OIC-CERT Journal of Cybersecurity
Volume 4, Issue 1 (April 2022)
21 - 36

OIC-CERT 5G Security Framework

Hulk Zhang[1], Aloysius Cheang[2], Xiaoxin Gong[3] Yang Ming[4]
[1,2]Huawei, Dubai, UAE
[3]Huawei, Shenzhen, China
[4]Huawei, Manama, Bahrain
[1]zhangshuo39@huawei.com, [2]aloysius.cheang@huawei.com,
[3]gongxiaoxin@huawei.com, [4]yang.ming@huawei.com

ARTICLE INFO

Article History
Received 01 Jan 2022
Received in revised form 21 Mar 2022
Accepted 28 Mar 2022

Keywords:
5G security framework; 5G risk repository; baseline security technical specification; certification mechanism; conformity assessment assurance.

ABSTRACT

OIC-CERT recognizes that 5G marks the beginning of a new era, and at the same time bringing in cybersecurity challenges to a successful 5G transformation. Thus, to effectively and timely address some of these challenges through a holistic way, according to the philosophy of both zero trust and team sports OIC-CERT has established the OIC-CERT 5G security framework as a foundation to demystify and simplify the journey of 5G adoption for OIC nation states where security is no compromise. In detail, it contains a 5G cybersecurity risk repository, a baseline security technical specification for addressing those risks, and a conformity assessment methodology to ensure the unified 5G cybersecurity conformity assurance level, respectively. This paper will systematically introduce OIC-CERT 5G security framework to continuously contribute OIC-CERT wisdom and effort to the 5G cyber security, and it is also time to show the related outstanding work to the world!

I. INTRODUCTION

Looking back the development of telecommunication technologies and industries over past decades, there are several outstanding features and functions impressing the world. Remarkably, the mobile telecommunication became possible when the first generation (1G) of wireless cellular technology was raised and applied. Then, the second generation (2G) technology made text messages be sent among mobile telecommunication users. And the third generation (3G) dramatically increased the user's experience in terms of surfing the internet and using the email through a mobile phone. Iteratively, during the fourth generation (4G) era, it is highly promoted that data transmission and video streaming speeds. By now, 5G or fifth generation is an advanced wireless network technology, and it is seen as a bigger step forward to improve connectivity on a massive scale, which are approached by three sets of use specifications defined by 3GPP, which are the ultra-reliable low-latency communication (URLLC), enhanced mobile board band (eMBB) and massive machine type communications (mMTC).

In this increasingly interconnected world, cybersecurity has become the fundamental guarantee. It has been the interest of all parties to ensure that the minimum endeavour has been provided to the digital transmission and management [1]. The fifth generation (5G) wireless technology represents a complete transformation of the telecommunication networks, which boosts the realization of the Fourth Industrial Revolution (4IR), where billions of devices will be connected to the Internet through this technology. It is predictable that 5G networks will have more than 1.7 billion subscribers worldwide by 2025 [2]. However, 5G digital transformation will continue to introduce new dimensions of attack vectors, surfaces, and vulnerabilities through the connected digital systems. Undoubtedly, cybersecurity has been the key guarantee for industry applications of 5G. In front of new changes and upcoming challenges, it is thus straightforward and indispensable to objectively and impartially consider 5G cybersecurity in a technical and non-political manner. Otherwise, it is impossible to effectively build, improve, manage and continuously optimize cybersecurity in 5G rollout and digital transformation.

Since the dawn of cybersecurity, inter border collaboration has always been a pillar in mitigating cyber threats. One of this collaboration is the Organization of the Islamic Cooperation- Computer Emergency Response Team (OIC-CERT), which is a platform for information sharing and development of cybersecurity capabilities for the members [3]. The OIC-CERT is an affiliate institution of the Organization of the Islamic Cooperation (OIC) and more information on this collaboration can be found at its official website www.oic-cert.org/en/. CyberSecurity Malaysia and Huawei UAE who are the OIC-CERT Secretariat and a Commercial Member respectively, to look at formulation the OIC-CERT 5G security working group at GISEC 2021 [19] to develop a systematic and fundamental safeguard under the situation of rapid ICT development. And this job is mainly intended for the regulatory authorities of the OIC member states, with the purpose of assisting them in making policies on regulating 5G equipment vendors, mobile network operators (MNOs), and the relevant service providers through a holistic way.

Same to all general cybersecurity objectives, OIC-CERT highly proposes to prevent against loss of availability and integrity of 5G network, related services and applications. Besides, OIC-CERT also concentrates on preventing against compromising the confidentiality of user information and leakage of any data that flows through the network or is stored in the devices connecting to the networks. To effectively approach these cybersecurity goals, OIC-CERT 5G security working group determined to establish OIC-CERT 5G security framework based on industry best cyber security practices and popular principles., such as zero trust [20] and team sports. At the same time, this framework is also supposed as a living document, so that it could be able to iteratively adapt the development of 5G security requests for different stakeholders of OIC regions.

