Ericsson White Paper
GFTL-24:000588
May 2024

ERICSSON

6G Security – drivers and needs

Content

Executive summary

Mobile networks are becoming an integral part of society, leading to stronger requirements and increased demands for security and availability. As the cyber and physical worlds merge, and the use of mobile networks evolves beyond communication, 6G security will need to take a more holistic view, considering both communication and computation to a greater extent than earlier generations. Building on security from 5G, 6G network security will also be based on open standards, with an increased focus on operational aspects. In addition, new use cases and technologies, such as immersive communication and zero-energy devices, will necessitate renewed threat analyses and new security solutions. This white paper outlines drivers and needs to define security for a global 6G network platform.

Introduction

The sixth generation of mobile networks (6G), like its predecessors, represents an evolution of the previous generation. 5G networks are now being deployed worldwide, offering capabilities and opportunities for connectivity and interaction that are transforming society and everyday life. With over 1 billion subscribers in 2023 and an expected increase to over 5 billion by 2029 [1], 5G is poised to meet the communication needs of individuals as well as connected industry, transportation, and healthcare. As society's demands for connectivity and interaction continue to evolve and grow, 6G will follow a similar path [2]. Alongside this evolution, threats to mobile networks and applications are also evolving.

To meet increasing demands on existing and new domains such as smart agriculture, enterprise support systems, robot navigation, and immersive communication and merged reality, a 6G network must serve as a comprehensive network platform and provide new capabilities. These capabilities need to bridge the cyber and physical domains. One example is efficient management, control, and collection of sensor data from fleets of remote zero-energy devices and actuators in a factory or farming facility. Other examples are sensing capabilities in radio cells and advanced digital twins. For these capabilities to be trustworthy and usable in their domains, new security controls are required. Examples of this are new access control and data protection mechanisms, along with solutions to ensure availability, performance, or scalability.

Addressing these security controls and managing the rapid changes in implementation technologies imply shifts in mobile network development, deployment, and operation. To bridge the cyber and physical domains, it is also essential to adopt a holistic view of their services, considering communication and computation in tandem. Moreover, this holistic approach extends to security, thus also encompassing secure communication and computation.

It is important to recognize that while the 6G platform offers many security features, it might not encompass all the necessary components to secure certain use cases. For example, regulations might mandate confidentiality protection of sensitive medical data collected by a sensor, extending from the sensor, across the internet, to a hospital server. Additionally, regulations might request the data to remain concealed even from the 6G

platform providers, with restrictions on crossing country borders. In such cases, additional security measures must be applied expanding those from within connectivity services as well as those from within the infrastructure of the 6G platform.

Defining the 6G platform, while meeting regulatory, country-specific, and user expectations on network availability and security demands a comprehensive understanding of the driving forces and needs. This white paper outlines drivers for 6G security and identifies focus areas which often build upon security already established for 5G [3].

The drivers

Drivers come from different directions: society's adoption and embracement of technology, a rapidly evolving threat landscape, technology advances, and reuse, maintenance, and capitalization on existing deployed technology.

Bridging cyber and physical domains

The design of the 6G platform will factor in, and in some cases contribute to, technological and societal paradigm shifts [2]. Perhaps the most significant change is the transition from separate physical and cyber domains to a cyber-physical continuum, intertwining cyber security with privacy and physical safety. Digital services like social media, once viewed as tools to achieve something in the "real world", are themselves becoming part of the "real world", as the concept of the "real world" transforms from equaling only the physical domain, to a cyber-physical continuum where life can be lived almost completely online, to a point where the cyber domain becomes the "real world". As an increasing part of everyday life shifts to cyber, more and more things will be connected even though they were not originally designed to be. The pace of this shift is accelerating and necessitating renewed threat analysis, risk assessment, and development of new security solutions.

A concrete example of a technological shift bridging the cyber and physical domains is immersive communication and extended reality (XR)[4]. Integrated sensing and communication (ISAC), a crucial component of those technologies, involves reusing communication infrastructure and spectrum for sensing purposes. While some of the exemplifying use cases already emerged in 5G, 6G will expand further into entertainment, manufacturing, maintenance, education, and healthcare. This will generate a need for 6G to provide a baseline security level sufficient to address the data security and privacy concerns stemming from this development.

