oppo

6G Security Architecture:
Intelligent Security Built on Zero Trust

OPPO 6G Security Whitepaper

oppo

Table of Contents

05

Key Security Technologies for 6g Era

06

Preface

01

Preface

In the 6G era, industrial Internet, ubiquitous Artificial Intelligence (AI), zero-power communication, integrated Sensing and Communication (ISAC) representing developing trends in new services, new terminals, new connections, and new architecture are bringing tremendous changes to the current communication landscape. More and more data are collected from the terminals, sent to the network, and become an integral part of rich digital assets that feed into data-hungry AI engine. 6G is about managing these high-value assets and 6G security will evolve from focusing on securing the data transport to securing the data and its privacy. When these high-value data assets are being utilized, efficient data authorization is required. This is to prevent data assets belonging to different stakeholders from being misused and abused by any unauthorized party. Considering the diversity of new services in 6G and their data sources, it is time to consider a multi-party trust model, carry out distributed data authorization for multi-source, distributed data, and at the same time provide the needed protection for data that contains huge amount of personal identification information.

As new terminals and new connection technologies continue to evolve, data transmission protection is no longer limited to the use of traditional higher layer protocols. Capabilities of data protection are migrating from the higher layers to lower layers to accommodate new security needs and requirements of 6G new terminals and new air interface.

Based on the " Versatile 6G with Minimized Kernel " 6G system conceptual design principles, the security protection mechanisms for data assets in different subsystems also need to be flexible and diversified. To accommodate this, a well-designed intelligent security architecture and security capabilities in 6G system also need to be flexible and dynamic to meet the security requirements of different scenarios.

Through the analysis of developing trends and security requirements in new services, new terminals, new connections, and new architectures in 6G and basing on the traditional mobile network security, this white paper explores technologies in blockchain, physical layer security, AI security, and post-quantum security and examine in detail how they impact 6G. Finally, this white paper proposes a 6G intelligent security architecture based on zero trust.

- 5G Security Two-Party Trust Model
- 5G Security Architecture
- 5G Transmission Security Mechanism

5G Security Summary

02

5G Security Two-Party Trust Model

2.1

3GPP 5G security[1] defines the security architecture of two-party trust as illustrated in Figure 2-1, that is, UE (User Equipment) and operator HE (Home Environment) share the (pre-provisioned) user root key as the credentials for establishing mutual authentication. In 5G, the UE credentials are stored in the UE's physically Tamper Resistant universal integrated circuit card or universal integrated circuit card (UICC). On the network side, the credentials are stored in the core network's unified data management (UDM) and authentication credential repository and processing function (ARPF) entities. As the network is deployed outward from the core network, other network functions become more distant from the core network, leading to a reduced trust level. Other network functions can no longer be the "keeper" of long term credentials, and communication processes carried out in these network functions require more comprehensive security protections.

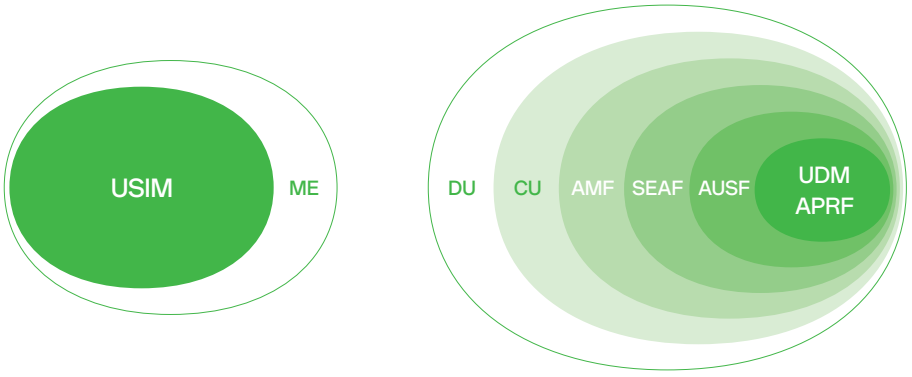

Figure 2-1: 5G Two-Party Trust Model

Before UE accesses the operator's network and uses network resources and services, the user (i.e., UE) and the operator network perform mutual authentication based on the user root key. Moreover, using the root key, the UE and operator network each derives a series of protection keys (both longer-term and short-term session keys) that are used to provide confidentiality protection (i.e., ciphering) and integrity protection of the signaling data and user data during two-way communication between the UE and the network.

In addition to the current two-party trust architecture in 5G, there are also two-party trust relationships between different stakeholders (i.e., between users and service providers, between devices and the network, and between two networks) that are not reflected in the 5G trust model. For example, there are two-way service contracts and interactions between users and service providers or between service providers and mobile networks, such as how to distribute identities and credentials to devices and how to perform mutual authentication between networks and devices based on those identities and credentials. The trust between these stakeholders forms the foundation of 5G services. Nevertheless, the trust models in 5G are still based on two-party trust, and therefore does not support multi-party trust among different stakeholders.

5G Security Architecture 2.2

The 5G security architecture defines five independent security domains [2], as illustrated in Figure 2-2.

- Network access security (I)

  the set of security features that enable a UE to authenticate and access services via the network securely and in particularly, to protect against attacks on the (radio) interfaces.

- Network domain security (II)

  the set of security features that enable network nodes to securely exchange signaling data and user plane data (between the access network and service network as well as within the access network itself) and to protect the wired network from attacks.

- User domain security (III)

  the set of security features that secure the user access to mobile equipment.

- Application domain security (IV)

  the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.

- Visibility and configurability of security (V)

  the set of features that enable the user to be informed whether a security feature is in operation or not, and whether the use and provision of the service should depend on this security feature or not.

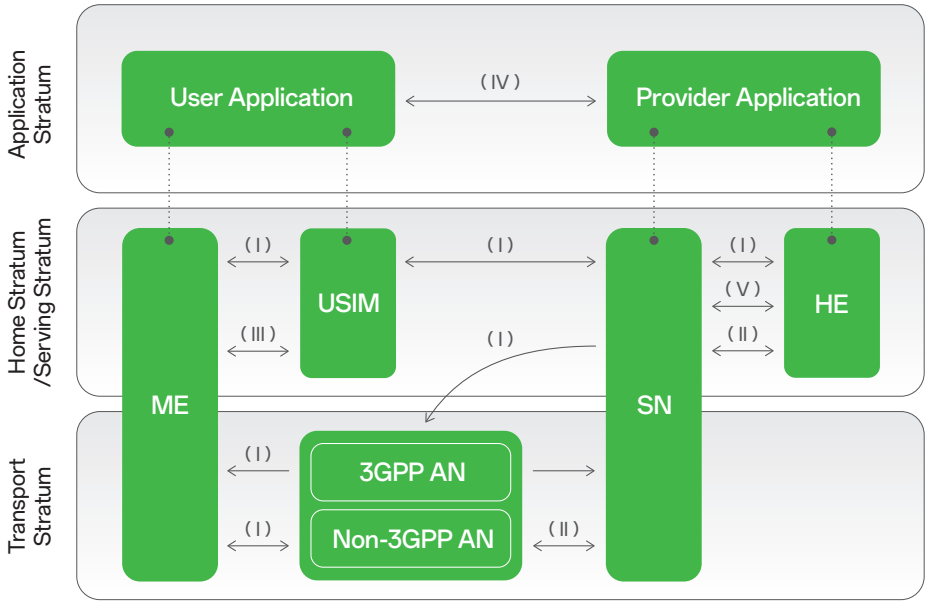

Figure 2-2 : 5G Security Architecture

The 5G security architecture in Figure 2-2 only includes the security domains within the home operator network. For roaming services, the home operator network needs to exchange roaming-related UE information with another roaming network. Networks exchange messages through the security edge protection proxy (SEPP) sitting at the perimeter of the operator network.

5G Transmission Security Mechanism

2.3

In the network access domain, the UE accesses the 5G network through the access network (AN). The security of access stratum (AS) is achieved by using keys at the lowest level of the 5G key hierarchy and one of the three cryptographic algorithms (i.e., AES, Snow 3G, ZUC) to provide the confidentiality protection and integrity protection of both user plane data and control plane signaling data. The protection of non-access stratum (NAS) signaling is implemented based on NAS keys using one of the same three cryptographic algorithms.

Network domain security (NDS) refers to the security protection between different network functions in the same operator network using the NDS security protocols specified by 3GPP. NDS/IP employs IP Security (IPSec) from IETF standards with specific profiles adopted for 3GPP. Service-based architecture (SBA) security introduced in 5G networks elevates the protection within the network domain to higher protocol layer(s), specifically the transport layer and the application layer. The 5G networks support utilization of TLS 1.3 defined by the IETF for transport layer protection, as well as end-to-end protection at the application layer.

5G supports flexible and diversified services. Application function (AF) or application servers can provide services directly to users through the 5G network. The application domain security between users and AF is still based on the 5G credentials. The 5G network and the UE generate key material based on access authentication (5G Authentication and Key Agreement, 5G AKA) to protect end-to-end applications between users and AF, so that the AF does not need to separately provide the required credentials and key material to the UE.

- Security Requirements of New Services
- Security Requirements of New Terminals
- Security Requirements of New Connections
- Security Requirements of New Architecture

Developing Trends and Security Requirements in 6G

03

Leveraging the advances of 5G, 6G is set to further enable a wider range of vertical industries, driving towards a future in which intelligent connectivity and digital twins are ubiquitous. Beyond offering individual-centric services, such as wearable technology and digital healthcare, 6G will facilitate more diverse vertical industries and scenarios, encompassing the industrial Internet, Zero-Power communication, intelligent transport system, and intelligent logistic.

In 6G everything is expected to be interconnected, characterized by an array of new services, new terminal equipment, and new connections:

Service Diversification:

Compared with traditional 2C (i.e.,To Consumer) service, new 2C services and 2B (i.e., To Business) services are developing rapidly, including eHealth, extended reality (XR), intelligent transport systems, smart home automation, industrial Internet, and intelligent logistics, etc.

Diversification of terminals:

Supporting new 2C and 2B services in 6G requires a wide variety of terminal devices, such as wearable devices, zero-power devices, intelligent vehicles, etc.

Diversification of connections:

in the 6G era, terminal devices will leverage ISAC to further push the boundaries of the digital realm to interact with the physical world. New forms of connectivity such as connectivity among large number of new terminal devices and spectrum sharing will also emerge.

These developing trends will lead to significant changes in the current communication model. An increasing amount of data is being collected from terminal devices and then transmitted to the network. This data is becoming an essential digital resource for artificial intelligence. The 6G system aims to manage these high-value data assets securely and efficiently.

