Policy analysis on telecommunication devices security standardization to support national security and defence policy

Analisis kebijakan standardisasi keamanan perangkat telekomunikasi untuk menunjang kebijakan pertahanan dan keamanan nasional

Wirianto Pradono[1], Yourdan[2]
[1,2]Pusat Penelitian dan Pengembangan Sumber Daya dan Perangkat Pos dan Informatika
[1,2]Jl. Medan Merdeka Barat No.9, Jakarta 10110, Indonesia
email: [1]wiri001@kominfo.go.id, [2]yourd@kominfo.go.id

INFORMASI ARTIKEL

Received 14-Desember-2015
Revised 22-Desember-2015
Accepted 23-Desember-2015

Kata kunci :
Telekomunikasi
Standarisasi perangkat
Kebijakan

ABSTRAK

Beberapa tahun terakhir, kejadian yang terkait dengan pembobolan informasi meningkat dengan signifikan dan menyebabkan kerugian yang tidak sedikit baik bagi pemerintah, industri maupun perorangan. Oleh karenanya diperlukan jaminan terhadap keamanan informasi terutama yang menyangkut informasi yang sensitif dan rahasia. Untuk mengatasi hal tersebut, diperlukan kebijakan di bidang standarisasi keamanan perangkat telekomunikasi untuk menjamin validitas dan kerahasiaan informasi yang dilewatkan melalui perangkat tersebut. Pendekatan kualitatif maupun kuantitatif digunakan dalam studi ini untuk memperoleh gambaran tentang kondisi penerapan standar keamanan perangkat baik oleh pemerintah maupun industri telekomunikasi serta mengidentifikasi kendala yang dihadapi dalam menjamin keamanan perangkat telekomunikasi baik untuk kebutuhan umum maupun kebutuhan khusus baik dari aspek teknologi, kelembagaan, maupun regulasi. Hasil penelitian menunjukkan belum ada regulasi yang mengatur standarisasi keamanan perangkat telekomunikasi untuk kebutuhan khusus. Selain *itu belum ada penetapan secara eksplisit tentang lembaga yang berwenang dalam pengujian dan sertifikasi keamanan perangkat telekomunikasi terutama untuk kebutuhan khusus. Sejumlah regulasi yang mengatur secara spesifik bidang standarisasi keamanan perangkat telekomunikasi saat ini masih dalam proses penyusunan oleh instansi-instansi terkait.*

Keywords:
Telecommuncation
Devices standardization
Policy

ABSTRACT

In the past years, incidents involving information security breach increase significantly and cause huge damage to industry, government or individual. Due to that, information security needs to be well guaranteed especially when it comes to sensitive and confidential information. One has to be done to cope with that is the availibility of policy on telecommunication devices security standardization to assure validity and confidentiality of all information going through the devices. Both qualitative and quantitative method used in this study to describe implementation of telecommnunication devices security that has been done by both government and ICT industry and also to identify obstacles in implementation of telecommunication device security assurance for both public and special purposes, from technology, institutional, and regulation aspects. This study showed that any regulation related with telecommunication device security standardization for special purposes has not been provided yet. Besides, authorized institution to examine and certify telecommunication devices security especially for specific purposes has not been assigned yet.

1. Introduction

Utilization of information and communication technology pervades virtually all sectors ranging from economy, education, and health to defense and security. Information and communication technology as a strategic element in support of defense and security should deserve more attention. Moreover, in recent years, crimes involving the theft of information became more frequent and targeting not only individuals and industry

but also the government in the form of tapping by foreign intelligence on a number of Indonesian government officials. Thus, information security should deserve priority, especially in support of the needs national defense and security (Kiblat.mht, 2015; Richardus, Eko, and Indrajit, 2011). Telecommunications devices used to exchange information should be guaranteed for security and there should be no loopholes of information steal or tapping. Therefore, there is a need for ICT policies related to security standardization of telecommunications devices in order for the function and use of telecommunication devices that circulated in Indonesia to be held accountable and especially for ensuring the security of information exchanged by means of these devices. It is carried out in order for the information exchanged to remain ensured for validity and confidentiality; thus, the accuracy of information can be held accountable and does not mislead other parties (Paryati, 2008). In addition, ensuring the security of information involves a number of relevant stakeholders, including both the government and industries (Wamala, 2011). Furthermore, the other things that also need to be considered is the availabiility of adequate security technologies, such applications to remove the valuable information out of a smartpohone to prevent the data from being stolen when the *smartphone* is lost (Wicaksono, 2007).

In relation to the need for the policy, the present study was conducted to obtain an initial picture of efforts to secure the current telecommunications devices and the potentials and obstacles faced in the effort to ensure the security of telecommunications devices, both for general needs of the public and industry and the special needs of the military, police, and state officials. It was carried out from both the technological, institutional, and regulatory aspects summarized into a number of research questions formulated on the basis of the emerging issues of security breaches of information obtained from various literature originating from both books and journals. The results obtained through the qualitative and quantitative methods can serve as benchmarks for authorities against the extent to which the efforts to ensure the security of the device have been done so far along with the strategic measures that need to be taken to realize the security standardization of devices. Security standardization of devices is to ensure that the telecommunications devices used are secure in the sense that the security of information passed through the devices is ensured, especially the telecommunications devices used for the purposes of national defense and security. The results showed there was no regulation governing security standardization of telecommunications devices for special needs. In addition, there was no explicit designation of the agency authorized to test and certify the security of telecommunication devices, especially for special needs. A number of regulations that specifically regulate security standardization of telecommunications devices are still in the drafting process by related agencies.