Another shift, already witnessed in 5G, is the use of artificial intelligence (AI) and automation. 6G is envisioned to move even further toward self-learning networks and machine-to-machine communication, underscoring the relevance of secure and trustworthy AI. Secure AI reflects that AI providing network functionality must be reliable and capable of resisting or mitigating attacks. This entails that 6G will need to consider not only threats against individual AI components but also threats arising from complex and emergent behavior among seemingly independent AI functions within the same network. Security and privacy solutions will need to be defined in a broader perspective, encompassing everything from data management to data ownership to strike a balance between data utility and data protection.

The transition from predefined services to a user-centric approach, where the network adapts to the applications that users run [2], partly depends on network exposure and the use of network application programming interfaces (APIs). While these APIs facilitate the sharing of network functionality with application providers, they also necessitate enhanced security to safeguard both network resources and the APIs themselves, along with enhanced privacy measures to ensure that user data is adequately protected.

As use cases and applications evolve, so too will devices, appliances, vehicles, buildings, and systems connecting to mobile networks. New kinds of devices will emerge with novel requirements, such as zero-energy consumption, demanding new, and more energy-efficient security mechanisms.

Connectivity is envisioned to transition from terrestrial 2D to global 3D, extending to truly global connectivity across rural land, sea, and air. Ongoing standardization work in 3GPP SA3 on security for satellite communication is expected to address the needs in 6G [5].

Responding to an evolving threat landscape

Threats against basic communication systems are well known, and carefully specified communication protocols have been introduced over time to mitigate these threats. Still the threat landscape is evolving. Current changes in the threat landscape for mobile networks, and new emerging threats, are not a consequence of the communication functions per se, but rather depend on other factors, such as the adoption of new implementation technologies like cloud and virtualization. Another factor is the introduction of new use cases, and the connection of new types of devices and systems to mobile networks, leading to the emergence of new threats. From a security standpoint, the most challenging threats arise when a service is used in ways it was not initially intended for.

The role of 5G and 6G mobile networks as part of the critical infrastructure brings about new regulatory requirements on security since the availability and proper functioning of the networks are of interest to society at large. Examples of such requirements include demands for higher security assurance and adherence to zero-trust [6]. Meeting these requirements goes beyond a single technology or standards. It requires a combination of standardization, implementation, deployment, and operational aspects and processes.

Taking this holistic view on 6G security is necessary to keep pace with an evolution where more traditional threats to data confidentiality or fraud are accompanied by larger-scale attacks on availability, by spyware, and by attacks on the critical national infrastructure [7] [8].

Building on security from 5G

As the mobile network evolves, security will continuously be enhanced. This means that 6G will inherit and build on the security defined and implemented for 5G [9]. This includes security standardized or specified in standardization related organizations like 3GPP, IETF, ETSI, NIST, O-RAN Alliance, as well as technology, processes, and tools used for security in 5G, such as defined in the security assurance scheme NESAS by GSMA. For 6G, standardization of security remains crucial, partly to keep the cost at a reasonable level, but also to provide a desired degree of vendor interoperability in 6G products.

5G security mechanisms include strong authentication, encryption, and integrity protection of signaling and data transmission, privacy-enhancing mechanisms such as temporary identifiers, and security assurance of implementations, to mention a few. Ongoing work in standardization also includes an update of access security algorithms to 256-bit ones with high performance both in hardware and software, and new security mechanisms for various use cases, such as northbound APIs, unmanned aerial vehicles (UAVs), and automated certificate management for the service-based architecture (SBA).

SBA constituted a pivotal shift in 5G and is notably influenced by new implementation patterns like virtualization and micro-service segmentation. These new implementation patterns come with new and different challenges in overhead, security, backwards compatibility, security assurance and management compared to past design patterns. It will be increasingly important to efficiently deal with these challenges as 6G will face higher demands on performance and security.

Merge of standard and implementation

As the use of networks expands across various services and scenarios, the standards governing them are becoming increasingly detailed. Existing implementations, for example, for cloud management and operating systems, are also becoming de facto standards that are assumed by traditional standardization organizations such as IETF and 3GPP. This means that more parties enter the ecosystem and need to align on security objectives, encompassing a broader spectrum of use beyond telecom alone. From a security point of view, it is important to note that convergence on single implementation components, while positive from a reuse perspective, reduces diversity and is known to increase the risk that many functions will be vulnerable because they all use the same component. Another trend driving down diversity is the increased use of micro-segmentation. All in all, this will make the effort of deploying and operating secure 6G networks increasingly a task of securely merging implementation and standard.

