicle management (fault analysis, software update), -Operation management (travel route search in logistics and passenger transportation, vehicle allocation planning, labor management, etc.), -Operation management of infrastructure (understanding road conditions, etc.) -Vehicle insurance
Content of Information	-Operation plan / status, -Traffic conditions / prediction, -Movement requests/ demands, -Vehicle condition, -Driver condition
Requirements of communication	Always connected
Communication Type	Wide range communication, (Partially) spot communication
Issues	・Reduction of communication cost, Ensuring privacy / security, ・Establishment of AI technology for real-time and dynamic driving route search and vehicle allocation planning

Schedule	Image of service advancement	Required Technology
Current		
Short term	・Operation management system in response to management of driver's physical condition ・Dynamically search for driving routes in real time according to operating conditions, traffic conditions, and movement requests / demands of people (passengers). ・In-vehicle software update (fixing bugs) ・Real-time monitoring and analyzing of road surface conditions	・Driver monitoring technology ・Failure prediction based on operation log (Analysis of sensor information in Cloud)
Middle term	・Reservation and dispatch of on-demand autonomous vehicles ・Real-time and dynamic route search in response to movement requests / demands of things (collection and delivery) as well as people (passengers) ・In-vehicle software update (Adding new function)	・Always-on wireless NW that sends and receives AI input / output (increased transmission frequency)

Figure 5.2.38 UC-2: Overview of vehicle management, operation management, infrastructure management, and automobile insurance services

Service overview (main features)	
Use case	-Video, music listening, online games, work
Content of Information	-Entertainment information (videos, music, images, online games, etc.)
Requirements of communication	Always connected, high throughput
Communication Type	Wide range communication, (Partially) spot communication
Issues	・Review of area design along roads due to increased of internet connection in vehicles ・Multi-system and multi-band on the in-vehicle device

Schedule	Image of service advancement	Required Technology
Current	Passengers watch videos and play games	
Short term	Rideshare will allow to work as well as videos and games while traveling	High-speed internet connection using the communication module of the vehicle
Middle term	Full automated driving becomes widespread, and drivers will be able to play videos, games, and work on the move.	ditto

Figure 5.2.39 UC-3: Overview of Internet Entertainment Services [29]

Service overview (main features)	
Use case	-Emergency call service in the case of a traffic accident, -Road assist
Content of Information	-Voice information, sensor information, driving monitor information
Requirements of communication	Always connected
Communication Type	Wide range communication
Issues	・Driving monitor technology ・Information analysis technology by AI

Schedule	Image of service advancement	Required Technology
Current	Emergency call when the airbag is operating	
Short term	-Transmission of detailed sensor information before and after the traffic accident -Response when the driver is in badly health condition	-Information analysis technology by AI -Driver monitoring technology

Figure 5.2.40 UC-4: Overview of emergency call / load assistant service [30]

(1) Network requirements

Here, the network requirements required for each of UC-1 to UC-4 are summarized (see Table 5.2.17).

Table 5.2.17 Various use cases and network requirements

	Use case	Network Requirement
UC-1	Dynamic map	High Throughput, Spot
	Vehicle control information	Low Latency, Always Connected
	Driver status	Always Connected
	Surrounding vehicle driving status	Low Latency, Short range communication (V2X)
UC-2	Operation plan / status, traffic status / prediction	Always Connected, Spot
	Movement requests/demands, Vehicle status, driver status	Always Connected
UC-3	Watching video	High Throughput, Always Connected
	Online games	Low Latency
UC-4	Audio Information, Sensor Information, Driver monitoring information	Always Connected

Table 5.2.18 shows the amount of data such as UC-1 map information for dynamic map, vehicle control information for autonomous driving support, or video information [28]. Since a large amount of data flows on the network for all video, still images, and ECU data, efficient transfer technology utilizing MEC etc. is required.

Table 5.2.18 Amount of data transferred by services in Connected Vehicle[29]

System Requirements *		V2Cloud cruise assist	High-resolution map generation & distribution	Intelligent driving
Major Data Source		Video Stream	Still Image (road surface image)	ECU data
Data Generation in vehicle		~ 1215EB/month[1]	~ 375EB/month[2]	~ 22.5EB/month[3]
Target Data Traffic Rate		~ 10EB/month in total (cost constraint might limit this number)		
Response Time	Uplink	< 10 seconds	< 1 week	< 1 week
	Downlink	< 10 seconds	< 1 week	< 10 minutes
Required Availability	Uplink	Continuous	Occasional	Occasional
	Downlink	Continuous	Occasional	Continuous

* - The numbers in Table 1 are total values for 100 million connected cars.

Table 5.2.19 shows the network requirements for various V2X services. The latency of the autonomous driving, which is automatically controlled based on the transmitting data, requires less than 1 ms. It is the strictest condition among V2X services. Further, for remote control, the latency is less than 20 ms, which is the condition that does not affect real-time human interface. In addition, Table 5.2.20 shows the network requirements for content viewing and online games in the infotainment services. In particular, in online games by multiplayer, response time should be less than7.5 ms.

Table 5.2.19 Network requirements for V2X services [30]

Service	Type	Latency	Throughput	Reliability
Safety and traffic control	V2V, V2P	100 ms	-	Not defined
Autonomous Driving	V2V, V2N, V2I	1 ms	10 Mbps (DL/DL)	Almost 100%
Remote driving (TeSo)	V2N	20 ms (end-to-end)	25 Mbps (UL: video・Sensor data) 1 Mbps (DL: Command control of application)	99.999%
Internet and Infotainment	V2N	100 ms (Web browsing)	0.5 Mbps (Web browsing) 15 Mbps (High definition video streaming)	-
Remote diagnosis and management	V2I, V2N	-	-	-

Table 5.2.20 Network Requirements for Infotainment service UC-3 [30]

Service	Average end-user throughput	Delay (end-end)	Delay (radio network)
High Definition Video 8K (Streaming)	< 100 Mbps (DL)	< 1 s	< 200 ms
High Definition Video (conversational)	< 10 Mbps (DL/UL)	< 150 ms	< 30 ms
Cloud Computer Game 4K 3D graphics	< 50 Mbps (DL/UL) (UL required for multiplayer games)	< 7.5 ms	< 1.5 ms

In addition, the latency of each message exchange for the automatic overtaking system should be less than 10 ms[31]. As the network delay of the wireless part in 5G URLLC is assumed to be 1ms, it is necessary to realize response time of about 1ms to 20ms for end-to-end communications. For this reason, effective authentication on URLLC and utilizing MEC should be considered.

2) Security requirements

In this section, we describe the security requirements for the Connected Vehicle. Here, security requirements common to use cases are studied while considering the requirements of individual use cases.

First, for the purpose of clarifying the security requirements on the service layer, the threats for vehicles, networks, clouds, and service applications will be clarified.

Threats on the service layer is as follows,

・Impersonation of service user

・Unauthorized access to data used by the services

・Data leak on the services

・Illegal alternation of data on the service

・DoS attack to the services

・Malware infection

Here, based on the security threats on the above service layer, the security requirements of vehicles, clouds, and networks, which is the component of the service will be clarified. Then the security functions and issues to be focused on when assuming 5G network will be organized.

- Impersonation of service user

The threat is for an unauthorized user to gets profits illegally by impersonating a legitimate user of the services. As an example, unauthorized use of content viewing in infotainment services, online games (UC-3), emergency call services such as traffic accident information (UC-4), and etc. is assumed. As a countermeasure, service-level user authentication is required.

- Illegal Alternation of data stored in the cloud and the car

The threat is for an attacker to get profits to him or damage to others by an unauthorized access to the data stored in the cloud or the car or transmitted on the network or tampering with the data. As an example, the driving log used for an automobile insurance service is altered to intentionally change the insurance rate (UC-2), the hazard information in the dynamic map is tampered with to induce an accident in another car (UC-1), and when software updating as vehicle management operations vulnerable software or malicious software is injected (UC-2).
As a countermeasure, there is a method to add a message authentication code to data stored in the cloud / the car or transmitted on the network.

- Unauthorized acquisition by unauthorized access to the data stored in the cloud and the vehicle or eavesdropping data on the network

The threat is for attacker to get profit or infringe on the privacy of others by unauthorized access to the data stored in the cloud and the vehicle or eavesdropping on the data transferred over the network. As an example, vehicle movement information in the driver monitor service (UC-1) and vehicle operation management service may be illegally obtained (UC-2).
As a countermeasure, there is a method of encrypting the data stored in the cloud or the vehicle and the data transmitting on the network.

- Overloading the cloud, vehicles, and networks, resulting in service outages (DoS attacks)

The service is stopped by occurring a large number of transactions (processes) in the system (cloud, vehicle, or network). DoS attacks are expected for all use cases (UC-1 to UC-4). Depending on the objective of an attacker, the target will change, such as the service itself or the specific vehicle.
As a countermeasure, there is a method of monitoring targeted traffic, detecting DoS attack and mitigating the corresponding traffic.

- Attacks on services due to malware infection and unauthorized access

By infecting a cloud, a vehicle, or network system with a malicious program and operating it, there is a possibility that the attacker may execute any intended operations to cause the

above attacks. In addition, unauthorized access to the cloud and the vehicle can change the system configuration and settings, enabling various attacks.
As a countermeasure, there is a method of introducing a function to detect malware or performing access control against unauthorized access.

- Attacks against vulnerabilities due to inadequate specifications and implementation of services

Abusing vulnerabilities of hardware or software in each service (UC-1 to UC-4), which are caused by inadequate specifications or implementation, the service may be exploited, misconfigured or misused. For example, in the case that the access control mechanism to personal data is insufficient, a malicious user may obtain privacy information of other user or change the history of service usage.
As a countermeasure, a development process to eliminate malicious programs and defective specifications in the software design / development process are required.
Table 5.2.21 shows the relationship between cybersecurity threats to vehicles described in WP29 and the above security threats. In the table, the above threats correspond to specific sections of the WP29. Specific countermeasures against these threats are listed in Annex A in WP29.

Table 5.2.21 Relationship between threats specified in this section and threats specified in WP29

Security Requirements of Connected Vehicle Service	Related Threat (see WP29)
Unauthorized use of services by spoofing	4.3.1(a)(b)(c), 4.3.2(a)(c)(d)(f), 4.3.6(b)(c)(d)
Illegal alternation of data stored in the cloud and vehicles	4.3.1(a), 4,3,2(b), 4.3.5(a), 4.3.6(a)(b)(c)(d)
Unauthorized acquisition by eavesdropping on data stored in the cloud, vehicels, and data on the network	4.3.1(a), 4.3.2(c)(h), 4.3.6(a)(b)(c)(d)(f)
Halt of Service (DoS attack) due to overloading cloud, vehicle and network	4.3.2(e), 4.3.5(c)
Attacks on services due to malware infection and unauthorized access	4.3.1(a), 4.3.2(g), 4,3.5(b)
Attacks against vulnerabilities due to inadequate use case specifications and implementation	4.3.4(a), 4.3.6(c)(d)

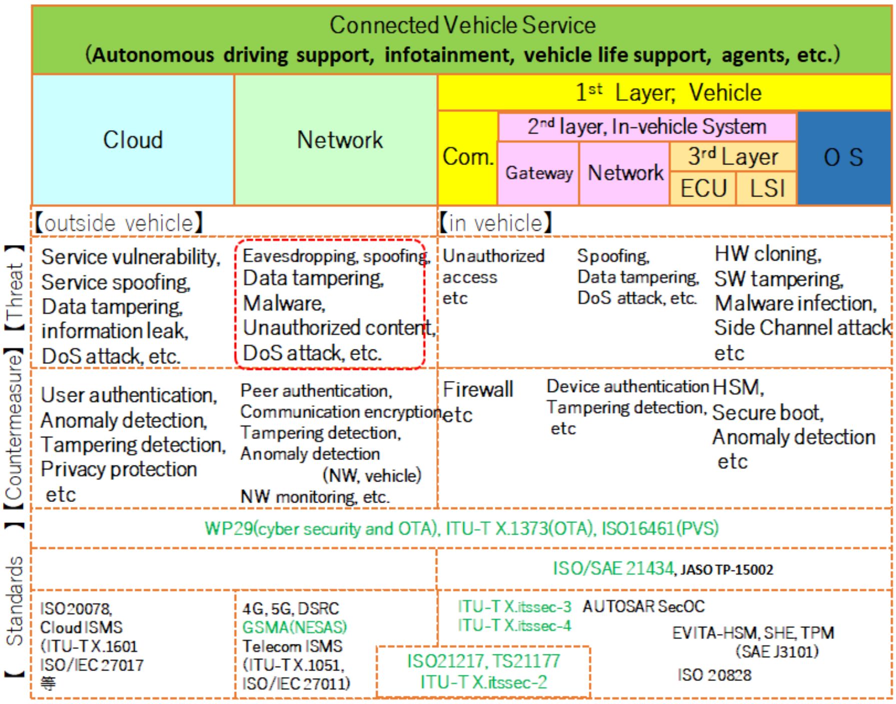


Figure 5.2.41 Diagram of connected vehicle system, its threats, and the corresponding standards

5.2.3.1.2. UC-3: Security issues related to digital Content in the infotainment service

Entertainment information such as video, audio, and games is used in the infotainment service. Digital content includes the technology of handling of information itself and its distribution. Since high-value content is handled, security measures against unauthorized use such as eavesdropping and unauthorized copying of the digital content is of a major concern. DRM technology is expected to solve the above problems. DRM is technology on a service layer that does not depend on the network. Therefore, the use of DRM, which is independent of 5G discussed later, is summarized in this section.

DRM is well known technology for premium digital content distribution over the Internet because digital content is easy to duplicate, alter, etc... DRM stands for Digital Right Management system, not a crypt technology. The essential of DRM describes usage rule of digital content for authorized person/device. Usually, DRM does not have any dependency on bearer like WAN(LTE/5G) / WiFi, etc..., in other words, DRM does not use any feature of bearer.

Of course, crypt technology is used if content owner and/or provider hopes to prevent copy. Such usage is defined in "license" data in each DRM scheme for each authorized person/device. DRM is realized by many patents and ways, so Fig 5.2.42 shows just concept.

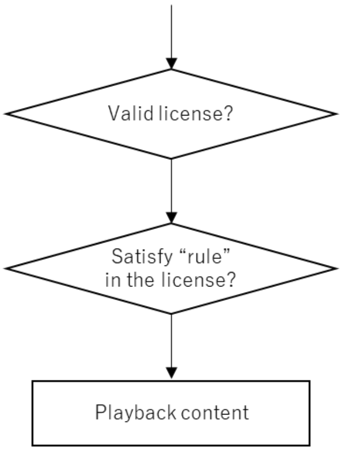


Fig 5.2.42 Playback flow

There are several DRMs in the real world; e.g. Widevice DRM of Google, PlayReady of Microsoft, FairPlay of Apple, Marlin of Marlin Trusted Management Org., etc… Content provider and/or aggregator usually uses one DRM technology for their service; means client system (player) needs to support the DRM to connect the service. If Car OEM hopes to support several content services, Car OEM needs to implement several DRM technologies. Usually, DRM technology is provided by DRM licensor such as the above together with agreement. In the agreement, licensor sometimes asks licensee to follow RR and CR to handle/playback DRM protected content (DRMed content).

RP (Robustness Rule)

RR stands for Robustness Rule. RR describes how to prepare HW and SW to prevent cracking activities as DRMed content player; e.g. using secure media bus for handling decrypted and decoded video data to prevent access by debugger for sniffing vide data.

CR (Compliance Rule)

CR stands for Compliance Rule. CR describes how to handle data if the data is sent to another device from DRMed content player to other devices including monitor. HDCP is known as content protection technology of HDMI and WiFi display (sometime such technology is called “link protection”). CR sometimes requires capability of this kind of link protection technology for DRMed content player.

Production

DRM licensor sometimes asks licensee to provision device unique key for each DRM at factory to realize more hardened DRM scheme. The key handling flow at factory is also defined in the RR.

Service

Sometimes content holder / aggregator asks OEM to show how to satisfy RR/CR and playback quality directly; it means it is not enough OEM to satisfy only CR/RR.

In case of Mobile Device like Smartphone, usage of DRMed content is now quite simple; streaming and cache for off-line playback. Formerly, the reason is that mainstream of service is now "streaming" over the Net.

Almost DRM scheme has authentication scheme, but does not include user authentication, so user needs to log-in to the service and bind their device to the service by using DRM feature.

For Car

It is recommended to use standard bus especially for AV signal handling like from head unit (receiver of DRMed content) to screen for back head, otherwise each Car OEM needs to negotiate their own technology with content holder/aggregator.

Car OEM also needs to consider which user authentication scheme is taken; simply carry today's mobile device system like ID/Password, use SIM auth system for log-in to the service.

5.2.3.1.3. Security of Connected Vehicles in 5G environment

Security in 5G is being considered in 3GPP SA3 for wireless access (RAN) and core networks (CN). In this section, we will clarify the subjects to be examined for the following 5G functions to realize the network or security requirements in the previous section.

- Trust model

In the use cases of the previous section, various players with different roles such as Connected Vehicle service users, service providers, car manufacturers, and network providers are involved. Accordingly, it needs to clarify the trust model among those players is considered in 5G network.

- Network Slicing

In the use cases of the previous section, different network qualities are required. Network slicing realizes to provide multiple logical networks with different qualities in RAN and NC on a common platform of 5G. It is also necessary to clarify the security issues of network slicing, considering the security requirements discussed in the previous section.

- MEC

MEC (Mobile Edge Computing / Multi-access Edge Computing) can reduce the network load by caching the content and reduce the latency by performing processing at the edge. Accordingly, MEC is expected to achieve the high throughput and low latency, which is one of the network requirements in the use case of previous section. When using MEC, it is also necessary to clarify the issues in consideration of the security requirements in the previous section.

- C-V2X

In order to realize use cases such as driving support, it is necessary to communicate with a large number of devices such as vehicles and roadside devices. C-V2X interface is also defined in 5G network. When using C-V2X, it is necessary to clarify the issues in consideration of the security requirements in the previous section.

- Authentication / authorization

In addition to service users, service providers, car manufacturers, and network providers in the above trust model, service-level authentication /authorization of network slice providers, MEC service providers, and C-V2X service providers shall be required.

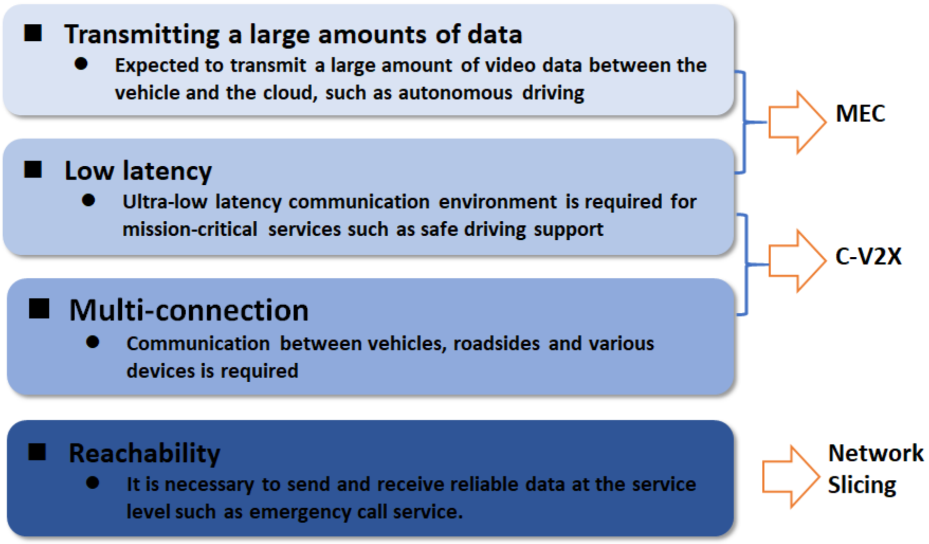


Figure 5.2.43 5G functions based on network requirements of Connected Vehicle

5.2.3.2. Trust model

It is expected that various players will be involved in the realization of the Connected Vehicle service. Here, in the four use cases selected in the previous section, the trust relationships between players and authenticity of the various data shall be established from the viewpoint of the service level.

In the Connected Vehicle service, users, vehicles, networks, and clouds are players. From the viewpoint of cyber security measures on communication channel defined in WP.29, a trust relationship shall be established between each player and a secure relationship (connection) is established. The target for building a trust relationship is the player or the data exchanged between the other party (Peer Entity) (see Fig. 5.2.44).

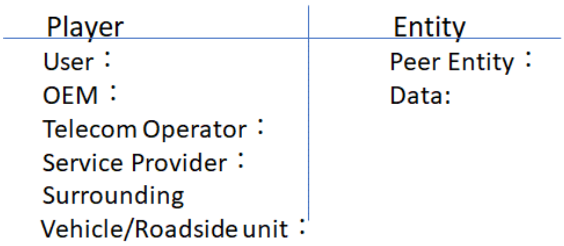


Figure 5.2.44 Trust model

Table 5.2.22 Information exchanged in the use cases

	Data
UC-1	・Surrounding vehicle driving status, ・Vehicle control information ・Dynamic map, ・Driver status
UC-2	Operation plan / status, traffic status / prediction, Movement requests/demands, Vehicle status, driver status
UC-3	Entertainment Information（Video, Audio, Image, Online Game, etc)
UC-4	Audio Information, Sensor Information, Driver monitoring information

Here, each player establishes a trust relationship depending on specific use case of the Connected Vehicle service.