2. Literature review

2.1. The concept of defense and security in the national interests

Robert Dorff (2004) argued that that the interests of a country is shown by their behavior in defending, pursuing and maintaining its basic interests. For many countries, the basic interests of a country is to maintain their region, people and sovereignty. All these elements must be maintained and championed to remain existent in a country. Maintaining these interests constitute the basis of the behavior of a country in dealing with other countries and other actors in the international system, including through war and diplomacy (Dorff, 2004). According to Alan Gyngell & Michael Wesley (2007), national interest is a permanent concept serving to orient a country's foreign policies. In other words, the concept of national interest always serves as the basis for all foreign decision making and also foreign policy analysis (Gyngell & Wesley, 2007: 23). National interest is a long-term goal of a country that binds to all the elements of the government and the nation to achieve. Thus, national security is also extended from the real to the virtual world, leading to a new threat to the national security system, called the cyber war, and each country compete to win the war. The powerfully destructive threat of the cyber war is immediate and serious to the national security system. In the globalization order all devices can access information anywhere and it can be also accessed from anywhere. This allows for misuse of

the information passed through such devices by planting a tool to extract and modify information for specific purposes.

2.2. Rationale and national ICT policy

The global developments of information and communication technology are highly transparent and allow for quick and easy access to any event and information in the world as if it negates borders among countries. This allows for the misuse of the information passed through telecommunications devices by tapping or modifying the information for specific purposes, posing a threat to the integrity of the state. Thus, it would be very dangerous for a country to constantly serve as only the user and receive devices manufactured by foreign parties without a guaranteed standardization of security or encryption evidenced by following national and international regulations established by the relevant authorities.

2.3. Standardization policy for general devices

Standardization as a supporting element of development plays an important role in an effort to optimize resource utilization and all development activities. Standardized devices, including those for management and control, are instrumental to increase domestic and international trade, the development of national industry, as well as user (operators and the public) protection where the purpose of standardization is to realize quality assurance. The National Standardization System (NSS) constitutes the basis and guidelines for implementation of each of standardization activities in Indonesia that should be referenced by all technical agencies in accordance with Government Regulation No. 15 of 1991 on Indonesian National Standardization and Presidential Decree No. 12 of 1991 on Formulation, Application and Control of Indonesian National Standards. In order to implement the National Standardization System, standardization is also developed and applied to the sector of telecommunications. The standardization of the telecommunications sector is fully handled by the technical agency, in this case the Directorate General of Resources and Equipment of Post and Information Technology (SDPPI) and implemented by the Directorate of Standardization of SDPPI. The inter-related subsystems or activities in the National Standardization System consist of standardization formulation, application, development and control, cooperation and information, metrology and accreditation. The purposes of the standardization of post and telecommunications are to:

a. securing the post and telecommunications networks, which are the national assets
b. ensuring interoperability and inter-connectivity of various post and telecommunications devices
c. providing opportunities for the emergence of the national manufacturing industry
d. protecting post and telecommunications users (operators and the public)
e. control the quality of devices
f. providing opportunities for the national products to compete in the global market

2.4. Standardization policy for specialized devices

The security standards of specialized devices are usually applied nationally, within the scope of any single country. Development of security standards of specialized devices in Indonesia is assisted by the relevant intelligence agencies, including:

a. State Intelligence Agency (BIN)
b. Armed Forces Strategic Intelligence Agency (BAIS)
c. National Crypto Agency (Lemsaneg)

BIN and Lemsaneg are non-ministerial government departments (LPNK), which in Indonesia are state agencies established to carry out certain government tasks as instructed by the presidential, while BAIS is

under the command of the Indonesian National Armed Forces Headquarter (Mabes TNI). Of the three state intelligence agencies, the one with the functions related to the security of military telecommunications systems is Lemsaneg. Pursuant to regulation of the Head of National Crypto Agency No. OT.001/PERKA.122/2007 on Organization and Work Procedures of the National Crypto Agency, the agency performs the governmental tasks in the crypto field in accordance with the provisions of the legislation in force. In performing these tasks, Lemsaneg carries out the following functions:

a. to examine and develop national policies in the crypto field;
b. to coordinate functional activities in the performance of Lemsaneg tasks;
c. to facilitate and develop activities of government agencies in the crypto field;
d. to develop general administration services in general general planning, administration, organization and governance, personnel, finance, archiving, legal, crypto, equipment and household.

2.5. Concept of the Security of National Information and Communication Technology

The concept of security in the ICT domain has a vast scope. Security encompasses four aspects, including privacy/confidentiality, integrity, authentication, and availability. In addition to the four aspects above, there are two other aspects that are often discussed, especially related to electronic transactions, namely access control and non-repudiation (Garfinkel, 1995).

a. Privacy/confidentiality: an aspect related to the confidentiality of the contents of information
b. Authentication: an aspect stating that the information is truly original, or the person accessing/providing the information is actually the person in question
c. Integrity: This aspect emphasizes that information should not be altered without the permission of the owner of the information
d. Accessibility: This aspect relates to the availability of information when needed
e. Access control: This aspect is related to how the access to information is regulated
f. Non-repudiation: This aspect is to prevent someone from denying the transaction he or she has done.