One of the most profound changes in 6G security is the pivot from emphasizing protection of data transmission to emphasizing protection of data and its privacy. As data collection, processing, storage, analysis, utilization, and sharing take place within the 6G framework, data still belongs to different stakeholders and the need to protect the value of digital assets and prevent the abuse of digital resources is more evident than ever. Furthermore, when data is collected from personal terminals, there is an inherent risk to individual's private information being exposed. In the 6G landscape, it will be more important than ever to explore how to effectively use this data while protecting user privacy at the same time.

In the 6G system, there will be a variety of new terminal devices supporting different services. With different service data being shared among services, networks, application servers, and other terminal devices, it makes perfect sense to consider a multi-party trust model in the 6G framework that can be used to establish secure domains for diverse terminals and diverse services, and to ensure not only the efficiency of data transmission but also to isolate multi-source data to within where the data is owned in order to prevent data from being abused or accessed by unauthorized party.

Vast number of Internet of Things (IoT) devices are expected to be used in 6G industrial scenarios, with a significant proportion being low cost and zero-power devices [3] with limited power consumption, storage and processing capabilities. For these types of devices, it is critical to consider how to maintain the same level of security protection as with other services and devices while adapting to the limitation of these devices.

When leveraging ISAC, the differences between sensing signals and signals being exchanged in traditional connections need to be considered. Sensing services use lower layer signals to explore the physical characteristics or attributes and protection of these lower layer signals (i.e., privacy protection) becomes important, especially since these lower layer signals are likely to carry sensitive personal information to support various use cases in ISAC.

In response to the trend of diversification of 6G services, terminals, and connections, the OPPO 6G white paper [4] proposes a new architecture of "Versatile 6G with Minimized Kernel", in which 6G = Minimized Kernal + N subsystems. A minimized kernel provides common capabilities such as native AI, security and flexible spectrum management that serve as a basis for designing subsystems that can be both flexible and versatile. This design allows individual subsystem in each scenario to be properly decoupled and optimized, truly achieving " Versatile 6G with Minimized Kernel " that is envisioned in the OPPO 6G white paper, a 6G system that will only provide the functionalities and capabilities when they are needed. The 6G system will have the capability to facilitate the transitions and integration of multiple subsystems by leveraging the dynamic nature of diverse and advanced AI algorithms. Similarly, for service data originating from multiple sources, intelligent orchestration of security features is essential to meet the diverse security requirements of different scenarios.

The value proposition of business applications and data carried by the 6G system in the future will appreciate greatly and in turn drives the development and enhancement of 6G security further. The 6G security should focus on safeguarding the value of industrial data assets and the privacy of users which encompasses of designing lightweight and distributed security mechanisms adapting to the low- and zero-power IoT terminals, providing lower layer protection for new connections, and leveraging AI to intelligently orchestrate security policies, as illustrated in Figure 3-1.

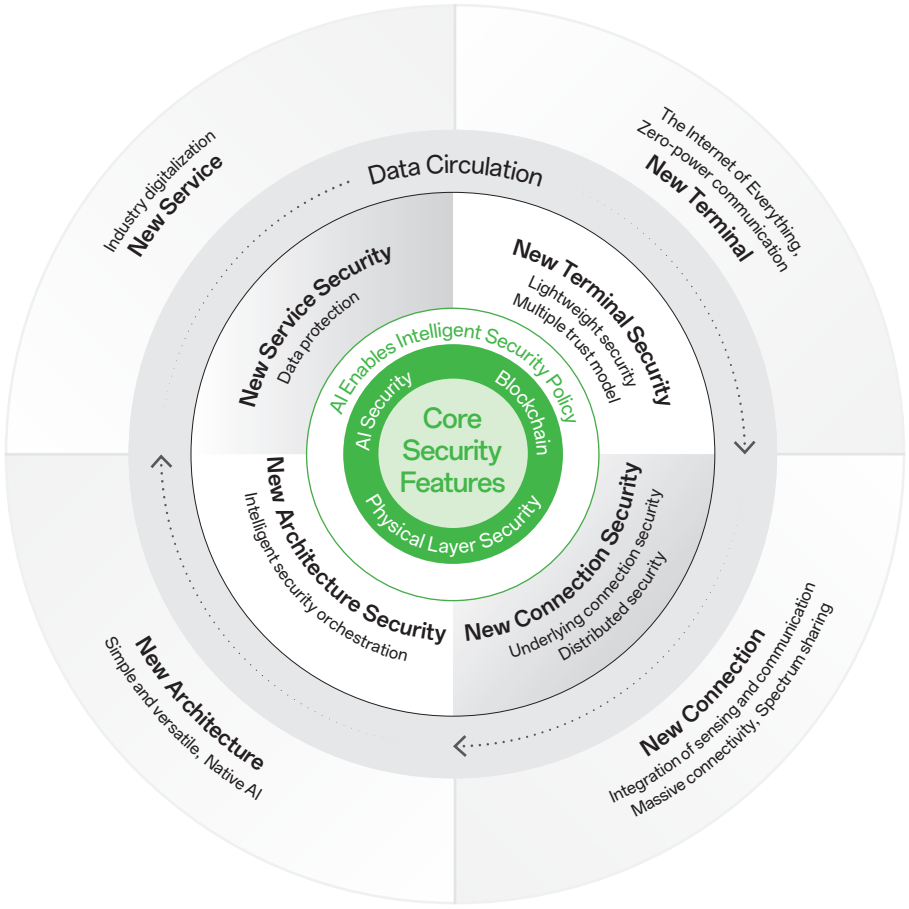

Figure 3-1: Overview of 6G Security Requirements

The key security requirements of 6G will be further discussed, including that of support for the following:

- Security requirements of new services
- Security requirements of new terminals
- Security requirements of new connections
- Security requirements of new architecture

Security Requirements of New Services

3.1

In 6G era, working with a digital world that extends the real world by using vast number of advanced sensors and AI [5]. AI will empower various domains such as the industrial Internet, eHealth, digital twins, and XR:

Integration Artificial Intelligence and Communication

With the popularization and rapid development of artificial intelligence and machine learning, image recognition, speech recognition, and natural language processing have been widely used by intelligent terminals, penetrating the communication systems and profoundly enhancing users' productivity and daily life. There will be numerous intelligent nodes in the 6G system capable of AI model training and inference, participating in local or distributed computing and federated learning processes. The 6G AI-Cube Intelligent Networking white paper [6] proposed by OPPO describes that the AI functional plane, AI user plane, and AI control plane jointly provide the 6G system with accurate decision-making ability, powerful reasoning ability, metamorphosis capabilities, and learning transfer ability.

Industrial Internet Scenario

With the development of industrial Internet, a vast number of IoT devices can be deployed in various factory settings such as production lines, warehousing management, and logistics transportation. IoT devices capture and generate data, sent through networks to relevant processing nodes and application servers to enable monitoring, automation control, and optimization of industrial workflows.

Ehealth Scenarios

The ongoing advancements in sensors, AI, and communication technology are unlocking unseen potentials in the 6G system to transform digital healthcare and introducing innovative applications. Examples of such innovative applications include the following:

Multi-dimensional sensing telemedicine to collect user health information and perform remote monitoring and diagnosis, offering extensive health data resources.

Enhanced data accumulation and analysis to improve health data processing efficiency and to provide quality datasets.

Establishment of digital twins that utilize data, models, and interfaces to replicate and manage human biological characteristics, to emulate patient conditions, health assessment, and disease progression forecasting.

Immersive Multimedia and Multi-Sensory Interactions

These services aim to extend the real-time interaction and full simulation of multi-sensory information, creating immersive, human-centric experiences for human-machine interaction, encompassing:

Immersive XR experiences in everyday activities like entertainment, social interaction, and work, using virtual reality (VR) and augmented reality (AR) technologies to enhance user immersion.

Multi-dimensional sensory interactivity that incorporates tactile, taste, and smell sensations to augment experiences in healthcare and entertainment.

Holographic communications that leverage real-time interactive 3D environments suitable for entertainment and holographic conferences.

The focus of security protection gradually shifts from emphasizing protection of data transmission to emphasizing protection of data and its privacy. Security requirements for new services reflect the shift of focus to data protection. Within industrial Internet and intelligent logistics scenarios, unauthorized access or eavesdropping on IoT devices' service data could lead to the compromise or loss of vital service information, leading to exposure of sensitive and private data of individual owners, both violating their privacy and harming businesses. In eHealth, immersive multimedia and multi-sensory interactions scenarios, a leakage involving personal data may not only serve as a privacy violation but also poses compliance and legal risks for business and network operators.

Security Requirements of New Terminals

3.2

Large-scale communication use cases for 6G include smart cities, transportation, logistics, healthcare, energy, environmental monitoring, agriculture, and the expansion and novel applications in many other areas. These use cases require various new types of IoT devices with either no battery or long-life battery [7]. These new devices can be applied to the following typical scenarios and technologies:

Zero-Power Communication Scenarios

These scenarios are driving the IoT towards energy efficiency and sustainability. Such scenarios are primarily based on three core technological fundamentals: radiofrequency (RF) energy harvesting, backscatter communication, and low-power computing. These technologies allow low-power IoT devices to harvest energy by capturing ambient radio waves and use this energy for communication, reducing dependency and reliance on traditional power supply methods [3]. Moreover, simplifying RF and baseband circuit structure can also greatly reduce the terminal cost, terminal size and circuitry energy consumption. The international standards organization 3GPP has already identified some potential scenarios for zero-power communications (i.e., Ambient IoT communication) [8]:

(1) Remote monitoring in smart city construction and the industrial Internet.
(2) Inventory tasks in logistics and warehouse management.
(3) Item location and intelligent control within smart home.

Indoor Positioning Scenarios

These scenarios are primarily aimed at high traffic areas such as office buildings, airports, and shopping malls to provide navigation and precision location service to enhance service efficiency. These scenarios can also be applied in factories and logistics centers to offer precise location support for intelligent goods management and tracking to reduce costs in providing goods and services. In the 6G, with the adoption of technologies like large scale antennas, wider bandwidth, and zero-power communication, it is expected that indoor centimeter-level positioning accuracy can be achieved to meet the demands for location services with higher precision requirements.

Intelligent Transportation Scenarios

With sensors, cameras, and advanced AI algorithms, intelligent vehicles are capable of autonomous navigation, detecting surrounding environments, preventing collisions, and even driving independently under complex urban road conditions. The data gathered from vehicle sensors shared among neighboring vehicles and infrastructures can be utilized in collaborative computing between the vehicle and the cloud that further enhances vehicles' ability to assess traffic conditions, pre-alert potential hazards, optimize navigation routing, and bolster the overall traffic flow's efficiency and safety.