Although, the users are assumed to be car owners, their families, rental users, car sharing users, and so on, the available services of the Connected Vehicle are restricted by the capabilities of the vehicle. For example, high-end cars generally have various additional services. In other words, it is realistic to think that the service on Connected Vehicle is determined by the combination of vehicle and the user.

The trust relationship of each player based on use cases is as follows.

・ Vehicle authentication by its user

As vehicle manufacturers are trusted in the real-world environment, there is currently no need for users to verify the credibility of their cars.

・ Network authentication by user

As the vehicle authenticates the network, the user does not need to authenticate the network.

・ Cloud service authentication by user

As the car authenticates the cloud service, the user does not need to authenticate the cloud service.

・ User authentication and identification by vehicle

Currently, user authentication is performed using a physical key, but in the future, services that identify drivers, such as automobile insurance services, are also expected. Thus, the technology to authenticate user and verify its identity is also required.

・ Network authentication by vehicle

As the vehicle authenticates the network, the user does not need to authenticate the network. (Depending on the infrastructure, authentication may not be possible)

・Authentication of cloud services by vehicle

As the Connected Vehicle service is assumed to be a service provided by the vehicle, the vehicle authenticates the cloud service.

・ User authentication by network

As the network authenticates the connected vehicle, no user authentication is required.

・ Vehicle authentication by network

In the Connected Vehicle service, the network authenticates the connected vehicle.

・ Cloud service authentication by network

In the Connected Vehicle service, the network authenticates the connected cloud service.

・ User authentication by cloud

As Vehicle service, the cloud authenticates the Connected Vehicle, no user authentication is required.

・ Vehicle authentication by cloud

In the Connected Vehicle service, the cloud service authenticates the connected vehicle.

・ Network authentication by cloud

In the Connected Vehicle service, the cloud authenticates the network. (Depending on the infrastructure, authentication may not be possible)

These trust relationships are summarized in Table 5.2.23.

Table 5.2.23 Trust relationship of each player

	User	Vehicle	Network	Cloud
User		Trust	Indirect trust	Indirect trust
Vehicle	Don't trust		Don't trust	Don't trust
Network	Indirect trust	Don't trust		Don't trust
Cloud	Indirect trust	Don't trust	Don't Trust	

5.2.3.3. Network slicing

Because the Connected Vehicle service requires different network requirements for each use case, it is required to use a logical network that meets these different requirements.

For example, in the case of UC-1 autonomous driving support, for example the dynamic map service, high-throughput network to transfer data from the cloud to the vehicle is required. whereas when vehicle control information on the cloud side is notified to the vehicle, low latency network is required. A mechanism for managing the QoS of the network is required according to each of these different network requirements. Here, as a feature of 5G, the network slicing function based on the network virtualization can be used.

5.2.3.3.1. Security in 5G network slicing function

Security issues on network slicing is discussed in 3GPP SA3 Phase 2. The security considerations for network slicing are as follows (3GPP TR 33.813) [32].

- Network slice authentication / authorization.
  It provides a mechanism for slice authentication and authorization to prevent network resource consumption and DoS attacks due to unauthorized terminal access. Slice authentication may be used in combination with primary authentication.
- Key separation in network slicing.
  To manage keys for each slice so that key leakage does not affect other slices, and to provide a mechanism for efficiently guaranteeing forward security against key updates.
- Slice providers should customize and provide services to each slice user.
  For customization, network characteristics (wireless access technology, communication bandwidth, delay, reliability, etc.) and security level shall be considered. Regarding the security level, it is necessary to specify the security function to be provided to the slice user and the method of providing the function.
- For slice authentication / authorization, it is necessary to manage IDs and credentials that are different from the subscriber information of mobile operators.
  In order to ensure the above security, a secure storage method for IDs and authentication information for slice authentication / authorization in UE (communication terminal) and a secure communication between a network for slice authentication provided by a third party, and a 5G core network (AMF, SMF or NSSF) are required.
- The access token to the network slice is issued by NRF. Using access tokens for shared slices, slice users can access to service provided by the same type of network service provider (NF service producer)
  NS-1 (NS-Producer-1)
  NS-2 (NS-Producer-2) shared slice level access token
  NS-3 (NS-Producer-3)

- Protect NSSAI information for privacy protection. Specifically, NSSAI information is not sent as initial NAS information until a secure session is established.
- Providing a means to cancel an invalid NSSAI so that the UE (communication terminal) can access the once rejected NSSAI.

The procedure for primary authentication and slice authentication is shown in Figure 5.2.45

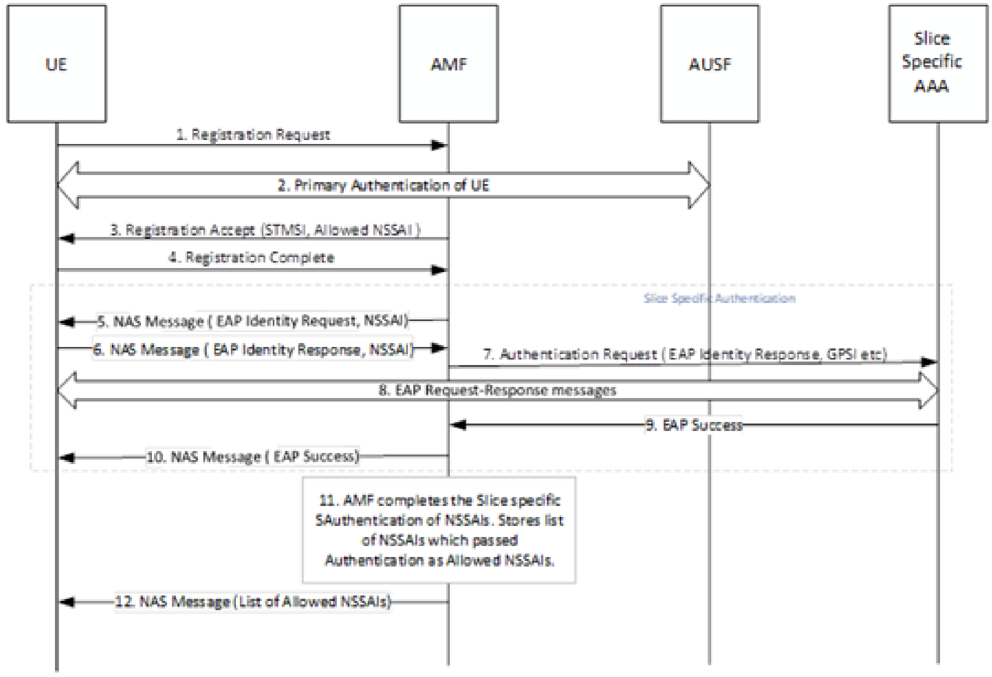


Figure 5.2.45 Overview of primary and slice authentication procedures

Based on the results of the above study of TR 33.813, a new technical specification TS33.501 (security Architecture) Release 18 [33] has been specified as clause 15 (Management security for network slices) and a new clause 16 (Security Release 18 (Security Architecture) Release 18. In addition, Release 18 has resulted in new Technical Report TR33.874 (Study on enhanced security for Network Slicing Phase 2) [34] and Technical Report TR33.886 (Study on enhanced security for Network Slicing Phase 3) [35] is being considered. In addition, Technical Specification TS33.326 [36] describes the security requirements and test items specific to the Network Slice Specific Authentication and Authorization Function (NSSAAF) of the network slice. The following is an overview of each of them.

Clause 15 of TS33.501 specifies the security of network slice management services for creating, operating, and decommissioning instances (actual state) of slices. Specifically, it specifies that mutual authentication between the slice management service and its users, data integrity, prevention of replay attacks, and confidentiality shall be achieved through TLS. In addition, it specifies procedures for the service management service to authorize users after mutual authentication.

In addition, TS33.501 clause 16 specifies the relationship between primary authentication and authorization for UE access to network slices. First, when the UE is authenticated by primary authentication, the UE is presented with a list of network slicing identities (S-NSSAI) that are available to the UE. The process of network slicing authentication and authorization is then performed for the specified network slices.

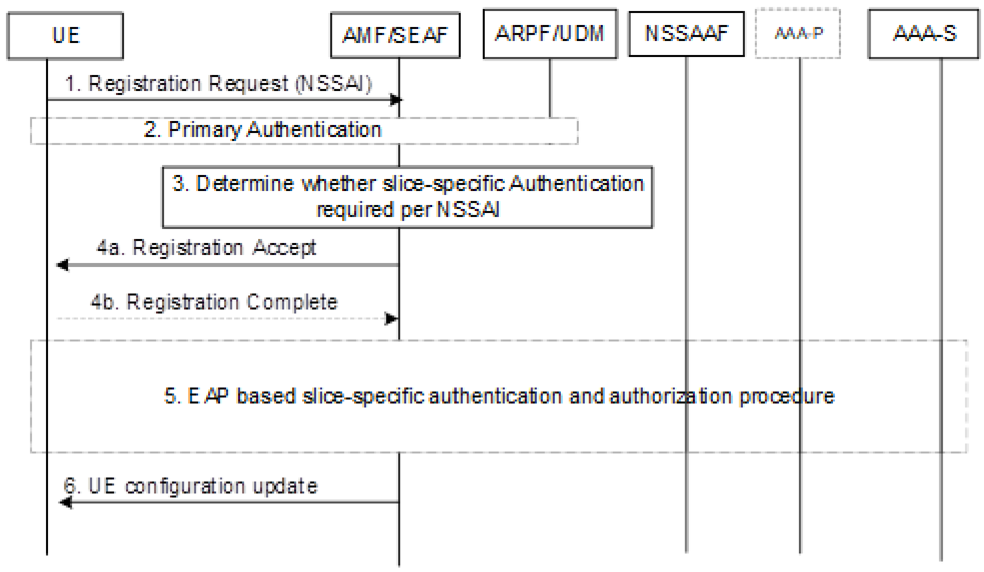


Figure 5.2.46 Relationship between Primary Authentication and NSSAA

Network slicing authentication can also use an external authentication server. In this case, a different credential is used than the 3GPP credential (authentication information) for the subscriber. The EAP framework is used for authentication and authorization to and from the authentication server (AAA). In addition, procedures for re-authentication/re-authorization and suspension of authentication from the authentication server (AAA) are also specified, assuming secure and efficient use of network slicing.

On the other hand, TR33.874, a new study item, examines countermeasures against privacy leaks due to the broadcast of slice information, DoS countermeasures related to the new NSAC (Network Slice Admission Control) procedure, and AF authentication and authorization.

In Technical Report TR 33.874, there is a consideration of reporting the same slice-related information to support fast cell selection and cell reselection for a particular network slice, which may lead to privacy leakage.

In addition, the Network Slice Admission Control (NSAC) procedure introduced in technical specifications TS23.501 and TS23.502 monitors the number of UEs registered in a particular network slice, and if the number exceeds a specified value, the mechanism denies usage by new UEs if a UE uses multiple slices, it may be a DoS attack to occupy the slice allocation.

Furthermore, since AF authentication and authorization has the ability to monitor the number of UEs using network slices and the number of PDU sessions, there is a risk that information may be leaked to unauthorized AFs, which may leak management information of network slices.

Technical Report TR33.886 discusses the following considerations.

- Secure procedures for providing VPLMN slice information to a roaming UE in order for the UE to need the network slices available in the area from other networks.

- Authorization procedures that support timed network slices with short lifetimes and slice service area authorization procedures that take into account issues such as UEs being able to access a network slice even if the network slice is down, or UEs not being able to access a network slice because the network slice lifetime information is not properly provided to the UE.
- Security considerations for extending the NSAC specified in Release 17 to Release 18. Specifically, network control improvements for UE behavior and security considerations for support of multiple NSACFs.

Technical Specification TS33.326 specifies the following Security Assurance Specification (SCAS) for NSSAAF.

The following security assurance specifications (SCAS) for NSSAAF are specified in Technical Specification TS33.326:

Messages for authentication and authorization of network slices for a specific S-NSSAI are sent and received directly to the AAA server (AAA-S) in case of an AAA in H-PLMN, or through an AAA proxy (AAA-P) in case of an external AAA server, so that the messages need to be properly routed. The SCAS defines the test items for this routing and the criteria for security requirements.

The SCAS defines test items and criteria for security requirements to check whether the AAA server (AAA-S) is authorized to re-authenticate and re-authorize UE.

The adaptation of eNodeB-specific robustness testing requirements and associated test items.

NSSAAF-specific vulnerability testing requirements and associated test items.

5.2.3.5.5. Security Issues on Network Slicing in Connected Vehicles

In order to ensure safe autonomous driving, it is necessary to transfer vehicle control information with high reliability and low delay. Therefore, a network slicing of 5G URLLC, which is dedicated to autonomous driving support shall be used. For this purpose, the appropriate security profile and the network requirements (delay, service area, etc.) for autonomous driving support shall be specified. In this section, the security requirements for network slicing in Connected Vehicles are considered below, based on the latest network slicing studies (see Figure 5.2.47). Here, the managing entity of the network slicing could be either the service provider of the Connected Vehicle or the telecommunication provider.

(1) User-centric Authentication and authorization

Network slicing dedicated to for autonomous driving support is a virtual communication network constructed on a mobile network. This network slicing is provided by service provider of autonomous driving support. Therefore, the autonomous driving support service authenticates a user who has made a contract with the autonomous driving support service and authorizes the access right of the user. In this way, the autonomous driving support service can be a service independent of the mobile communication carrier.

If the Connected Vehicle service provider is the managing entity of the network slicing, it is assumed that an external authentication server (AAA) will authenticate the user. In this case, the procedure for slice authentication and authorization by an external server specified in Technical Specification TS33.501 is applicable.

In order to use the above services on the virtual network safely, as considered in 3GPP TR 33.813, ID and authentication information (Credential) for slice authentication shall be securely stored and managed in UE (communication terminal). For this purpose, a hardware tamper-resistant module such as SIM or TEE may be used. In addition, it will be necessary to manage the status of primary authentication and slice authentication in the UE. For example, the slice authentication works while the primary authentication is established. Connected Vehicle service via multiple mobile carriers is also assumed, and it will be necessary to consider a roaming mechanism of slice authentication.

(2) Secure network slice management by Connected Vehicle service provider

If the Connected Vehicle service provider is the management entity of the network slicing, the TLS-based mutual authentication, integrity, replay attack prevention, and confidentiality features in the management interface of the network slicing specified in clause 15 of Technical Specification TS33.501 The network slice management interface can be utilized. On the other hand, when the telecommunication carrier is the management entity of the network slice, the control of the network slice by the Connected Vehicle Service Provider is not possible, so an out-band control interface between the telecommunication carrier and the Connected Vehicle Service Provider is required. Therefore, an out-of-band control interface between the telecommunication carrier and the Connected Vehicle Service Provider is required.

(3) Optimization of security profiles for CV services

Depending on the level of security required by the Connected Vehicle service, it is necessary to specify the level of authentication of the user (UE) when using the network slice. As discussed in 3GPP TR 33.813, slice providers provide slice users with customized services. Specifically, it is necessary to specify the network quality and security level for the slices assumed by each Connected Vehicle service.

An example of the parameters is shown below.

Network quality: delay, error rate, jitter

Security level: encryption method, key length, key management mechanism (key update interval, Perfect Forward Security etc.)

(4) Secure management of ID and authentication information on mobile devices to access multiple network slices

Connected Vehicle services via multiple mobile carriers are also expected, and it will be necessary to consider a roaming mechanism that includes slice authentication used for Connected Vehicle services.

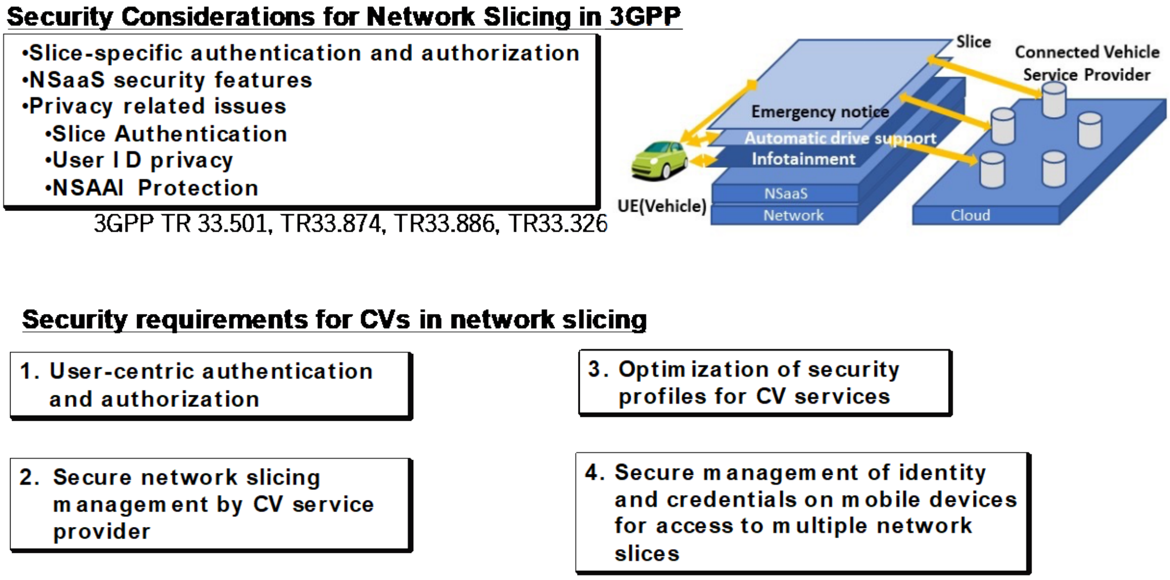


Figure 5.2.47 Overview Diagram on Security Requirements for 5G Network Slicing in Connected Vehicles

5.2.3.4. MEC

5.2.3.4.1. MEC Overview

MEC is an architecture that is expected to reduce latency and network load. Therefore, MEC is promising technology for Connected Vehicles. The MEC technology is studied in ETSI MEC, 3GPP and 5GAA respectively, as shown in Figure 5.2.48 [37]. ETSI MEC is promoting the standardization of APIs based on the MEC reference architecture and various use cases. 3GPP is studying the 5G architecture to incorporate the concept of MEC as a network function. As for AECC, automobile manufacturers and telecommunications carriers are studying network designs of Connected Vehicle services for the purpose to realize a distributed cloud environment based on the edge computing that covers multiple telecommunications carriers [38].

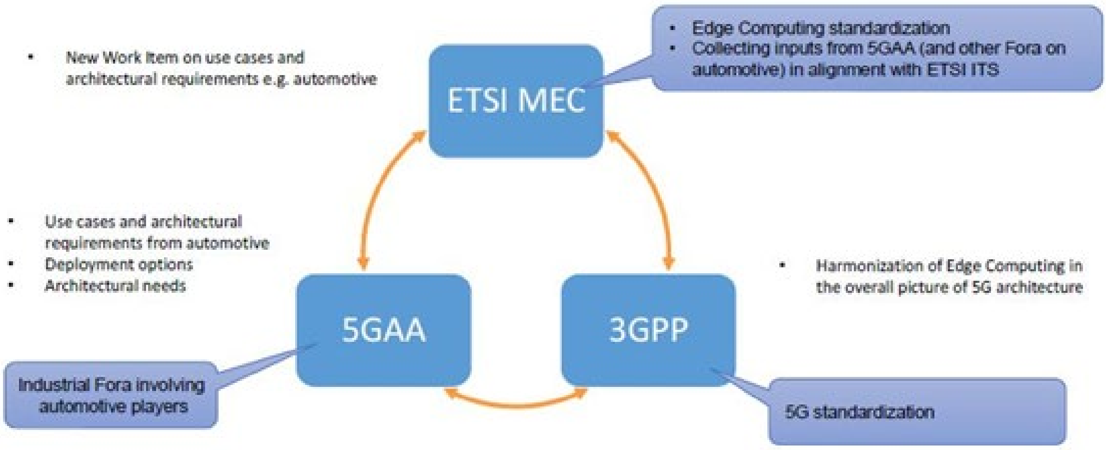


Figure 5.2.48 Relationship diagram of 5GAA, ETSI, and 3GPP regarding MEC

Figure 5.2.49 shows the relationship between the 5G system architecture and MEC being considered in ETSI and 3GPP [39] [40]. MEC functionality is realized by way of an interface based on the SBA architecture of the 5G core. In detail, MEC is categorized as AF (Application Function) that uses the services provided by other network functions defined in 3GPP. MEC is constructed by accessing to various network functions (NF) via NEF (Network Resource Function) of 5G core. For example, network functions are authentication function (AUSF), network slicing (NSSF) and/or function for directing 5G traffic to MEC (UPF).

