Journal of Theoretical and Applied Information Technology
31st August 2018. Vol.96. No 16
© 2005 – ongoing JATIT & LLS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EXPLORATION STUDY OF CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT DESIGN FOR CERTIFICATION AUTHORITIES IN INDONESIA

[1]YOVA RULDEVIYANI, [2]ARFIVE GANDHI, [3]YUDHO GIRI SUCAHYO
[1, 2, 3]Faculty of Computer Science, Universitas Indonesia, Indonesia
E-mail: [1]yova@cs.ui.ac.id, [2]arfive.gandhi@ui.ac.id, [3]yudho@cs.ui.ac.id

ABSTRACT

Certification Authority (CA) must unveil its Certificate Policy (CP) and Certification Practice Statement (CPS) as obligatory and fundamental documents to describe its technical information security, business processes, and legal compliance. Although had been initiated since 2014, Indonesia National Public Key Infrastructure (INPKI) still cannot be operated completely by Root CA, Sub-CA's, and other involved participants. This situation affected by CA's inability to produce adequate CP and CPS that cover necessary information required above. As Root CA in INPKI, Ministry of Communication and Information Technology (MCIT) shall propose CP and CPS for itself and also provide CP and CPS framework for its Sub-CAs. Previously, Sub-CAs confronts difficulties to propose CP and CPS due to their low proficiency. Using the concept of knowledge management, MCIT needs to regulate and educate Sub-CAs and itself as Root CA by proposing CP and CPS as knowledge transfer and guidelines. Proposed CP and CPS become empirical externalization and internalization so that each CA can compose its own CP and CPS with decent content to cover the required issues. This research explores how CAs in INPKI formulates their CP and CPS based on Request for Comment (RFC) 3647 with larger point of view. This exploration aims to extend and criticize whether the proposed CP and CPS are qualified to encourage the CA's readiness and the preparation of INPKI. This exploration contributes significant impact through preparation of CP and CPS. Produced CP and CPS will be more qualified and enhanced in unveiling necessary information to obtain trustworthiness in three aspects: governance; technical; and human resource requirements.

Keywords: *Certification authority; Certificate policy; CP; Certification practice statement; CPS; Information security; Public Key Infrastructure*

1. INTRODUCTION

Digital business in Indonesia requires information security as fundamental aspect to enhance its quality service. Information security becomes significant aspect that provides adequate protection to stakeholder and complies with related regulation. Ministry of Communication and Information Technology (MCIT) has initiated Indonesia National Public Key Infrastructure (INPKI) to strengthen information security in national digital business and to comply with Government Regulation of Electronic System and Transaction Authority (*PP-PSTE*) [1]. Those regulations mandate legalization of certification authority, certificate practice, and electronic signature as Public Key Infrastructure (PKI) components. PKI enables the principles of information security, i.e. Authentication, Integration, Confidentiality, and Non-repudiation [2] using those components.

The ecosystem of INPKI involves of MCIT as Root Certification Authority (Root CA); several Subordinate CAs (Sub-CAs); Registration Authorities (RAs); and citizens as subscribers [3] [4]. As certificate issuer for Sub-CAs, MCIT has fundamental roles. MCIT need to ensure that INPKI follows the necessary international standards and comply with national regulations. Sub-CAs has important role as the issuer of certificate in government or private services and therefore should follow the standardized framework of MCIT.

Required standards that should be completed immediately by Root CA and Sub-CAs are Certificate Policy (CP) and Certification Practice Statement (CPS). They have become common mandatory documents in PKI industry that provide trustable stipulation regarding information security and management in a CA. They are required to establish trust relationships between the PKI provider, the subscribers and relying parties [5].

Root CA must appraise the Sub-CA's feasibility and reliability as part of accreditation program by MCIT. Root CA and Sub-CA must deliver certification practice based on their CP and CPS respectively.

The big challenge that MCIT faces in INPKI is low proficiency in formulating CP and CPS. This challenge also becomes problem for CAs in Indonesia since PKI ecosystem and components are still relatively new in Indonesia. It indicates lack of knowledge as significant issue which affects this basic problem. If Root CA proposes poor CP and CPS, it will reduce its trustworthy significantly. Sub-CA's CP and CPS with inadequate content will endanger its reliability from subscribers' view. Existing and candidate of CAs should be facilitated by appropriate knowledge management system which actualized using CP and CPS as prepared by MCIT. Hence, MCIT should formulate its CP and CPS as Root CA and construct CP and CPS framework for Sub-CA.