Smart Logistics Scenarios

With advancements in digitalization and automation technologies, smart logistics is revolutionizing the management of assets and labor force by leveraging IoT, big data, AI, and machine learning. For instance, precision data exchanges among devices, products, vehicles, and workers can support highly efficient warehousing operations from the movement and storage of goods to their loading, unloading, and inventory management. The 6G system will provide massive connectivity and pinpoint location accuracy, enhanced system capacity to boost system bandwidth and allowing real-time tracking of cargo, paving the way for automation in intelligent logistics operations.

Security requirements of new terminals are the following:

Lightweight Security Requirements of Zero-Power Devices

Given the simplicity, reliance on ambient energy supply, and ultra-low power consumption of zero-power devices, adopting traditional security mechanisms is challenging due to their high computational complexity. These zero-power devices have much simpler protocol designs and less computational complexity compared to other IoT devices such as NB-IoT (Narrowband Internet of Things) devices and RedCap (Reduced Capability) devices. Developing a lightweight security framework is critical to protect zero-power communications. Security functions should follow a lightweight design approach to meet the following requirements:

- Lightweight, trustworthy access and data authorization under limited resources that are compatible with the extremely low complexity terminal.
- Simplified security mechanism for data transmission to prevent attackers from data interception during transmission.
- Defense against network threats including data interception, manipulation, spoofing, and replay attacks.

Multi-Party Trust Model Requirements for Diverse Terminal Devices

As diverse terminal devices serving a variety of services in 6G networks, different types of service data, models, and control messages may be shared among 6G services, networks, and terminals. It is critical to manage access rights and authorization of data for different service. This means that the data is only consumed by the authorized parties and not shared or misused by other unauthorized services or network functions. To support handling of data in a multi-source, multi-stakeholder environment in 6G, a multi-party trust model should be taken into account. Secure domains for different terminals and service data need to be established to ensure efficient data transmission while isolating multi-source data to within where the data is owned in order to prevent data from being abused or accessed by unauthorized party.

Security Requirements of New Connections

3.3

6G will introduce the following key scenarios of new connections:

Integrated Sensing and Communication Scenario

As a new typical scenario in 6G, ISAC leverages communication signals to detect, locate, identify, and image targets [9]. The requirement development group in 3GPP (i.e., SA1) has identified a range of sensing scenarios [10]. For individual users, these potential applications include:

- Ultra-precise position with or even without using of devices.
- Target identification based on biometric features such as gestures, actions, and gait.
- Visitor identification and control in smart homes.
- Construction of high-resolution real-time maps, etc.

Additionally, ISAC will help to enhance communication performance and efficiency, for example, by optimizing wireless resources utilization considering user movement trajectories and other environmental conditions.

Ultra-Massive Connectivity Scenario

The connectivity density in the 6G system will increase from one million connections per square kilometer in 5G to ten million connections per square kilometer [5]. Building on the massive machine-type communications of 5G, ultra-massive connectivity expands the number of devices, application fields, and capacity boundaries. It supports interconnectivity among hundreds of millions of devices, applied in scenarios such as smart cities, smart agriculture, and the industrial Internet, etc. [11]

Spectrum Sharing Scenario

With the increasing spectrum needs of mobile services, spectrum sharing and coordination are very beneficial. The advantages of spectrum coordination include promoting economies of scale, enabling global roaming, reducing the complexity of device, and increasing spectrum efficiency (including potentially reducing cross-border interference) [5]. Operators can share idle spectrum or even underutilized spectrum with another operator for use by non-subscribers, in turn, unlocking new revenue streams.

Security requirements of new connections:

Authorization and Privacy Protection Requirements for ISAC

Given that sensing technology has the capability to track and potentially identify everything within the environment where the subject is located, including subjects without associated devices, privacy protection should be top consideration in security [10].

The data generated by different sensing objects varies. Specific individuals or areas of sensing may involve sensitive information, such as the location or physical attributes of the sensed object, and individual's vital signs. At the same time, the acquisition of sensing data must comply with regional laws and regulations. For

different sensing subjects and regions, different granularity in terms of authorization mechanisms and privacy protections may be necessary to prevent abusing sensing operations and associated data.

Physical Layer Security Requirements for ISAC

Since sensing signals and measured data usually originate from the lower layer, attackers can easily access state information of sensing channel, and then infer results which may involve privacy of the targeted subjects if the lower layer signals are not protected. For example, eavesdroppers might monitor wireless transmissions without decoding the frame content and measure data to obtain relevant human body information in smart home or intelligent health/medical scenarios. Additionally, even if the waveform and signal parameters are kept confidential, attackers can still obtain the sensing signal parameters through parameter estimation techniques, potentially leading to replay attacks, delaying measurements at receiver point, or incorrect parameters being extracted. It becomes critical to authenticate the origin of sensing signals and to protect transmission with a focus on security measures in the physical layer.

Distributed Security Requirements for Ultra-Massive Connectivity

Designing a uniform 6G security mechanism faces substantial challenges due to the diversity of terminal devices, services, and connectivity. Moreover, vast number of devices connecting to dynamic and heterogeneous networks can cause substantial security signaling overhead which becomes challenging for traditional centralized security management. Efficiency and timely handling of secure accesses for vast number of devices is necessary. Devices can also connect to mobile communication systems within specific geographic regions, resulting in services and systems with cross-regional and wide distribution. Therefore, distributed access authentication and data authorization for massive number of terminal devices need to be considered. For ultra-massive connectivity scenario, efficient, locally adaptive, and distributed security mechanisms and functions can be considered.

High Reliability Security Requirements for Spectrum Sharing

In order to ensure the security sharing of idle spectrum and protect the interests of operators, a secure user access mechanism and reliable cross-operator charging rules are needed. The existing cellular system roaming mechanism may not be efficient and reliable and was not designed for spectrum sharing. GSMA (Global System for Mobile Communications Association) is researching on blockchain-based roaming optimization [12]. For spectrum sharing, the distribution and multi-party trust characteristics of blockchain can be further considered in a highly reliable security design.

Security Requirements Of New Architecture

3.4

The OPPO 6G white paper “A versatile 6G with minimized kernel: To build the mobile world” proposes a new architecture of “Versatile 6G with Minimized Kernel”, in which 6G = Minimized Kernal + N subsystems. A minimized kernel provides common capabilities such as native AI, security and flexible spectrum management that serve as a basis for designing subsystems that can be both flexible and versatile. This design allows individual subsystem in each scenario to be properly decoupled and optimized, truly achieving " Versatile 6G with Minimized Kernel " that is envisioned in the OPPO 6G white paper, a 6G system that will only provide the functionalities and capabilities when they are needed. The 6G system will have the capability to facilitate the transitions and integration of multiple subsystems by leveraging the dynamic nature of diverse and advanced AI algorithms [4]. Similarly, for service data originating from multiple sources, intelligent orchestration of security features is essential to meet the diverse security requirements of different scenarios.

The Security Requirements of New Architecture Include The Following:

Diverse security requirements comes from multiple subsystems with different service scenarios and terminal types. Satisfying diverse security requirements requires that a powerful AI to intelligently orchestrate both basic security functions and differentiated security capabilities. With a focus on the value of data assets, the security requirements of service scenarios should be dynamical and flexible to enable the implementation of security functions within subsystems. Zero trust is an architectural approach that emphasizes data protection and allows for the formulation of dynamic policies to determine accesses to data and resources [13]. Therefore, an intelligent security protection architecture that adapts to various 6G subsystems must also be based on zero trust.

- Zero Trust Background
- Intelligent Security Based on Zero Trust Architecture

6G Intelligent Security Architecture Based on Zero Trust

04

Zero Trust Background 4.1

Since Forrester proposed the zero-trust concept in 2009, the zero-trust security model has been widely adopted in finance, Internet, cloud services and other industries. Zero Trust concept promotes three core principles: all entities are untrusted by default, least privilege access is strictly enforced, and comprehensive security monitoring is implemented. Through identity authentication and authorization, zero trust security is designed to ensure access to data and other resources comply to a set of defined security policies.

In the zero-trust logical architecture well-accepted by the industry[13], the policy engine (PE) located on the control plane is based on a series of information sources (including Continuous Diagnostics and Mitigation (CDM) systems, industry compliance, threat intelligence, events logs, data access policies, public key infrastructure (PKI), ID management, security event management systems) to dynamically decide to grant or deny subjects' access rights to relevant requested resources. The policy administrator (PA) will generate access credentials based on policy enforcement's decisions, establish, maintain, and terminate access sessions. Policy Enforcement Point (PEP) is a component that interacts with the access subjects and establishes and terminates communication sessions according to the policy instructions issued by the PA.

Many variants of zero trust architecture exist. Different architecture variants can be customized for specific workflows in many ways and still adhere to the zero trust principles. For example, using network infrastructure and a software-defined perimeter approach, and with the PA acting as the network controller, the network can be redesigned and reconfigured based on the decisions made by the PE to grant client access request through PEP in an architecture that meets security requirements suited for the business.

With the development of zero trust technology and the emergence of policies and standards that support zero trust, business models and markets based on zero trust are gradually maturing. According a 2023 "Zero Trust Development Research Report" [14] released by China Academy of Information and Communications Technology, statistical data shows that zero trust growth is trending upward in key industries such as finance and telecommunications. Furthermore, zero trust is being applied in many different application scenarios in remote office, remote operation and maintenance, multi-branch organization interconnects, etc.

Intelligent Security Based on Zero Trust

4.2

As data sources related to businesses and services are changing rapidly, one of the key focuses in 6G security is the shift in data transmission security to that of data security and data privacy. To meet the security requirements of diversified subsystems, applications, and services and to protect the business data assets in 6G, intelligence in security is a must. A more comprehensive security assessment of the system, subsystem trust model, data access authorization, and data transmission security as well as the implementation of flexible and dynamic security policies are all prerequisites to the intelligent security architecture in 6G era.

In 6G, consideration should be given to a security architecture based on zero trust that can be used to support intelligent security policies, to orchestrate security policies flexibly and dynamically, and to configure security functions intelligently accordingly to meet the security requirements. Compared to a more static 5G security architecture, the intelligent security architecture in 6G not only provides support for identifying security requirements, subsystems, and security capabilities, but is also intelligent to configure security policies dynamically. As applications and services in 6G business scenarios grow and as security technology in 6G further develops, the intelligent security architecture can flexibly introduce new security capabilities and configure security policies to support new business scenarios and to meet the development needs yet maintaining backward compatibility. The 6G intelligent security architecture based on zero trust is shown in Figure 4-1.