For the structure of OIC-CERT 5G security framework, there are three closely related parts. Part one focuses on sufficiently demonstrating existing 5G cybersecurity threats, which can be also used as a template for upcoming risk analysis purposes. Then, part two constructs a baseline security technical specification to provide fundamental requirements and references for the purpose of effectively mitigating identified and upcoming risks. And part three defines a cross-recognition assurance methodology, to harmonize the designing, implementing, maintaining and optimizing cybersecurity conformity assessment among OIC member states, so that an individually certified security assurance could be mutually recognized by other member states. Furthermore, the OIC-CERT 5G security framework specifies roles and responsibilities of implementing 5G cybersecurity for different kinds of stakeholders, which include the network carriers, equipment suppliers and application providers. In other words, this proposed OIC-CERT 5G security framework is expected to dramatically enhance the entire level of 5G cybersecurity in OIC regions.

In the following paper, section two would compare and analyse related works, section three would demonstrate how we develop this framework, and section four clearly illustrates three parts of this 5G security framework and last section will conclude this paper.

II. RELATED WORK

Since OIC-CERT 5G working group proposes to develop a framework dedicated to regulation and authority agencies through a holistic way. It means that this framework is designed to assist 5G

ISSN 2636-9680
eISSN 2682-9266

cyber security governance, including security implementation, management and optimization. Related works below are identified and analysed accordingly.

Technically, like all kinds of aspects of cybersecurity management, 5G cybersecurity is also based on effectively controlling related risks. So, first and foremost, it is required to identify cybersecurity risks directly. And the risk identification should be based on the objective, impartial and complete assessment. In this way, risk control solution can be created. Otherwise, risks cannot be effectively mitigated, which would hamper the digital transformation in consequence. Nowadays, many efforts have been totally paid for identifying 5G cybersecurity risks. For example, the GSMA has conducted a comprehensive threat analysis [4] involving industry experts from across the eco-system including mobile network operators, vendors, service providers, and regulators, as well as collecting input from public sources such as 3GPP [21], ENISA [22] and NIST [23]. Also, these threats are mapped to some appropriate and effective security controls. Besides, based on the industry mature experience and good practices, the risk could be assessed by both the impact of an identified threat, and the likelihood of this threat, which could refer to ISO/IEC 27005:2018 [5]. In this way, risk can be represented by two dimensions, so that mitigation measures can be deployed accordingly.

Simultaneously, since 5G usage contexts are very complex and various, it is impossible to use an all-in-one approach to addresses all existing and upcoming cyber risks. Therefore, it is urgent for the industry and oversight agencies to make clear a whole picture of 5G cybersecurity for different stakeholders, which should clarify the roles and responsibilities, requirements and controls focusing on the lifecycle of 5G equipment, network and application services. Referring to the communication protocols (OSI seven layers [6] and TCP/IP four layers [7]), since the telecommunication industry has been divided into a three layers, which cover network equipment, network and application services. It is thus more practical to distinguish 5G cybersecurity into three layers, including network security layer, equipment layer and application layer, respectively.

Nevertheless, it is just the first step to implement, manage and optimize 5G cybersecurity through a holistic way. It is also essential to design security controls and other activities to mitigate cyber security risks from management, technical and other aspects. For controls, there have been some well-recognized standards, and it is very helpful to refer those best practice to set cybersecurity requirements for each layer. For instance, GSMA FS.16 Network Equipment Security

Assurance Scheme-Development and Lifecycle Security Requirement v 2.0[8], clarifies security requirements about 5G network equipment development and usage lifecycle. And 3GPP TS 33.117 Catalogue of General Security Assurance Requirements [9] indicates security functions of equipment. For the network security layer, we noticed that there is no unified or internationally recognized solution or framework, currently. But there are some helpful standards. In detail, the most famous one is ISO/IEC 27001, information security management [10], providing requirements for an information security management system to keep information asset secure. Also, the other very well-known one is NIST cybersecurity framework [11], which raised the IPDRR methodology for security operation. For some detailed aspect, such as the study on security aspects of network slicing enhancement [12] released by 3GPP, is useful to obtain knowledge for slice security in 5G context. After that, because of the complexity and massive number of 5G applications and contexts, the related works about their cybersecurity is much more fragmented, while they are good baseline requirements that can be referred. For example, ISO 62304 (secure development of medical device software), ISO 14971[13] (risk management of medical devices), and ISA / IEC 62443 EDSA [14] for embedded device security assurance are released to focus on healthcare cybersecurity. ISO/SAE 21434 [15] is set for vehicle cybersecurity, while OWASP IoT verification standard [16] and ETSI EN 303 645[17] are for IoT cybersecurity.