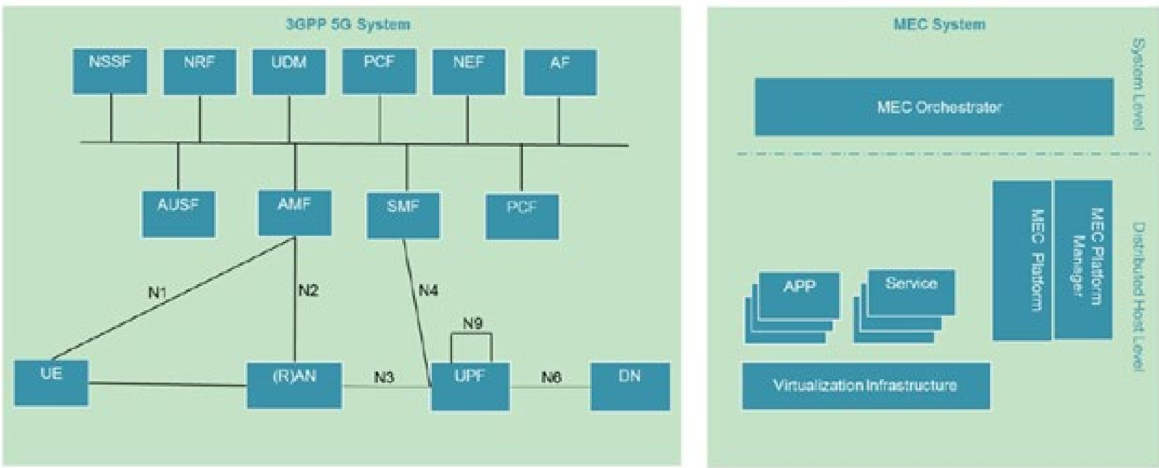


Figure 5.2.49 Relationship between 5G Service Based Architecture and MEC Architecture

5.2.3.4.2. Security in 5G MEC functionality

Release 17 technical specification TS33.839 [41] specified the security specifications supporting Edge Computing (EC) in the 5G core. Figure 5.2.50 shows the architecture of EC. Here, the ECS (Edge Configuration Server) is a function that manages the settings necessary for EC, the EEC (Edge Enabler Client) is a function to realize EC services on the terminal side, the EES (Edge Enabler Server) is a function to realize EC services on the server side, and the ECS is a function to manage the settings for EC. EAS (Edge Application Server(s)) provides functions for server-side EC service applications, and AC (Application Client(s)) provides functions for terminal-side applications to use server-side EC service applications. The following functions are considered in Technical Specification TS33.839.

Key Issue No. 1: Authentication and authorization between EEC and EES
Key Issue No. 2: Authentication and authorization between EEC and ECS
Key Issue No. 3: Authentication and authorization between EES and ECS
Key Issue No. 4: Edge Data Network Authentication and Authorization
Key Issue No. 5: Edge Data Network User Identifier and Credential Protection
Key Issue No. 6: Transport security for the EDGE-1-9 interfaces.
Key Issue No. 7: Security of Network Information Provisioning to Local Applications with low latency procedure
Key Issue No. 8: Authentication and authorization in EES capability exposure
Key Issue No. 9: Security of EAS discovery procedure
Key Issue No. 10: Authorization during Edge Data Network change

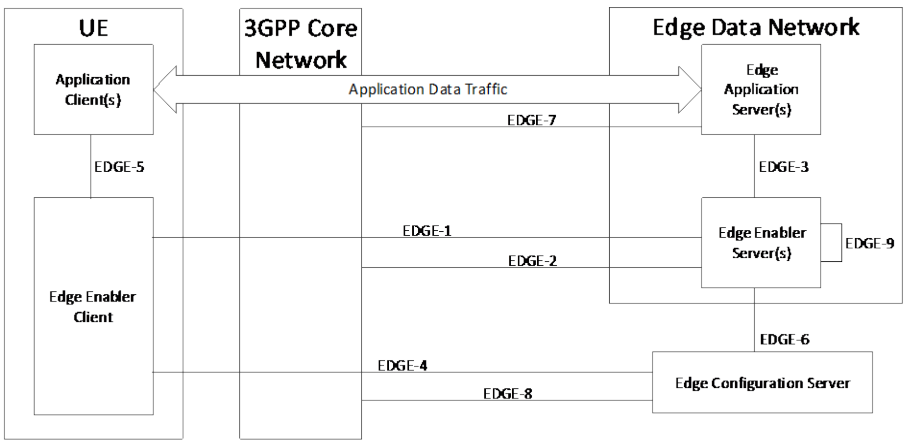


Figure 5.2.50 Architecture of EC

In addition, 31 technical specifications (Solution) for security are specified to achieve the above functions. The following two examples are described here.

Solution No. 2: Authentication between EEC and ECS based on primary authentication.
The authentication procedure between EEC and ECS is as follows (see Figure 5.2.51).
(1) As a result of the primary authentication, the key KAUSF is shared between the user terminal (UE) and the authentication server (AUSF). This TR33.839 also specifies how the shared key is generated.
(2) The user terminal and the authentication server both create credentials (authentication information and its ID) based on the shared key and the terminal identifier.
(3) The user terminal makes an authentication request to the ECS with the credential.
(4) The ECS requests the authentication server to confirm the validity of the credential via the NEF, and returns an authentication response to the user terminal based on the results.

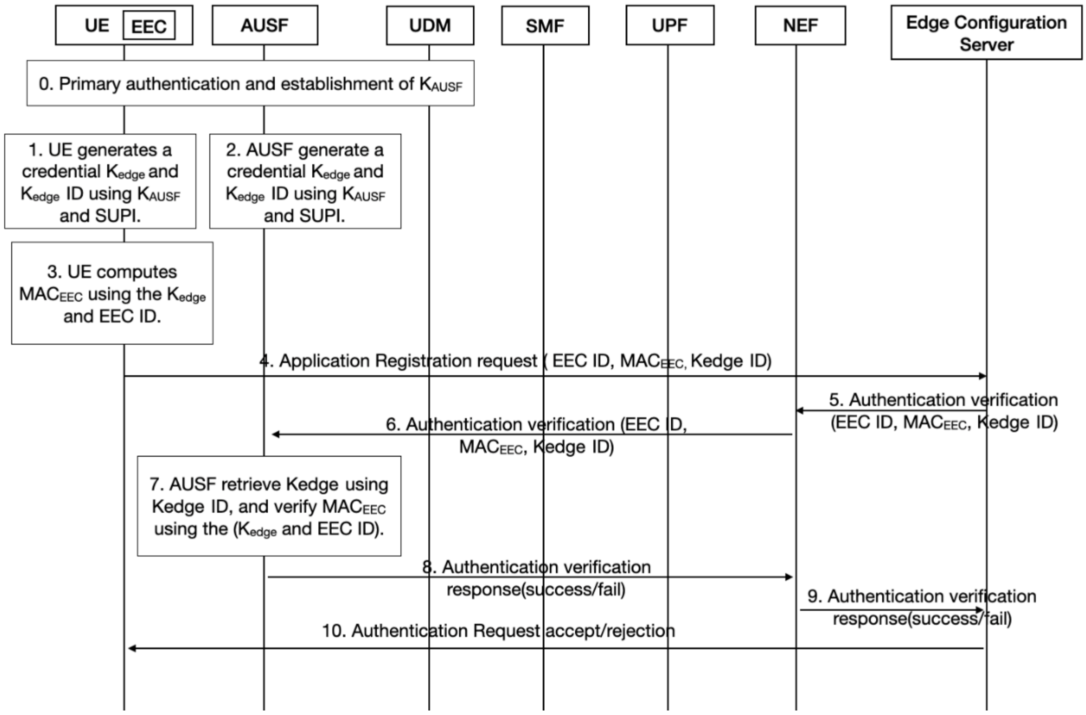


Figure 5.2.51 Authentication procedure between EEC and ECS based on primary authentication

Solution No. 4: Authentication/Authorization framework for Edge Enabler Client and Servers

The authentication and authorization procedure between EEC and EES is as follows (see Figure 52). This procedure is unique in that, in the context of an edge computing environment, the ECS authenticates the EEC as the AAA server for secondary authentication, and the EEC (client) plays the role of issuing and verifying the access token of the EES (edge server) as the authorization server based on OAuth2.0.

(1) The user terminal (UE) accesses the network through primary authentication.

(2) The user terminal (UE) initiates service provisioning procedures with the ECS to establish a PDU session. In this session, the AMF selects the SMF/PSA that provides a data connection to the DN-AAA server provided by the ECSP and SMF performs secondary authentication. Here, the ECS can act as the DN-AAA server.

(3) After the secondary authentication and authorization established by the DN-AAA server, the user terminal connects to the ECS for provisioning the EEC with ECS. User terminal performs EEC registration with the EES.

(4) The EEC authenticates to the EES by TLS through the EDGE-1 interface. The user terminal invokes the EEC's registration procedure with EES including the access token obtained in (3). The EES requests the ECS to verify the access token.

(5) The EEC makes a service request (discovery) to the EES using an access token obtained in (4). the EES verifies the signature of the access token by the ECS, and if correct, the EES

server grants the EEC's service request according to the authorization information in the access token.

(6) The UE obtains service from EAS by producing the access token obtained from the EES over the secure TLS connection. (Note: Authentication and authorization services between the AC and the EAS are outside the scope of 3GPP. i.e., note that item (6) is for reference only)

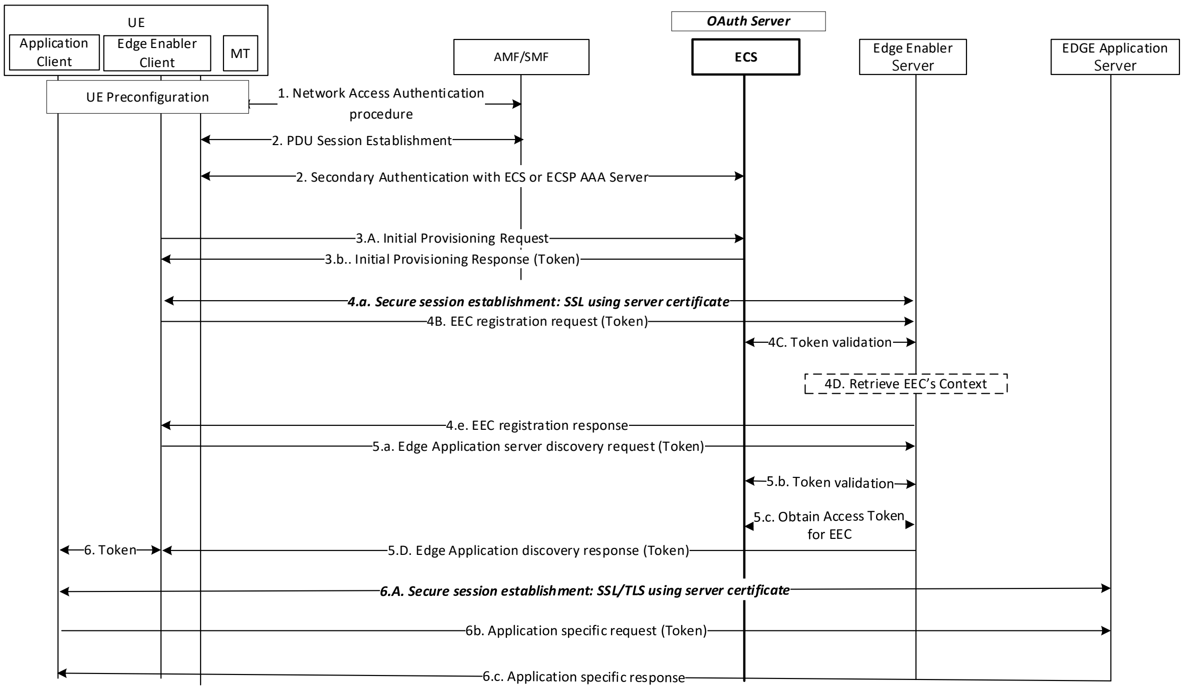


Figure 5.2.52 Secondary Authentication Based Authentication/Authorization framework for Edge Enabler Client and Servers

Release 18 Technical Specification TS33.558 [42] specifies the security functions and mechanisms that support the architecture for enabling 5G edge applications, namely interface security, authentication and authorization between entities in the application architecture procedures, and procedures for publishing EES functions.

In addition, Technical Report TR 33.739 builds on the results of Technical Report TR 33.839 and Technical Specification TS 33.558, work on supporting edge computing in 5G systems (Technical Report TR 23.700-48 [43], "5G Systems for Edge Computing Extensions" and "Extended Architectures for Enabling Edge Applications" in Technical Report TR 23.700-98), the security aspects associated with new features and procedures arising from the continuation of this work are being considered.

5.2.3.4.3. Security requirements for MEC in Connected Vehicle services

The security of the MEC architecture is currently under consideration [44] [45]. Here, when some of the functions of the Connected Vehicle work as a MEC application, the attack surfaces are network, other MEC applications, MEC infrastructure, malicious code embedded in the MEC application itself, and etc. The threat to that application is, as is the similar case of the cloud in the Figure 5.2.41, spoofing, illegal data alternation, data leakage, and DoS. Therefore, the same security measures as specified in Figure 5.2.41 are required.

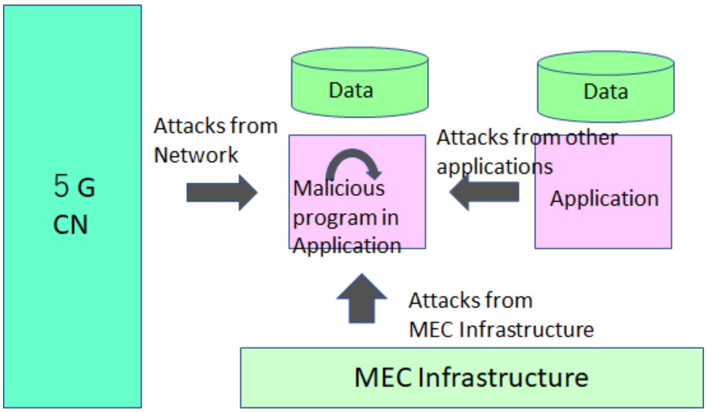


Figure 5.2.53 Attack Surfaces for the MEC app

As a countermeasure against spoofing, user authentication by the MEC infrastructure is considered. In the case, the authentication function (AUSF) of the 5G core can be used. When each MEC application provides a service with a user, the function of user authentication / authorization of MEC application by the MEC infrastructure is required. Although the detail procedure is for further study, secondary authentication is candidate mechanism of user authentication. Assuming the use of MEC by autonomous driving support, the owner of the MEC application corresponds to the provider of the autonomous driving support service. Therefore, the owner of MEC application, which is the provider of autonomous driving support service, shall authenticate the user who has made a contract for using the autonomous driving support service and authorize the access right thereof.

Autonomous driving support services over multiple mobile carriers are also envisioned, and it is necessary to consider the roaming mechanism. In addition, it is necessary to have a mechanism to take over the security policy associated with services and users during roaming while maintaining consistency.

MEC applications such as autonomous driving support are third-party applications from the perspective of telecommunications carriers. When registering and operating as MEC applications, it is necessary to set certain criteria of security and verify MEC applications.

The security requirements for MEC in Connected Vehicle services based on the above considerations are shown in Figure 54. The study on Connected Vehicle across multiple mobile operators will be discussed in the 5GAA below.

(1) User-centric authentication and authorization

To prevent unauthorized Application Client from accessing the Edge Application Server (EAS), it is necessary to consider the authentication and authorization of the Application Client. Authentication and authorization between AC and EAS are outside the scope of 3GPP, but it is pointed out that EAS may use the access token management service of the

Edge Configuration Service (ECS), which acts as an authorization server. (See earlier Technical Report TR33.839 Solution No. 4)

(2) MEC application registration, update, and verification

When the Connected Vehicle Service Provider is the management entity of the MEC application, it is necessary to provide a management interface to securely register, update, and verify the validity of the MEC application. On the other hand, if the MEC application is managed by a telecommunication service provider, the MEC application cannot be managed by the connected vehicle service provider. Then interface between the telecommunication carrier and the Connected Vehicle Service Provider is required.

(3) Secure connectivity with other MECs and clouds

Mutual authentication, confidentiality, integrity, and anti-replay attack capabilities must be provided to securely connect to external MECs and clouds.

(4) Application data privacy protection

For sensitive information handled by MEC applications, technical measures may be required to prevent information leakage to MEC platforms.

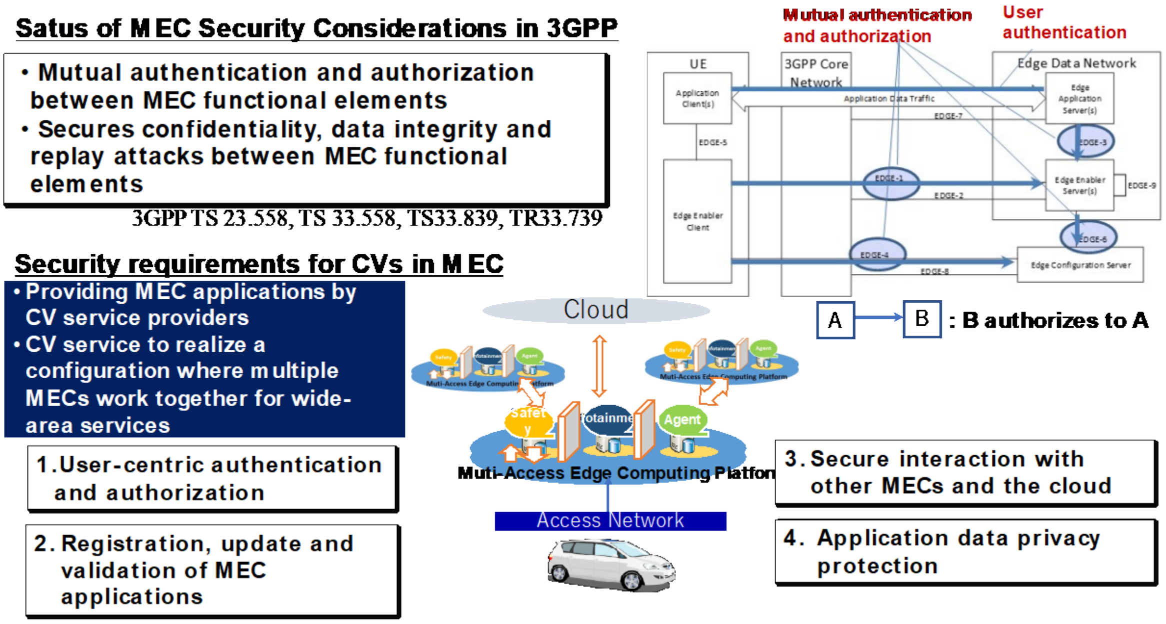


Figure 5.2.54 Overview on Security Requirements for 5G MEC in Connected Vehicles

5.2.3.4.4. 5G Automotive Association (5GAA) Study Survey of Edge Utilization

The 5GAA was established in September 2016. It is a cross-industry organization of companies in the automotive, technology, and communications (ICT) industries with the goal of developing end-to-end solutions for future mobility and transportation services. 5GAA examined the system model of MEC and its security for multiple carriers working together, and the white paper "MEC for Automotive in Multi-Operator Scenarios (2021.03)" [46] has been published. This section outlines the above white paper, focusing on the security perspective.

5.2.3.4.4.1 Reference Architecture for MEC with Multiple Intermediaries

In the above white paper, as shown in the reference architecture in Figure 55, there is an MEC Platform (MEC Platform) realized as a function of AF and an MEC Application (MEC App) running on it, and three scenarios in which the MEC Platform and MEC Application are provided by each MNO are defined.

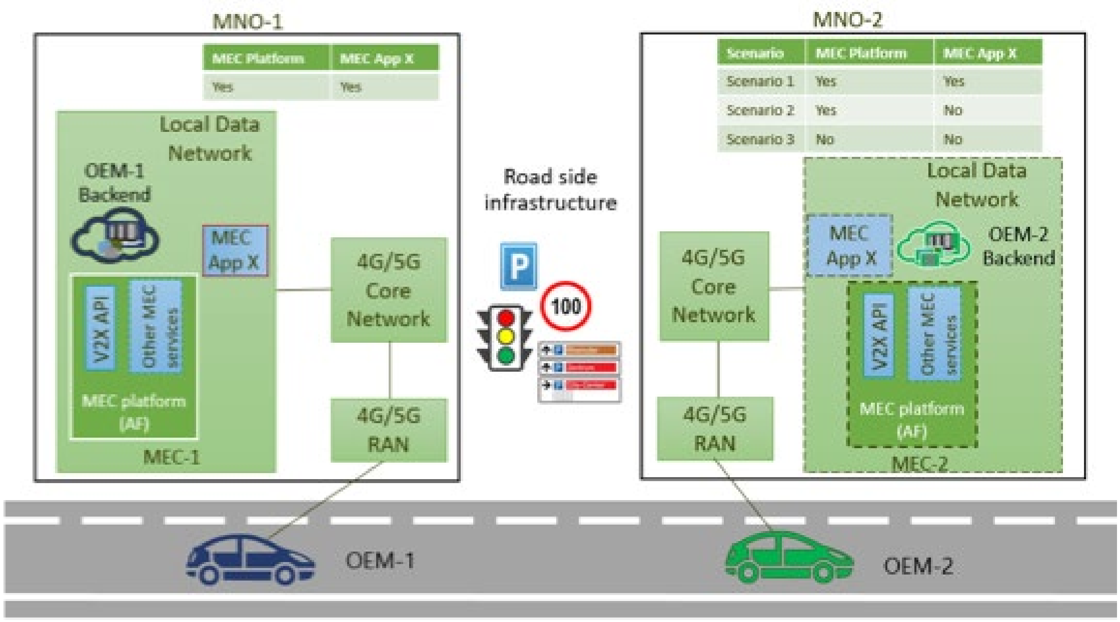


Figure 5.2.55 Reference Architecture for MEC Utilization in Connected Vehicles

Two different MNOs (MNO-1 and MNO-2) own the MEC infrastructure and MEC applications.