After formulates in [3] and [4], this research extends and criticizes the result of proposed CP and CPS for Root CA and Sub-CAs in INPKI. CP and CPS for Root CA cover certification practice that performed in Sub-CA's certificate management. Then CP and CPS framework for Sub-CA cover how a Sub-CA certifies its subscribers and maintain their certificate. The exploration scrutinizes their suitability between produced CP and CPS with required issues and also specifies how far customization permitted.

This research organized into following sections. Section 2 describes literature review from relevant study, especially on CP and CPS. Section 3 unveils the methodology of this exploration. Process of CP and CPS structure adoption is exposed in Section 4. Section 5 details the exploration result of Root CA's CP and CPS, include how this research improves the WebTrust criteria compliance. Then, exploration result of Sub-CA's CP and CPS is conducted in Section 6. Section 5 and 6 are revealed using three aspects as thematic content of CP and CPS. This research also proposes improvement for future that explained in Section 8. Finally, Section 8 summarizes this research and will be complemented by Section 9 with recommendation.

2. LITERATURES REVIEW

2.1. Structure Model of INPKI

MCIT has established INPKI using hierarchical model with Root CA operated by MCIT. This hierarchical model offers scalability, easier and shorter certification paths [6] [7]. Root CA governs several subordinate-CAs which can be categorized into two types [3]: government CA and non-government CA. Government CA delivers certification practice only for government environment and public service. The INPKI ecosystem is illustrated in Figure 1. The symbol '1' in Root CA Indonesia indicates its existence as singular entity and 'n' informs Sub-CAs, RAs, and Subscribers as plural entities in INPKI. *PP-PSTE* [8] explains three categories of CA in Indonesia, i.e. registered CA, certified CA, and also rooted CA. They are allocated as Sub-CAs in INPKI.

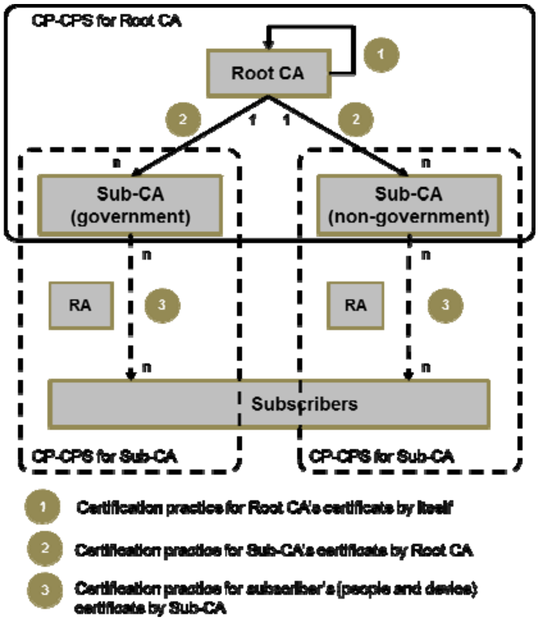
CP-CPS for Root CA
Root CA
1
2
1
1
2
n
n
Sub-CA (government)
Sub-CA (non-government)
n
n
RA
3
RA
3
n
n
Subscribers
CP-CPS for Sub-CA
CP-CPS for Sub-CA
1 Certification practice for Root CA's certificate by itself
2 Certification practice for Sub-CA's certificate by Root CA
3 Certification practice for subscriber's (people and device) certificate by Sub-CA

Figure 1: INPKI Ecosystem, improved from [3] [4]

Until 2018, there are three governments CAs, i.e. National Cyber and Cryptography Agency (formerly National Cryptography Agency); Agency for the Assessment and Application of Technology (Ministry of Technology Research and Higher Education); and Directorate of Tax (Ministry of Finance). They have specific purposes respectively, tax services, such as registration, report, and payment for Directorate of Tax. A non-government CA provides certification practice for private context and commercial. Since 2016, several local

CAs have been operated in Indonesia with their limited scope for internal community. To reduce operational load and enlarge service area, Sub-CA can employ Registration Authorities (RAs) for maintaining the subscribers, such as registration process, certificate delivery, and customer services.