Security issues are often given even less attention, particularly where the application of security measures interfere with the system performance. Not infrequently, security measures are reduced or even abolished (Dowd & McHenry, 1998). Based on the vulnerabilities, the security can be classified into (David J. Icove, 1997):

a. Physical security. Physical security includes access to buildings, equipment, and media used. There is a possibility of an easy access to the archives that have been disposed of that may have security information, such as password records or manuals removed without destroyed. Wiretapping or issues relating to access to cables or computers used can also be classified into in this class. Denial of service can also be classified into this class. Denial of service is the impact that leads the supposedly accessible services to cease. This can happen, for example, by turning off the equipment or flooding communication channels with messages not originating from the service requester, making the service provider busy.
b. Personnel-related security. This classification includes identification of the persons who have access, for example, employees of an organization. Security flaws are often dependent on humans. The "social engineering" technique is often used by criminals, for example by pretending to be the person authorized to access information but forgot the password.
c. Security of data and media communications technique. This classification includes the flaws of the software used to manage data. Attackers can deploy viruses or trojans to collect information (e.g. passwords*)* not authorized to be accessed.
d. Security of operation, including the procedures for organizing and managing system security, as well as the procedures for post-attack recovery. Specifically, security attacks within an information system can be

viewed on the function of a computer or computer network as an information provider. There are several possible attacks (William Stallings, 1995; Rahardjo, 1999), including:

1) Interruption: system devices become corrupted or unavailable. Attacks are aimed at the availability of the system. An example of this attack is "denial of service attack".
2) Interception: an unauthorized party successfully accesses assets or information. An example of this attack is wiretapping.
3) Modification: The unauthorized party not only successfully gain access, but it can also tamper assets. An example of this attack includes modifying the contents of a website with messages that harm the owner of the website.

e. Fabrication: The unauthorized party inserts false objects into the system. An example of this type of attack is to insert false messages, such as false e-mails, into a computer network.

2.6. Related studies

Within the scope of the national public telecommunications system, studies on security of devices are rarely found. Commonly found but related studies are those on information security. Specific studies on the security of devices are more often found in relation to the communications systems commonly used in the realm of defense and security of a country, hereinafter referred to as specialized communications systems. This is reasonable given that communications devices have a low level of variation globally, especially in the scope of a country. In the specialized telecommunications systems, the security of communications systems is often known with a specific term 'COMSEC' (communications security). The area of COMSEC study specifically examines the devices used. COMSEC can include cryptosecurity, transmission security (TRANSEC), and physical security of specialized telecommunications devices. A group of researchers may have their own focus of study, for example in terms of emission security. Some previous studies investigated the application of security mechanisms to specialized telecommunications devices. Development of research on low probability of interception (LPI) in transmission security is often found on the radar. LPI radars are used by military personnel to detect and lock the targets/enemies, but the radar itself is difficult to be detected by the counterparty's passive detection devices (Stove, 2004).

Examples of other applications can be seen in the protection of satellite communications systems by means of the security methods at the transmission level and support of secure communication channels such as a virtual private network (VPN) (J.M. Rodriguez Bejarano, 2012). Studies on detection of system insecurity typically involve an analysis of communications traffic. Numerous studies focused on vulnerability of such systems (Juslin, 2003; NargesArastouie, 2011). In 2012 the media was shocked with the finding of vulnerabilities in the electronic components often used in military devices. A study at the University of Cambridge found that the chips used in the space system devices and missiles, fighter aircrafts, flight computer systems, weapon systems, radar systems and other have a hidden backdoor in them. A backdoor is an additional undocumented feature deliberately inserted into a component to provide additional functions that are hidden from the user (Woods, 2012).

Backdoor traces have been found in the file system of the software developed by Actel, a manufacturer of field-programmable gate arrays (FPGA) chips that are widely used in military systems. The danger of backdoor is the significant effects it has since FPGA is designed for systems with a high level of security. Despite the claim by Actel that the device is highly secure since there could be no physical line of data configuration from outside the FPGA chips, but the implementation of vulnerabilities by means of Actel-specific hidden and closed methods makes FPGA chip security questionable. Thus, even though devices are equipped with a number of security features, potential security leaks remain. In an article that discusses security evaluation of smartphones, various vulnerabilities are found in a number of applications installed on smartphones (Schrittwieser *et al*., 2012).

2.7. Implementation of the national ICT security standards

2.7.1. General devices

One of the bases of the implementation of general device security standards in Indonesia can be seen in Regulation of the Minister of Communication and Information Technology No. 18 of 2014 on Certification of Telecommunication Tools and Equipment. Certification means a document declaring that a device has gone through a series of testing process. This certificate ensures that the device is able to connect to and communicate with an existing device or system without disturbing and disturbed by other communication systems. This regulation sets out that the certificate for such devices is issued by a certification agency, namely the Directorate of Standardization of Post and Information Devices. To obtain the certificate, the device submitted must be tested by the designated Testing Agencies, namely the Telecommunication Equipment Testing Center (BBPPT) of the Ministry of Communications and Information Technology and the Innovation and Design Center (IDEC) of PT. Telekomunikasi Indonesia.