In this scenario, when a vehicle moves from MNO-1 to MNO-2, the MEC application used also moves from MNO-1 to MNO-2. Therefore, the shortest path between the vehicle and the MEC application is secured, and low latency communication is possible.

Two different carriers (MNO-1 and MNO-2) own the MEC infrastructure and MNO-1 owns the MEC application.

In this scenario, when a vehicle moves from MNO-1 to MNO-2, it needs to connect to the MEC application of MNO-1. In this case, the MECs of both MNOs are interconnected by a control plane and a data plane between the vehicle in the area of MON-2 and the MEC application of MNO- 1 is established. The vehicle and the MEC application communicate using this data plane.

Only MNO-1 owns MEC infrastructure and MEC applications.

Two cases are assumed in this scenario.

When a vehicle moves from MON-1 to MON-2's area, a vehicle in MON-2 connects to MEC application in MNO-1 by roaming.

When a vehicle moves from MNO-1 to MNO-2, a vehicle in MNO-2 connects to data network (DN) in MNO-1 by offloading through UPF in MNO-2.

(2) Security Boundary in MEC

In MEC, the MNO, the MEC Tenant Application Provider, and the Application User are the players. In this white paper, tenant applications and services not provided by the MEC are outside the scope of responsibility of the MEC, and the application user and the MEC tenant application provider assume responsibility and control. Therefore, the security perimeter based on the scenario in the previous section is defined as follows.

The case of one MNO and one MEC infrastructure as shown in Figure 5.2.56, the MEC infrastructure and MEC applications are the security boundary.

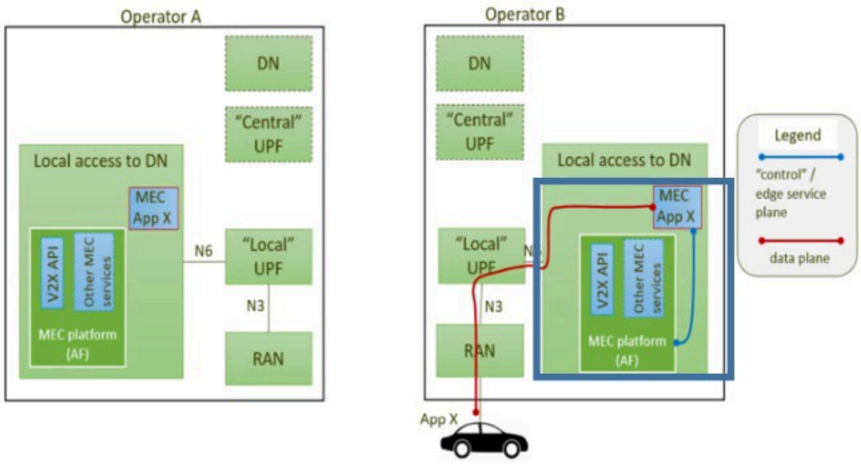


Figure 5.2.56 Security Boundary when both MNOs have MEC platforms and MEC application X (single vehicle OEM use case)

When the MEC infrastructure and MEC applications span multiple MONs as shown in Figure 5.2.57, the security boundary is the connection path between the MEC infrastructure of the MNO in whose area the vehicle belongs and the MEC applications that exist in other MNOs.

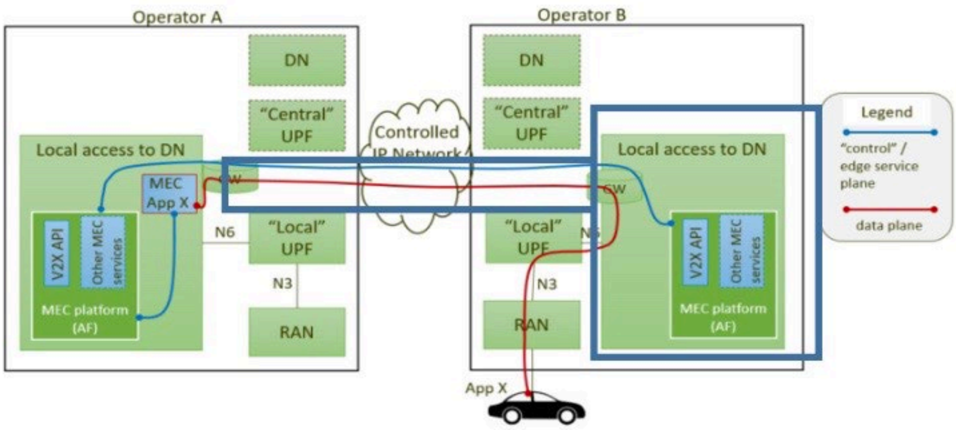


Figure 5.2.57 Security Boundary when both MNOs have MEC platforms, but MEC application is available only in MNO A (single vehicle OEM use case)

When one MNO, as shown in Figure 5.2.58, has an MEC infrastructure and an MEC application and is roaming from another MNO, the DN connecting the MEC infrastructure, the MEC application, and the MNO shall be the security boundary.

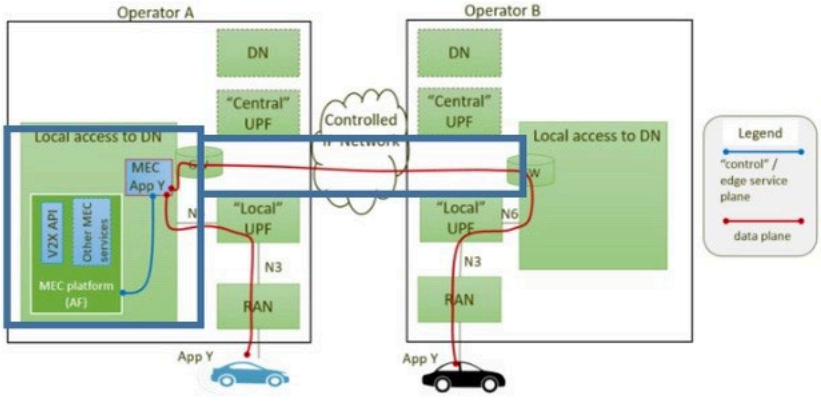


Figure 5.2.58 Security Boundary when only MNO A has a MEC platform and MEC application, and inter-MNO connectivity is by means of N9 tunnelling (single vehicle OEM use case)

(3) Security Analysis

The security perimeter specified in the previous section is targeted, and based on the European ENISA guidelines, the security requirements are organized from the perspective of the five items of the US NIST Cyber Security Framework (Identity, Protect, Detect, Respond, and Recover) plus the six items of privacy that take GDPR into account (see Table 5.2.24).

Table 5.2.24 Security requirements for MEC

		Overview (excerpts)
Identity	Entity Management	The vehicles, data, personnel, devices, systems, and facilities that enable the MNO(s) to achieve MEC functionality are identified and managed consistent. with their relative importance to business objectives and the MNO's risk strategy.
	Risk Assessment	The MNOs understand the cybersecurity risk to MEC operations (including services, functions, and service availability), MNO assets, and individuals.
Protect	Access Control	To physical and logical MNO and MEC assets and their associated facilities. It is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to activities and services. A policy of least privilege shall be implemented for all MEC access and control.

	Data Security	Information and records (data) are managed consistent with the MNO's risk strategy, privacy policy and applicable laws in order to protect the confidentiality, integrity, and availability of information.
	Information Protection	Security policies, processes, and procedures are maintained by the MNO and used to manage protection of information systems and assets. Consumer privacy related information shall be protected at levels consistent with applicable laws or MNO privacy guidance.
Detect	Anomalies and Events	Anomalous activity shall be detected in a timely manner and the potential impact of events is understood. The MNO MEC provider shall detect misuse and malicious behavior against services hosted by the MEC, where possible with regard to privacy constraints.
	Security Continuous Monitoring	The MEC and related assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. MNO/MEC best practice shall be to provide automated monitoring for non-major attacks and malicious activity.
Respond	Response Planning	MNO MEC response processes and procedures are executed and maintained to ensure timely responses to detected cybersecurity events. Cybersecurity best practice is to have a security incident response plan that acknowledges the reality of MNO MEC Shared Responsibility paradigm.
	Response Communications	Response activities are coordinated with internal and external entities (OEMs and subscribers), as appropriate, to include external support from governmental agencies.
	Mitigation	MNO MEC cybersecurity activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
Recover	Response Planning	MNO MEC cybersecurity recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
Privacy	MEC privacy security services may vary depending on location and MNO, but given broad agreement on certain privacy controls, it is prudent to provide certain MEC privacy preserving functions. GDPR and laws inspired by GDPR	

	such as CCPA are considered models upon which most MNO MEC operators should turn for privacy guidance.	
	Anonymity Services	The MNO MEC shall provide anonymity services as applicable by law or MEC service (e.g. safety messaging)
	Personal Privacy Data Management	The MNO shall allow (where applicable by law) a mechanism for subscribers to manage privacy data.
	Do Not Track Services	The MNO shall allow (where applicable by law) a mechanism for subscribers to invoke services to prevent tracking.

5.2.3.5. C-V2X

5.2.3.5.1. Overview of C-V2X

The C-V2X is standardized by 3GPP as a means of communicating between vehicles and between vehicles and roadside devices by cellular communication. Among these, the wireless interface standard PC5 is used for boundary communication of V2V (between vehicles), V2I (between road vehicles), and V2P (between pedestrians). In addition, V2N (between vehicle networks) is specified as wide area communication via the mobile communication network. In the study of 5G in 3GPP, V2N (reference point: Uu) will be specified in 3GPP Release 15, and V2I and V2V (reference point: PC5) will be standardized in Release 16. [47] Three data transfer methods are specified: unicast, groupcast, and multicast.

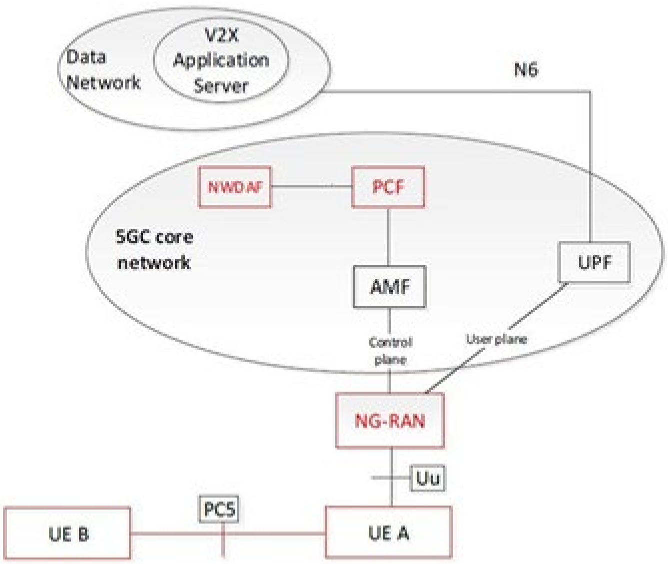


Figure 5.2.59 V2X architecture specified in 5G system architecture on 3GPP Release 16 [48]

5.2.3.5.2 Security in 5G C-V2X functionality

Regarding security at the reference point of PC5 (communication without mobile network), the following functions are examined in 3GPP SA3 TS33.836[49], where the target is mainly privacy protection of Layer 2 ID and source IP address [50].

- Privacy protection for unicast messages on PC5
  Eliminate traceability and linkability by regularly updating device ID (L2-ID)
- Security in V2X unicast messages on PC
  Establishing security associations (sessions) between devices
- Privacy protection for multicast messages on PC5
  Prevents source ID (L2-ID) tracking in multicast sessions
- Privacy protection for group communication ID
  Protects the device ID (L2-ID) from being linked from the group ID
- Security related to multicast communication settings
  Since L2 signaling is used when performing multicast communication, attacks on the protocol (MitM, etc.) are prevented.
- Security related to device service authorization and destruction
  Concealment, tampering prevention, and replay attack prevention for device service authorization and destruction protocols
- Security related to Cross-RAT (LTE and 5G) service authorization

In addition, based on the above, Technical Report TR33.836, Technical Specification TS33.536 [51] is being studied in Release 17.

5.2.3.5.3. Security Requirements for C-V2X in Connected Vehicles

Regarding C-V2X, security issues are summarized in Section 5.2.2.4, "Survey Report for Advancement of ITS / Autonomous Driving Using Cellular Communication Technology". The common security issues for each use case in the above report are as follows.
"The authenticity of information and its responsibility are important. In this use case, message origin authentication from the information provider is required. For the purpose to prevent information from illegally altered by an uncertified organization, digital signature embedded in the distribution information and a secure connection with the information provider, distribution server, or vehicle shall be used. It is also necessary to consider privacy issues on vehicle tracking using control information. "

- The security specifications of application data in C-V2X are not covered by 3GPP. The specifications of security association between devices in short-range communication PC5 refers to PKI-based mechanism of security services for application and management messages defined in IEEE 1609-2, which is the part of IEEE DSRC (WAVE: Wireless access in Vehicular Environment). Where, IEEE1609-2 provides message confidentiality, integrity, and authentication / authorization.

- In the case of UC1, a vehicle shall obtain information on the running condition of surrounding vehicles from other vehicles and roadside devices with low latency. When confirming the authenticity by means of PKI certificate, performance issues shall be taken into consideration, which is also pointed out in the above report. In particular, it is necessary to consider efficiently verifying the certificate signature, checking revocation list (CRL), and communicating the large amount of certificate data.
- As for privacy issues to prevent vehicle from being traced, 3GPP SA3 TS33.836 defines a protocol to periodically change the Layer 2 ID and source IP address. Furthermore, if the application data is not encrypted, there will be also a traceability problem due to the data of the subject field in the certificate which describes person name, address, and etc.
- Roadside device may handle plural connected vehicle services over C-V2X. Application data of each service are exchanged between roadside device and vehicles. The service provider or subscribers of the service need to verify the authenticity of the above application data. This message origin authentication is independent of the device authentication of roadside device.
- The PC5 interface for direct communication specified in C-V2X provides groupcast and multicast functions. However, if confidentiality is required for application data in these connection modes, a new group key management scheme for broadcast mode and groupcast mode needs to be specified to securely share and update encryption keys among multiple communication partners.

The above requirements are shown in Figure 5.2.60.

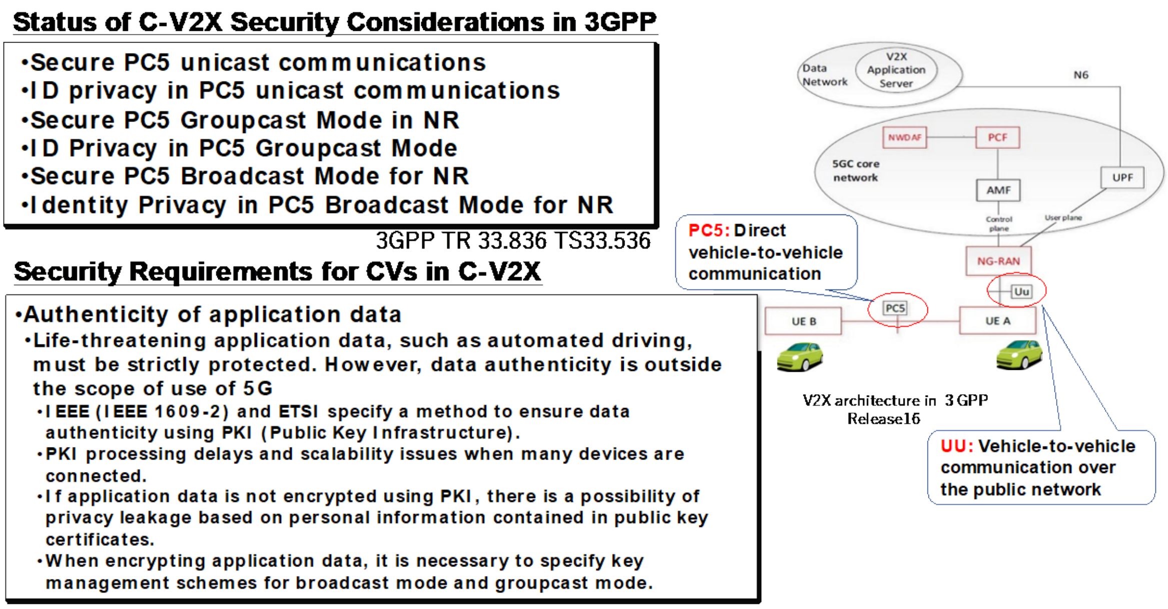


Figure 5.2.60 Overview on Security Requirements for 5G C-V2X in Connected Vehicles

5.2.3.5.4 C-V2X Security Considerations in 5G Americas

5G Americas is an industry association of leading telecommunications service providers and manufacturers whose purpose is to advocate and promote the advancement of 5G and beyond throughout the ecosystem of networks, services, applications, and connected devices in the Americas. The white papers "Privacy by Design Aspects of C-V2X" (2020.10) [52] and "Vehicular Connectivity: C-V2X & 5G" (2021.09) [53] were published in the above 5G Americas. This section outlines the security requirements described in these white papers. “Privacy by Design Aspects of C-V2X" (2020.10) focuses on Cooperative Awareness Messages (CAM) and Decentralized Environmental Notification Messages (DENM) as messages that are specified in C-ITS (Cooperative ITS) and are regularly broadcasted by vehicles, including vehicle location and speed. The requirements for the protection and privacy of these messages are summarized in this document. The privacy requirements are as follows

- Minimal presentation of information
  The amount of information a user reveals in a communication should be kept to a minimum.
- Conditional anonymity
  Individual vehicles should be anonymous within the set of potential participants.
- Unlinkability
- Ensure that different pseudonyms of a particular vehicle cannot be linked to each other.
- Forward and Backward Privacy

Credential revocation does not affect the unlinkability of previously signed messages. Nor should an attacker recovering the identity of the sender of a particular credential affect the privacy of other messages signed by the same sender.
In addition, the technical requirements to realize the above privacy requirements are organized in Table 5.2.25 below.

Table 5.2.25 Technical Requirements for Privacy Requirements

Privacy Requirement	Controls – Technical Requirements
Minimum disclosure	No explicit identification. Pseudo-identifiers are temporary. Vehicle identifying information (e.g. vehicle dimensions, etc.) is coarse.
Conditional anonymity	The system should be able to identify misbehaving vehicles and take corrective measures.
Unlinkability	Pseudonym changing properties: a pseudonym should be used for a limited time, and multiple pseudonyms should be available to a vehicle in order to enable pseudonym change. Transmission behaviour in lower layers should change when pseudo-identifiers change.
Forward and backward privacy	Supported by revocation mechanism: certificates for current and future time periods are revoked; messages signed in past time periods cannot be linked.

For privacy solutions using pseudonymous IDs, the Security Credential Management System (SCMS) proposed by the Automotive OEM Consortium and the U.S. Department of Transportation (USDOT), and the Coordinated Certificate Management System (CCMS) developed by the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI) are referred in the document. This issue is discussed in detail in the next section.

(1) Sandboxing

To prevent attacks by receiving unauthorized data in C-V2X, intentionally restrict the types of data that devices can accept. Specifically, application IDs (AIDs) are standardized, and only applications corresponding to the AIDs will accept data during transmission. Each message is for a specific application and is processed only by that application, thus preventing spillover to other applications or other components in the vehicle. Here, the AID is the Provider Service Identifier (PSID) in the United States and the Intelligent Transportation Systems Application Identifier (ITSAID) in the ETSI/ISO system.

(2) Authentication

In C-V2X, message authentication is based on PKI, but since the number of individual devices is enormous and immediate authentication becomes difficult, a method that authenticates applications (AID) without authenticating individual devices is used (see Figure 61). This allows for confirmation of data generated by legitimate applications and avoids the privacy issue of individual devices being traceable at the time of authentication.

(3) Cryptographic Techniques Used for Authentication

Because of the limited communication bandwidth of C-V2X, IEEE1609.2 uses a compact form based on elliptic curve cryptography.

(4) Malfunction Detection

Malfunction detection is the process of ensuring that all incoming messages to an application are appropriate. If a message does not match sensor data, other messages from the same sender, or messages from other sensors, it is rejected.

(5) Privacy protection

User privacy can be ensured by not including the user ID in the message and using only privilege. In addition, multiple certificates may be issued and used to prevent vehicle tracking. In Europe, 60 to 100 certificates are issued per week.