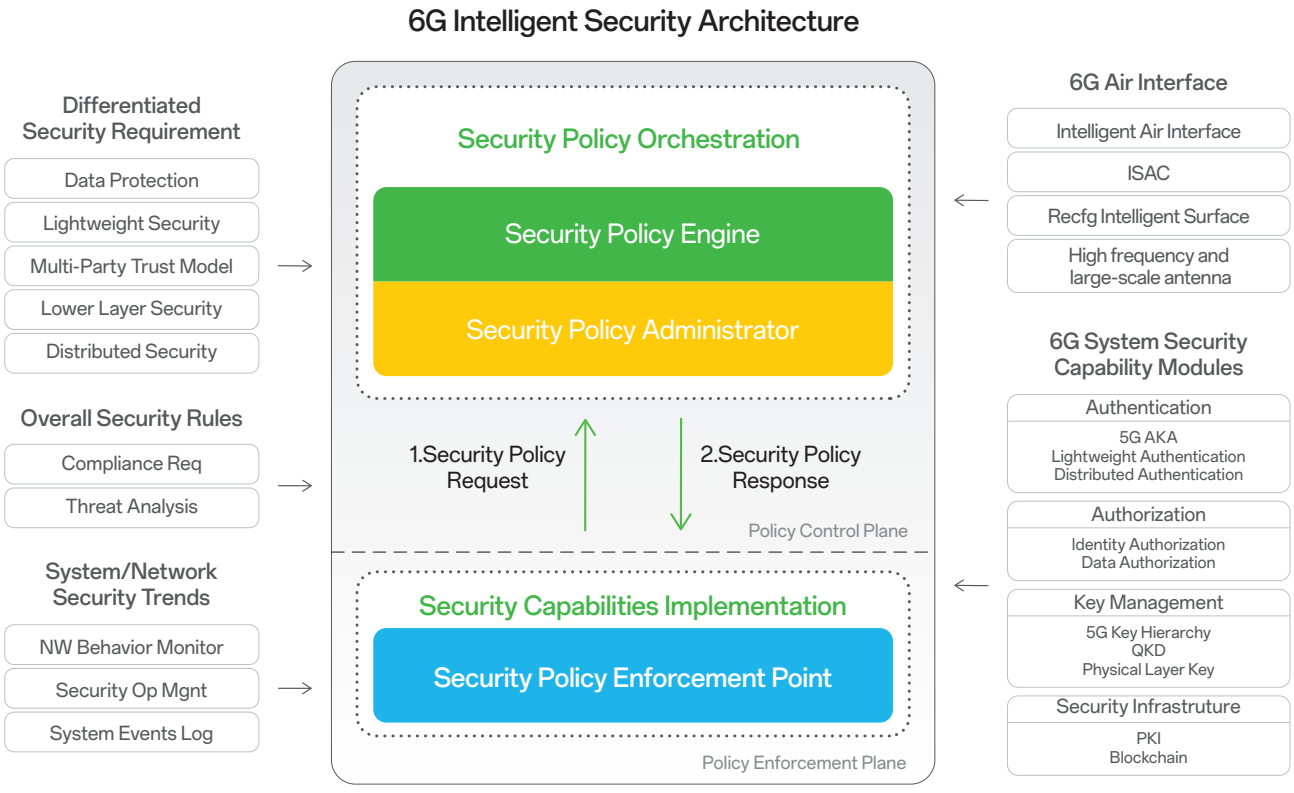

Figure 4-1: 6G Intelligent Security Architecture Based on Zero Trust

Core Components of 6G Intelligent Security Architecture Based on Zero Trust:

Security Policy Engine (SPE)

Built on the Zero Trust Policy Engine function PE, SPE develops security policies based on inputs from the "Versatile 6G with Minimized Kernel".

Security Policy Administrator (SPA)

Built on the Zero Trust Policy Administrator function PA, SPA establishes communication path between security policy engine and security policy enforcement point and to provide both input and output.

Security Policy Enforcement Point (SPEP)

Built on the Zero Trust Policy Enforcement Point function PEP, SPEP provides differentiated security capabilities for each subsystem.

Principles for developing security policies and implementing security capabilities:

6G intelligent security architecture accommodates two dynamic variables, namely security variable and business/system variable and develops or adjusts security policies accordingly and intelligently:

Security Variable

Security variable refers to global security rules and system/network security posture. Because of the dynamic nature of external regulatory requirements, network conditions, business needs, and security threats in 6G environment, security policies need to be able to promptly adapt to changes. Global security rules include universally recognizable compliance requirements and accepted industry threat analysis. System/network security posture includes status of the real-time attack attempts on the system and network and status of secure operations in the network.

Business/ System Variable

Business/system variable refers differentiated business security requirements, differentiated network capabilities and modular security capabilities of the 6G air interface. The " Versatile 6G with Minimized Kernel" supports the efficient launch of new businesses and new services. Doing so requires the quick development of security policies for the new services and the configuration of appropriate security functions and capabilities for the subsystems. The capabilities of the 6G air interface support enabling and optimizing security functions for the new services. For example, Reconfigurable Intelligent Surfaces (RIS) and intelligent air interfaces can improve the efficiency and security of physical layer security key generation. 6G security capability modules include authentication, authorization, key management, security infrastructure, etc., which are decoupled from other 6G system functions and protocols. These modules are decoupled from other 6G system functions so that security capabilities that are required to support a specific service can be allocated and configured flexibly and dynamically while not impacting other services.

Below is an example of how security policies and security capabilities are configured :

As illustrated in Figure 4-2, SPE develops differentiated security policy for each subsystem while SPEP configures the security capabilities for that subsystem.

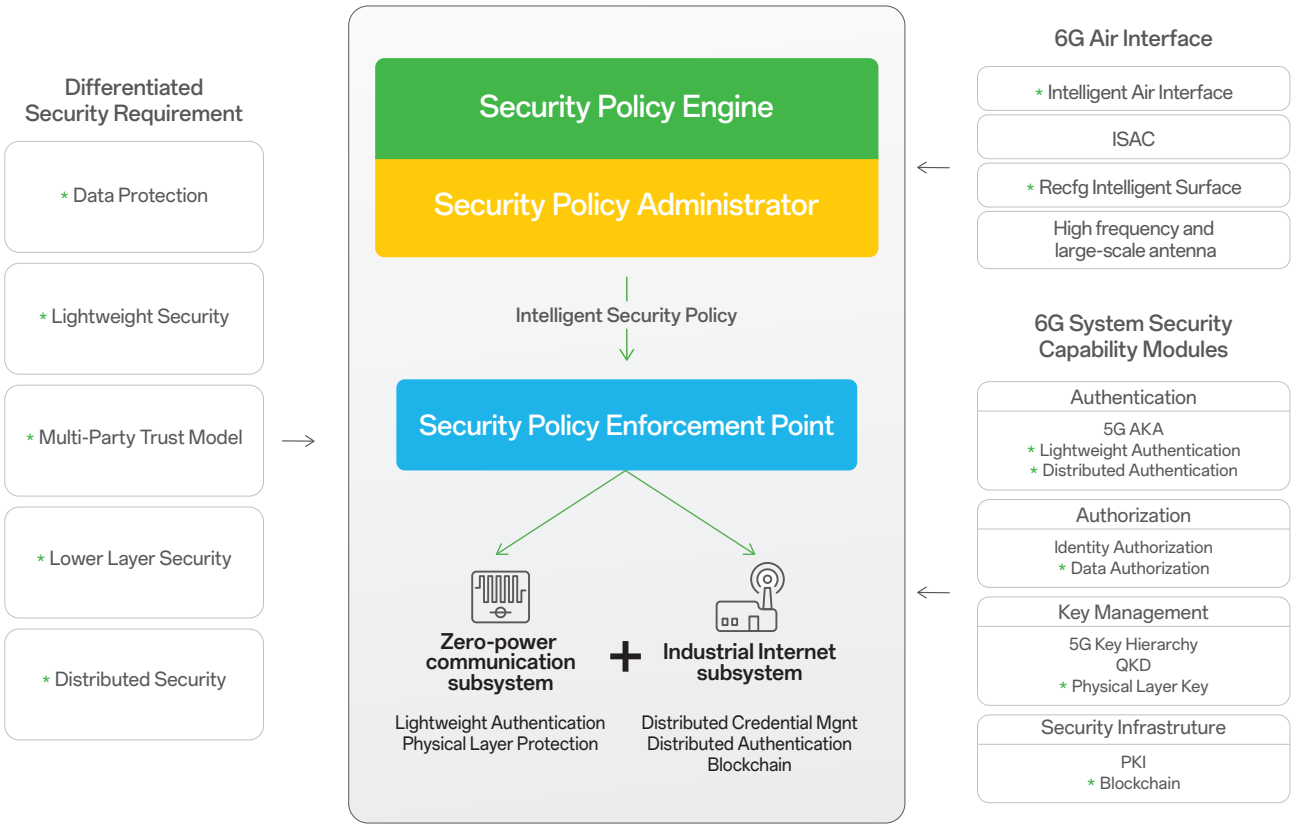

Figure 4-2: Subsystem Differentiated Security Capabilities

Industrial internet + Zero-power communication subsystems security policy orchestration and security capability configuration

SPEP requests security policies from SPE through SPA. Taking industrial Internet + zero-power communication subsystem as an example, entire industry chain, how data is collected and processing at different locations are taken into consideration. To support such subsystems and services, a multi-party trust model, distributed authentication and business data protection are called for. At the same time, considering that zero-power devices need to perform and complete required security functions under limited computing and processing resources, lightweight security and physical layer security are required.

SPE formulates security policies:

SPA obtains a list of security capabilities in the 6G system security capability module and reports them to SPE. SPE selects security functional capabilities based on the above security requirements, such that lightweight authentication and distributed authentication in the authentication module, data authorization in the authorization module, the physical layer key in the key management module, and blockchain in the security infrastructure module are selected as the required security capabilities for the subsystems. SPE further formulates the security policy for the subsystems based on the selected security capabilities.

SPEP configures security functions:

SPA obtains the subsystem security policy formulated by SPE, obtains the list of available 6G air interface capabilities, and sends it to SPEP. SPEP implements and enhances security capabilities and functions based on security policies and the available air interface capabilities. For example, if the security policy includes physical layer keys and the system supports intelligent air interface and reconfigurable intelligent surface capabilities, SPEP can use these air interface capabilities to further enhance the security of the physical layer keys.

At the end, the following security capabilities are allocated to the industrial Internet + zero-power communication subsystems: lightweight authentication, distributed authentication, data-based authorization, physical layer keys, and blockchain.

- Blockchain and 6G Security
- Physical Layer Security and 6G Security
- 6G Era and AI Security
- Post-Quantum Security

Key Security Technologies for 6G Era

05

Blockchain and 6G Security 5.1

Blockchain, with its decentralized and trustworthy features, can facilitate data sharing and will become a key foundational infrastructure for industry digitalization during the 6G era. For industrial applications, telecom operators and blockchain service providers are actively developing blockchain infrastructure and offering blockchain services targeted at various industries and applications. These blockchain services include identity management, access authentication services, and security services.