After understanding those security technical specification for risk mitigation, it is still essential to assess if targeted 5G cybersecurity requirements and standards are well deployed and implemented in reality. Therefore, harmonization of designing and implementing cyber security conformity assessment and cross-recognition of certified results are indispensable for OIC member states, which would be uniformly supervised and governed by OIC-CERT 5G security working group for this goal. Virtually, this is about the “reference” of designing, maintaining, supervising the cybersecurity certification, rather than a 5G cyber security schemes. Nevertheless, there are less related references compared with exact cyber security certification schemes. Nowadays, it is noticed that the ENISA has prepared some standard-based certification schemes, such as the candidate EUCC scheme [18]. However, we realized that designing a unified conformity assessment system requires much more than those schemes, so that the individually certified could be mutually recognized by others.

III. METHODOLOGY

As mentioned earlier, the OIC-CERT 5G framework is developed based on the zero trust and team sports philosophy. And it is also mentioned that this framework is also designed as a living document to adopt the dynamic 5G cyber security requirements. This section would introduce the methods about how these two aspects are approached.

For zero trust model, people are very familiar with the sentence: "Never trust, always verify". However, this is said for IT security, rather than ICT security. So, we need to "translate" this sentence a little bit. Firstly, never trust in cyber security domain means that we assume nothing about what kinds of network is secure or not, or whose network equipment are secure, which are nothing to do with security. Rather, for security, it is necessary to purely identify and analyse 5G security risks and threats to objectively and impartially design unified baseline security specification and standard references for various stakeholders. With clearly identified and analysed risks, it is possible to come up with targeted risk mitigation ways and security requirements. And that's why the part one of OIC-CERT 5G security framework is set as a risk repository. Then, part two designs related technical specification as baseline 5G security requirements. Once the risks are identified, the mitigation should be done by related actors with proposed security requirements. However, it is impossible to say that the implementation of security requirements is good or bad by different actors without proper verification. It means that we should believe nobody before security verification, let along make decision about which kinds of actors do well in 5G security assurance. So, according to the "always verify", we believe nobody, and we need to sufficiently verify the conformity assurance of actors against all targeted 5G security requirements.

Furthermore, for the "always verify", it still means that everything related to verification should be unanimous. Otherwise, results of the verification may be not well recognized widely. The widely recognized security assurance is critical for ICT industry, because of the global market requires unanimous conclusions for cyber security, which is also applicable for OIC member stats' ICT industry. Therefore, to make sure that individually verified 5G security assurance are well recognized, it is definitely needed to check everything, to effectively ensure that everything involved into conformity verification is harmonized and verification results are cross-recognized as a result. For this reason, part three's methodology is designed.

Additionally, because the ICT industry could be categorized by different stakeholders, and the cyber security goals are similar among those stakeholders. Thus, all contents of these three parts are assigned by the specifically defined roles and responsibilities, so that the entire implementation of 5G cyber security is a teamwork.

At the same time, the purpose of timely and effectively adoption of dynamic 5G security requirements, means this framework should be valid for the future. Part one could be used as a risk store and analysis template, and future risks can be recorded by it. Also, according to layered 5G cyber security technical specification of part two, where security requirements and recommended standards could be updated in practice. This layered structure and baseline requirements could be useful to guide such update. Last but not least, part three's methodology has defined how to build a cyber security certification, which could be used to guide following certification establishment among OIC member states.

With understanding of how the OIC-CERT 5G security framework was designed, next section would systematically introduce contents of each part.

IV. CONTENTS OF THE OIC-CERT 5G SECURITY FRAMEWOFK

This section introduces main contents of the OIC-CERT 5G security framework, while this section cannot completely demonstrate all details of the framework.

Part I: OIC-CERT 5G Cybersecurity Risk Repository

Generally speaking, with widely deploying 5G network and services, 5G cybersecurity has become a common concern for different stakeholders, which include mobile network operators, network equipment vendors, application providers, and regulators, et al. It is thus important for all stakeholders to comprehensively understand threats and take effective mitigation measures. Focusing on developing a global 5G risk register and dictionary used for risk assessment and management of 5G security risks in CERT work, this risk repository systematically records and explains currently existing 5G cybersecurity threats.