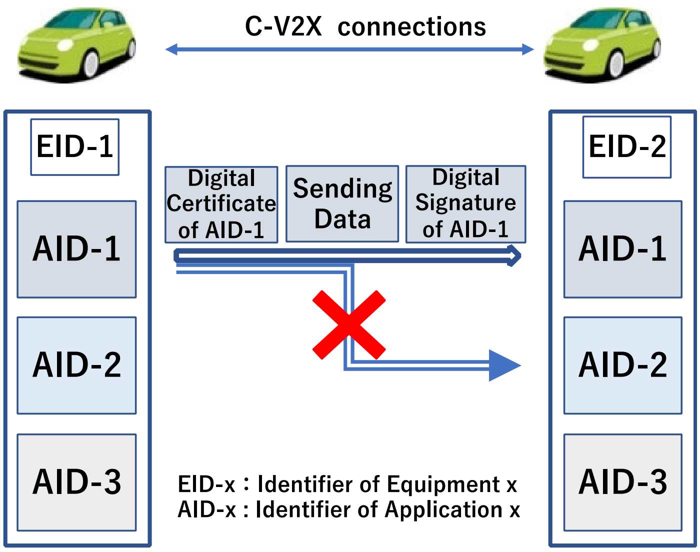


Figure 5.2.61 Message Authentication with AID in C-V2X

5.2.3.5.5. Survey of overseas trends in data reliability and privacy protection in V2X

In this section, we discuss overseas trends related to ensuring the reliability of messages sent by V2X and privacy protection technologies, as pointed out in the issues in the white paper. In order to ensure the reliability of V2X messages, it is possible to use message authentication using PKI. However, since the PKI certificate itself contains information such as the holder of the certificate, it is possible to track the location of a particular vehicle (see Figure 62). As a technique for solving the privacy issues involved in the use of such PKI, a method that uses short-term pseudonyms is being considered. Each vehicle can protect the privacy of its location information by using multiple pseudonyms that are updated frequently. Such a method is being considered by several organizations. For example, the Security Credential Management System (SCMS) proposed by the Automotive OEM Consortium and the U.S. Department of Transportation (USDOT) [54], [55], and the Coordinated ITS Certificate Management System (CCMS) developed by the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI), China's C-SCMS, developed by the CCSA (China Communications Standards Association), and others. Any of these specifications use pseudonym certificates with short expiration dates to protect privacy, and they are renewed periodically to make them difficult to trace. However, it may be difficult for a vehicle to store a large number of pseudonym certificates or to connect to the back end frequently. Therefore, it is necessary to solve the problem method of managing (issuance, storage, and revocation management) a large number of pseudonym certificates.

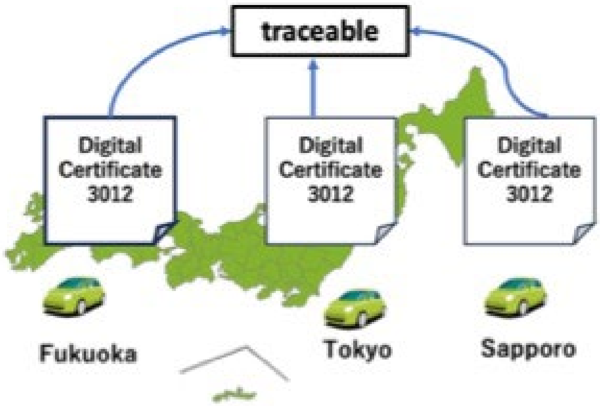


Figure 5.2.62 Privacy issues when using digital certificates in CV

Figure 5.2.63 shows the basic configuration and procedures of the V2X credential management system based on PKI.

(1) Register a vehicle and have the registration certificate issued by a certification authority for registration. (① and ② in the figure)

(2) The Pseudonym Certificate Authority (PCA) issue a pseudonym certificate (③, ④ in the figure)

(3) The vehicle (sender) signs the V2X message using the pseudonymous certificate and sends it (⑤, ⑥ in the figure)

(4) The vehicle receiving the V2X message (receiver) verifies the message using the pseudonymous certificate (⑦ in the figure)

(5) After a certain period of time, the vehicle (sender) updates the pseudonym certificate (⑧ in the figure).

(6) When the vehicle (receiver) receives a message signed with an invalid pseudonym, it notifies the MBA, which forwards the information on the invalid usage to the revocation authority (RA). The revocation authority (RA) notifies the pseudonym revocation request to the pseudonym certificate authority (PCA), obtains ID information as a reply, and updates the revocation list (⑨-12 in the figure).

(7) The vehicle (receiver) obtains the revocation list from the revocation authority (RA) as appropriate (13 in the figure).

It is pointed out that the above procedure requires the operation of five certification authorities, which complicates the entire system.

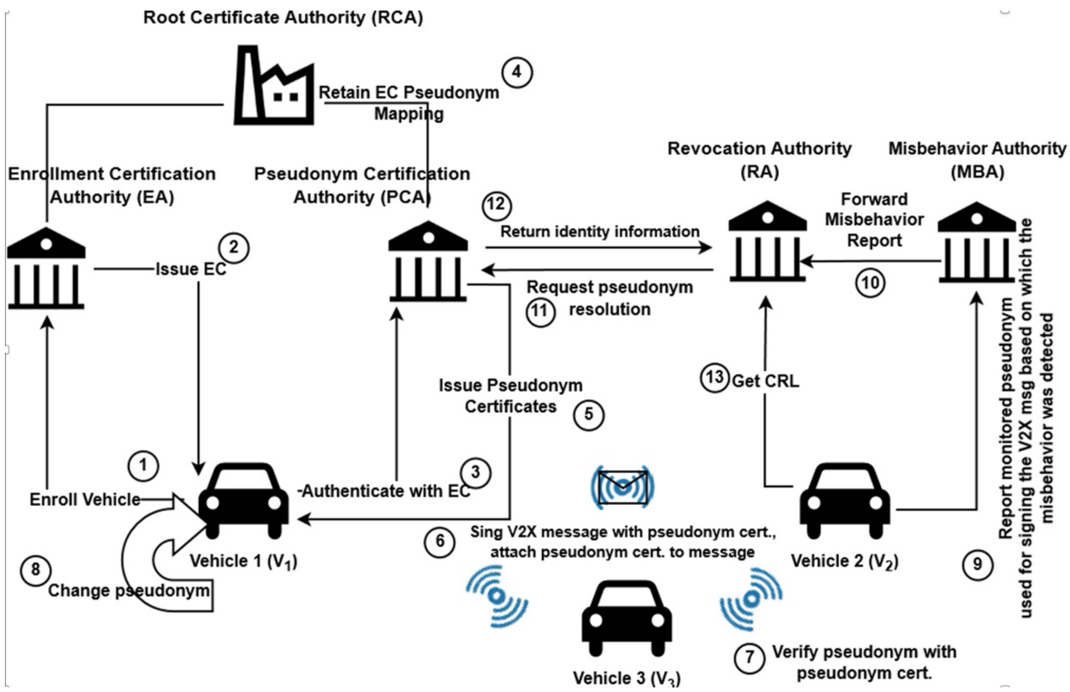


Figure 5.2.63 Basic configuration and procedures for a V2X credential management system based on PKI

It is impractical to manage a large number of pseudonymous certificates as described above. For this reason, the U.S. Department of Transportation (USDOT) has proposed a scheme called Butterfly Key Expansion, which can efficiently generate an arbitrary number of public keys. This scheme is an algorithm that can create multiple pairs of private and public key from a single pair of private and public keys in public key cryptography. This scheme enables the efficient issuance of a large number of OBE (on-board device) certificates. As shown in Figure 5.2.64, the OBE expands the original private key using the private key seed to create multiple private keys. On the other hand, the original public key and public key seed corresponding to the original private key are sent to the registration authority. At the registration authority, the public key sent from the OBE is expanded into multiple public keys using the public key seed corresponding to the private key seed. The pseudonym certification authority signs the expanded public keys and issues multiple pseudonymous certificates. This method makes it possible to efficiently create an arbitrary number of pseudonym certificates even within the limited communication bandwidth between the OBE and the registration authority.

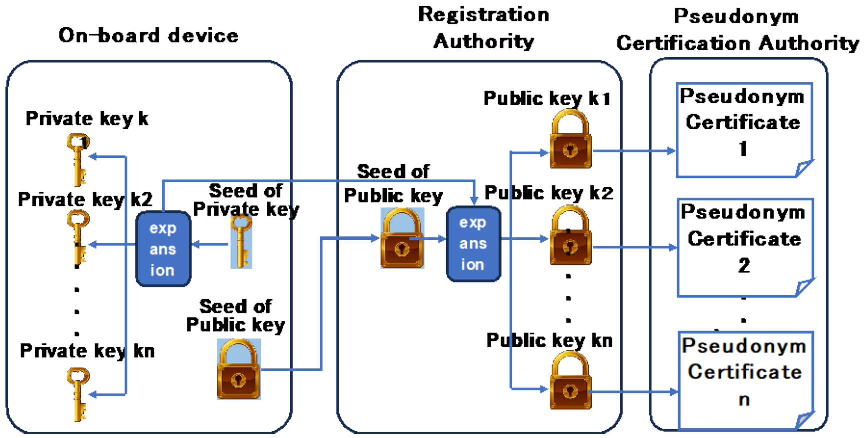


Figure 5.2.64 Method for issuing a large number of pseudonymous certificates (Butterfly Key Expansion)

SCMS has also proposed a method of inserting Linkage Values into pseudo certificates as a solution to the problem of managing the revocation of a large number of issued pseudonym certificates. As shown in Figure 5.2.65, this scheme uses a hash chain to provide a chain and ordering to linkage values, so that when a pseudonymous certificate at a certain point in time is revoked, all subsequent virtual certificates chained to the linkage values embedded in that pseudonymous certificate can be efficiently revoked.

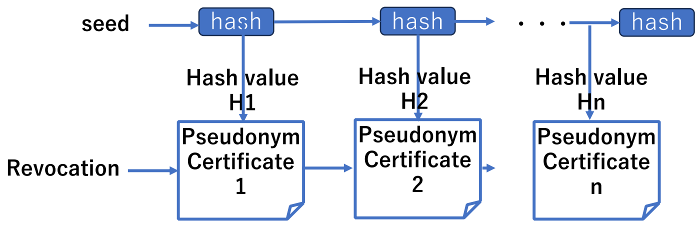


Figure 5.2.65. How to revoke pseudonymous certificates in batches (Hash Chain)

Decentralized Message Trust and Privacy Protection Schemes

As mentioned above, the centralized pseudonymous certificate scheme based on the PKI shown in Figure 5.2.63 is pointed out to be a problem that makes the system complex. To solve this issue, a de-centralized pseudonym management scheme by introducing a Trusted Computer (TC) as the Root of Trust in the OBE is being considered. The basic concept of this architecture is based on a scheme called DAA (Direct Anonymous Authentication), which is a cryptographic protocol using group signatures to enhance user privacy in the remote authentication process. TCG (Trusted Computing Group) has adopted this mechanism. By applying this technology to the V2X environment, a decentralized approach is being considered that shifts the starting point of trust from the complex and centralized PKI-based back-end infrastructure to the vehicle itself by installing a TC in the vehicle [56].

As shown in Figure 5.2.66, a de-centralized pseudonym management scheme would follow these steps.

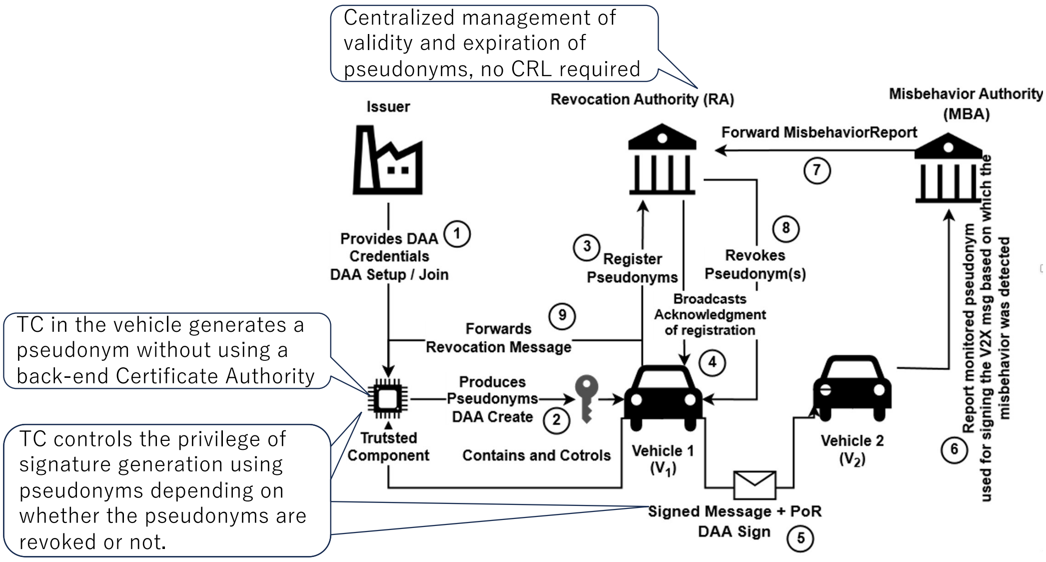


Figure 5.2.66 Overview of decentralized message reliability and privacy protection schemes

(1) The setup/join procedure allows the issuer to verify the legitimacy of the TC and generate a credential for later use in creating a pseudonym. This credential does not contain any information about the vehicle. In addition, since the TC's signature key is not linked to the vehicle and is authenticated blindly by the issuer, it is impossible for the verifying vehicle to link the pseudonym to the TC's identity, i.e., the long-term EC (Enrollment Certificate) of the vehicle. (① and ② in the figure)

(2) A vehicle may use a pseudonym after it has been registered with a revocation authority (RA). (③ and ④ in the figure)

(3) The vehicle (sender) signs the V2X message using the pseudonym and sends it to other vehicles. (⑤ in the figure)

(4) The vehicle (receiver) that receives the V2X message verifies the message using the group public key corresponding to the pseudonym (⑦ in the figure)

(5) If the vehicle (receiver) receives a message signed with an invalid pseudonym, it notifies the MBA (Misbehavior Authority), which forwards the information on the invalid usage to the revocation authority (RA). The revocation authority (RA) notifies the TC of the request for revocation of the pseudonym and revokes the corresponding pseudonym in the TC (⑥-⑧ in the figure).

The anonymity of this scheme is based on the DAA's group signature scheme, as shown in Figure 5.2.67. A group signature is a signature created by a body belonging to a group that does not contain information identifying the signer, and that allows the recipient of the signature to verify that the signature was created by a correct signer belonging to the group, using the group public key.

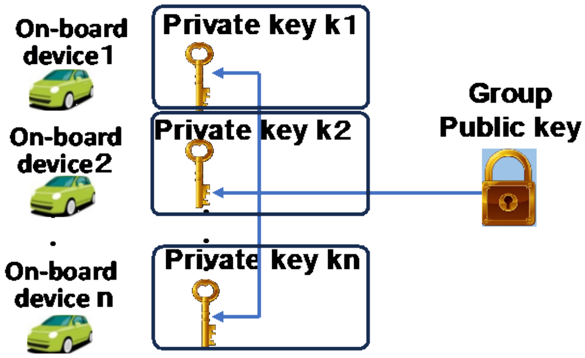


Figure 5.2.67 An Image of Group Signature Key Management Mechanisms

Another important difference from conventional PKI-based schemes is that the revocation process does not require an extensive Certificate Revocation List (CRL). Specifically, a pseudonym cannot be used by a TC unless it has been registered with a revocation authority (RA) and revoked. When a pseudonym is revoked by the RA, the information is notified to the car side, and the status of the corresponding pseudonym is updated (revoked). In this way, the availability of a pseudonym is completely synchronized with the revocation status of the pseudonym managed by the RA, and the availability of the pseudonym by the TC can be strictly controlled. Therefore, this method eliminates the need for distribution and management of CRLs required for PKI and can be applied to large-scale systems. Furthermore, since pseudonyms are hashed at the time of registration, even if a TC uses two pseudonyms, it is difficult for the RA to link the two pseudonyms.

5.2.3.6. Authentication

With the result of studying characteristics of 5G in the use case of connected vehicle from section 5.2.3.2 to section 5.2.3.5 focusing on security, authentication can be considered as a common security issue.

This section summarizes the security issues from the perspective of authentication (see Figure 5.2.68).

- User authentication by vehicle
  The vehicle authenticates the driver and passenger.
- Vehicle Authentication by mobile carrier
  The mobile carrier authenticates the vehicle that connects to the mobile network. Here, it is assumed that the vehicle authenticates the user (driver or passenger) of the vehicle, and that the mobile carriers authenticate the communication module equipped in the vehicle.
- User authentication by network slicing provider
  The network slicing provider authenticates the user of the network slicing. The network slicing provider is assumed to be a service provider because the quality of network and security required for each use case of connected vehicle (service) are different. If the

available use case of connected vehicle depends on the model of the vehicle, the network slicing provider authenticates the vehicle. If the available use case depends on the privilege of user, the network slicing provider authorize the user. Both cases shall be considered.

- Authentication by MEC infrastructure
  If the use case of the connected vehicle may depend on the vehicle model, MEC infrastructure authenticates the vehicle. If the use case of the connected vehicle depends on the user (driver or passenger), MEC infrastructure authenticates the user. Both cases shall be considered.
- MEC application authentication by the MEC infrastructure
  The MEC infrastructure authenticates the MEC application.
- Vehicle authentication by vehicle (V2V), Roadside device (V2I), or Pedestrian (V2P) authentication
  In C-V2X, vehicles, roadside devices, and pedestrians authenticates vehicle.
- Authentication by the service provider
  If the service depends on the model of the vehicle, the service provider authenticates the vehicle. If the service depends on the user (driver or passenger), the service provider authenticates the user. Both cases shall be considered.

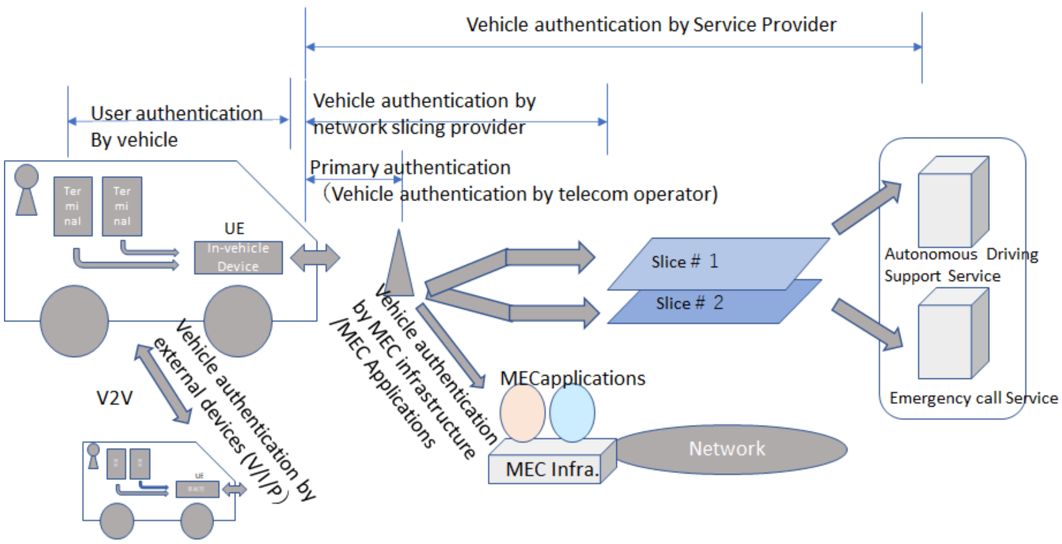


Figure 5.2.68 Summary of authentication in Connected Vehicle

Service providers may use network slicing to provide MEC application which requires specific network and security qualities. In this case, it is assumed that the service provider, network slice provider, and MEC application provider are the same entity.

5.2.4. Summary of Use Case Connected Vehicle Security

As mentioned above, regarding the security of Connected Vehicle, we have summarized the security issues in 5G networks based on the discussions in related standards and forums. The 5G security functions being considered by 3GPP and ETSI are currently in progress, and changes and specifications are expected to be materialized in the future. Based on these progresses, we plan to consider specific measures for security issues.

5.3. FinTech Security Use Cases

5.3.1. Introduction

As development of 5G has progressed, new FinTech services are being created and developed as FinTech firms as well as companies in other fields are connecting to networks of existing financial institutions to offer services that have traditionally been conducted face-to-face. There is, however, an increasing need to think more deeply about and further study security issues, while still considering customer convenience, as planned use cases that demand user authentication increase and as firms from different fields become involved in FinTech so that services that require authentication and authorization between these different firms increase, as well. This chapter will discuss the different security issues arising from specific FinTech services as well as other security related issues that require further study.

5.3.2 5G FinTech Services

In this section, before getting into study issues related to FinTech security, provides a summary of the current state of FinTech services as well as the state of those services as they relate to 5G.

5.3.2.1 Major FinTech services

Figure 5.3.1 categorizes FinTech services into financial products and payments services, which can themselves be divided into those that target individual consumers and those that target businesses.

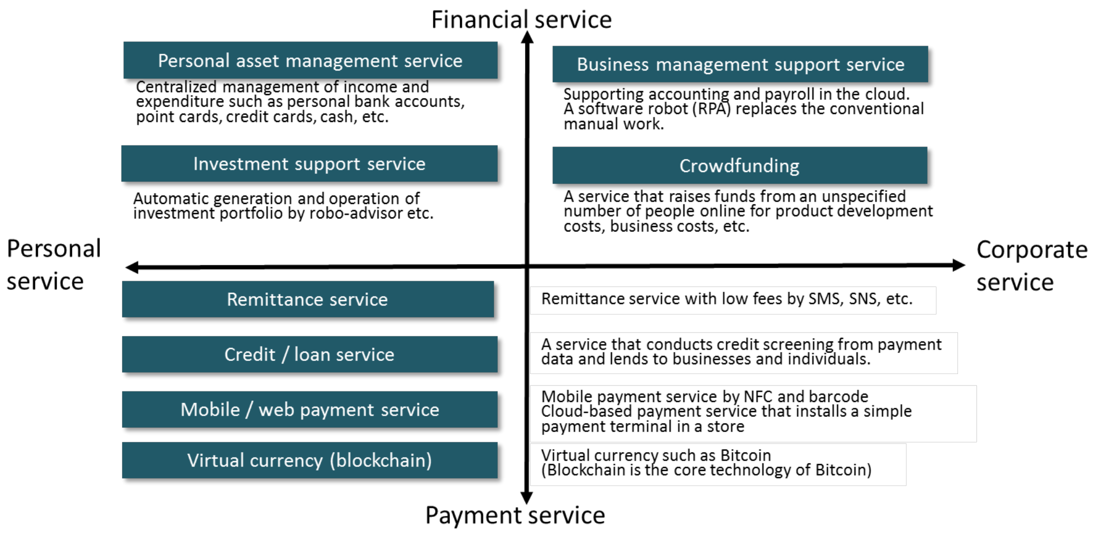


Figure 5.3.1 Main FinTech Services

5.3.2.2 Financial services using 5G

Services that financial institutions have offered online have been until now aimed at increasing convenience for users.