2.2. Certificate Policy and Certification Practice Statement

CP describes authenticity for a certificate user, signifying that the public key of the CA is bound to the certificate that is referred to by the CP [6]. CPS informs detail of practices in issuing and managing certificates by a CA. CPS typically includes the following type of information: the CA with which the CPS is associated; the CPs implemented by the CA; the CA policy for issuing and renewing certificates; the validity period of the CA certificate; the conditions in which the CA might revoke the user certificate; the CRL policies; and the cryptographic algorithm used [6].

CP and CPS can be distinguished based on their different focus and function. The purpose of CP is explanation and summary about requirements and standards imposed that performed in digital certificate. The CPS endeavors how a CA and other entities in PKI ecosystem implement procedures and controls to conform what CP requires [4] [8].

2.3. RFC (Request for Comments) 3647

RFC 3647 is a common international framework to construct CP and CPS. This framework offers comprehensive list of topics that potentially need to be covered in a CP or CPS [4]. RFC 3647 decomposes CP and CPS structure into nine provisions as follows [9].

- **Introduction**: reveals basic information, such as identity and authority of CP/CPS;
- **Publication and Repository Responsibilities**: stipulates how information released in a repository;
- **Identification and Authentication**: describes procedure about applicant verification;
- **Certificate Life-Cycle Operational Requirements**: specifies requirements imposed for related entities with respect to the life-cycle of a certificate;
- **Facility, Management, and Operational Controls**: reveals necessary infrastructure non-technical (procedural and human) security control
- **Technical Security Controls**: defines the security measures, such as cryptography keys and activation data;
- **Certificate, CRL** (Certificate Revocation List), **and OCSP** (Online Certificate Status Protocol) Profiles: specifies of certificate format;
- **Compliance Audit and Other Assessments**: defines required appraisal that should be performed by the related authority;
- **Other Business and Legal Matters**: explains the financial, legal, and administrative circumstances.

2.4. WebTrust for CAs v1-Disclosure Criteria

WebTrust has encouraged Trust Service Principles and Criteria for CA Version 2.0 as contribution from CICA (Canadian Institute of Chartered Accountants) Task Force [10]. This product attaches “WebTrust for CAs v1-Disclosures Criteria” as best-practice for CA to appraise its trustworthiness and security aspect in its certification practice using WebTrust’s quality standard [4]. The appraisal will be conducted using 45 criteria in four categories: General, Key Life Cycle Management, Certificate Life Cycle Management, and CA Environmental Control [10]. Through this self-assessment, CA can determine what topics should be informed in its CP and CPS. Therefore, CA can confirm whether current CP and CPS has been comprehensive, adequate, and sufficient. This appraisal will be performed only for Root CA due to its status as highest role in INPKI. MCIT will also propose Root CA Indonesia to be recognized in global digital world. This plan will be established through WebTrust certification. Hence, MCIT attempts to follow WebTrust standard.

2.5. Related National Regulations in Information Security Area

Government has recognized CA as legal organization in information technology business. Electronic Information and Transaction Act 11/2008 (*UU-ITE*) has mandated each CA to disclosure accurate, clear, and exactly information about electronic signature scheme for its subscribers [8]. Government Regulation 82/2012 on the Implementation of Electronic System and Transaction (*PP-PSTE*) instructs CA to manage its issued certificate and comply with several requirements such as human resource general background or data center and disaster recovery center location [1]. *PP-PSTE* also sets mandatory CA's activities [1]: subscriber's verification, certificate issuance, extension of certificate's validity period, certificate revocation, certificate validation, and list of certifications depend on status.

As electronic system authority, CA should conform to the Regulation of MCIT 4/2016 on the Information Security Management System (*SMPI*). This regulation establishes the security level categorization for electronic system [11]. Hence, Root CA and Sub-CAs must follow the specific stipulations that instructed for their respective category.

To encourage INPKI ecosystem, MCIT has assigned itself as Root CA Indonesia through Regulation of MCIT 1/2016. Based on this regulation, MCIT oversees Sub-CAs and issue their certificates. The detail mechanism for Root CA's task will be stipulated using other regulation that ratified by MCIT soon.