The OIC-CERT 5G cybersecurity risk repository includes industry-consensual threat landscape, attack methodologies, mitigation strategies and measures for different stakeholders, references of standards and best practices. For the threat landscape, the current OIC-CERT 5G cybersecurity risk repository summarizes 34 exact threats, such as DDoS attacks on core networks, forged core network element, virtual machine abuse and so on. Those threats are classified according to where they might emerge. For the category, there are access network threats, generic threats, core network threats, transport network threats, operation

& maintenance (O&M) threats, application threats and supply chain ones. Simultaneously, according to the public's perspective, high-level threat is indicated with related malicious activities. For example, the high-level of network roaming fraud could be sensed by nefarious activity and eavesdropping/ interception. In addition to the description of each threat, causes of those threats are also introduced. In the most case, this 5G cybersecurity risk repository outlines mitigation measures of different roles. As for the counter measures of each threat, the repository systematically shows the needed activities for vendors, operators service providers and governments and national regulators, respectively. For example, to prevent DDoS attacks on core networks, government and national regulators could regulate the illegal action of initiating DDoS attacks against core networks and enforce penalties. Simultaneously, MNOs could deploy anti-DDoS devices at the network border, in addition to, security edge protection proxies and signalling firewalls. Besides, vendors can develop a flow control mechanism of core network elements. For application service providers, it is applicable to monitor application servers to prevent starting DDoS attacks. Additionally, this risk repository

Obviously, from this repository, it has been clearly demonstrated that 5G cybersecurity is under a shared responsibility of key stakeholders, including MNOs, interconnection providers, vendors, application developers, service providers and governments. So we can say that 5G cyber security must be constructed upon the shared responsibilities of all stakeholders, which would be further specified in part Ⅱ. Each of them has been allocated with a clearly defined mitigation activities, which (when fully met) can enable the deployment and operation of 5G systems in a secure manner. With full use of these recommendations and references, we believe that 5G cybersecurity is verifiable and manageable, although there may exist upcoming new challenges.

Part II: Baseline Security Technical Specification

Focusing on developing and/or adopting a baseline 5G security open standard for OIC member state usage or adoption, this technical specification not only describes what 5G cybersecurity responsibility exactly means for stakeholders, but also provide baseline requirements to guide OIC member states to build, improve and manage 5G cybersecurity. As shown in the OIC-CERT 5G cybersecurity risk repository, it is clear that 5G cybersecurity has been facing serious challenges. Furthermore, it is also seen that these threats can raise various cybersecurity risks on the access network, transport network, core network, supply chain, O&M, application services, and so on.

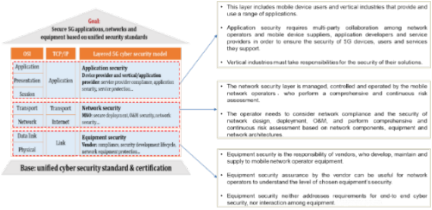
Undoubtedly, if there is no appropriate security approach, those risks can then lead to invalid or incomplete applications, services, network access, and data breach which mainly surround the confidentiality of information in networks and equipment, availability and integrity of 5G based services, equipment and network functionality, etc. Concerning increasingly worse cybersecurity threats and challenges, understanding, mapping and mitigating identified and upcoming threats in a well-designed, cost effective and practical manner is essential. Therefore, to not only systematically define a 5G cybersecurity architecture and security necessities, but also guide OIC member states to build, improve and manage 5G cybersecurity in a holistic way.

Firstly, this technical specification defines a layered 5G cybersecurity model to explicitly distinguish roles and responsibilities in securing 5G equipment, networks and applications, respectively. This layer architecture and corresponding roles and responsibilities are shown by the figure below. In this model, the goal includes secure equipment, secure network and secure application related to 5G. And the foundation is unified cyber security standards and certification. This is because trust must be based on verifiable facts, which should in turn be based on unified standards. In this way, each layer's cyber security requirements and implementation can be well-recognized and reproducible. Such reproducible and recognition are critical for different OIC member states, so that the 5G cyber security could be accepted unanimously.

For the roles and responsibilities, we conclude that equipment security is the responsibility of vendors, who develop, and maintain network equipment and supply them to MNOs. Network equipment security assurance is a key tool, which provides a basis to evaluate whether network equipment and components have been designed and operated in accordance with proposed security requirements. Security assurance programmes should adhere to globally recognised and unified standards to ensure that their operation is cost effective, sustainable for the ecosystem, and security guaranteed.

Then, the network security layer should be managed, controlled and operated by MNOs. During the network design and operation, MNOs perform comprehensive and continuous risk assessments. The operator needs to consider network compliance and the security of network design, deployment, O&M, and perform comprehensive and continuous risk assessment based on network components, equipment provided by vendors, and network architectures.

Besides, the application layer includes mobile device users and vertical industries that provide and use a range of applications. Application security requires multi-party collaboration among MNOs, mobile device suppliers, application developers and service providers in order to ensure the security of 5G devices, users and services they support. An application security extends beyond the MNO and, therefore, beyond the responsibility of MNOs. And vertical industries must take responsibilities for the security of their solutions. They must introduce mechanisms to protect confidentiality, integrity and availability on top of the built-in security controls offered by MNOs, to further improve the overall security offerings.