Blockchain can be categorized into public blockchains, private blockchains, and consortium blockchains. Among these, consortium blockchains and private blockchains are considered trustworthy blockchains. Consortium blockchain allows multiple parties to participate and establish trust relationships among them through security algorithms. Thus, consortium blockchain can be used to realize a multi-party trust model in the 6G, building an inherent and trustworthy root of trust among multiple stakeholders. Based on blockchain, the technology of Decentralized Digital Identity (DID), can support distributed identity management and can be used to realize distributed authentication when multiple parties are involved.

Zero-power devices are a type of lightweight IoT terminal and are limited by computational and storage resources. These limitations may preclude them from supporting traditional authentication computations. IBC (Identity-Based Cryptography) on the other hand, supports lightweight identity management and authentication mechanisms that can be used for low-cost authentication.

Spectrum sharing needs multi-party trust and an efficient billing mechanism. Leveraging blockchain's inherent trust features, consortium blockchain and smart contracts can support reliable cross-operator spectrum sharing. This ensures the credibility of billing for spectrum usage and reduces disputes.

5.1.1 Multi-party Trust Based on Blockchain

During the credential issuance phase, operators can flexibly establish security management with multiple service providers. Isolation between the various service providers are required allowing for independent management of security credentials. By leveraging blockchain technology, a consortium blockchain maintained by multiple parties can be utilized to facilitate multi-party trust establishment. Nodes within a consortium blockchain trust each other and are used for storing credentials of IoT devices. These credentials can be stored on the blockchain and obtained across different domains. As shown in Figure 5-1, while standalone certificate storage alone does not facilitate multi-party trust, certificate storage based on a consortium blockchain does support mutual trust among multiple parties.

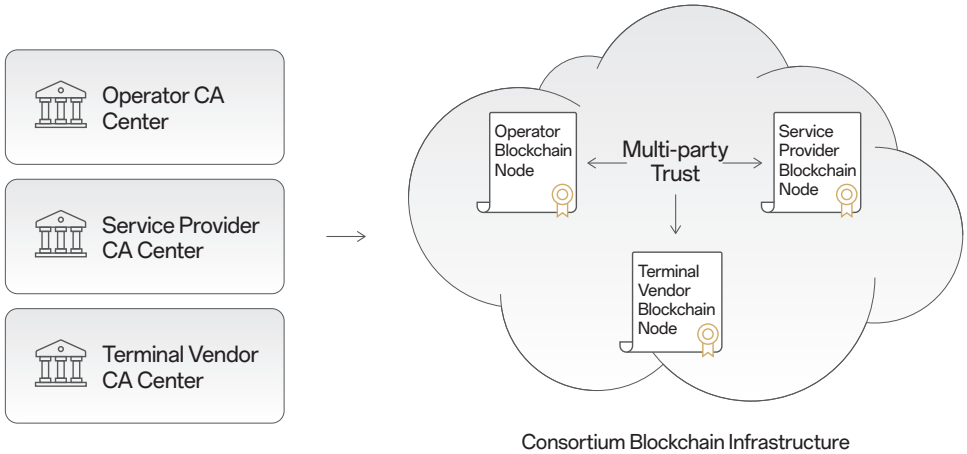

Figure 5-1: Independent Certificate Storage vs. Consortium Blockchain-Based Certificate Storage

Combining hierarchical security credential management and blockchain technology can achieve both multi-party trust and distributed trust, a useful feature for many new services in 6G.

During the security credential issuance phase, a tiered security credential management mechanism can facilitate efficient security management of mobile communication systems for vast number of IoT devices as well as enable operators to adopt flexible security management strategies for different service providers using these IoT devices.

Tier 1 CA center: based on secure multi-party computation (MPC), it manages and authorizes different service providers, while a subordinate CA center issues security credentials to the vast number of IoT devices. Such a hierarchical management mechanism makes the security management by service providers more efficient.

The hierarchical security credential management mechanism can be categorized into both a two-tier security credential management structure and a three-tier security credential management structure. A two-tier security credential management structure uses DID technology to manage the security credentials of connected devices, whereas a three-tier security credential management structure uses IBC to manage the security credentials of IoT devices.

Taking the three-tier security credential management structure as an example, it includes the following functional entities, as shown in Figure 5-2:

Three-tier Credential Management Structure

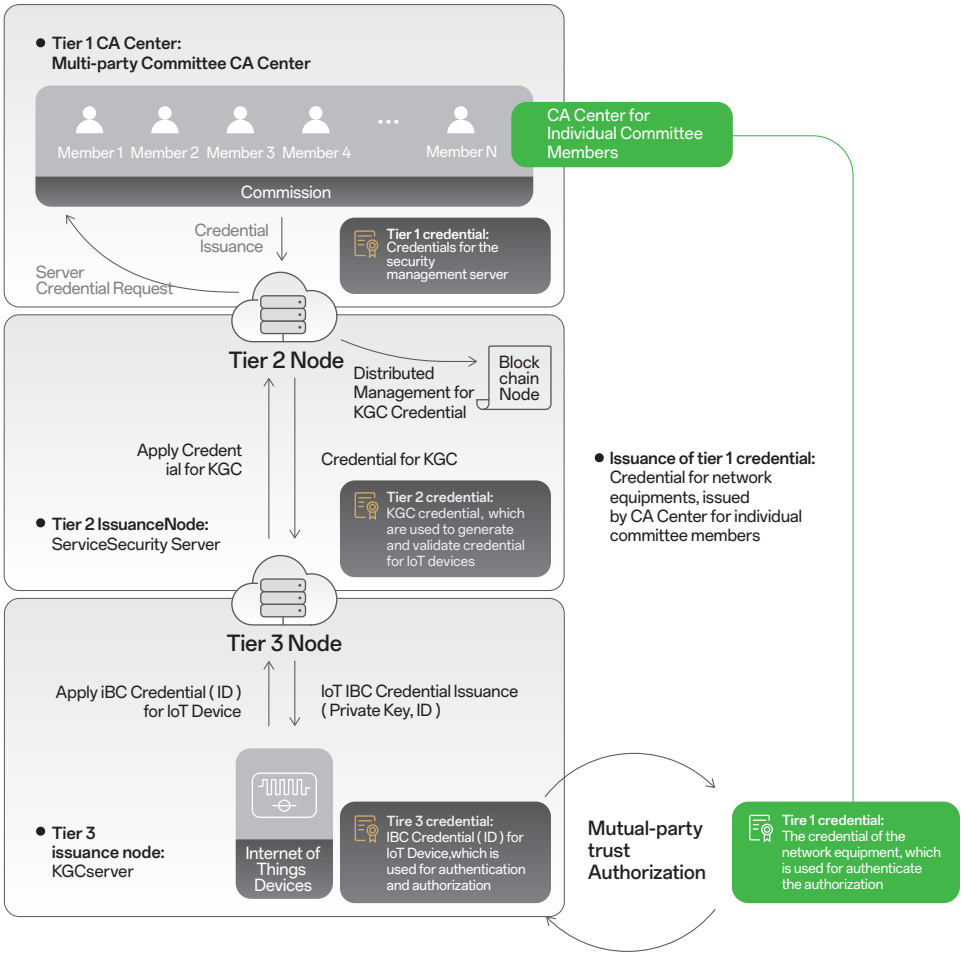

Figure 5-2: Three-Tier Security Credential Management Structure and Multi-Party Trust

The Tier 1 credential issuer

The CA center is jointly established by members of a multi-stakeholder committee, which can include national nodes, major operators, and terminal vendor. Its function is to issue credentials to Tier 2 security credential management servers and maintain revocation lists for the credentials. This is conducive to the collaborative establishment of a trusted root of multiple parties.

One of the operator committee members within the committee CA center can individually issue credentials to network equipment for that specific operator, and the credential for this network equipment is a Tier 1 credential.

The Tier 2 credential issuer

Service security credential management server, whose main functions include issuing credential to the IoT device Key Generation Center (KGC) servers and maintaining revocation lists, as well as storing the security credentials of the KGC servers on the blockchain.

Since the Tier 1 credential issuer is a virtual node and lacks the capability to access the blockchain, a Tier 2 credential issuer is required to access to the blockchain and complete the process of storing credentials on the blockchain. Subsequently, it is necessary for the Tier 2 credential issuer to issue credentials to the KGC, rather than having the Tier 1 credential issuer directly issue credentials to the KGC.

The Tier 3 credential issuer

KGC, (i.e., the IoT devices security credential management server), can be deployed by service providers, operators, or even be delegated to service platforms and terminal manufacturers for deployment. Its function is to issue and revoke credentials to IoT devices using IBC technology. The KGC uses IBC to manage the security credentials for a massive number of IoT devices under its trust domain. At this point, the security credential of an IoT device is simplified to an ID endorsed by the issuer KGC. In this case, the security certificate of an IoT device consists of {ID, KGC credential}. In addition, the KGC maintains a revocation list for the IDs of IoT devices, recording the identity information of revoked IoT devices to prevent the misuse of credentials from devices that have been revoked.

Hierarchical management structure facilitates the distributed dissemination and management of security credentials for a massive number of IoT devices within a mobile communication system, greatly improving the efficiency of security management. Since the IoT device credentials management servers are issued with the involvement of operators, this hierarchical security credential management structure also improves the security management efficiency for various IoT devices in different services under the control of operators, reducing the complexity of management.

In a three-tier security credential management structure, the Tier 1 credential issuer is a CA center jointly established by members in a multi-party committee, which can consist of mobile network operators, terminal device manufacturers, etc. The jointly established CA center issues security credentials to KGC. KGC issues security credentials to service providers, and finally, service providers issue security credentials to IoT devices. As a result, the Tier 3 credentials of IoT terminals and the Tier 1 operator equipment security credentials issued by the individual operator committee are mutually trusted by each other. Therefore, IoT devices whose credentials are issued by service providers can authenticate and authorize with operator equipment, as well as mutually authenticate and authorize with the service provider servers, thus establishing multi-party trust among operators, service providers, and terminal manufacturers.

5.1.2 Blockchain Supports Distributed Identity Management and Data Authorization

When an IoT device receives a data request, it needs to perform identity verification and data authorization for the requesting functional entity to confirm that the counterpart has appropriate permissions before transmitting the data. Due to the adoption of multi-party trusted security credential management, mutual authorization among multiple parties becomes possible. The security credentials of IoT devices can be trusted mutually with the security credentials of operator's devices and the security credentials of business entities, thereby authorizing the corresponding business entities to access the data provided by the IoT devices.

During the authentication and authorization phase, since blockchain supports the distributed management of security credentials, it enables distributed authentication, which does not require access to centralized nodes for performing authentication. Instead, security credentials can be stored on a consortium blockchain, and network edge nodes can access the consortium blockchain to obtain credentials and perform verification and authorization. This greatly improves authentication efficiency in scenarios involving a massive number of IoT devices, reduces the workload on network equipment, and avoids network authentication service interruptions due to potential single point of failure.