3. METHODOLOGY

This research comprises three primary phases; i.e. formulation of CP and CPS structure; CP and CPS exploration for Root CA Indonesia; and CP and CPS exploration for Sub-CAs. Some parts of this research are cascading into [3] and [4] using Focus Group Discussion (FGD), literature review, and content analysis as qualitative approaches.

CP and CPS structure has been formulated in first phase using literature review to determine proper standard. It also considers benchmarking or comparison with other national PKI in several countries considering hierarchical model as criteria. This phase produces decision on which standard of CP and CPS structure for CA in INPKI. In second phase, the chosen standard will be explored to obtain suitable adaptation for Root CA's CP and CPS through [3]. This phase reflects how Root CA certifies its Sub-CAs in INPKI, see Figure 1.

After formulating CP and CPS for Root CA, FGD will explore the structure for Sub-CAs in INPKI in third phase and actualized [4]. This phase cascades Root CA's CP and CPS to Sub-CA ones. It analyses related regulations in Indonesia and interpret them into relevant provisions in Sub-CAs CP and CPS. This analysis encompasses governance, technical and human resource requirements. This phase represents how Sub-CA certifies its subscribers, see Figure 1. To enhance content of CP and CPS, FGD will be supplemented with benchmarking about empiric implementation of Sub-CAs in other countries and also latest technology in PKI industry. This research also review the substance of current CP and CPS that issued by CAs as candidate of Sub-CA in INPKI.

Based on second and third phases as conducted in [3] and [4], there are some topics that probably have not been solved yet. To ensure this research's sustainability, those topics will become target for the further exploration. In this article, research also collects some consideration for each topic and also informs how to manage them in other case studies.

4. FORMULATION OF CP AND CPS STRUCTURE

INPKI has been designed using hierarchical model. Considering two factors. First factor is the standard of CP and CPS adopted by MCIT as Root CA. Compatibility and interoperability alignment can be built well if the Root CA and its Sub-CAs adopt the same standard for their CP and CPS structure. Since MCIT has followed RFC 3647 for its CP and CPS structure [3], so that Sub-CAs should also implement RFC 3647 also.

The second factor is standard of CP and CPS structure that performed in many countries using the same PKI model. Based on result of benchmarking, many Sub-CAs in national PKI have established CP and CPS using RFC3647. Sub-CAs that implemented RFC 3647 are Government CA of National Centre for Digital Certification in Saudi Arabia [12]; Infrastructure CA in Qatar [13]; Citizen and Resident CA in Qatar [14]; and several accredited CAs in Philippine National PKI [15]. It indicates that RFC 3647 has empirical experience as standard of CP and CPS structure in Sub-CA context.

5. CP AND CPS EXPLORATION FOR ROOT CA INDONESIA

5.1. Governance Requirements for Root CA's CP and CPS

This subsection portrays hierarchical relationship in INPKI, especially how Root CA interacts with other participant. These explanations are derived from interpreting the Figure 1. Root CA's CP and CPS should provide these stipulations explicitly as follows [3]:

- Root CA's proclamation as highest entity in INPKI (Provision/Prov. 1.1, 1.3). Furthermore, Root CA has important duty to certify itself. This duty produces Root CA certificate to sign Root CA's CRL and Sub-CA's certificate (Prov. 1.4.1).
- Root CA's affiliation to MCIT (Prov. 1.1, 1.3 in Sub-CA part).
- All related participants in INPKI (Prov. 1.3). Based on current business requirement and comparison to other national root CA, Root CA will manage Sub-CA without Registration Authority. However, Root CA allows RA to assist Sub-CA. (Prov.1.3 in RA part).
- Root CA's CP and CPS publication versioning and frequency (Prov. 1.2) and amendments mechanism (Prov. 9.12). This stipulation reflects Root CA's commitment to maintain life cycle of CP and CPS based on necessary adaptation.
- Compliance with related regulation (Prov. 9.12, 9.14, 9.15). This compliance also include Root CA's assurance to protect Sub-CAs' information and other confidential business information Generally, Root CA should comply with government policy about digital business and intellectual property.