Goal:
Secure 5G applications, networks and equipment based on unified security standards
OSI
TCP/IP
Layered 5G cyber security model
Application
Presentation
Session
Application
Application security
Device provider and vertical/application provider: service provider compliance, application security, service protection...
Transport
Network
Transport
Internet
Network security
MNO: secure deployment, O&M security, network security...
Data link
Physical
Link
Equipment security
Vendor: compliance, security development lifecycle, network equipment protection...
Base: unified cyber security standard & certification

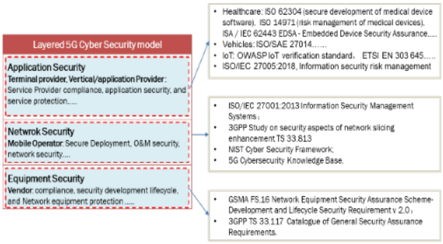
- This layer includes mobile device users and vertical industries that provide and use a range of applications.
- Application security requires multi-party collaboration among network operators and mobile device suppliers, application developers and service providers in order to ensure the security of 5G devices, users and services they support.
- Vertical industries must take responsibilities for the security of their solutions.

- The network security layer is managed, controlled and operated by the mobile network operators , who perform a comprehensive and continuous risk assessment.
- The operator needs to consider network compliance and the security of network design, deployment, O&M, and perform comprehensive and continuous risk assessment based on network components, equipment and network architectures.

- Equipment security is the responsibility of vendors, who develop, maintain and supply to mobile network operator equipment.
- Equipment security assurance by the vendor can be useful for network operators to understand the level of chosen equipment's security.
- Equipment security neither addresses requirements for end-to end cyber security, nor interaction among equipment.

Fig. 1: Layered architecture and corresponding roles and responsibilities

Next, for each layer, corresponding baseline security requirements are given. Nevertheless, for stakeholders, it is up to actual requirements to apply or develop a standard or certification scheme, and there have been some verified standards and certification schemes able to be applied directly. In this way, some requirements would be well implemented through the adoption of cybersecurity standards. The relationship among those layers and requirements and references could refer to the following figure 2. The reference mapped with each layer is clearly given in the box.


Layered 5G Cyber Security model
Application Security
Terminal provider, Vertical/application Provider: Service Provider compliance, application security, and service protection.....
Netwrok Security
Mobile Operator: Secure Deployment, O&M security, network security....
Equipment Security
Vendor: compliance, security development lifecycle, and Network equipment protection .....

- Healthcare: ISO 62304 (secure development of medical device software), ISO 14971 (risk management of medical devices), ISA / IEC 62443 EDSA - Embedded Device Security Assurance.....
- Vehicles: ISO/SAE 27014......
- IoT: OWASP IoT verification standard, ETSI EN 303 645.....
- ISO/IEC 27005:2018, Information security risk management

- ISO/IEC 27001:2013 Information Security Management Systems;
- 3GPP Study on security aspects of network slicing enhancement TS 33.813
- NIST Cyber Security Framework;
- 5G Cybersecurity Knowledge Base.

- GSMA FS.16 Network Equipment Security Assurance Scheme-Development and Lifecycle Security Requirement v 2.0;
- 3GPP TS 33.117 Catalogue of General Security Assurance Requirements.

Fig. 2: Requirements and reference standards

Actually, requirements for developing, improving and managing 5G cyber security are dynamic along with many other aspects, such as security technologies, security mindset and awareness, laws and regulations, and current threat landscape. It means that an iterative update of security requirements in different periods is essential.

Besides, according to existing best practices and well-recognized standards or other frameworks, the 5G equipment layer's cybersecurity is confirmed to apply network equipment security assurance scheme (NESAS) and security assurance specification (SCAS) for network products, which are developed by GSMA and 3GPP, respectively. In addition, further requirements customized from OIC member states will be applied according to individual states need.

After understanding security requirements involved in the baseline security technical specification, it is still it is still essential to assess if targeted 5G cybersecurity requirements and standards are well deployed and implemented in practice. It is thus necessary to set standard-based certification schemes for each security layer's security requirements and standards, accordingly. Nevertheless, security requirements and existing references of those three layers in the baseline security technical specification are various. It means that member states need to decide what exact certification scheme is useful and essential for them. It is thus unrealistic to design and confirm specific certification schemes in this document. By comparison, it is reasonable to design a unified certification mechanism to guide any possible certification scheme's deployment and implementation in OIC member states. This mechanism is illustrated below. In this mechanism, CB represents certification body, which is a third-party conformity assessment body operating certification scheme. The CB is in charge of the activities of certification related to the issuance of certificates. EB represents evaluation body, and it is also the third-party conformity assessment body that performs one or more activities: audit, test, sampling, and associated with subsequent evaluating activities. CAB represents the conformity assessment body, which accredits and supervises both the certification body and evaluation body. Also, possible actors who can play those roles are also given in this figure.