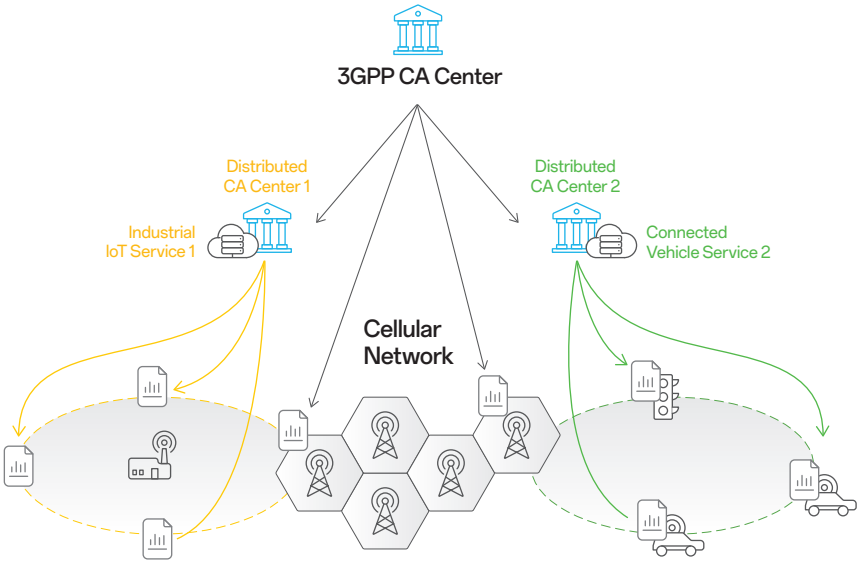

Figure 5-3 : Distributed Identity Management

As shown in Figure 5-3, for service that requires distributed access (such as cross-domain logistics service), IoT devices need to connect to the mobile cellular network at multiple locations. In this case, security credentials can be stored on a consortium blockchain, and network edge nodes can access the consortium blockchain to obtain these credentials, thereby achieving distributed identity authentication and data authorization.

For lightweight IoT devices, storing of IoT device security credentials on blockchain can reduce the cost of security management. In addition, an agent model can be adopted to implement identity authentication and authorization, where a UE or proxy agent device verifies the security credentials for lightweight IoT devices. This can reduce the storage and computational overhead for lightweight IoT devices. Moreover, the agent model can be used manage and securely verify IoT devices in a group fashion, which, compared to the process of individually security verification for each IoT device, reduces the latency of processing.

Distributed Identity Authentication

When operator network equipment or service provider servers need to verify IoT device credentials, they can use the IoT device's ID and the location of its credentials on the blockchain to obtain the corresponding credentials from the distributed blockchain nodes. There is no need to obtain credentials from the core network, allowing for distributed authentication to be performed.

Multi-party Trust Data Authorization

When an IoT device needs to authenticate the identity of operator network equipment or service provider servers and permit them to access data, the IoT device can receive the security credentials sent by the operator network equipment or service provider servers. After verifying the identity, it grants access to the data based on the permissions associated with that identity. The IoT device will only send data upon successful authorization and will only send it to the corresponding operator network equipment or service provider servers.

The process of identity authentication and data authorization between IoT devices and network equipment based on the three-tier security credential management structure is shown in the following Figure 5-4:

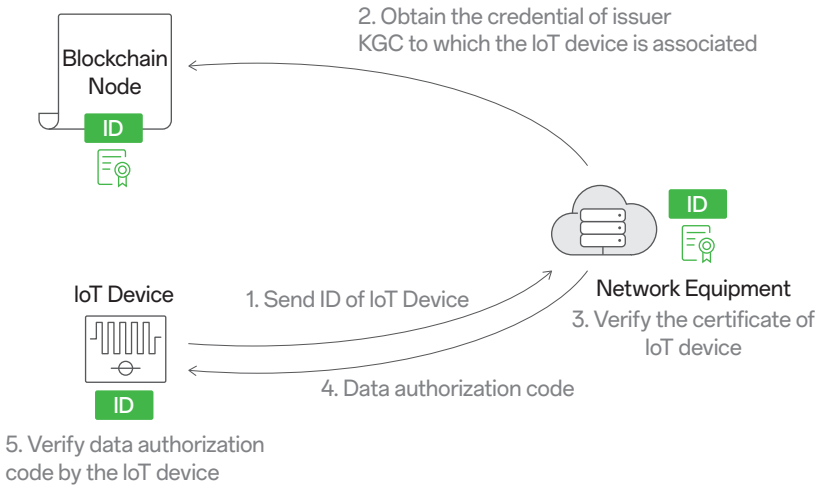

Figure 5-4: Process of Identity Authentication and Data Authorization between IoT Device and Network Equipment

The process of authentication and authorization between network equipment and IoT device can be divided into the following steps:

01	The IoT device sends its ID and the location information of its corresponding KGC certificate on the blockchain to the network device and uses its private key to calculate an identity authentication code.
02	After receiving the ID and location information on the blockchain, the network equipment retrieves the KGC's credential associated to the IoT device from the blockchain node. The network equipment is a node that can access the blockchain, and considering the distributed nature of blockchain nodes, the network equipment can be an edge node like a base station or a core network device. The blockchain nodes of the consortium blockchain support multi-party trusted credential storage. For network equipment, credentials obtained from consortium blockchain nodes can be trusted, even if the credentials were not issued by the issuer of the network equipment.
03	Based on IBC technology, the security credentials of an IoT device consist of {ID, KGC certificate}. The network equipment uses the ID sent by the IoT device along with the KGC credential to verify the identity authentication code, thus completing the authentication of the IoT device's identity.
04	The network equipment sends a data request message and a data authorization verification code to the IoT device. The message includes the network equipment's ID and credential, and it can also include the service provider's ID and credential. The purpose is to inform the IoT device which operator and which service provider are requesting to obtain the related data. The data authorization verification code is generated using the private key corresponding to the credential.
05	The IoT device uses the received credential to verify the data authorization verification code.

After completing identity authentication and data authorization, the IoT device sends data to the network or to the service provider.

5.1.3 Blockchain Supports Highly Reliable Spectrum Sharing

For spectrum sharing scenarios, operators can sell (e.g., rent or lease) parts of their vacant spectrum resources to other operators, allowing users from other operators to access the acquired spectrum resources in a secure and controllable way. To prevent resource abuse and billing disputes, and to ensure authorized access to the spectrum, and execute transparent, reliable, and real-time billing, a secure and efficient system can be established through the collaborative actions of blockchain and smart contracts.

Blockchain and Distributed Ledger Guarantee Trust and Authorization

Blockchain technology provides a foundation for distributed security management in spectrum sharing. The distributed ledger of the blockchain records and stores information about spectrum authorization credentials and smart contracts. This distributed storage mechanism supports transparency and security, ensuring that all parties involved can view and verify the status of the credentials and guaranteeing that spectrum authorization information and smart contracts are tamper-proof.

Smart Contract Ensures Automated Billing

Smart contract, stored on the blockchain, automates the process of spectrum authorization and billing by executing predefined rules. It can automatically trigger the spectrum authorization process based on preset conditions, ensuring real-time and reliable spectrum allocation. Smart contract also supports an automated billing process that automatically deducts (or bills) the predetermined fees based on the spectrum usage. This reduces the possibility of human error, increases the accuracy of billing, and effectively avoids disputes over spectrum sharing billing between operators.

The identity management of users and the authentication and authorization process for spectrum sharing are described in the following figure.

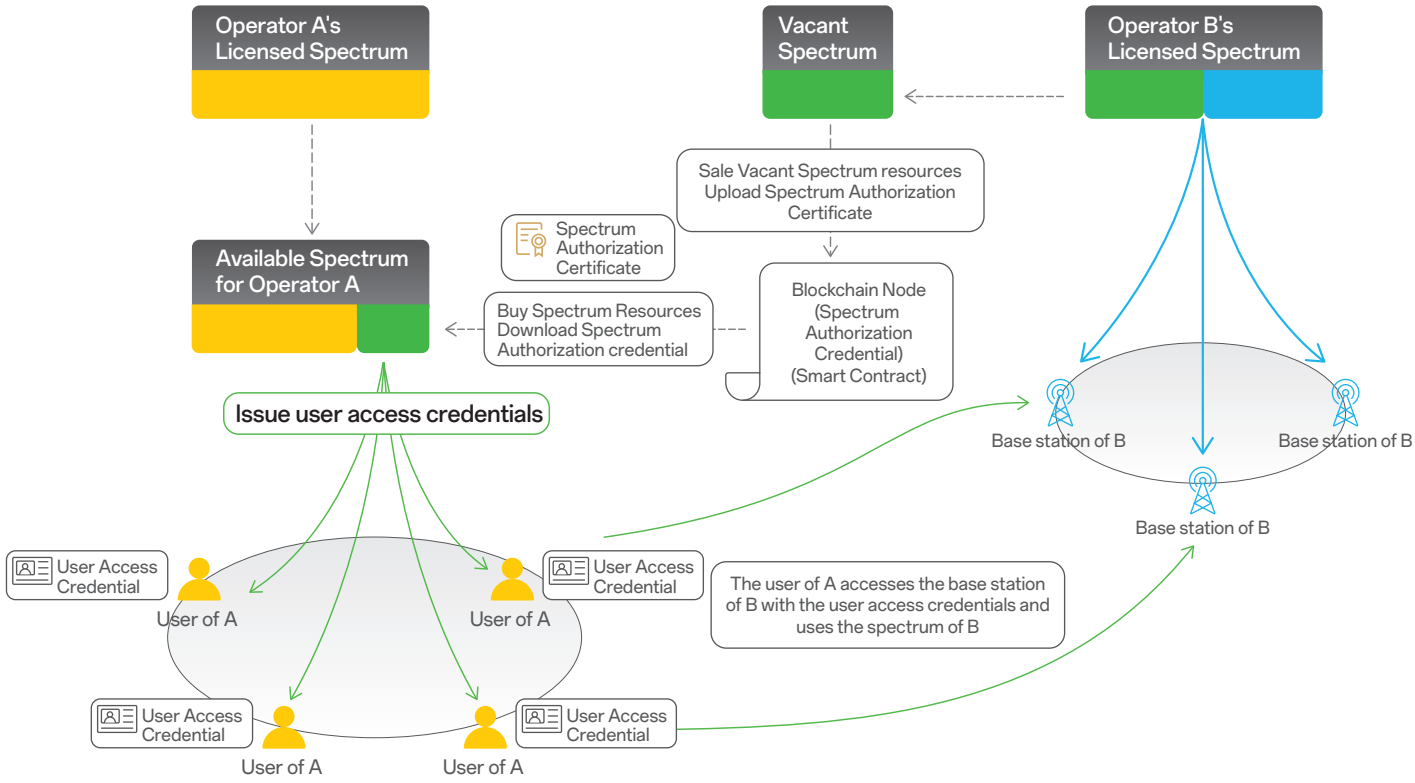

Figure 5-5 Blockchain Supports Intelligent Billing for Spectrum Sharing

If Operator B wants to share the vacant spectrum with another operator, Operator B can store the authorization credentials for this segment of vacant spectrum on blockchain nodes. Due to the transparency and security of the blockchain, the spectrum authorization information can be verified by members of the consortium chain and is tamper-proof. Authorization credentials stored on any distributed blockchain node can be used for user access, thus ensuring efficient and rapid user access and authorization. If base stations can access the blockchain nodes, then users can complete the spectrum sharing access authorization at the base station side, without the need to go through the roaming authentication process in the core network.