5.2. Technical Requirements for Root CA's CP and CPS

Technical requirement establishes adequate standard actualized in certification practice. In this subsection, technical requirements refer to how Root CA certifies its Sub-CA. To enhance its quality service, Root CA should consider international standard and best-practice, as follows [3]:

- Basic Distinguished Name (DN) for Root CA's certificate using this structure "c=id, o=Root CA Indonesia, cn=Root CA Indonesia", while structure for Sub-CA's one is "c=id, o=<Sub-CA name>, cn=Root CA Indonesia" (Prov. 3.1.1). This structure adopted from ITU X.500, RFC 4514, and RFC 2256 as standards.
- Sub-CA's certificate is only managed using these statuses as life-cycle: issuance, revocation, renewal, re-issuance, and expiration. Suspension status will not be recognized (Prov. 4.9.13, 9.14, 4.9.15, 4.19.16). Hence, its certificate's status is only provided by CRL without OCSP (Prov. 4.9.9, 4.10.1, 7.3.1, 7.3.2). Root CA also determines that key escrowing for Sub-CA is not permitted (Prov. 4.12.1 and 6.2.3).
- After issuance stage, Root CA should not modify its Sub-CA's certificate (Prov. 4.8). Sub-CA also does not have permission to modify its certificate. This policy aims to ensure certificate's integrity. If any necessary amendment about identity in Sub-CA's, such as affiliation change, then Sub-CA will ask Root CA to revoke its current certificate and Root CA will issue a new one. Detail current certificate revocation mechanism stipulated in related provisions below.
- Sub-CA's certificate revocation will be applied based on these circumstances (Prov. 4.9.1): [a] Identifying information or affiliation components of any names in the certificate becomes invalid; [b] Any information in the certificate becomes invalid; [c] There is a reason to believe that the private key has been compromised; [d] The Sub-CA or other authorized party (as defined in the CPS) asks for its certificate to be revoked; or [e] Sub-CA termination.
- Root CA's data center and data recovery center must be in Indonesia [6, 7]. CP and CPS only reveal premises address without unveil complete location (Prov. 5.1.1, 5.7.4). For necessary assessment, Sub-CA can provide open-access to external auditor depends on assessment scope.
- Other technical standards acquired in Root CA's certification practice detailed in Table 1.

Table 1: List of Standards Adopted by Root CA in CP and CPS.

Standard	Usage
Network Time Protocol	Sub-CA's server internal clock shall be synchronized with Agency for Meteorology, Climatology, and Geophysics (BMKG)
PKCS #10	The method to prove possession of a private key (Prov.3.2.1)
FIPS 140-2 Level 3	Hardware cryptographic module validation for signing operations (Prov.6.2.1)
RFC 5280	Certificate and CRL profile (Prov.7.1 and 7.2)
Joint-ISO-ITU OID number	Registration for OID (Prov. 1.2 and 7.1.6)
4096-bit RSA Key with SHA256	Certificate and CRL signing (Prov. 6.1.5 and 7.1.3)

5.3. Human Resource Requirements for Root CA's CP and CPS

Human resource in this exploration portrays personnel's profile should be confirmed by Root CA's personnel. Basically, "human resource' terminology informs to 'experts' in a CA as component of electronic system authority [1], "personnel' in RFC 3647, or professional. Generally, Root CA utilizes international best-practice and national latest regulations as consideration to establish human resource distribution, availability and competence. MCIT also has reviewed how root CAs in other national PKI organize their human resource.

Root CA establishes roles and responsibilities using these considered factors: business process, IS architecture and IT infrastructure. Business process describes interaction among certification practice participants. Business process in Root CA can be more complex depends on how INPKI grows in the future; accordingly Root CA will consider its necessary personnel later. IS architecture hints how Root CA's business process cascaded into processed data/information and related application, include specialized application to maintain its certificate and Sub-CA's certificate. IT infrastructure covers appropriate technology in INPKI deployment. Through comparison with other root CA and review WebTrust best-practice, Root CA in INPKI should establish these following roles (Prov. 5.2.1): system administrator, operator, registration officer, and auditor. As information security consideration, segregation of duties among available roles should be established strictly. This segregation concept should be allocated in CP and CPS (Prov. 5.2.3, 5.2.4). Hence, Root CA explains explicitly minimum allocated personnel for each established role (Prov. 5.2.2).