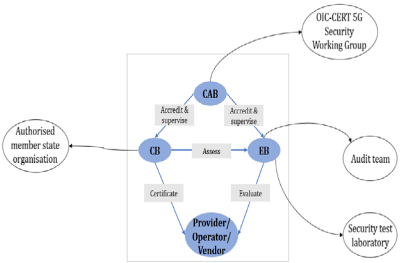


Fig. 3: Certification mechanism

This security baseline specification is mainly intended for regulatory authorities of member states, with the purpose of assisting them in making policies on regulating 5G equipment vendors, mobile network operators (MNOs) and relevant service providers. So, the precise technical solution is out of this part.

Part III: Cross-Recognition Assurance Methodology

With part two, securing 5G network equipment, networks and applications have been deemed as a critical objective in an effort of promoting digital transformation for all stakeholders. At the same time, those involved cybersecurity requirements and referred standards are helpful and essential to approach this objective in a holistic way for OIC member states.

Adjacently, it becomes more valuable and essential to assess the conformity of implementing those cybersecurity requirements and standards in a harmonised and cross-recognised way among OIC member states. In this way, individually certified 5G cybersecurity assurance of the 5G network, equipment or application in one country or a region could be also accepted by different states. With such cross-recognition, it is straightforward to reduce the worries of repeatedly doing certifications of the same purposes and increase efficiency of deploying 5G with a common security level. Specifically, vendors, network operators and service providers would understand the 5G cybersecurity quality in consensus, and benefit from the authoritative evidence for their customers. Regulatory authorities can also establish cybersecurity assurance requirements on 5G industries in a unified manner. Also, the threat information sharing for OIC member countries could be promoted, such as rapidly and collectively response of a previously undetected vulnerability or a newly identified malicious attack scenario. In other words, a cross-recognition of 5G cybersecurity assurance could be able to ensure the entire level of 5G cybersecurity in OIC regions.

To achieve this excited and urgent goal, a cross-recognition assurance methodology is created in OIC-CERT 5G security framework. This methodology is still under the scope of the Baseline Security Technical Specification, to precisely clarify the certification mechanism as a way to further unify the "reference" or the "language" about designing, implementing and managing any possible standard-based 5G cybersecurity certifications of 5G network equipment, networks or applications. In short, this proposed methodology is the baseline specification of that certification mechanism, in order to build and maintain the harmonised cybersecurity standard-based certification and cross-recognised certified result. The positioning of this methodology is shown by following two figures:

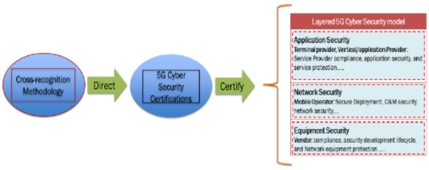
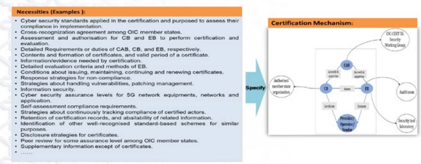

Cross-recognition Methodology
Direct
5G Cyber Security Certifications
Certify
Layered 5G Cyber Security model
Application Security
Terminal provider, Vertical/application Provider: Service Provider compliance, application security, and service protection....
Network Security
Mobile Operator: Secure Deployment, O&M security, network security....
Equipment Security
Vendor: compliance, security development lifecycle, and Network equipment protection ....

Fig. 4: Relationship

Cyber security certification normally indicates requirements of evaluating products, services or processes by an independent and accredited body against a defined set of criteria, standards and so on. The result can demonstrate the security assurance to different stakeholders about the level of conformity against targeted standards. By comparison, this proposed cross-recognition assurance methodology summarizes basic requirements and necessities to unanimously direct the construction of different 5G cyber security standard-based certifications. This methodology is not a specific cyber security certification. Clearly, the certification can help different stakeholders to understand the level of cyber security assurance of the products, services and processes they use according to a same way within a region. Differently, the cross-recognition assurance methodology could help a one-region certified security assurance to be also accepted in different OIC member states.