One example of specified implementations is the growing trend in standards to provide detailed instructions on establishing session layer security directly between functions. This contrasts with the past, where instead of individual functions, relatively large network layer security domains were deemed sufficient. The connections between the domains were designed to be protected with Internet Protocol security (IPsec), but the actual implementation of IPsec was quite open, leaving many options for both implementation and deployment.

Earlier generations of mobile networks are based on open and globally agreed standards, to provide interoperability, and from a security perspective to allow for verification of security protocols, interface definitions, and strength of cryptographic algorithms. 6G networks are envisioned to follow the same path, benefiting from the transparence added by the open and accessible nature of standards from organizations such as 3GPP, IETF, and O-RAN Alliance. While this process is partly fueled by using new efficient technologies and their design patterns, from a security perspective one can advocate standards to be free of implementation details.

The needs

6G security work, like all other security work, needs to be based on thorough threat analysis for use cases and technologies. Such work combines formal threat models like STRIDE with mobile-specific methods such as MITRE FIGHT [10], GSMA MOTIF, and the ENISA 5G Matrix [11], with enhancements to address more 6G-specific threats. While upfront threat analysis can never be exhaustive, the main threats need to be identified early on to guide and prioritize standardization and design.

Drawing from threat analyses, the security framework for 6G, akin to that of 5G, will rely on open standards and technologies, as well as methods and processes employed throughout the development, deployment, and operation of mobile networks. Five focus areas and corresponding needs to form 6G security are outlined as follows.

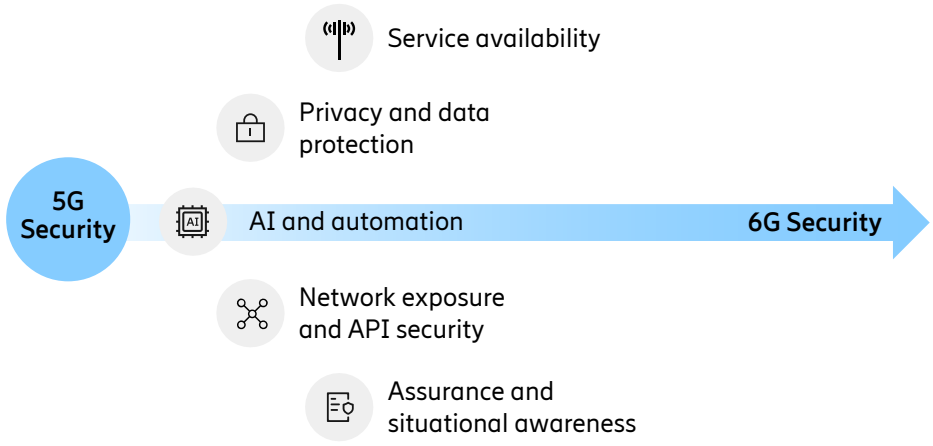

Figure 1: Focus areas for 6G security

Service availability

The 6G platform, in its various forms, will offer a range of services, with different types of users accessing different sets of these services. The availability of these services is vital for users and might even draw attention from regulators, particularly when a service is considered critical for society's functioning. Service availability refers to users being able to rely on the service to function during normal conditions, as well as when impacted by accidental or nature-induced failures, and even when the network is under attack. The extent to which such reliance is met depends on the criticality of the service. While the 6G platform will provide a base level, it will also allow for configuration to increase the degree of reliance when necessary. This adjustment could be made for specific services, in certain geographical areas, or on a larger scale.

Resilience against intentional attacks that affect availability is often achieved through considerations in architecture, protocol design, and network configuration instead of being added on as specific security measures. Measures also address networks in operation to mitigate attacks such as denial-of-service, signaling storms, and jamming. Cyber threat intelligence, extended to telecom use cases, will become increasingly important moving towards 6G.