Competence factor in human resources requirement depends on how government enforces the minimum competence. In *PP-PSTE*, government requires every expert must own a competence certificate [1] that will be detailed by related authority. That regulation has been supplemented by Ministry of Manpower (MMp) and MCIT. MMp has released Regulation of MMp 55/2015 about national competency standard (SKKNI) in information security [16]. It details competencies should be held by professional in information security field. Because certification practice has strong relationship with information security, then Root CA must comply with this SKKNI and declare the compliance through CP and CPS Prov. 5.3.1, 5.3.2, 5.3.3, 5.3.4. Root CA describes explicitly that SKKNI in information security has been complied as standard competencies or describe the detailed items in CPS. MCIT enforces *SMPI* [11] which specify required standard for electronic system authority depends on its classification. Based on *SMPI* exploration, Root CA has been classified as strategic electronic system that must implement ISO/IEC 27001 [11] in its system. As consequence, Root CA should require its personnel has competencies in ISO/IEC 27001. (Prov. 5.3.1, 5.3.2, 5.3.3, and 5.3.4).

Root CA also should establish non-technical knowledge to its personnel. Its personnel must understand and aware strongly the legal aspect of information security, such as *UU-ITE*, *PP-PSTE*, and *SMPI* [4]. As strategic electronic system, Root CA's personnel must be Indonesian citizen [3] to ensure his/her integrity. Hence, Root CA should check the background of its personnel (Prov. 5.3.1, 5.3.2).

5.4. Compliance to WebTrust's Disclosure Criteria

Root CA has important roles as highest entity in INPKI that issues Sub-CA's certificate. In order to improve INPKI quality and achieve global recognition, Root CA gradually establishes business processes using WebTrust's standard.

Standard that adopted immediately is WebTrust for CAs v1-Disclosure Criteria. The criteria examine the coverage of CP and CPS' topic so Root CA can appraise whether its CP and CPS provide appropriate and necessary information. Appraisal has been acquired by mapping 45 required criteria to related provisions in CP and CPS. Each criterion will exploit relevant provisions and criticize whether their provided content has been comprehensive and adequate. Based on the result of exploitation in [3], Root CA's CP and CPS meet 43 of 45 criteria. This research performs advance exploration to review the suitability of compliance.

The exploration evaluates the ecosystem that explained in Root CA's CP and CPS. As an example, in previous research [3], definition of Subscriber in Root CA's CP and CPS still ambiguous between Subscriber as end-user of INPKI (such as citizen or enterprise) and Sub-CA as entity that certified by Root CA. In other case, terminology CA is also ambiguous whether Root CA or Sub-CA. Root CA should emphasize these differences.

This exploration determines that CA hints Root CA while subscriber terminology represents the Sub-CA. This consideration comes from basic business concept as regards CA certifies subscriber. In Root CA case, certification practice performed by Root CA for Sub-CA, and therefore this exploration conduct new examination to check and improve its suitability. As a result, this advance exploration produces new relationship between WebTrust's Disclosure Criteria with Root CA's CP and CPS as shown in Table 2 (Annex A).

This exploration has demonstrated advance exploration of all 45 criteria. It offers few different results than previous one in [3]. This difference appears after this exploration conducted new definition of CA and Subscriber from those criteria into Root CA's business process. Furthermore, this advance exploration has succeeded to redefine the relevant provisions for 11th, 12th, 14th, 17th, 18th, 19th, 20th, 22nd, 23rd, 24th, 26th, 30th, 33rd, 34th, 36th, 39th, 41st, 44th, and 45th criteria. Those criteria have been signed by 'r/v' that reflects 'revision' from previous research in [3]. Content of Root CA's CP and CPS have been improved to adapt its business process. This improvement produces 40 criteria has been fully mapped into related provisions in Root CA's CP and CPS.

Criteria that can't meet related provisions 12th, 16th, 26th, 34th, and 38th criteria. The 12th (RA obligations) and 26th (Registration requirements where external RA are used) have not been mapped since Root CA certifies Sub-CA without RA participation. In Note column, it hints by 'n/p' which means 'not performed'. Root CA's CP and CPS describe this circumstance in 4th provision about Certificate Life-Cycle Operational Requirements. The 34th (Certificate Suspension) and 24th criteria have not also been mapped since Suspension status is not still recognized in INPKI. By comparing Table 1 above result of previous research in [3], the 16th and 38th criteria are still not covered with same reason.