2.7.2. Specialized devices

Specialized devices have closed security standards. Military devices have proprietary security standards set by the parties concerned. With the highly strict requirements of military telecommunications security, the standards of each party concerned are generally not allowed to be known by other parties. In other words, there are nearly no internationally applied standards. Some standards that possibly exist are usually general communications standards between one military party and another one where there is no exchange of very confidential information in the ongoing communications. Security standards of military equipment are usually applied nationally, within the scope of any single country. Development of military device security standards is generally assisted by the military intelligence agency of the country concerned. In Indonesia, military communications devices used by the armed service branches (Army, Navy, and Air Force) are reportedly certified by the research and development agency of each armed service branch. However, the National Crypto Agency (Lemsaneg) has a plan to require the application of security standards. Currently, Lemsaneg has the Sub-Directorate of Accreditation and Certification to certify devices with security features. Lemsaneg has a plan to require certification of specialized devices by seeking legislation on such certification in 2016 to govern the technical requirements of crypto devices.

3. Method

The present study was conducted using a mixed quantitative and qualitative method. The quantitative methods used were the Analytical Hierarchy Process (AHP) and the Strength, Weakness, Opportunity, Threat (SWOT). AHP was used to determine the factors or criteria related to the standardization of security devices that include standards of procedure, vendors' security assurance, operators'/vendors' superior qualification, institutionalism, and auditing and the sub-criteria of each of these factors which include policy, development, and law enforcement. Based on the weight of the criteria and sub-criteria prioritized criteria could be determined that have a significant effect on the implementation of the standardization of security devices and the most appropriate approach to sub-criteria for use whether it is policy, coaching or law enforcement approach. SWOT method was used to identify the advantages and disadvantages currently faced in the implementation of device security. Based on identification results, the appropriate strategy models could be formulated to achieve the goal of the realization of security standards. Qualitative methods were carried out by field observations, in-depth interviews and focus group discussion to describe the current condition of the implementation of device security. The mixed method was used since this study was aimed at describing the current condition of the implementation of telecommunication device security and identifying the potentials

and obstacles serving as the basis for formulating the appropriate handling strategies to achieve the goal of the realization of security standardization.

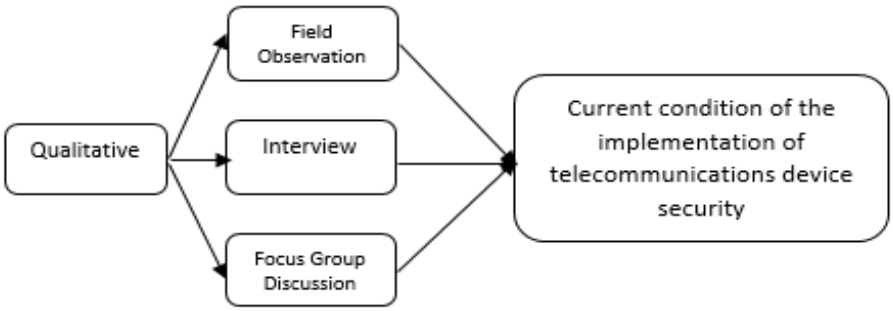

Figure 1. Qualitative method

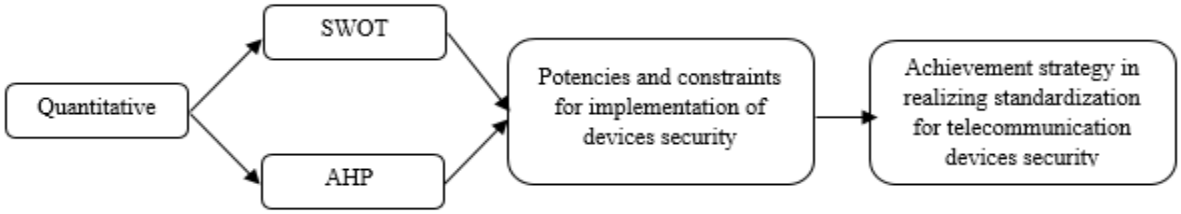

Figure 2. Quantitative method

The technique for determining the informants/resources was based on the involvement with the issues raised and expert in the respective field. The informants/resources in a qualitative approach were the ICT industry players such as mobile network operators, telecommunications device vendors, academia and government agencies in Indonesia. The present study was conducted in Jakarta, Bandung and Batam considering that those locations were ones of the ICT industry players and where the centers for device testing were available. Analysis of the data began with presuming the present conditions including the ecosystem of telecommunications equipment, potential security breaches, experts' projections and estimate of the increasingly higher degree of dependence on foreign vendors and empowerment of testing agencies to apply the security standards.

4. Result and Discussion

4.1. Implementation of Security Standards, Including Audit and Completeness of ICT Device Testing

4.1.1. General devices

The current implementation of the security standards of ICT devices for general purposes commonly adopted international standards, such as ISO/IEC, ETSI, ITU, COBIT 5, CC (Common Criteria) and device manufacturers' standards. In addition to these standards, the industry also make internal policies for device and system security. This is done by the industry due to the perceived better assurance of the security of ICT devices. A number of industries have been performing internal and external audits (related to certification, such as ISO, etc.) but there is no obligation to report the auditing results to the government. Availability of testing facilities remains very limited with regard to the quantity and completeness of the testing equipment. These results showed that ICT devices for general purposes have had standards, but continuing efforts are needed with regard to the completeness of the testing facilities and periodic reporting of auditing results to the government.

4.1.2. Specialized devices

The current implementation of the security standards of ICT devices for specialized purposes followed those standards derived from the ICT vendors and the internal information security policy of each agency. ICT devices for transmitting confidential information, such as cryptographic instruments, adopted the procedures of Lemsaneg which referred to the international standards ISO 19790 and ISO 24759 on security standards of cryptographic equipment. Availability of the testing facilities and device security audits remained very limited in terms of both the quantity and completeness of the testing equipment. These results demonstrated that ICT devices for special purposes had no specific security standards separate from those of devices for general purposes.