Examples include:

- Internet banking services that act as a virtual bank counter, allowing customers to check their balances as well as transfer and remit money online.
- Payment services that can be used online and in stores, facilitating retail payments via the customers mobile device rather than a physical card.
- Asset management services with AI-powered advisors.

As shown in Figure 5.3.2, as 5G continues to develop, FinTech services are also expected to continue to grow to include services that connect different industries, the creation of new services that use data from a variety of industries, and new services that are optimized for each individual user.

Examples of these anticipated services include:

- Individual authentication services based on use and activities.
- Authentication services for individuals based on usage and behavioral data.
- Financing services based on payment data.
- Insurance services based on driving records.
- Health food discount based on healthy lifestyles that are connected to insurance providers.
- Billing services based on usage (time, volume).

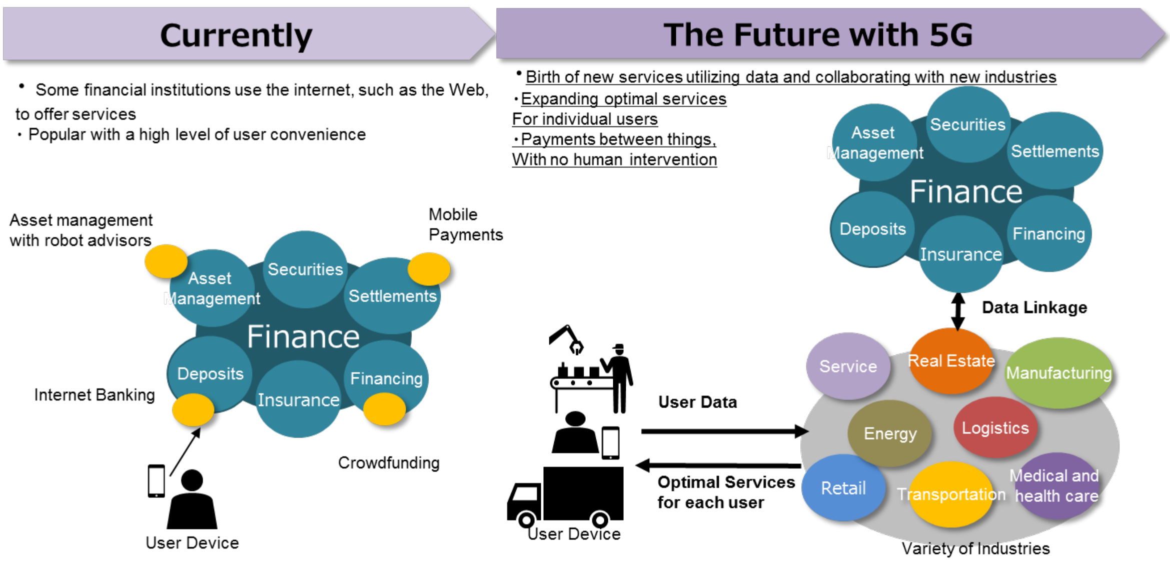


Figure 5.3.2 Fintech services using 5G

5.3.3 Collaborations between FinTech firms and other Related Organizations

FinTech firms and other related organizations were asked about their expectations for FinTech services that will utilize 5G.

5.3.3.1 ACSiON, Ltd.

Seven Banks's authentication service provider ACSiON, Ltd. offers the following products

- proost

A personal authentication platform that offers a method utilizing image processing technology to match an individual's photo data with their photo identification. It can also be used to implement a strict personal authentication process with information collected from other resources, as well.

- Detecker

An AI powered big data analysis platform that continuously monitors and detect fraud and unauthorized access to systems.
(1) Service Outline: Detecker
This platform monitors for fraud at each stage of a transaction, from when a company's customer purchases a product or service until they utilize that product or service, utilizing knowhow and experience from Seven Bank.

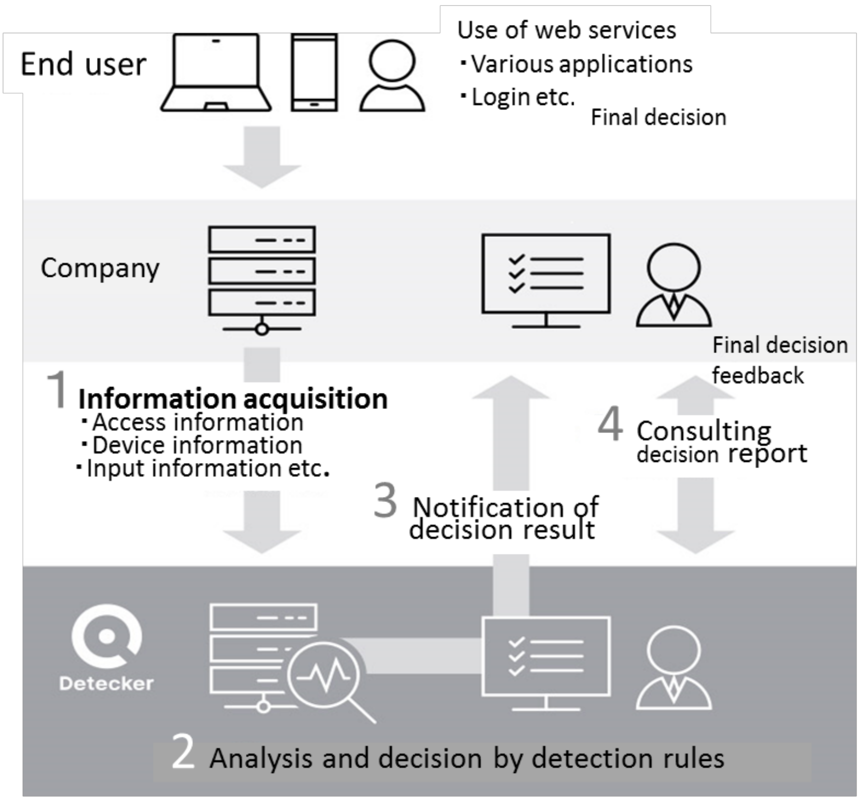


Figure 5.3.3 Service Overview (from the ACSiON, Ltd. Website)

a. Aims

- As a joint platform that detects fraud in areas such as unauthorized account openings, firms that utilize this service will allow sharing of information with each other, so that all participating companies can provide safe and secure services to their customers.
- The service will grow stronger as it detects and prevents unauthorized uses, as unauthorized uses are detected they are then added to its database of examples to further detect and prevent such actions in the future.

b. Examples of preventable attempts of unauthorized access

- Fraudulent online applications for services such as opening a bank or credit card account.
- Unauthorized access to a user's online account (impersonation or identity theft).
- Unauthorized access to internet banking accounts (access to accounts by third parties).
- Unauthorized online purchases.

(2) Expectations for 5G

5G is expected to bring about stronger authentication processes with ways to identify individuals that go beyond facial recognition.

- Using 5G's characteristic low latency to monitor behavior and exchange authentication data at high speeds between devices.
- Using 5G's 28 GHz high frequency band's radio directivity for accurate position locationing.

Figure 5.3.4 Strengthening Personal Authentication with 5G

5.3.3.2. Collaboration with the Fintech Association of Japan

(1) Overview of the Fintech Association of Japan

a. Overview

The mission of the Fintech Association of Japan is to conduct activities, collaborate, cooperate, and exchange ideas with relevant bureaucracies and organizations in Japan and abroad, to promote open innovation and an environment that promotes the creation of new FinTech services, and contributes to sound business development an active FinTech ecosystem that can contribute to Japan's presence in the global financial IT business world. The association's membership includes about 270 firms, including 130 FinTech startups, as well as financial institutions, telecommunication firms, and construction firms.

b. Committee Structure

The table below lists the Association's committees.

Table 5.3.1　Committee Structure of the Fintech Association of Japan (from the Association's website)

#	Subcommittee name	Overview
1	Compliance	Examination of cross-cutting regulations, eKYC, etc. Attended "Online Transaction research society in the Fintech Era" with the Financial Services Agency.
2	API/Security	API and security research. Attended API study meetings at JBA, FISC, Ministry of Economy, Trade and Industry, etc.
3	Cashless	Examining issues related to payment, promoting cashless payments. Participated in installment sales subcommittees, card API study groups, etc. at the Ministry of Economy, Trade and Industry.
		Examination of promotion of electronic receipts and improvement of accounting / tax payment environment.
4	Loan	Examination for new loan business model, examination of environment improvement.
5	Investment asset management	Examination of environment improvement in line with Fintech, exchange of opinions with other organizations.
6	Insurance	Examination / study session on InsurTech, examination on environment improvement.
7	Capital Markets	Study / examination about ICO / token sale. (Global case, etc.)
8	Remittance	Discussion about eKYC and related regulations.

		Research on the impact of the lifting of payroll and the efforts of each company.
9	RegTech/SupTech	Examining the ideal form of new governance utilizing data and technology represented by RegTech / SupTech, and the ideal form of using technology for supervision and regulatory compliance.

(3) Expectations for 5G

The authors participated in the 20th meeting of the Fintech Association of Japan's API and Security Committee. The first presentation session of the meeting was entitled "5G and Fintech", which included a panel discussion. In this session, the CEO of Kuwadate, Ltd., KUROSAKA Tatsuya outlined the digital twin concept, in which 5G and sensors work together to follow and record the data of people, their behavior and location, as well as the surrounding environment, in real time.

KUROSAKA explained the various new services that businesses working in the field of FinTech are expected to provide, including "scoring services" using real time data, moving from cashless to cashier-less payment systems, personal authentication services that connect telecommunications and finance, and new financial services through the authentication of things from people.

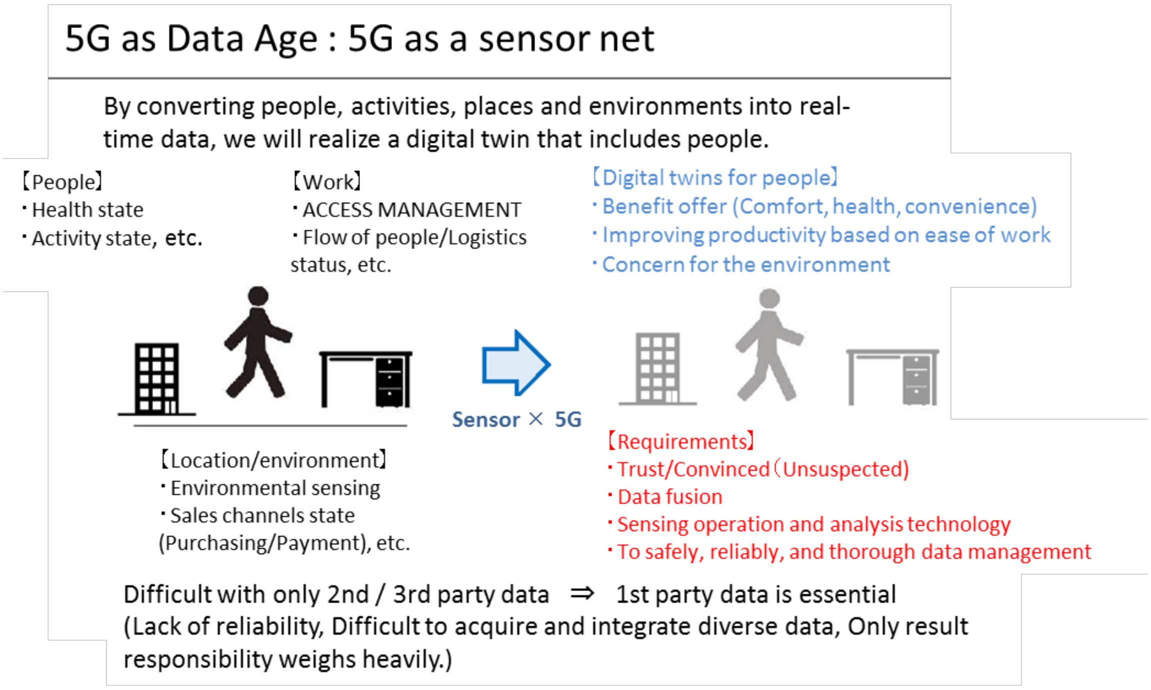


Figure 5.3.5 Overview of 5G Related Services and Products (source: KUROSAWA Tatsuya, Kuwadate, Inc., "5G and FinTech", 20th meeting of the Fintech Association of Japan's API and Security Committee.)

5.3.4 Points to consider for security and financial services with 5G

Here are some financial services that are expected to use 5G.

These new services can be sorted into categories that include Cross industry collaborative transactions, financial services that are linked to vehicles; Individualized small private transactions, changes to financial services based on an individual consumer's daily behavior; the realization of the self-explanatory flexible transactions based upon usage; and high-speed transactions for use in, for example, trading stocks.

Table 5.3.2 Financial Services expected to utilize 5G

#	Financial Services
1	Transactions through collaborations with other firms: Example 1) Automatic payments at coin parking lots when parking and leaving. Example 2) Using IoT to check the state of driving and vehicular usage.
2	Transactions that are more personalized, smooth, and private: Example 1) Advising on and realizing dynamic pricing through analyzing usage, health levels, or daily shopping habits. Example 2) Dynamic gasoline pricing based on distance travelled. Example 3) "Robot Advisor Services" (for example, utilizing data from the daily use of smartphones to provide portfolio management and investment advice).
3	Flexible payments based on usage: Example 1) Payments based on time/impression rather than frequency of use. Example 2) Payments triggered by the wearing of clothes.
4	High speed transactions: Example 1) High speed transactions for financial instruments such as stocks.

Security issues that must be considered in order to realize these services, as shown in figure5.3.6 include authentication between service providers with the realization of a cross industry collaborative service data API and personal authentication that can be shared in real time for that different firms to allow for collaboration across individual user devices and networks.

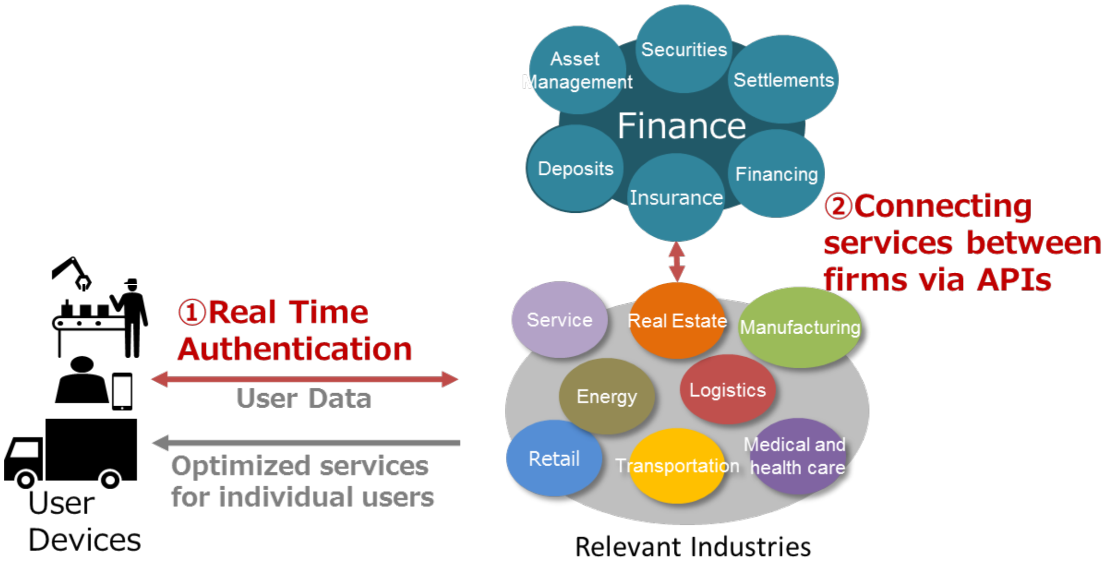


Figure 5.3.6 Security Related Points to Consider

5.3.5. Issues for Authentication Between Service Providers and Points for Operators to Consider

5.3.5.1 Changes to financial firm's service models

Although financial firms at the moment offer their own personal customer services vertically, as different industries using FinTech begin to offer new, unique services such as Money Forward, for example, as well as with the implementation of the Revised Banking Act, many financial firms have begun to publish their own APIs.

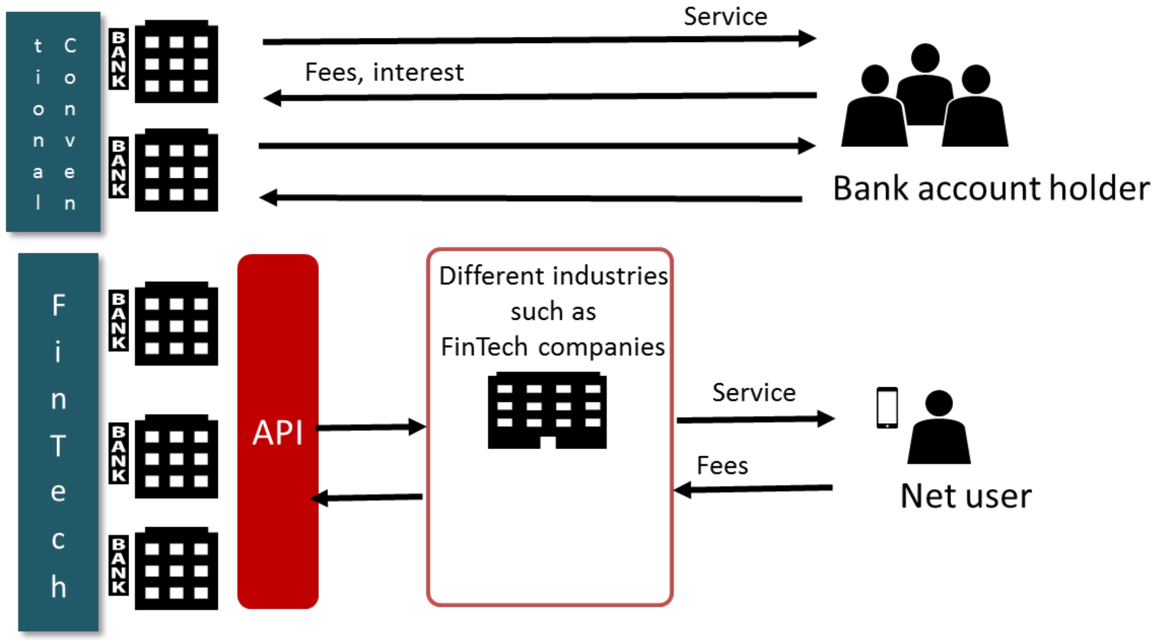


Figure 5.3.7 Changes in Financial Institutions' Business Model

5.3.5.2 Revised Banking Act

The Act for Partial Revision of the Banking Act was approved on May 26, 2017, and enacted on June 2, 2018. With this revision, FinTech firms, with the agreement of individual customers, can access accounts and exchange information with financial institutions. The following issues must be considered, however.

- Security issues
    - Information related individual authentication, such as IDs and passwords, which are retained by firms other than financial institutions can be used to access financial services.
    - Technical problems with account information transactions.
    - Since APIs are not published for inquires of account information from financial firms, fintech firms need to acquire information from analysis of financial firms' websites.
    - As APIs are not published for inquiries for account information from financial institutions, FinTech firms must receive such information by analyzing the websites of financial institutions.
    - Problems related to open innovation.
    - As the legal position of FinTech firms is unclear, collaboration between financial institutions and FinTech firms cannot progress due to several issues including the uncertainty around financial institutions and the high level of security needed by financial institutions from FinTech firms.