Privacy and data protection

While previous mobile network generations focused mainly on communications security, 6G will need to consider the entirety of confidentiality and integrity protection for data in transit, data being processed or at rest, as well as key establishment, key management, and logging. In 6G, this will lead to an expansion of the scope: from protecting data to ensuring the wholesale service delivery, including protection of the network and processing infrastructure. By doing so, 6G will shift focus from data management to data ownership, covering functions to ensure control and privacy of personal and critical digital assets toward third parties.

Secure communication, data ownership, and API ownership increasingly contribute to place secure identities and the management of these identities at the forefront. While many modern digital identities are used over the top, 6G will leverage identities for controlling network access, managing network APIs and infrastructure, and regulating access to network exposure and edge compute APIs. For network access, the current trend in use of eSIM, the possibility to use authentication schemes based on the Extensible Authentication Protocol (EAP), and the ability to delegate authentication are setups that give 5G and 6G a wide range of options for human-held devices and IoT, as well as industrial devices to support future 6G use cases.

Much of 5G security is based on symmetric-key cryptography components that are generally accepted as quantum-resistant. However, some essential parts are based on asymmetric key cryptography, and subject to threats from future quantum computers. The adoption of new quantum-resistant cryptography that will mitigate such threats is expected from the first release of 6G [12]. NIST-defined algorithms will be integrated into 3GPP, often via updates to IETF standards to ensure quantum resistance. Many 3GPP-defined interfaces such as those in the 5G core SBA can support the new NIST algorithms without significant performance issues. The communication overhead of the new public key

algorithms should, however, be kept in mind, for example, for the radio access. Increasing demands on performance and data protection will also lead to the adoption of standardized high-performance security algorithms and protocols, such as high-performance 256-bit algorithms for radio access.

Immersive communication and ISAC will bring new performance and isolation requirements to ensure that expectations on data protection and user privacy are met. From a security and privacy perspective, measures and technical solutions will vary depending on the use case. In cases where there is no information indicating specific persons, or for use in closed environments, such as an automated factory building, security and privacy can most likely be achieved through existing technology and processes. In public networks, where multiple sources of data might be combined to provide information identifying persons, there is a need for further work.

AI and automation

AI is anticipated to play a significant role in both managing the 6G platform and offering service to users. Automation combined with AI can optimize performance, improve efficiency, and enhance the ability to respond to cyber attacks on the mobile network. Examples of AI being used to detect or respond to attacks in mobile networks include detecting misbehaving devices, detecting false base stations, and detecting and responding to signaling attacks. As the transition to 6G progresses, there will be a continuous increase in AI and automation for cybersecurity, for example, for threat intelligence or compliance verification.

From another perspective, the growing reliance on AI and automation imposes more pronounced requirements for AI to be robust, explainable, privacy-preserving, and safe. Addressing these requirements involves not only technological enhancements but also a deeper understanding of which properties are important from a security standpoint in any given application. Additionally, it requires knowing how to utilize AI technology effectively in potentially adversarial settings while acknowledging its limitations.

With the introduction of intent-based networking, it becomes essential to ensure that higher-level intents are appropriately translated into lower-level AI usage and automatic network reconfiguration.

Despite the increasing role of AI in cybersecurity, it does not replace skilled human expertise. Technology will assist cybersecurity experts in optimizing and improving response to cyber attacks on the mobile network through mechanisms such as threat intelligence, threat hunting, and attack detection. In the development of security standards, AI may serve as an aid for formal security analysis. Likewise, in systems development, AI may be valuable in identifying and explaining bugs.

Research on privacy-preserving mechanisms for AI in a 6G setting has been conducted in EU projects such as Hexa-X [13] including methods like differential privacy, homomorphic encryption, and secure multi-party computation.

Network exposure and API security

The expansion of services in 6G beyond communication will benefit from the flexibility of network exposure through APIs [14], to empower application and service developers with greater freedom and capabilities to customize use of the network platform. Accessibility to network capabilities and data can enhance gaming performance, drone management, or the broader use of XR in 6G [1], but will also require a focus on securing the API usage.

APIs both internally and for external exposure already exist in 5G with security according to telecom standards. This security includes, for example, authentication, authorization, and audit logging. With 6G, there is an expectation of increased exposure of network functionality to support use cases and foster innovation, inducing a need to enhance API security with proactive threat analysis, API posture management, and API runtime monitoring. While some API security aspects will be specified in standards, some will be part of mobile network operations. In mobile networks, there is a shared responsibility between vendors and service providers to handle security throughout the API life cycle.