4.2. Implementation Regulation Status of ICT Device Security Standards

Law No. 11 of 2008 on Information and Electronic Transactions, Law No. 3 of 2002 on National Defense, Law No. 36 of 1999 on Telecommunications, Regulation of the Minister of Communications and Information Technology No. 18 of 2014 on Certification of Telecommunications Tools and Equipment, Regulation of the Head of National Crypto Agency No. 9 of 2010 on Guidelines for Certification of Cryptographic Equipment, Regulation of the Minister of Communication and Information Technology No. 1 of 2015 on the Amendment to the Regulation of the Minister of Communication and Information Technology No. 18 of 2014 are among the regulations related to defense and security and also certification of equipment and devices. However, these regulations have not specifically included standardization of security devices including the levels of security standards both for general and special purposes. Thus, there is a need for legislation that specifically govern security standards of devices.

4.3. Role of Regulator in Regulating and Controlling National Implementation of Security Standards of ICT Devices

The National Crypto Agency has its own unit to test and certify ICT devices with special security features used within the government scope despite the absence of national standards. Lemsaneg has drawn up an internal reference for testing and certification of security devices that refers to the international standards ISO 19790 on security aspects that must be satisfied by a cryptographic module, ISO 2459 on testing methods for a cryptographic module and based on the experience of Lemsaneg's research and development division with handling cryptography for government agencies. Meanwhile, the Ministry of Communications and Information Technology also had a separate unit for testing and certification of ICT devices but only included security device in terms of health, rather than in terms of information security. With regard to government agencies with no testing facilities, the unit authorized to handle internal security of devices in their respective agencies coordinated with Lemsaneg for testing and certification of ICT devices for confidential or special purposes. Thus, in this case regulators played a vital role in policy formulation as well control of implementation of device security standardization.

4.4. Obstacles faced in ensuring the security of ICT Devices for General and Special Purposes

A number of obstacles faced with regard to security assurance of telecommunications devices included the lack of national regulations for the implementation of standards and procedures as well as security assurance of ICT devices that could be adopted by the government and industry, the lack of local experts in the field of information security, the limited testing facilities for testing device security that could technically support the regulations have been and will be defined, the high dependence on foreign vendors, and the lack of collaboration and synergy between both the industry and government.

4.5. AHP and SWOT Analysis

4.5.1. AHP (Analytical Hierarchy Process)

The AHP structure used in the present study is shown in Figure 3 and the results are presented in graphical form in Figure 4 to Figure 9. Figure 4 shows that the criteria or factors of standard of procedure, vendors' and operators' device security assurance and operators'/vendors' superior qualifications are the three significant factors in achieving security standardization of telecommunications devices, particularly with regard to supporting national defense and security policies with a weight of 55%, 22.6% and 13.4%, respectively.