If operator A wants to access the vacant spectrum of operator B, a multi-party trust established based on blockchain technology allows direct access to operator B's vacant spectrum using the user's credentials, completing the processes of identity verification and spectrum authorization.

The billing between operator A and operator B can be completed through smart contracts stored on the blockchain. Due to the transparency and security of the blockchain node storage mechanism, the storage and execution of smart contracts can be verified by the members of the consortium blockchain and cannot be tampered with. Operators A and B can agree on billing rules and billing trigger conditions within the smart contract according to business arrangements, so that once a user accesses the shared spectrum, billing can be triggered and executed according to the agreed-upon rules.

Physical Layer Security and 6G Security

5.2

The emergence of new terminals and connection modes in 6G represented by zero-power communication, ISAC, and massive connectivity poses challenges to existing security mechanisms. The current authentication and key agreement mechanisms that rely on secure computation based on shared root key require devices to have certain computational capabilities, which may not be supported by zero-power terminals or devices. Moreover, the existing cryptographic security mechanism used by the upper-layer protocol for encryption and integrity protection cannot be used to protect the physical layer signal, such as the sensing signal. Traditional key distribution mechanism for vast number of devices attempting to establish communication leads to a lot of security signaling overhead as well as computational overhead. More efficient key management methods are needed. In 6G, it is beneficial to consider extending the existing upper-layer security mechanism to the physical layer to ensure the authenticity, confidentiality, integrity and availability of communication and lower layer signals. Physical layer security, by taking advantage of the characteristics of wireless channels, propagation environments and communication devices to provide a security defense mechanism based on information theory, is not only able to improve the efficiency of key agreement compared to traditional security mechanisms but also can be combined with existing higher-layer security mechanisms to achieve a full-stack and bottom-up security protection.

With the advancement of 6G air interface technology, the potential for applications of physical layer security has improved significantly. The higher frequency, increased bandwidth, larger antenna arrays, and more controllable electromagnetic environments introduced by RIS create a wealth of channel resources for the design of physical layer security in 6G systems. Moreover, the introduction of ISAC along with intelligent air interfaces further enhances the appeal of the wireless environment when coupled with these extensive channel resources. Based on the wireless environment, physical layer security mechanisms tailored for 6G can better meet the security needs under 6G telecommunications service scenarios by choosing appropriate physical layer security capabilities, such as physical layer key generation, physical layer authentication, physical layer secure transmission, and physical layer encryption. The integration of 6G and physical layer security technologies is illustrated in Figure 5-6.

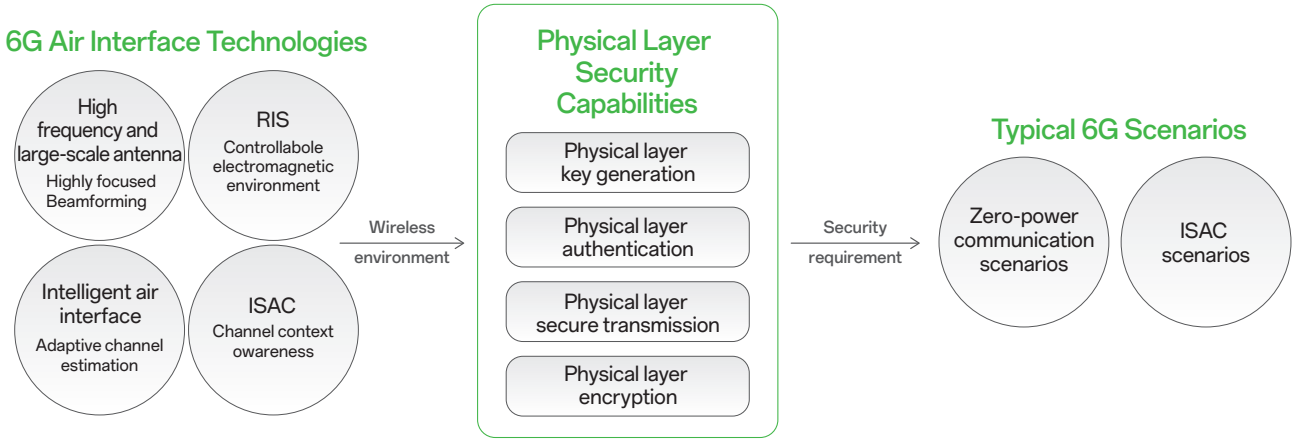

Figure 5-6: The Integration of 6G and Physical Layer Security.

5.2.1 Wireless Environment and Air Interface Technology

The development of 6G will integrate a variety of new air interface technologies, which creates favorable conditions for the application of physical layer security.

Integrated Sensing and Communications

In ISAC, sensing nodes can dynamically obtain contextual information of wireless channels. ISAC will facilitate the interoperability of communication capabilities and sensing capabilities. On one hand, ISAC, with the aid of communication systems, can enhance the sensing precision, improve the sensing timeliness, and achieve seamless and ubiquitous sensing services. On the other hand, ISAC can enhance wireless communication system performance by leveraging the perception, recognition, and prediction of the wireless channel environment. Additionally, it can empower the involved communication parties to implement physical layer security techniques over wireless channels, such as physical layer key generation.

Intelligent Air Interface

AI can aid 6G systems in training air interface channel datasets to obtain and predict precise channel state information, thereby enhancing the performance of physical layer key generation. Furthermore, AI-based beam management can achieve precise beamforming, which is instrumental in facilitating the secure transmission of wireless signals. Given the increasing heterogeneity of 6G system deployment scenarios, spectrum usage, application requirements, and device capabilities, the number of physical layer parameters is expected to increase exponentially, further enhancing the appeal, efficiency, and accuracy of physical layer security. AI will play an increasingly pivotal role in the air interface, further creating favorable conditions for the application of physical layer security.

High Frequency and Large-scale Antenna

6G is anticipated to push communication into higher frequencies bands and greater bandwidths with larger-scale antennas. Physical layer key generation, which relies on the entropy of the wireless channels rather than fixed parameters provided by specific entities, will benefit from the transition to higher frequencies as this provides greater entropy, thus increasing the efficiency and performance of key generation in the physical layer. Furthermore, large-scale antenna systems that utilize higher frequency bands such as millimeter-wave and terahertz usually require directed transmission to focus energy on the receiver, and this narrow beam directional transmission further helps in resisting targeted eavesdropping attacks.

Reconfigurable Intelligent Surfaces

RIS can precisely control and adjust the wireless channel propagation environment that in turn enhances the security performance in terms of physical layer secure transmission and physical layer key generation. By reflecting incident waves and steering them towards the desired direction, it is possible to control and finetune the wireless propagation environment to better aid physical layer key generation. Additionally, with the aid of RIS, sharp pencil-beam can be configured for secure transmission, making it difficult for attackers to eavesdrop.

5.2.2 Physical Layer Security Capabilities in Typical 6G Scenario

The physical layer security capability can be an independent module that can be integrated into nodes and protocols in 6G access network. Based on wireless environment, deployment scenario, and security requirements, the best physical layer security feature suited for the scenario can be selected, incuding physical layer key generation, physical layer authentication, physical layer secure transmission, and physical layer encryption, etc. For example, to reduce the power consumption of zero-power devices, physical layer key can be generated to protect AS secure transmissions. For ISAC scenarios, properly designed sensing reference signals based on shared information exchanged between the sensing and sensed nodes can be used to protect sensing result from eavesdroppers. For deployment scenarios involving massive connections and vast number of devices, physical layer authentication techniques can reduce the signaling overhead traditional authentication methods brings to the network and at the same time improve the efficiency of security management.

Physical Layer Key Generation

The fundamental principle in physical layer key generation is based on the randomness, time-variance, and reciprocity of wireless channel to generate shared key between two devices. Since an eavesdropper will not share the same channel characteristics as the sender and receiver, he cannot generate the same shared key. The physical layer key generation process includes channel probing, feature extraction, randomization, bit quantization, reconciliation, and privacy amplification. Channel probing is the process of exchanging probing signals between two nodes within the channel coherence time using techniques such as channel estimation or other similar techniques to extract the needed signal characteristics. Considering the power consumption limitation of zero-power device being in the receiving end, simpler operations related to direct measurement of the signal characteristics from the received signal, bit quantization, and extraction of key bits can be left to the low-power receiving node to perform while leaving other more complex signal processing such as channel estimation to a more powerful transmitting end (e.g., a base station or a UE). This power-friendly key generation mechanism can suitably support key generation for resource-constrained devices such as zero-power IoT devices. In addition, for indoor zero-power IoT communication scenarios where the wireless channel condition changes are slow, the key generation rate can be improved by artificially introducing randomness in the transmitted signal or in the randomization process.

Physical Layer Authentication

The fundamental principle of physical layer authentication is based on the uniqueness, randomness, and unpredictability of wireless channel. Unless two communication nodes share a completely consistent time domain, frequency domain and air interface domain, they cannot be spoofed in theory. Physical layer authentication can be based on either RF fingerprinting or based on physical wireless channel characteristics. Hardware fingerprinting physical layer authentication can be used in zero-powered IoT communication taking advantage of certain unique characteristics of hardware devices (such as a Physical Unclonable Function, PUF) to extract unique identifiers that can be bound to a zero-powered IoT device as a security credential and therefore removing the need to pre-provision or store such a credential (e.g., pre-shared secret) in Non-volatile Memory (NVM) of the device. In doing so, lightweight authentication and key agreement can be achieved at the same time. Physical layer authentication based on wireless channel characteristics can be used in integrated sensing and communication scenarios for authentication of sensing signals. Taking advantage of the incoherent characteristics between wireless channels of devices coming from different locations, the receiver can calculate the similarity of two received sensing signal frames to determine whether the sensing signal comes from a legitimate source.