Maintaining subscriber privacy is crucial when exposing network capabilities to external parties. Mechanisms to safeguard privacy extend beyond API security and require consideration.

Assurance and situational awareness

Security assurance has long been on the agenda for mobile networks. One outcome is the ongoing work on a cybersecurity certification framework by ENISA, and another is NESAS [15], a joint initiative by 3GPP and GSMA. NESAS already provides assurance by verifying compliance through mandatory testing of products, secure supply chains, and a secure software development lifecycle. This could be described as preventive assurance. In addition to this, 6G will need operational assurance of deployed networks, including system monitoring and applying reactive countermeasures.

Advanced monitoring in 6G will be used not only for assurance but also to offer a higher level of situational awareness regarding the operational status of the network to management systems and security teams – an important aspect of a zero-trust architecture (ZTA). Many of the zero-trust principles today defined by NIST [6] have already been applied in the standardization of 3G, 4G, and 5G networks by 3GPP, although not always explicitly identified as such, and 6G standardization will continue to apply such principles. Examples include the use of strong identities, securing communication between network functions, and authenticating and authorizing API use based on access to selected data exposed from the underlying network.

Adopting approaches such as those formulated for a zero-trust architecture will help establish a holistic framework for 6G security. This framework not only demonstrates that protection measures are in place but also allows for adapting to changes in operational conditions due to network dynamics, attacks, or part of the network failing (Figure 2). The concept of minimizing implicit trust between entities also extends to minimizing implicit trust between network layers and strengthening solutions to still provide some security even in the event of an initial compromise. An example of this is the effort to incorporate forward secrecy into the network access authentication and the Authentication and Key Agreement

(AKA) procedure in 3GPP. Overall, 6G standards are envisioned to build upon a zero-trust architecture and leverage technology enablers such as remote attestation and confidential computing vertically throughout the compute stacks.

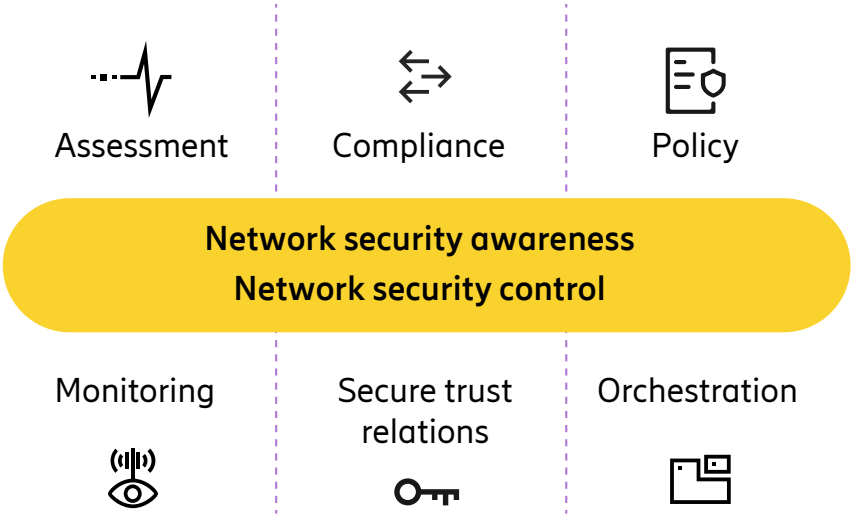

Figure 2: Combining different approaches to build a holistic security framework for 6G, for assurance and situational awareness

Conclusion

Evolving from 5G security the security for 6G will use additional measures to respond to an evolving threat landscape and to support new use cases, shifts in technology and society, and regulatory requirements. With mobile networks increasingly being considered as part of critical infrastructure, and with the cyber-physical merge emphasizing the role of connectivity in everyday life, 6G security will need to be based on a holistic view, combining different solutions and approaches to gain situational awareness. Automated security and threat management, operational assurance, and mechanisms adhering to zero-trust principles will contribute to the situational awareness.

Global open standards will continue to form the base for mobile networks, ensuring interoperability, security, and providing transparency. In addition, there is an increasing merge of standard and implementation, and deploying and operating 6G networks securely will to an increasing degree be a task of securely merging standards, open source, and various implementation technologies.