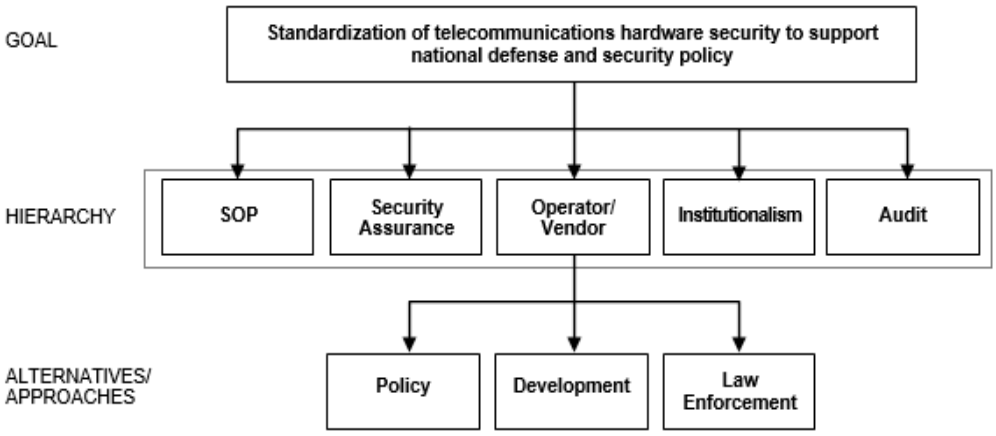

Figure 3. AHP Analysis

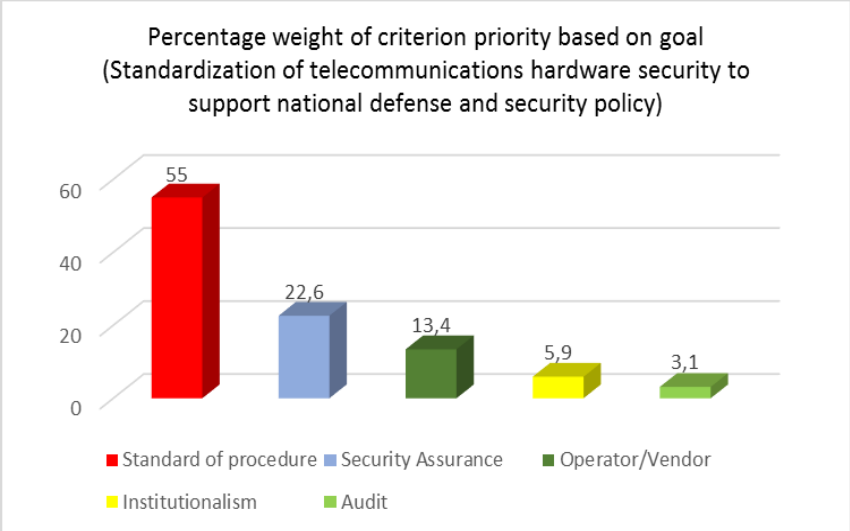

Figure 4. Results of AHP-percentage weight of criteria

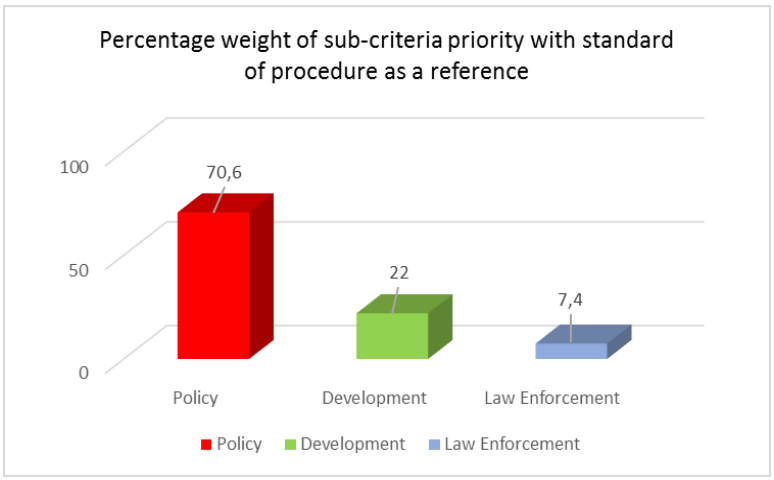

Figure 5. Weight of sub-criteria with SOP as a reference

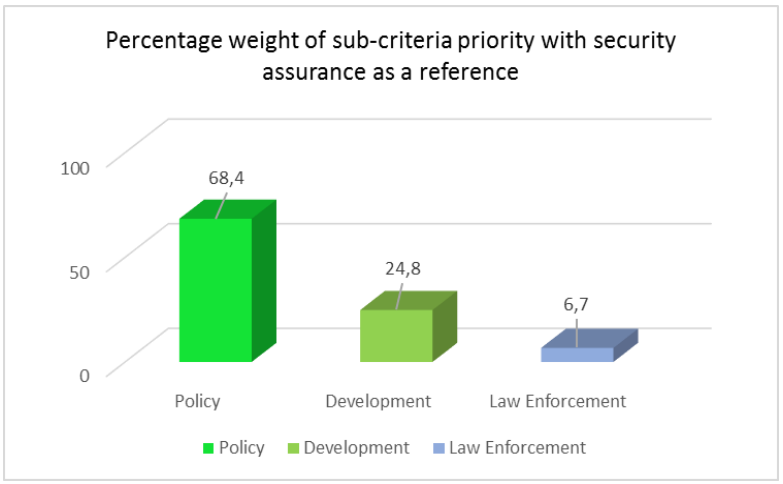

Figure 6. Weight of sub-criteria with security assurance as a reference

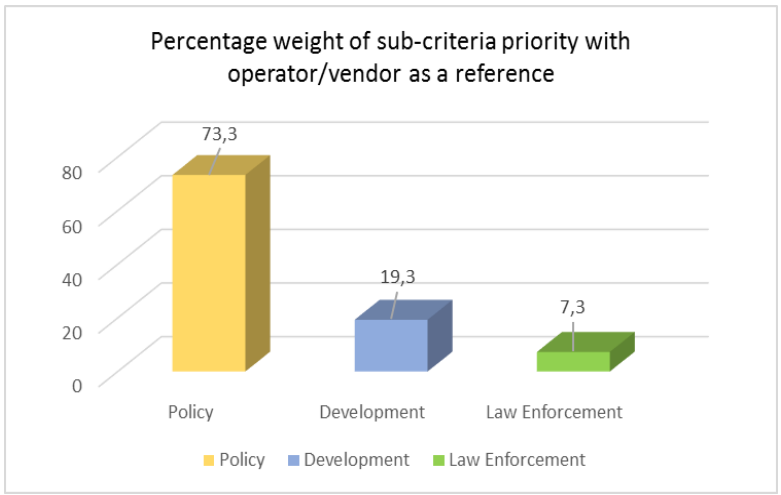

Figure 7. Weight of sub-criteria with industry qualification as a reference

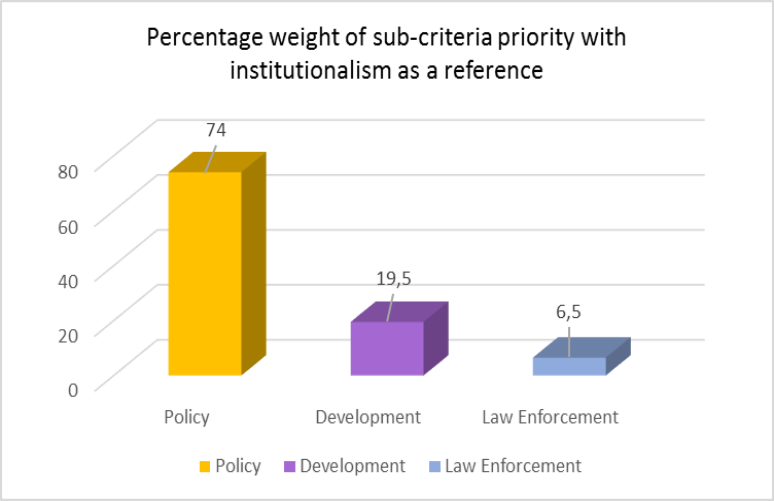

Figure 8. Weight of sub-criteria with institutionalism as reference

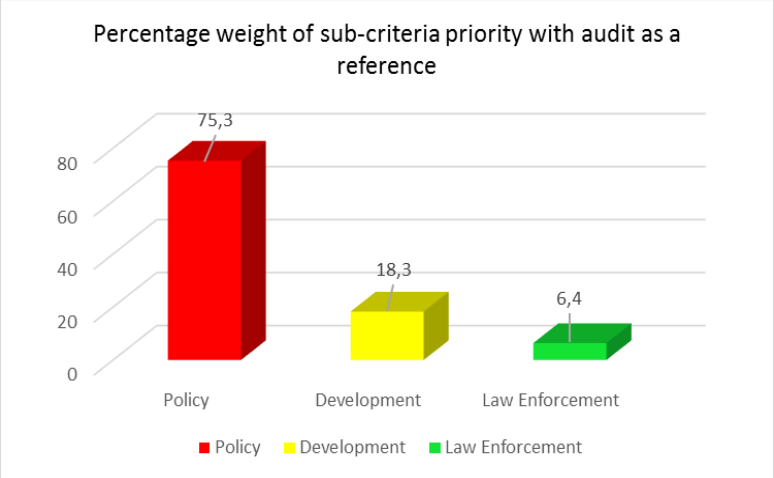

Figure 9. Weight of sub-criteria with audit as a reference

Figure 5 to Figure 9 show that with regard to realizing security standardization of telecommunications devices for each of such criterion or factor, the policy approach has the highest weight. In other words, in order to realize the security standardization of telecommunications devices by means of SOP development, vendors' security assurance, operator/vendor qualifications, institutionalism and audit, a policy approach is required, in this case presence of regulation as a legal basis to realize security standardization of telecommunications devices.

4.5.2. SWOT (Strength, Weakness, Opportunity, Threat)

SWOT analysis identifies internal and external factors with regard to achieving the goal of standardizing telecommunications device security including strengths, weaknesses, opportunities, and threats divided into four quadrants as shown in Figure 10. Quadrant I is located in the upper right area, quadrant II in the lower right area, quadrant III in the lower left area, and quadrant IV in the upper left area. The SWOT calculation produced the weights for strength–weakness comparison of –0.3, while the weight for opportunity–threat comparison was –0.28, or located in quadrant IV. It means that in order to achieve the goal of standardization of device security there are still many weaknesses and challenges encountered. Thus, based on these results, in