Necessities (Examples):

- Cyber security standards applied in the certification and purposed to assess their compliance in implementation.
- Cross-recognization agreement among OIC member states.
- Assessment and authorisation for CB and EB to perform certification and evaluation.
- Detailed Requirements or duties of CAB, CB, and EB, respectively.
- Contents and formation of certificates, and valid period of a certificate.
- Information/evidence needed by certification.
- Detailed evaluation criteria and methods of EB.
- Conditions about issuing, maintaining, continuing and renewing certificates.
- Response strategies for non-compliance.
- Strategies about handling vulnerabilities, patching management.
- Information security.
- Cyber security assurance levels for 5G network equipments, networks and application.
- Self-assessment compliance requirements.
- Strategies about continuously tracking compliance of certified actors.
- Retention of certification records, and abailability of related information.
- Identification of other well-recognised standard-based schemes for similar purposes.
- Disclosure strategies for certificates.
- Peer review for some assurance level among OIC member states.
- Supplementary information except of certificates.
- ……

Fig. 5: Example

From this example, we can see that the cross-recognition assurance methodology mainly contains essential requirements or necessities to approach the harmonised conformity assessment and cross-recognised result, and it is the baseline technical specification of the certification mechanism. Obviously, to assure that harmonised certifications and cross-recognition of certified results, we should consider much more than a common cybersecurity standard. It requires many other aspects, such as signing the cross-recognition agreement, unifying the authorization and evaluation criteria, and tracking the non-compliance. In this way, a common cybersecurity standard's conformity could be assessed in a harmonised way by different certification and evaluation bodies, so that the cross-recognised certification result could be possible.

More specifically, as we have seen, the part two has unified the 5G cybersecurity role types and responsibilities by the layered security model. Accordingly, baseline cybersecurity requirements and standards proposed for each layer are unified. With these already harmonised standards and the OIC-CERT 5G working group who play the role of CAB, to obtain the cross-recognised certification results, it is needed to create each standard-based certification scheme, and authorise different OIC member state's certification bodies and evaluation bodies, et al, uniformly. Also, after implementing the certification, it includes the different evaluation criteria, duties and other maintenance actions. In particular, extra strengthening measures are necessary, such as signing an agreement together. Therefore, it is to say, the cross-recognition of individual certification result is guaranteed by harmonised standards, certification actors, related processes, strategies and maintenance.

Particularly, the harmonization does not mean the complete same. Rather, it only means the consensus and unanimity about supervising and governing related elements of design, implementation and maintenance of certification schemes. Otherwise, it would be

ISSN 2636-9680
eISSN 2682-9266

very unrealistic to obey one or few types of certification schemes for member states directly. Because their cybersecurity expertise, capabilities, and risks are various. Cross-recognised individual certification outcome is definitely impossible for OIC member states.

So, the most practical way to achieve cross-recognition is to use harmonised requirements to stipulate the construction of specific certification schemes, while the scope and implementation scenarios of each created scheme by one or more OIC member states could be divergent, so do the eventually certified results. In particular, it means those different individually certified outcomes based on a same standard could be cross-recognised by other states. And those states may not be able to ensure that all kinds of conformity levels are certified by each countries CB and EB. Such cross-recognition working mechanism is descripted by an example in the figure 6.

In this example, with the pre-defined conformity level by CAB, different CBs and EBs of different states do the certification of a same specific standard. The conformity level that they can certify is different. In detail, the level 2 certified by CB 2 and EB 2 in state 2 could be recognised by both other countries, and level 4 certified by CB 1 and EB 1 are also accepted by other two ones, although they cannot certify such a higher level.

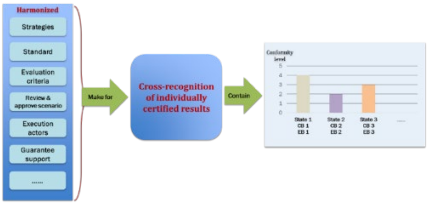


Fig. 6: Example of the mechanism

After understanding positioning of this cross-recognition methodology and working mechanism, the logic flow and elements of this cross-recognition assurance methodology is demonstrated by following figure, and here are major actions must do for different actors. Also, this flow chart is shown through the viewpoint of regulatory authorities of member states. So, it is not proper for certification applicants to guide applying a certification.

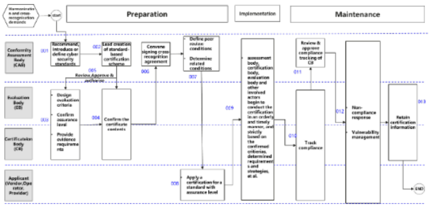

Harmonization and cross-recognisation demands
start
Preparation
Implementation
Maintenance
Conformity Assessment Body (CAB)
Evaluation Body (EB)
Certification Body (CB)
Applicant (Vendor,Operator, Provider)
001
Recommend, introduce or define cyber security standards
002
Lead creation of standard-based certification scheme
005
Review,Approve & authorize
006
Convene signing cross-recognition agreement
Define peer review conditions
Determine related conditions
007
003
Design evaluation criteria
Confirm assurance level
Provide evidence requirements
004
Confirm the certificate contents
008
Apply a certification for a standard with assurance level
009
assessment body, certification body, evaluation body and other involved actors begin to conduct the certification in an orderly and timely manner, and strictly based on the confirmed criterias, determined requirements and strategies, at all.
010
Track compliance
011
Review & approve compliance tracking of CB
012
Non-compliance response
Vulnerability management
013
Retain certification information
END

Fig. 7: Logic flow chart of cross-recognition assurance methodology

Practically, the methodology is structured according to the procedures, which are about before, during and after executing a specific cybersecurity certification, respectively. And these three procedures are further named as “Preparation”, “Implementation”, and “Maintenance”. Clearly, CAB’s responsibility is mainly about decision making and supervision as shown in the flow chart. Then, CB and EB mainly focus on executing approved items and decisions from CAB.