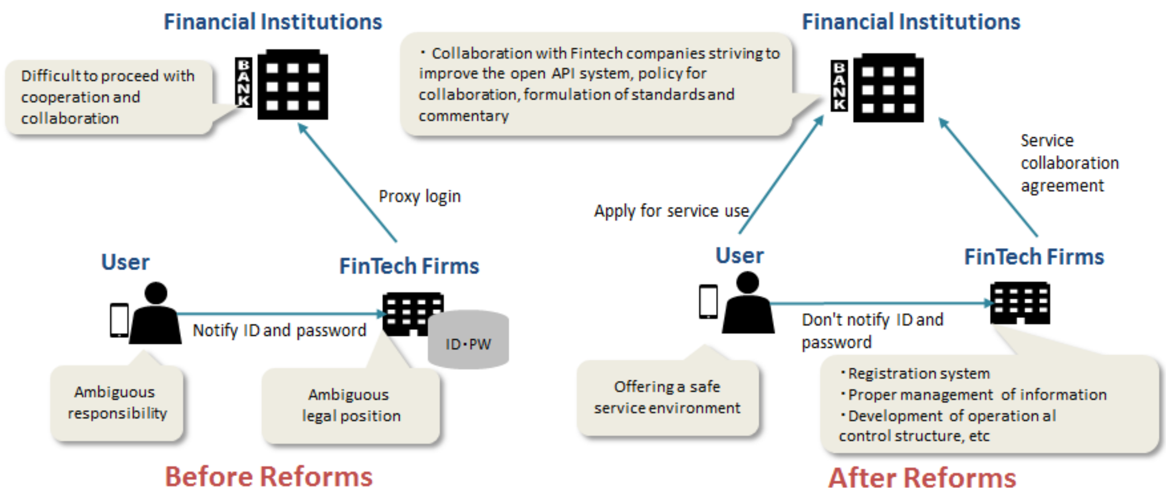


Figure 5.3.8 Revised Banking Act

5.3.5.3 An example authorization process using a financial-grade open API

In order to securely use an open API, users need to authorize FinTech firms to allow access to their financial institutions. In order to facilitate this, it has been recommended that the financial world use the OAuth 2.0 protocol for authorization in their open APIs.

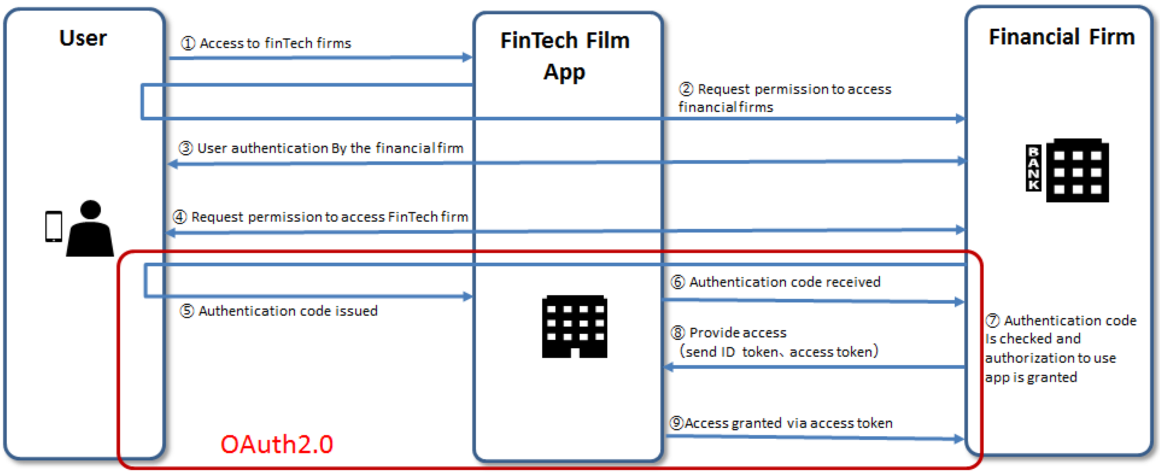


Figure 5.3.9 Example of an Authorization (OAuth 2.0) Process Flow using a Financial Open API.

5.3.5.4 Industries currently targeted for Financial API

Listed below are businesses that currently use financial APIs. Generally, services for individuals are those accessed via PCs and smartphones.

Table 5.3.3 How Financial APIs are Currently Used

#	Classification	Contents
1	Household account book service	・ Web service that automatically creates a household account book by collectively managing multiple accounts of banks and securities companies. ・ A household account book is automatically created based on bank deposits and withdrawals and card information.
2	QR code payment service	・ QR code payment service using smartphones. ・ Charge and settle from a pre-registered bank account or credit card.

5.3.5.5 Examples of Financial Services using IoT Devices

As 5G becomes more widespread, the following financial services are planned to be offered with products such as automobiles and household electronics.

Table 5.3.4 Expected FinTech Services on IoT Devices utilizing 5G

#	Classification	Service	IoT device
1	Car	・ Payment for gasoline (Price fluctuations according to mileage, amount, etc. ・Transit fare (GPS linked, payment according to distance other than highway) ・ Parking lot price (charged by the time you parked) ・ Drive-through ・ Purchase digital contents and game items ・ Sharing (charged according to mileage) ・ Insurance (Insurance according to safe driving, mileage, driver, etc.)	Car (In-vehicle terminal, etc.)
2	Industry	・Lending of corporate computer resources at night ・Equipment leasing (Payment according to usage time) ・Financing ・Inter-company settlement	System equipment such as servers
3	Sharing (token) economy	・Person-to-person settlement Example: The lender pays the entire electricity bill, and the borrower is billed individually according to usage. Example: The lender pays the entire electricity bill, and the borrower is billed individually according to usage. (Example: the lender to pay the electric bill of the whole, the individual claims in accordance with the available to the borrower, Trading of surplus electricity from private power generation.) Target: Utility bills, telephone, internet, home appliances, private lodging, cars, bicycles, parking lots, water servers, etc.	Home appliances, etc.
4	Settlement	・Settlement by biometrics at unmanned convenience stores, etc.	Cash register

5.3.5.6. Financial Open API Security Issues with IoT Devices

The major security issues with financial open API authentication processes on 5G powered IoT devices are listed below.
The following
(1) Attacks on IoT devices: unauthorized access, tampering, impersonation, etc.
(2) Attacks on the communication path between entities: communication data eavesdropping and tampering.
(3) Attacks on FinTech company and financial institutional systems: exploit vulnerabilities on system and network devices, DDoS attacks, etc.

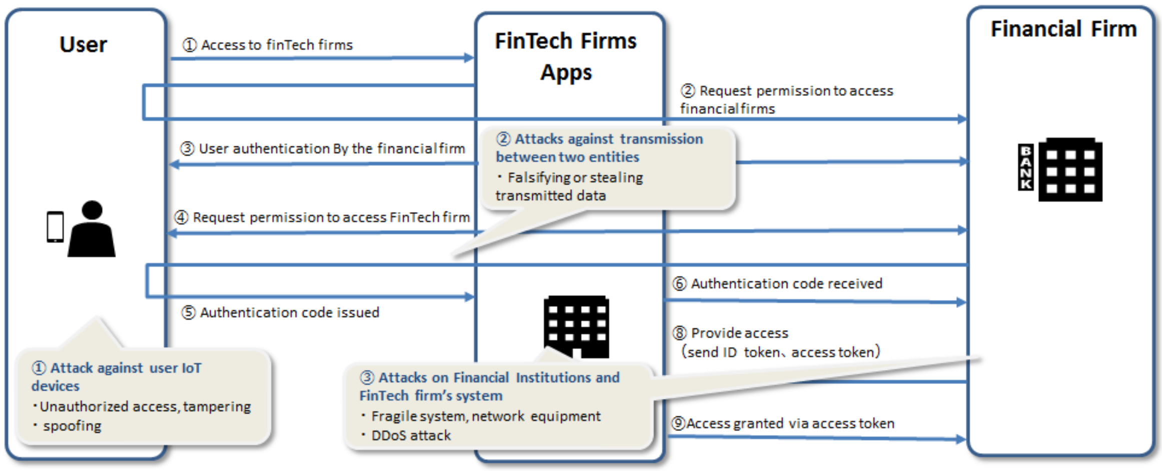


Figure 5.3.10 Security Considerations for Financial Open API s

5.3.5.7 Points for operators to consider concerning security

(1) Attacks on IoT devices
① Tampering and leaks of credential information
In the case of IoT devices, an environment where anyone can access a device increases the possibilities of physical analysis and operation of the device. Telecommunications firms, when using contract credentials to authenticate connections to their networks, can use tamper resistant credential storage functions and store the credentials via secure storage. Operators that manage and operate IoT devices with unique credential data should also store these credentials on authorized, tamper resistant authentication devices.
② IoT devices used over a long period of time
As users generally purchase new mobile phones and smart phones every few years, it can also be expected that SIM cards will also be replaced every few years, as well. However, with the expected wide-spread introduction of 5G's special characteristic of massive multiple connections a single IoT devices can now expected to be used over a long period of time, making SIM cards more difficult to replace. Currently, a secret key is stored on SIM cards for user authentication which is written on the SIM card by the manufacture, which cannot be rewritten. Therefore, the SIM card itself must be changed if a security threat is discovered. Considering this risk, it should online modifications of SIM cards should be allowed.

(2) Attacks on communications between entities

Network slicing will be introduced with 5G. Each slice will be able to be virtually independent from each other on the network so as to not adversely affect other slices, allowing an individual slice to use an encryption algorithm that is suitable for the service being run on it. For example, in the case of an IoT device, if a battery needs to be used continuously over a long period of time, it is possible to use a low power, low energy algorithm such as a light encryption. 3GPP SA3 Phase 2 studies will be held for network slicing security, which is outlined in section 4.2.4.3.1.

(3) Attacks on FinTech firms as well as financial company organizations

It is necessary to further understand how access control should function for various types of data collected for different services as well as to authenticate and authorize access to the application and network layer. For 5G, this may mean implementing an access control policy for services that require a secondary authentication protocol that forms the basis of a uniform secure access management system. Secure authentication can be realized using AKMA (Authentication and Key Agreement for Applications) for systems that communicate directly with each other without needing to go through a centralized point.

It is also necessary for trust service mechanisms to ensure data is being safely and security distributed through cyberspace, including ensuring reliable data transmission and preventing data tampering and impersonation, in order to realize Society 5.0. Key players in this field through the use of financial-grade open APIs will include users, firms that work on related IoT devices and networks, FinTech-related firms that offer such services as well as financial institutions. Looking at this from a cybersecurity perspective, in which attacks are expected against data transmission channels, a trust service infrastructure built between these varied players is necessary in order to ensure data is transmitted over a secure network.

The MIC established the Trust Service Working Group as part of the Research Group for Platform Services in January 2019, and is now currently working on the issues related to the following trust services:

- Authentication of an individual's true identity (electronic signatures).
- Authentication of an organization's identity (authentication for the target organization, website authentication).
- Authentication of the true identity of things connected to IoT devices.
- Ensuring the proof of data's existence and that it has not been tampered with (time stamp).
- Ensure the data is delivered (e-delivery).

5.3.6 Points for operators to consider and security issues related to real time authentication

5.3.6.1 Issues related to Authentication

Although currently personal authentication is mostly handled through ID/password combinations or login names, recently biometric data has begun to be utilized. However, it is a burden on users to register this data. Examples for whom this is true include health care workers and equipment maintenance personnel. In addition, when biometric authentication is required, it is often the case that biometric data must be retained when needed to authenticate media which is carried by individuals, making this unsuitable for cases which connect data between various firms, such as closed services, that 5G networks are expected to handle. As this is the case, processes that are more convenient for users, such as unique IDs assigned to mobile phones or ID cards, are increasing. However, although user convenience is high with these authentication processes, the possibility for falsification also increases.

5.3.6.2 Individual Authentication Possibilities with 5G

5G is expected to be able to identify human behavior through high speed, high-capacity sensors, GPS, and purchasing data, as well as identify people online through visual authentication. For example, the Mithra Project at the Graduate School of Information Science and Technology, the University of Tokyo Social ICT Research Center is researching the ability to "lifestyle authentication", where big data such as geographic data from smart phones and wearable devices is analyzed to provide user authentication.

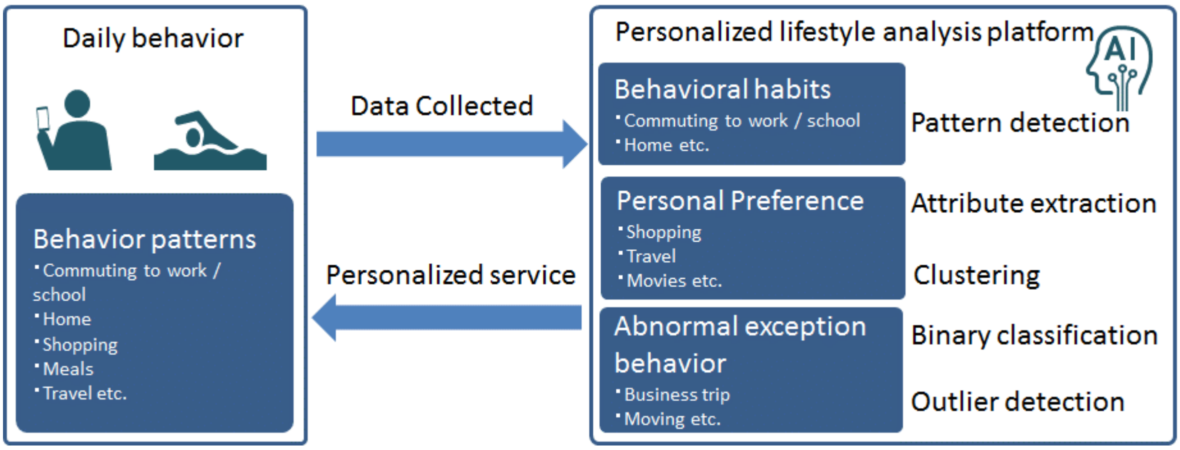


Figure 5.3.11 Overview of how daily behavior can be analyzed via of data input and output
Source Lifestyle authentication technology using lifelogs" website at the University of Tokyo

5.3.6.3 Security Issues with Lifestyle Authentication

Security issues that arise from the realization of lifestyle authentication include:

In order to conduct lifestyle authentication, it is necessary to analyze and efficiently collect a massive amount of visual and geographic data. This data cannot all be uploaded and processed in a cloud computing system, but instead must use edge computing, at a location on the network that is close to the user, which will reduce latency during data analysis and allow for the realization of utilizing broadband applications in real time. One technology that will facilitate this is Multi-access Edge Computing (MEC), a standard which is being promoted by ETSI.

The MEC platform replaces cloud servers to facilitate quicker responses from IoT devices that are located in their vicinity. It has been shown that when data is processed on MEC platforms, the response time from IoT devices is shown to be reduced. This brings about an additional advantage with the reduction of the need for transmission capacity with the reduction of data that is sent to the cloud. On the other hand, in order to move computer resources and data storage from the cloud to the MEC platform at the edge of the access network, there needs to be a network connecting IoT devices and the MEC platform. This network will be accessible to the many users of the MEC platform, which brings about greater security risks. (Attacks can come the MEC platform or from applications that other platform users have developed, etc.). Currently, these issues related to the MEC are being studied not only by the ETSI but the 3GPP as well, which are summarized in section 5.2.3.4.

(2) Preventing tracing of terminal identifiers.

TMSI will be used instead of IMSI in order to prevent the tracking of terminal devices. Although the transmission of the plain text ISMI is no longer a problem, issues related to the tracking or specifying the location of a device still exists.

(3) Precise Personal Authentication

The analysis of GPS location data of an individual's movements is currently possible. With additional progress on 5G, additional behavioral data can also be collected and analyzed, bringing with its improvements to personalized capabilities. It is expected that financial services that require personal authentication will require more advanced personal authentication protocols in the future.

5.3.6.4. Points for Operators to Consider Regarding Security

(1) Security issues when using Edge computing (MEC Platform)

The same countermeasures implemented to prevent impersonation, data falsification and data leakage in cloud networks are also needed on MEC platforms. For example, as there will be direct connections between IoT devices and MEC platforms that will not go through a cloud network, further studies are needed on the various types of access data controls integrated into services and authentication and authorization to access the application layer, which is used by many different users, as well as the network layer.

Additionally, the network will require low latency and high throughput as behavioral data from IoT devices is sent back and forth between those devices and the cloud and MEC platforms. Using the network slicing functionality that is characteristic of 5G will allow theoretical networks to be safely utilized to meet these requirements.

(2) Terminal Identifiers

5G uses SUPI, which corresponds to IMSI from previous telecommunication generations, as the Identification number, which is recorded on SIM card, from which authentication occurs using the SUCI, which is a randomly encrypted identifier using the SUPI as the public key of the network operator. This resulted from privacy concerns related to the IMSI identifier. Additionally, devices that have already been authenticated are given a temporary identifier called a GUTI. However, for mobile telecommunication firms must consider cases during which updates do not occur for some time, so the specifications in 5G can state that updates occur on a more regular basis.

(3) Improving the accuracy of personal authentication

Biometric authentication is expected to be implemented, for example, use of facial features or fingerprints. However, the following issues still exist for biometric authentication:

a. Shared uses between various services

Up until now, biometric systems, using fingerprints, veins, irises, etc., for biometric data has been safely secured by being managed for an isolated system. In order to use biometric authentication across different, shared systems, it is necessary to register the biometric data in each system, a burdensome process which will limit the widespread use of biometric data for authentication.

b. Ensuring the privacy and security of biometric data

Biometric data includes extremely sensitive data about personal characteristics, including race, ethnicity, and health status. Looking at it from the standpoint of privacy issues, strict management of this data is required. Biometric data is such that it cannot be altered or discarded over the course of an individual's lifetime, so it would be very difficult to recover safely and securely after just one data breach, which could result in the occurrence of such crimes as identity theft.

One solution to this problem is the Public Biometric Infrastructure (PBI) template that has been proposed by Hitachi for use. Biometric data such as veins or fingerprints are used to create a public key that cannot be reverted to its original biometric source data, creating a digital signature that is able to use biometric data to for personal authentication. The currently used public key infrastructure (PKI) authentication systems such as electric IDs like IC cards requires strict management of authentication data. With PBI, however, biometric data can only be converted one way (as forward conversions are easy to do while reverse conversions are not) and this data is newly generated each time authentication is required. The user then does not need to manage the data nor is not possible to restore the biometric data from the digital signature.

Up until now, in order to keep biometric data secure, authentication functions utilizing it have been kept within individual, closed environments. However, if PBI is used, it can be deployed in the cloud and shared across many different services.

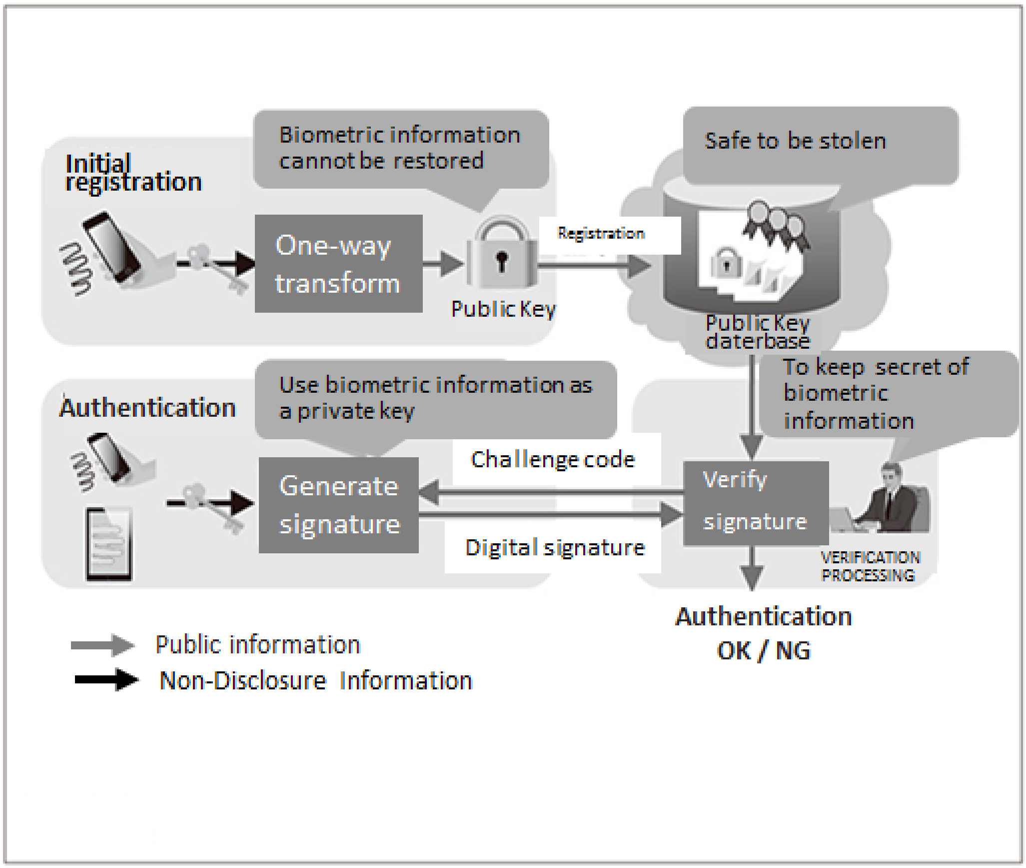


Figure 5.3.12 Public Biometrics Infrastructure Template (source: Hitachi website)

5.3.7 Additional research and validation findings for real-time authentication use cases.

Currently, in collaboration with companies that are researching and developing authentication using behavioral data, we investigated the issues and needs of 5G, and evaluated and verified the results of the 2020 use case study.

5.3.7.1. Exploring additional use cases

a. Discussions were held with the Social ICT Research Center of the Graduate School of Information Science and Technology, the University of Tokyo, and Hitachi, Ltd., which has established a social collaboration course on lifestyle authentication. The current issue is that it can be used for authentication during daily life, but it is difficult to authenticate when you do something different from your daily routine (business trip, travel). In that case, it will be necessary to authenticate the person using biometrics or information that only the person himself or herself knows. Also, people who behave similarly. For example, if two people work at the same place and live in the same dormitory, authentication becomes difficult.