the diagram the best possible strategy for the comprehensive management of security standardization of telecommunications, particularly in national defense and security is the 'consolidation' strategy in quadrant IV. The strategy requires efforts of utilization and optimization of the opportunities in order to minimize the weaknesses.

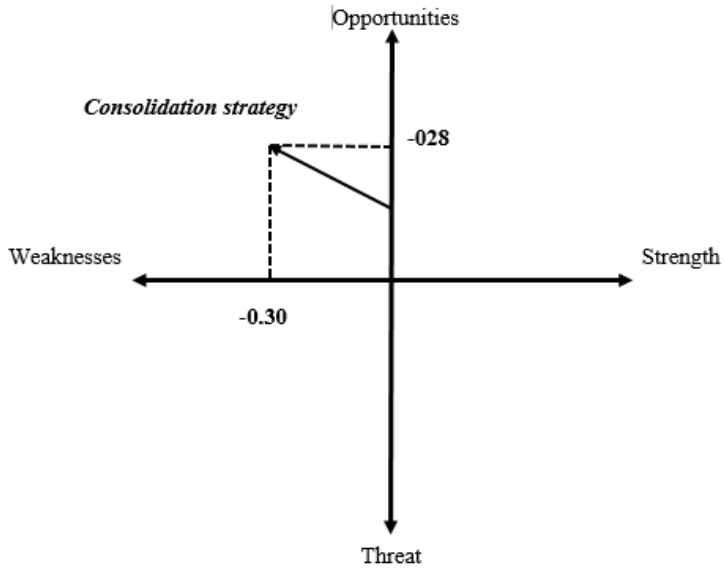

Figure 10. Results of SWOT analysis

5. Conlusions and recommendations

5.1. Conclusions

Current efforts to implement security standards of telecommunications devices only covered devices for general purposes, while devices for special purposes did not have their own security standards. The current regulations for security standards of telecommunications devices remained inadequate, especially those for telecommunications devices for special purposes. There were a number of obstacles related to security assurance of telecommunications devices, such as the lack of local experts in the field of information security, the limited testing facilities for testing device security that could technically support the regulations have been and will be defined, the high dependence on foreign vendors, and the lack of collaboration and synergy between both the industry and government. As the regulator, the government plays a vital role as both the policy maker and controller of the implementation of security device standardization. In order to achieve the goal of standardization of telecommunications device security, especially with regard to supporting defense and security policies, further efforts are needed to make it happen.