Physical Layer Secure Transmission

Not relying on upper layer protocol and encryption algorithm to provide security, physical layer security is based on Shannon's perfect secrecy theory and Wyner's wiretap channel model [15] to establish secure channels. Zero-powered devices are limited by compute and storage resources and cannot support traditional security mechanisms such as PDCP layer encryption using encryption such as 256-bit AES. In this case, physical layer secure transmission provides a good alternative and a good supplement to the traditional security mechanisms for the zero-powered devices to achieve light-weight security communication. For example, to prevent uplink eavesdropping, an auxiliary node can introduce or inject randomly generated artificial noise to the Manchester coded uplink information being sent by the zero-powered device. Since auxiliary node and the primary node have pre-shared knowledge of the artificial noise injected into the Manchester coded uplink information while the eavesdropper lacks; the main node can easily recover the information sent while the eavesdropper cannot.

Physical Layer Encryption

Physical layer encryption uses phase rotation, amplitude adjustment, symbol ambiguity and symbol sequence changes techniques to generate physical layer signals to protect the modulation method and modulation symbol information and prevent eavesdroppers from recovering the correct information. It is a technique that can be used to prevent eavesdropping of sensing signals in integrated sensing and communication. In one aspect, the two receiving ends of the sensing signals use the shared encrypted reference sequence. Since the shared reference sequence is not known to an eavesdropper, he cannot perform channel estimation. At the same time, both receiving ends can use the shared information to generate random phase, random amplitude, and random subcarrier and other parameters to encrypt the modulation signals. Since eavesdropper is not aware of the shared information, again, he cannot generate the same random phase, random amplitude, and random subcarrier, etc., and cannot obtain the channel state information or the sensing results.

6G Era and AI Security 5.3

5.3.1 Secure Use of AI in 6G

As a basic infrastructure component to support new users, new applications, and new services, AI and related capabilities will be integral part of communication in 6G. 6G is expected to use native AI for designing new air interface as well as enhanced air interface capabilities. Wireless networks that support AI will be the base for all 6G network design and to provide services for all kinds of AI applications [5].

The secure use of AI in 6G (Security for AI) and how to enhance 6G system to use AI securely is a fundamental topic. The security of 6G air interface will include how to securely use AI to enhance upper layer application, how to prevent attackers from misuse channel estimation impacting services.

Security for AI maps to the AI/ML learning model and is subdivided into three stages and are exposed to seven risks. Thes are training stage, inference stage and transfer stage. The associated risks are data theft and data modification, privacy leakage, model compromise, adversarial attack, model inversion, and model extraction.

Training Stage

Attacker targets the security and privacy of training data. Attacker injects malicious or misleading data into a federated learning training data in an attempt to observe impact to the training result in order to infer or extract privacy information from the training data. The associated threat is data theft and privacy leakage.

Attacker targets the training model. Attacker poisons the federated learning model by injects malicious data in order to impact the accuracy and reliability of the training model. The associated threat is model compromise.

Inference Stage

Attacker targets the inference result. Attacker injects malicious into the training data in order for the training model to produce an incorrect output. The associated threat is model inversion.

Attacker target is the data model. Attacker uses some background knowledge and feeds large amount of data to produce outputs in order to learn about internal structure and functionalities of the data model as well as inferring certain parameters used in the model. The associated threat is a model extraction.

Attacker target is security and privacy of training data. Attacker uses some known information of the training model and background knowledge in order to recover the training model. The associated attack is model inversion.

Transfer Stage

Attacker targets are training data, training model, gradients, test data, inference results, etc. Attacker uses attempts to intercept or modify data during transfer by attacking the networks. The associated attack is data theft and data modification.

ML Stages / Attacker Target	Training Stage	Inference Stage	Transfer Stage
Data and Privacy	Data Theft Privacy Leakage	Model Inversion	Data Theft Data Modification
AI Model	Model Compromise	Model Extraction	Data Theft Data Modification
Inference Results		Adversarial Attack	Data Theft Data Modification

Table 5-1 AI Security Risk Analysis in 6G

How AI security research complements 6G development and adaptation needs to take into consideration the system capabilities and requirements in 6G. For example, how to use the existing user authorization and authentication mechanisms to reduce security risks brought by malicious users in mobile networks, how to integrate upper layer and secure transport mechanisms in mobile network to protect and prevent data intercept or modification and user privacy compromise over the air interface, whether or not and how to introduce new mechanisms such as privacy-preserving computation or homomorphic encryption, how to introduce federated learning over distributed computing, etc., are all important 6G security research topics. This is especially important considering that more and more AI related training is taking place in the mobile network and by the UEs.

5.3.2 Intelligent Security Policies

6G will morph into an architecture for native intelligence. Ubiquitous AI provides the network enhancement capabilities for 6G, including security capabilities. This is AI for security.

Faced with diversified services and data from multiple sources in 6G, security policies must be intelligent, flexible, and dynamic. New services introduced by 6G will vary greatly such that differences in security requirements and security capabilities are expected, for example, zero-powered devices and NB-IoT devices will co-exist, both of which have differences as well as similarities in security requirements and security capabilities. Distributed trust model and distributed authentication mechanisms will not replace centralized authentication mechanisms. Lightweight security and secure transmission will supplement existing security in zero-power communication scenarios.

Security architecture based on zero trust uses intelligent security policy orchestration and can effectively adjust to different security requirement needs of different services and provide appropriate security capabilities for all subsystems in 6G. For the specific security mechanisms please refer to Chapter 4.2 (Intelligent security based on zero trust) of the present document.

Post-Quantum Security 5.4

Quantum computing in the 6G is rapidly maturing. Since quantum computing capabilities are expected to far exceed existing computing capabilities, cryptography research to resist quantum-based attacks has become an important research area. This area is called post-quantum security that include research to develop quantum resistant techniques in key generation, key distribution mechanisms, quantum-resistant security algorithms (including encryption algorithms, hash algorithms), and quantum-resistant security protocols.

5.4.1 Vulnerabilities Brought about Advance in Quantum Computing

The advance in quantum computing has opened up a new page where tremendous computing capabilities in 6G are required. However, the development in quantum computing also introduces serious security challenges to the entire industries.

Currently, the cryptographic algorithms commonly used in the industry are designed based on highly complex mathematics such as large integer factorization and discrete logarithms arithmetic. Reversing these mathematical calculations that are used to achieve security (or cracking the encryption) requires existing supercomputers to spend hundreds or even thousands of years. With quantum computing maturing, supercomputers based on quantum computing can perform large numbers of calculations that traditional computers cannot achieve in a short period of time. Existing cipher algorithms are faced with unprecedented threats, especially for security algorithms based on asymmetric keys, they risk being broken within days or even hours.

If such algorithms are broken by the use of quantum computers, not only is the encrypted information in the current communication systems susceptible to be intercepted, the encrypted data in storage is also in risk of being recovered, threatening the security of communication, security of data and the privacy of users. Post-quantum security has become one of the most important considerations in quantum computing.

5.4.2 Post-Quantum Security Research and Considerations

Post-quantum security is primarily focused on the following considerations:

Post-quantum key generation and quantum key distribution

Traditional key generation and distribution is based on communicating parties having pre-configured pre-shared key or credentials. Sessions keys are generated mathematically as a result of successful authentication based on the pre-shared key. Quantum Key Distribution (QKD), on the other hand, is not dependent on complex mathematical computation. QKD is based on the principle of quantum transmission through optical links to send the key from the communicating party to the other party. In QKD, any observation and interference of the key transmission process will lead to key inconsistency, in that any theft and interference of the key during the communication can be easily detected by both parties, thereby ensuring the security of key transmission.

Post-quantum security algorithms

Hash algorithms that provide single-use (e.g., one-time pad) or time-limited signature all have quantum-resistance capacities. Based on the latest research and cipher algorithm design, lattice cryptography, multivariate public key cryptography, and coding-based cryptography are also capable of being quantum-resistant.

Post-quantum security protocols

Insecure algorithm negotiation, key-length negotiation, and initial parameter or vector negotiation, etc. can introduce potential risk and vulnerabilities even for secure quantum-resistant algorithms. The key to secure protocol starts with simplification. Starting with default configuration such as preferred algorithm and key length can reduce unnecessary negotiations and increase security at the same time.

Post-quantum key length enhancement

Both asymmetric algorithms as well as symmetric algorithms are used in the current mobile communication networks. Symmetric algorithms are used in more places such as in user authentication in key hierarchies based on shared root keys and ciphering. The impacts to asymmetric algorithms are greater than that of symmetric algorithms in quantum computing. Still, to lessen the impact of quantum and to increase the long-term security of symmetric algorithms being used in today's networks, 3GPP is in the process of enhancing the key lengths used in symmetric algorithms from 128 bits to 256 bits [16].

Concluding Remarks

6G security technologies and architectures will evolve around a plethora of new services, new end user terminals, new connections, and new architecture that are being developed in 6G. This white paper has explored in details key technologies such as blockchains, physical layer security, artificial intelligence security, post-quantum security that are expected to enhance the security in 6G. Additionally, this white paper has introduced an intelligent 6G security architecture based on security requirements, subsystem security capabilities, and security policy orchestration that can take into account best-practice security principles and security postures to flexibly adjust security policies on the fly. More importantly for operators, vendors, service providers and all 6G stakeholders, the 6G security architecture can flexibly introduce new security capabilities based on dynamic changes in service offering, adjust to new security requirements to securely configure capabilities and security policy for new services.

References

[1]. https://www.3gpp.org/news-events/3gpp-news/sec-5g

[2]. 3GPP TS 33.501 Security architecture and procedures for 5G System.

[3]. OPPO White Paper: 《Zero-power Communication》.

[4]. OPPO 6G White Paper: 《A versatile 6G wit minimized kernel: To build the mobile world》.

[5]. ITU Framework and overall objectives of the future development of IMT for 2030 and beyond.

[6]. OPPO White Paper: 《6G AI-Cube Intelligent Network》.

[7]. 3GPP TR 22.840 3rd Study on Ambient power-enabled Internet of Things.

[8]. 3GPP TS 22.369 Service requirements for ambient power-enabled IoT.

[9]. IMT 2030 6G Promotion Group: 《6G Vision and Candidate Technologies》.

[10]. 3GPP TR 22.837 Study on Integrated Sensing and Communication.

[11]. IMT 2030 6G Promotion Group: 《6G Typical Scenarios and Key Capabilities》.

[12]. https://www.gsma.com/services/blog/blockchain-technology-and-streamline-roaming-processes/.

[13]. NIST SP 800-207"Zero Trust Architecture".

[14]. China Academy of Information and Communications Technology: 《Zero Trust Development Research Report》.

[15]. Wyner A D. The wire-tap channel[J]. Bell system technical journal, 1975, 54(8): 1355-1387.

[16]. SP-231788 SID NEW New Study on enabling a cryptographic algorithm transition to 256-bits.