One possible use of 5G is during online banking, where it is necessary to confirm the identity of the person in real time at regular intervals while carrying the person around. Also, are the products being manufactured correctly in the IoT factory? It is envisaged that the blockchain will be used to store information such as identification of workers, whether things are being made according to design specifications, testing and inspections, etc.

b. A discussion was held with AnchorZ Co., Ltd. AnchorZ Inc.'s DZ Security® is an authentication technology called Background Authentication® that determines whether the same person continues to use the service even after logging in. Specifically, it adds behavioral information (habits when using the device) to biometric information such as faces and voices that can be learned naturally when using a smartphone and recognizes multiple elements in the background at any time. It continues to authenticate whether the device user is the registrant at any time and prevents the threat of ``spoofing'' without being tied to login. The behavioral information used includes personal habits such as the distance between the device and the user's eyes, and the way the device is tilted. Additionally, all of the data used for authentication is stored within the user's device, making it unnecessary for the service provider to maintain personal information.

※"DZ Security®" and "Background Authentication®" are trademarks or registered trademarks of AnchorZ Co., Ltd. （Reference source: AnchorZ Co., Ltd. Website）

5.3.7.2. Privacy issues in behavioral data

There is the issue of whether using GPS data etc. will violate privacy issues. Therefore, we investigated companies that provide services that utilize location information. Currently, many companies are entering location information services, as shown in Figure 5.3.13. Additionally, the data that this location information providing service companies provide to external companies differs depending on the company, but in addition to location information, it includes information such as gender, age group, place of residence, and place of work. At that time, the location of residence, place of work, etc. will be estimated based on GPS data. Please note that this data has been anonymized so as not to identify individuals.

Figure 5.3.13 List of location service companies (Source: X-locations website)

5.3.7.3. Verification results

Based on the results of lifestyle authentication conducted by the University of Tokyo, it is currently difficult to authenticate individuals using GPS data alone, and it is necessary to improve the accuracy of identity authentication by combining authentication with biometric information, which is also used in Background Authentication®. In addition, the behavior information when using a smartphone, which is used in Background Authentication®, can be said to be one of the effective pieces of information for authenticating the person. By combining multiple types of authentications in addition to GPS data, such as biometric authentication and behavioral information, it is possible to continuously improve the accuracy of user authentication during use. Furthermore, in the future, beyond 5G is expected to improve accuracy by adding various data such as purchase data in addition to GPS data. Regarding privacy issues regarding the use of behavioral data, during the novel coronavirus infection (COVID-19), big data analysis was conducted using GPS data on the number of people at major points as reference information for avoiding close contact. Information was widely provided to the public through television and other means. The data used for this analysis is anonymized and does not identify the individual, so there is less resistance to using personal location information services than in the past. It is also important to take measures such as restricting use for purposes other than identity authentication without the consent of the person in question.

5.3.8. Organizing the relationship of mobile communication in the standardization trend of payment and authentication.

5.3.8.1. Standardization trend survey by FIGI (Financial Inclusion Global Initiative)

FIGI is a collaboration between ITU, the World Bank, and the Bank for International Settlements with the aim of making financial services necessary for economic activity available to all people. research, technical tools, and recommendations. One of these working groups, the SIT (Security Infrastructure and Trust) Working Group, is investigating threats to mobile DFS (Digital Fintech Services).

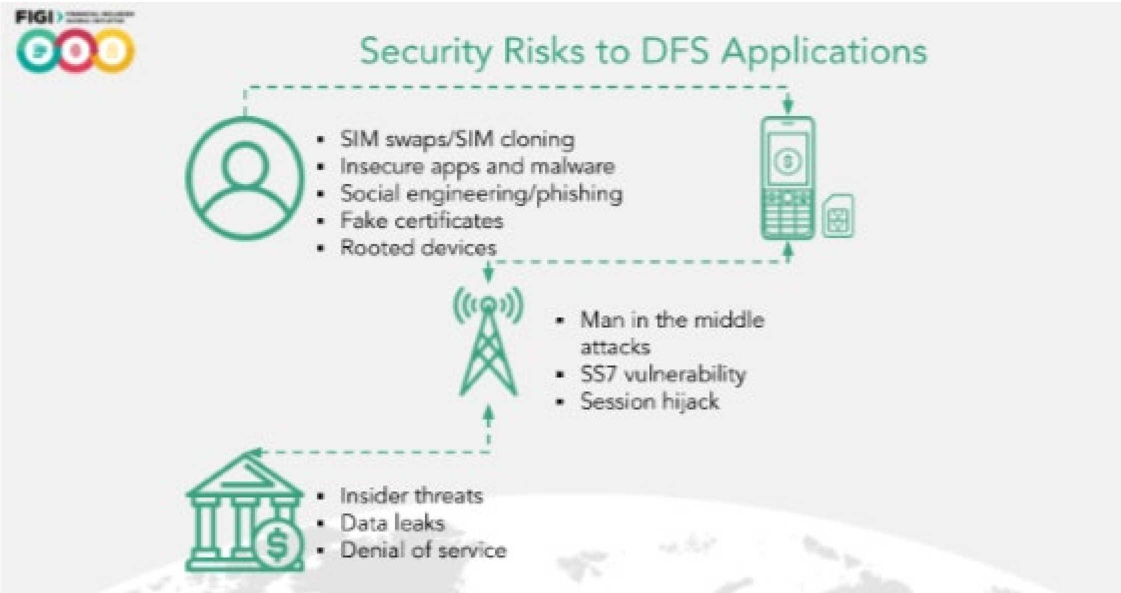


Figure 5.3.14 DFS Ecosystem Threats (ITU) Overview
(Source: FIGI website)

Threats for DFS applications based on USSD, SMS, IVR, STK, and NSDT according to ITU (International Telecommunication Union) are shown in Figure 5.3.15.

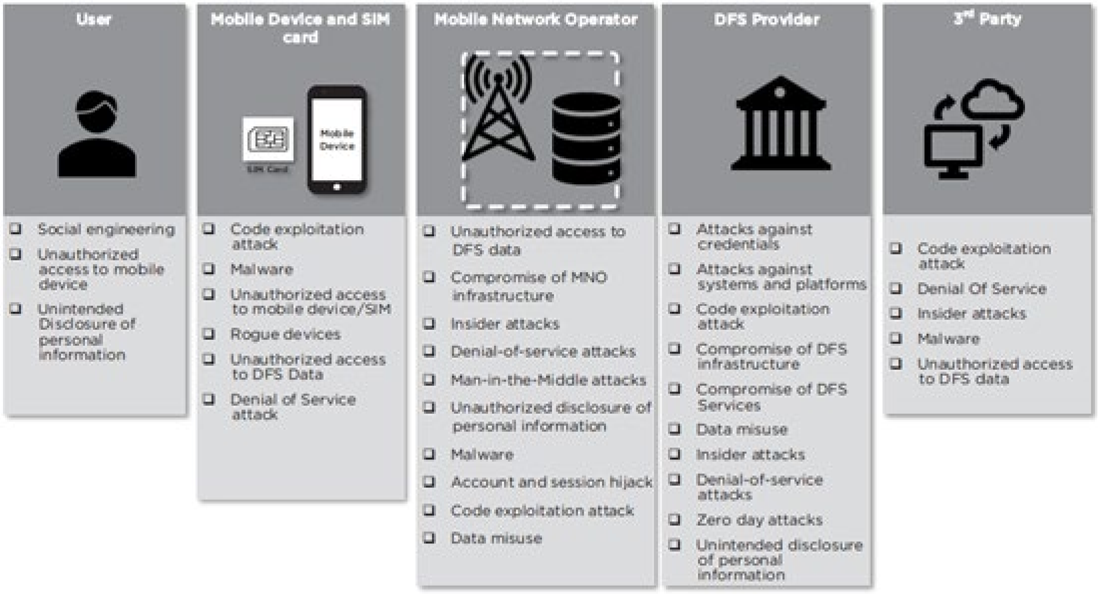


Figure 5.3.15 Threats to DFS in USSD, SMS, IVR, STK, and NSD
(source: ITU, Digital Financial Services security assurance framework)

5.3.9. Summary of Fintech security based on additional research and verification

So far, we have conducted interviews with Fintech companies and related organizations regarding Fintech services in 5G, financial open APIs, and lifestyle authentication, and have summarized security issues and security considerations for operators. After the publication of this 5GMF white paper "Security in 5G Use Cases Version 1.0", we investigated the threat of DFS in FIGI's mobile to investigate and verify use cases related to real-time authentication and to investigate standardization trends in payment and authentication. The government aims to build a society where cyberspace and real space are integrated (CPS (Cyber Physical Systems)) and create a human-centered society that realizes economic development and the resolution of social issues (Society 5.0). To achieve this, safe and secure payments and personal authentication that seamlessly connect cyberspace and real space are essential. In real space, there are physical keys, but in cyberspace, IDs and passwords are generally used. Seamless integration is difficult if multiple keys are used for each space. Therefore, the combination of authentication of identity using behavioral data and biometric authentication, which has been considered so far, will be effective for smooth authentication and payment. In the future, a wide range of behavioral data, including actions in cyberspace, will be included in the collection and analysis, which we believe will lead to improved authentication accuracy. At that time, it is expected that it will be applied to NFTs, virtual currencies, wallets, etc. *NFT (Non-Fungible Token): Non-fungible digital data created based on blockchain.

6. References

6.1 IoT Security Use Cases

[1] IoT Security with 5G, 5G Security Research Ad Hoc Resources, October 2018. (only Japanese)
[2] IoT Security Guidelines, Ministry of Economy, Trade, and Industry (METI), Ministry of Internal Affairs and Communications (MIC), IoT Acceleration Consortium (IOTAC), July 2016. (only Japanese)
[3] General Framework for Security for Safe IoT Systems, The National Center of Incident Readiness and Strategy for Cybersecurity (NISC), August 2016. (only Japanese)
[4] General Measures for IoT Security, Ministry of Internal Affairs and Communications (MIC), October 2017.
[5] Cyber Physical Security Measures Framework (Draft), Ministry of Internal Affairs and Communications (MIC), April 2018.
[6] Guide to IoT Research Security Design, Information-technology Promotion Agency, May 2016, revised April 2018.
[7] IoT Security Value Verification Guidelines, Connected Consumer Device Security Council, June 2017.
[8] IoT Security Standards/Guideline Handbook, Japan Network Security Network, May 2018.
[9] IoT Security Checklist, Japan Smartphone Security Forum, March 2018.
[10] Draft NISTIR 8200 - Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things, National Institute of Standards and Technology, February 2018.
[11] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, The European Union Agency for Cybersecurity, November 2017.
[12] Security Guidance for Early Adopters of the Internet of Things, Cloud Security Alliance (CSA), February 2016.
[13] OWASP IoT Top 10, The Open Web Application Security Project (OWASP), December 2018 (Revised).
[14] Technical Specification TS-0003 Security Solutions, OneM2M, April 2018.
[15] IoT Security Guidelines, GSMA, October 2018
[16] Security Studies Ad Hoc Activity Overview, 2018, Security Ad Hoc Secretariat, November 2018.
[17] Prasad, Anand R. "Key Points of 5G Security," NEC Corporation, July 2018. (https://cybersecurity-magazine.com/key-points-of-5g-security/)

[18] 3GPP TR 38.913, "Study on Scenarios and Requirements for Next Generation Access Technologies; (Release 15)"

[19] 3GPP TR 22.186, "Enhancement of 3GPP support for V2X scenarios; Stage 1 (Release 16)"
[20] Cimpanu, Catalin, "Newer Diameter Telephony Protocol Just as Vulnerable as SS7," July 2, 2018. (https://www.bleepingcomputer.com/news/security/newer-diameter-telephony-protocol-just-as-vulnerable-as-ss7/)
[21] 3GPP TR 23.724, "Study on Cellular Internet of Things (CIoT) support and evolution for the 5G System (5GS) (Release 16)"
[22] oneM2M - Home, https://www.onem2m.org/
[23] Ace (Authentication and Authorization for Constrained Environments) Status Pages, https://tools.ietf.org/wg/ace/
[24] OpenWeave, https://openweave.io/
[25] SP-190711, "New WID Authentication and key management for applications based on 3GPP credential in 5G"
[26] 3GPP TR 33.805, "Study on Security Assurance Methodology for 3GPP network products"
[27] 3GPP TR 33.916, "Security Assurance Methodology (SCAS) for 3GPP network products"

6.2. Connected Cars Use Cases

[1] “Proposal for draft guideline on cyber security and data protection,” WP29, 2016.
[2] “Proposal for a Recommendation on Cyber Security, WP29,” 2020.
[3] “Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues,” WP29, 2018.
[4] “TTC TR-068：Current standardization movement and issues before practical use for Over the Air updating in vehicle,”　TTC, 2019.
[5] “Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system,” WP29, 2021.
[6] “Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system,” WP29, 2021.
[7] “Cyber Security Measures in Automated Driving System, Automatic Driving Business Study Group,” 2019.
[8] “Status of the Development of ISO/SAE 21434,” 25th European Conference, EuroSPI 2018, 2018.
[9] “ITS Standardization 2018,” Society of Automotive Engineers of Japan, 2018.
[10] CEN TC278 WG16 - CO-OPERATIVE SYSTEMS.
[11] “ISO21217: Intelligent transport systems - Communications access for land mobiles (CALM) – Architecture,” 2014.
[12] “ISO16461: Intelligent transport systems — Criteria for privacy and integrity protection in probe vehicle information systems,” 2018.
[13] “ISO21177: ITS station security services for secure session establishment and authentication between trusted devices,”2019.
[14] “TS21185: Intelligent transport systems - Communication profiles for secure connections between trusted devices,” 2019.
[15] “Security Guideline for Driver Assistance Communication Systems,” ITS Forum RC-009, 2011
[16] “Issue Survey Report on Advanced ITS and Automated Driving Using Cellular Communications Technologies,” ITS Info-communications Forum, 2019, revised in 2021.
[17] “ITU-T X.1371: Security threats to connected vehicles,” 2020.
[18] “ITU-T X.1371: Secure software update capability for intelligent transportation system communication devices,” 2019.
[19] “Network Equipment Security Assurance Scheme Overview Version 0.3,” GSMA, 2016.
[20] “The GSMA will work with ENISA to secure 5G networks,” GSMA, 2020.
[21] “Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures,” EU, 2020.
[22] “JAMA/JAPIA Cybersecurity Guidelines V2,” JAMA/JAPIA, 2023.

[23] Shinichi Kazuki, "ITS International Standardization Trends in ISO/TC204," JARI Research Journal, 2017.
[24] "Network Equipment Security Assurance Scheme (NESAS)," GSMA.
[25] "ISO27011（ITU-T X.1051）Information technology - Security techniques - Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations,"　2016.
[26] "ISO27017 (ITU-T X.1601) Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services," 2015.
[27] "Study Group for Realization of Connected Car Society," Ministry of Internal Affairs and Communications.
[28] "General Principle and Vision White Paper Ver 1.0.0," AECC, 2017.
[29] Claudia Campolo, Antonella Molinaro, Antonio Iera, Francesco and Menichella Antonella, "5G Network Slicing for Vehicle-to-Everything Services," IEEE Wireless Communications, 2017.
[30] "TR 22.891, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility Study on New Services and Markets Technology Enablers; Stage 1 (Release 14)," 3GPP, 2016.
[31] Maria A. Lema, Andres Laya, Toktam Mahmoodi, Maria Cuevas, Joachim Sachs, Jan Markendahl and Mischa Dohler, "Business Case and Technology Analysis for 5G Low Latency Applications," IEEE Access, March 2017.
[32] "TR33.813, Study on security aspects of network slicing enhancement," 3GPP, 2020.
[33] "TS33.501, Security architecture and procedures for 5G system," 3GPP, 2023.
[34] "TR33.874, Study on enhanced security for Network Slicing Phase," 3GPP, 2022.
[35] "TR33.886, Study on enhanced security for Network Slicing Phase 3," 3GPP, 2023.
[36] "TS33.326 Security Assurance Specification (SCAS) for the Network Slice-Specific Authentication and Authorization Function (NSSAAF) network product class," 3GPP, 2023.
[37] "Toward fully connected vehicles: Edge computing for advanced automotive communications: White Paper," 5GAA, 2017
[38] "AECC General Principle and Vision," White Paper, 2018.
[39] "MEC in 5G networks," ETSI White Paper No.28, 2018.
[40] "ETSI MEC: An Introduction (almost) everything you want to know about ETSI MEC," 2023.
[41] "TS33.839, Study on security aspects of enhancement of support for edge computing in the 5G Core (5GC)," 3GPP, 2022.
[42] "TS33.558, Security aspects of enhancement of support for enabling edge applications; Stage 2," 3GPP, 2023.
[43] "TR23.700.98, 5G System Enhancements for Edge Computing; Phase 2," 3GPP, 2022.
[44] "Cloud and MEC security," 2018.

[45] “5G security package 3: Mobile Edge Computing/Low Latency/Consistent User Experience,” NGMN, 2018.
[46] “MEC for Automotive in Multi-Operator Scenarios,” 5GAA, 2021.
[47] “TS23.285: Architecture enhancements for V2X services (Release 16),” 3GPP, 2019.
[48] Karthikeyan Ganesan, Prateek Basu Mallick, Joachim Lohr and Dimitrios Karampatis, “5G V2X Architecture and Radio Aspects, IEEE Conference on Standards for Communications and Networking (CSCN),” 2019.
[49] “TS33.836, Study on security aspects of 3GPP support for advanced Vehicle-to-Everything,” 3GPP, 2020.
[50] “TR33.836: Study on Security Aspects of 3GPP support for Advanced V2X Services (Release 16),” 3GPP, 2019.
[51] “TS33.536, Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services,” 3GPP, 2022.
[52] “Privacy by Design Aspects of C-V2X,” 5G Americas, 2020.
[53] “Vehicular Connectivity: C-V2X & 5G,” 5G Americas, 2021.
[54] “Security Credential Management System (SCMS),” USDOT, 2018.
[55] Benedikt Brecht, Dean Therriault, Andre ´ Weimerskirch, William Whyte, Virendra Kumar, Thorsten Hehn, and Roy Goudy, “A Security Credential Management System for V2X Communications,” IEEE Transactions on Intelligent Transportation Systems, 2018.
[56] Anna Angelogianni, Ioannis Krontiris, and Thanassis Giannetsos, “Comparative Evaluation of PKI and DAA-based Architectures for V2X Communication Security,” IEEE Vehicular Networking Conference (VNC), 2023.

6.3 FinTech Security Use Cases

[1] “5G and FinTech”, 20th meeting of the Fintech Association of Japan’s API and Security Committee, December 3, 2019
[2] “Report of Review Committee on Open APIs: Promoting Open Innovation”, Review Committee on Open APIs July 13, 2017
[3] "Use of Open APIs in the Financial Sector: Its Effects on Cybersecurity and Countermeasures," Bank of Japan Review Series, no. 18-J-3, June 2018.
[4] “Digital Solutions to Innovate Society: Technology and Future Prospects for Finger Vein Authentication Using Visible-light Cameras”, Hitachi Review 2018, Vol. 67, No. 5, August 2018.
[5] ACSiON. Ltd., https://www.acsion.co.jp/
[6] Fintech Association of Japan, https://www.fintechjapan.org/members
[7] Social ICT Research Center, Graduate School of Information Science and Technology, University of Tokyo, http://www.sict.i.u-tokyo.ac.jp/research/lifestyle.html

7. Summary

The research on 5G security that the Security Study and Research Committee has conducted has been compiled in this report. Based on the opinions of the participating committee members, (1) IoT, (2) Connected Vehicle, and (3) Fintech were considered as items based on the trend of 5G security standardization that is common to the entire group.
In July 2020, the 5GMF White Paper "Security in 5G Use Cases Version 1.0" was released. After the publication of version 1.0, the results of research activities on each item of study (standardization, connected vehicle, and Fintech) were reflected in version 1.1.

Revision History

Revision Number	Date	Content	Notes
1.0	August 4, 2021	Publication of First Edition	
1.1	March 29, 2024	〔Add Item〕 (5.2. Use Case Connected Vehicle Security) 5.2.2.1.3. UNR155[5], UNR156[6] (5.3. FinTech Security Use Cases) 5.3.7 Additional research and validation findings for real-time authentication use cases. 5.3.8. Organizing the relationship of mobile communication in the standardization trend of payment and authentication. 〔Partially updated or changed items〕 1.Introduction (Report Overview) (4.Trends in Standards for 5G Security) 4.1 Introduction 4.2 5G Standards and Introduction Schedule 4.3 Non-stand Along (NSA) Security 4.4 5G phase 1 security 4.5 3GPP Security issues in 3GPP Release 16（5G phase 2）and the State of Release 17 4.6 Other organizations studying 5G security 4.7 Summary of 5G security standards trends (5.2. Use Case Connected Vehicle Security) 5.2.1 Overview 5.2.2.2. ISO TC 22 (Road vehicles) 5.2.2.4.2. Problem investigation report for the advancement of ITS / autonomous driving using cellular communication technology	

		5.2.2.5. ITU-T 5.2.2.8 Japan Automobile Manufacturers Association, Inc. (JAMA)/ Japan Auto Parts Industries Association (JAPIA) 5.2.2.9. Summary 5.2.3.3. Network slicing 5.2.3.4. MEC 5.2.3.5. C-V2X (5.3. FinTech Security Use Cases) 5.3.9. Summary of Fintech security based on additional research and verification (6. References) 6.2 Connected Cars Use Cases 7.Summary	