5.2. Recommendations

Government agencies should immediately draw up a roadmap for the implementation of telecommunications device security standards, including a number of stages for the preparation and adoption of regulations that specifically regulate the standardization of security devices, the determination of the agency authorized to test and certify security devices, and preparation of technical guidelines for device security auditing and certification. Additionally, it is also important to strengthen the partnership with the national industry and international standardization organizations for improving ICT security standards and accelerating the transfer of technology, provided that it is based on the principle of mutual respect for sovereignty among

countries. Strengthening collaboration and synergy among government agencies is required, for example by establishing an information security council comprising government authorities such as the Ministry of Telecommunications and Information Technology, Lemsaneg, BIN, BAIS, Police, Indonesian National Armed Forces, Ministry of Defense, and so on. Results of the present study are expected to serve as a reference for further studies, with a focus on the aspects associated with the stages of the roadmap preparation.

6. Acknowledgements

The author would like to thanks to and highly appreciate Mr. Ian Yosef and Mr. Daniel Wiyogo of ITB, Mr. Herdis Herdiansyah of Universitas Indonesia, Mr. Ahmad Hashim of Puslitbang Aptika IKP of the Ministry of Communications and Information Technology who have been willing to contribute to the completion of the present study. The author would also like to thanks to the Puslitbang SDPPI of the Ministry of Communications and Information Technology for facilitating this study from the initial stage to the completion.

References

Allan Gyngell, M. W. (2007). *Making Australia Foreign Policy (Second Edition)*. New York.

Brown, L. (n.d.). Lecture Notes for Use with Network and Internetwork Security by William Stallings. Retrieved from http://www1.shore.net/~ws/Security-Notes/index.html

Creswell, J. W. (1994). *Qualitative and quantitative approaches*. London: SAGE Publications.

David J. Icove. (1997). Collaring the cybercrook: an investigator's view. *IEEE Spectrum*, 31–36.

Direktorat Keamanan Informasi Kementerian Kominfo. (2015). Standar Keamanan Penyelenggaraan dan Perangkat Telekomunikasi.

Direktorat Standardisasi Kementerian Kominfo. (2015). Penerapan SNI ISO/IEC 15408 tentang Common Criteria.

Dowd, P. W., & McHenry, J. T. (1998). Network Security: It's Time To Take It Seriously. *IEEE Computer*, *September*, 24–28.

H.Dorff, R. (2004). Some Basic Concept and Approaches to the Study of International Relations. Dalam J.Boone Bartholomess, Jr (Ed). US ArmyWar College: Guide To National Security Policy And Strategy. Retrieved from http://www.strategicstudiesinstitute.army.mil/pubs/download.cfm?q=409

http://www.zdnet.com/article/gemalto-our-sim-cards-are-secure-despite-nsa-hack-claim/. (n.d.).

ID-SIRTII. (2015). Security Assurance for Telco's/IP/IT Equipment Certification.

Indrayanto, A. (2015). Industri Perangkat Telematika Indonesia.

J.M. Rodriguez Bejarano. (2012). Security in IP satellite networks: COMSEC and TRANSEC integration aspects. In *Security in IP satellite networks: COMSEC and TRANSEC integration aspects*. The Sixth Advanced Satellite Multimedia Systems Conference.

Juslin, J. (2003). Automatic backdoor analysis with a network intrusion detection system and an integrated service checker. Information Assurance Workshop.

Kiblat.mht. (n.d.). http://www.kiblat.net/2015/02/25/dan-inggris-retas-ponsel-seluruh-dunia-ini-10-hal-yang-perlu-anda-tahu/.

Lembaga Sandi Negara. (2014). Sosialisasi Draft Perka Lemsaneg tentang Standar Peralatan Sandi.

NargesArastouie, E. S. dan. (2011). Backdoor detection system using artificial neural network and genetic algorithm.

Paryati. (2008). Keamanan Sistem Informasi. *Seminar Nasional Informatika 2008*.

PT LEN INDUSTRI. (2015). Kesiapan PT LEN INDUSTRI Dalam Mendukung Pembangunan Sistem Keamanan Perangkat Telekomunikasi Untuk TNI dan POLRI.

Rahardjo, B. (1999). *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT Insan Komunikasi / Infonesia.

Raharjo, B. (2015). Pengantar Keamanan Sistem Informasi.

Richardus, Eko, & Indrajit. (2011). MANAJEMEN KEAMANAN INFORMASI DAN INTERNET.

Sebastian Schrittwieser, Peter Fr¨uhwirt, Peter Kieseberg, M. L., & Martin Mulazzani, Markus Huber, E. W. (2012). Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. *SBA Research gGmbH*.

Simson Garfinkel. (1995). *PGP: Pretty Good Privacy*. O'Reilly & Associates,Inc.

Stallings, W. (2011). *Network Security Essentials*. PrenticeHall.

Stove, A. G. (2004). Low probability of intercept radar strategies. *IEEE Proceedings on Radar, Sonar and Navigation*, *151*(5).

Wamala, F. (2011). ITU National Cyber Security Strategy Guide. ITU.

Wenjun Gu, Neelanjana Dutta, S. C. and X. B. (2012). Providing End-to-end Secure Communications in Wireless Sensor Networks. *Missouri University of Science and Technology*.

Wicaksono, N. (2007). AUREN: Sistem Pengamanan Smartphone dengan Penghapusan Informasi Berharga dan Pengiriman Informasi untuk pelacakan otomatis. Bandung.

William Stallings. (1995). *Network and Internetwork Security*. PrenticeHall.

Woods, S. S. dan C. (2012). Breakthrough silicon scanning discovers backdoor in military chip.