Besides, to better understand the contents of this methodology, all elements are summarized below:

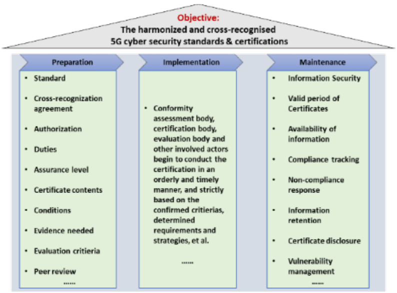

Objective:
The harmonized and cross-recognised
5G cyber security standards & certifications
Preparation
• Standard
• Cross-recognization agreement
• Authorization
• Duties
• Assurance level
• Certificate contents
• Conditions
• Evidence needed
• Evaluation critieria
• Peer review
......
Implementation
• Conformity assessment body, certification body, evaluation body and other involved actors begin to conduct the certification in an orderly and timely manner, and strictly based on the confirmed critierias, determined requirements and strategies, et al.
......
Maintenance
• Information Security
• Valid period of Certificates
• Availability of information
• Compliance tracking
• Non-compliance response
• Information retention
• Certificate disclosure
• Vulnerability management
......

Fig. 8: Elements of cross-recognition assurance methodology

In each phase, elements are chosen in necessary to represent the baseline requirements in about designing deploying and implementing a cybersecurity conformity assessment. And each element would be precisely explained to guide the user of this methodology.

As we could see from the logic flow chart and elements, before and after implementing a certification, there are actually more elements should be taken account of. In this way, through those elements in Preparation and Maintenance phases, the cybersecurity standard-based certifications could be firstly harmonized, and then those certified results produced during and after implementing certification can be cross-recognised, respectively. Nevertheless, concerning the development of cybersecurity, and similar to any other standardized documents, those necessities of the methodology could be updated or replaced with other better ones in the future.

V. CONCLUSION

Above all, the OIC 5G security framework is now officially published. 2022 will be the year where the OIC-CERT 5G Security Working Group will be hard at work ironing out issues on the ground where OIC 5G security group will be leading efforts to drive adoption and implementation of the framework across member states, especially on key areas such as mutual recognition and certification.

VI. REFERENCES

[1] The OIC-CERT 5G Security Framework: Bracing for What's Coming. Available at https://teletimesinternational.com/2021/the-oic-cert-5g-security-framework-bracing-for-whats-coming/

[2] Forest Interactive, "Positive 5G Outlook Post Covid-19: What Does It Mean for Avid Gamers?," Forest Interactive, 29 June 2020. Available at https://www.forest-interactive.com/newsroom/positive-5g-outlook-post-covid-19-what-does-it-mean-for-avid-gamers/

[3] Organization of the Islamic Cooperation- Computer

Emergency Response Team, "OIC-CERT," Available at https://www.oic-cert.org/en/missionstatement.html

[4] 5G Cybersecurity Knowledge Base, https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

[5] Information technology — Security techniques — Information security risk management, https://www.iso.org/standard/75281.html

[6] THE OSI MODEL: OVERVIEW ON THE SEVEN LAYERS OF COMPUTER NETWORKS

[7] TCP-IP Model in Data Communication and Networking

[8] FS.16-NESAS Development and Lifecycle Security Requirements v2.0

[9] 3GPP Specification #: 33.117

[10] Information security management, ISO/IEC 27001:2013

[11] Cybersecurity framework, NIST

[12] Study on security aspects of network slicing enhancement, 3GPP

[13] Medical devices — Application of risk management to medical devices

[14] Embedded Device Security Assurance (EDSA) - version 3.0.0

[15] Road vehicles — Cybersecurity engineering

[16] OWASP IoT Security Verification Standard

[17] Cybersecurity for Consumer Internet of Things:Baseline Requirements

[18] Cybersecurity Certification: Candidate EUCC Scheme V1.1.1

[19] OIC-CERT launches 5G security working group at GISEC 2021

[20] Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero trust

[21] About 3GPP

[22] About ENISA-The European Union Agency for Cybersecurity

[23] About NIST