While the 6G security view will have to be all encompassing, there are specific topics that deserve attention moving forward: availability of network services, new requirements for data protection and privacy, ensuring 6G is quantum-resistant, secure AI and automation to enhance network security, network exposure and API security, and operational security assurance.

Research, innovation, and collaboration in these areas will contribute to the foundation of 6G security and will be integral to ongoing work on standards and technology that will shape the 6G platform security and the security of its future use cases.

Glossary

3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
API	Application Programming Interface
EAP	Extensible Authentication Protocol
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
GSMA	GSM Association
IETF	Internet Engineering Task Force
ISAC	Integrated Sensing And Communication
NESAS	GSMA Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
O-RAN Alliance	Open Radio Access Network Alliance
SBA	Service-Based Architecture
UAV	Unmanned Aerial Vehicle

References

1. Ericsson Mobility Report November 2023
2. 6G – Connecting a cyber-physical world - Ericsson
3. 5G security - enabling a trustworthy 5G system
4. Immersive technology: The future of entertainment - Ericsson
5. Promising new 3GPP technology for satellite communication - Ericsson (Using 3GPP technology for satellite communication)
6. NIST Zero Trust Architecture
7. GSMA Mobile Telecommunications Security Landscape report 2023
8. ENISA Threat Landscape 2023
9. A guide to 5G network security 2.0 - Ericsson
10. MITRE | FiGHT™
11. 5G Security Controls Matrix — ENISA (europa.eu)
12. Quantum technology and its impact on mobile network security - Ericsson
13. Hexa-X – EU flagship project on 6G
14. Networking trends: A platform for next-level digitalization - Ericsson
15. GSMA Network Equipment Security Assurance Scheme (NESAS)

Authors

Karl Norrman has been working with cryptographic protocols and security architectures since he joined Ericsson in 2001. He played an active role in the standardization of 4G/5G security and served as Ericsson's security coordinator in 3GPP for four years. Currently, he is involved in 6G security research, focusing on standardization and software security. Karl holds a Master of Science (MSc) degree in Computer Science from the Department of Mathematics at Stockholm University, Sweden, and is pursuing a PhD in theoretical computer science, with a focus on formal cryptographic proofs at KTH Royal Institute of Technology.

Deeply involved in security standardization, **Bengt Sahlin** leads the security group at Ericsson Research NomadicLab in Finland. He joined Ericsson in 2000, initially focusing on mobile systems security and product security as a technical coordinator for security implementation projects. His engagement in standardization includes participation in 3GPP, ETSI, GSMA, and IETF. From 2010 to 2013, he served as the chairman of the 3GPP security working group Technical Specification Group Service and System Aspects (TSG SA) WG3. Bengt holds an MSc in Computer Science from the Helsinki University of Technology, TKK, Finland.

Ben Smeets primary area of expertise lies in trusted computing. His current work is centered around trusted computing technologies in conjunction with containers and secure enclaves. Ben earned his Ph.D. in information theory from Lund University, Sweden, where he currently serves as a professor. He began his career at Ericsson Mobile Communications in 1998, focusing initially on developing security solutions for mobile phone platforms.

Erik Thormarker's primary focus areas include cryptography, security protocols, and 6G security. He actively contributes to standardization efforts in cryptography within organizations such as the Internet Engineering Task Force (IETF), GSMA, and 3GPP. Erik holds an MSc from the joint master's program in mathematics at KTH Royal Institute of Technology and Stockholm University, Sweden. He wrote his master's thesis at Ericsson on post-quantum cryptography and joined Ericsson Research in 2018.

As head of the security department at Ericsson Research, **Eva Fogelström** and her team are deeply involved in researching and standardizing technologies that will build security for 5G and beyond, towards 6G. Their focus encompasses various areas such as trusted computing, identity management, AI, post-quantum crypto, and methods for security assurance. Driving security topics in standardization forums is an important part of their work. Additionally, they actively collaborate with academia and engage in external projects, leveraging their expertise in mobile network security. Eva holds a Ph.D. in Telecommunications and an M.Sc. in Electrical Engineering, both from the Royal Institute of Technology (KTH) in Stockholm, Sweden. Eva has been with Ericsson since 1997, contributing to advancements in security, mobility, and standardization.