6. CP AND CPS FRAMEWORK EXPLORATION FOR SUB-CA INDONESIA

6.1. Governance Requirements for Sub-CA's CP and CPS

This subsection portrays hierarchical relationship between Sub-CA with its related participant. These explanations are derived from interpreting Figure 1 above. CP and CPS should provide these stipulations explicitly as follows [4]:

- Sub-CA's proclamation as INPKI participant under Root CA's supervision (Provision/Prov. 1.1, 1.3 in Root CA part). Therefore, Sub-CA's certificate shall be signed by Root CA. When a Sub-CA signs its CRL and subscribers' certificate using Sub-CA's certificate (Prov. 1.4.1). This stipulation relates to how Root CA certifies Sub-CA that revealed in Root CA's CP and CPS.
- Sub-CA's ownership or affiliation (Prov. 1.1, 1.3 in Sub-CA part). As an example, if General Directorate of Immigration (Ministry of Foreign Affairs) establishes a CA to provide online immigration service, then CP and CPS should declare that the Sub-CA affiliates to General Directorate of Immigration. This stipulation also applies for a CA in Indonesia as branch of foreign CA.
- Sub-CA type and category (Prov. 1.3: Sub-CA part). This provision is to confirm the type of CA whether the Sub-CA is a government CA or a non-government CA in INPKI. It should be followed and aligned with segmentation of certification practice, see differentiation of Sub-CA type in Structure Model of INPKI above.

CA also should hint its category in accordance with *PP-PSTE* [1].

- Subscriber's profile (Prov. 1.1, 1.3: Subscriber part, 1.4). Profile can describes segmentation subscriber, such as ordinary citizen, civil servant, enterprise, or may be device. This stipulation can be supplemented with the information about sector industry, such as tax payment, immigration, banking service. Sub-CA must describe clearly permitted and prohibited usage of subscribers' certificate (Prov. 1.4). Sub-CA also need to ensure that scope of its usage conforms to national regulation in Indonesia, i.e. *UU-ITE*, *PP-PSTE*, and *SMPI*.
- All related participants in certification practice (Prov. 1.3). Based on the business model, Sub-CA can involve Registration Authority to maintain subscribers. This collaboration should be declared clearly in CP and CPS (Prov.1.3 in RA part). If necessary, Sub-CA can provide technical guideline to distinguish the roles and responsibility between Sub-CA and RA.
- CP and CPS publication versioning and frequency (Prov. 1.2) and amendments mechanism (Prov. 9.12). This stipulation reflects Sub-CA's commitment to maintain life cycle of CP and CPS based on necessary adaptation.
- Compliance with related regulation (Prov. 9.12, 9.14, 9.15). This compliance also include Sub-CA's assurance to protect subscribers' information and other confidential business information Generally, Sub-CA should understand and comply with government policies on digital business and intellectual property. For Sub-CAs in specific sector industry, they should cover all related regulations in respective sector. Sub-CA can invite relevant authority to appraise its compliance with specific regulation.

6.2. Technical Requirements for Sub-CA's CP and CPS

To improve adequacy of standard implemented in subscribers' certificate issuance, Sub-CA needs to consider international standard and best practice. Sub-CA also should follow MCIT's technical requirements, as follows [4]:

- Basic DN for subscribers' certificate using this structure "c=ID, o=<organization name>, cn=<person name><VirtualIDnumber>" (Prov. 3.1.1). This structure adopted from ITU X.500, RFC 4514, and RFC 2256. The ID indicates Indonesia's country code. VirtualIDnumber reflects hash value from citizen identification number (NIK). However, NIK is considered as confidential information. MCIT proposes the usage of VirtualIDnumber concept.
- Similar to Sub-CA, subscriber's certificate is only managed using the following life-cycle states: issuance, revocation, renewal, re-issuance, and expiration. Suspension status will not be recognized (Prov. 4.9.13, 4.9.14, 4.9.15, 4.19.16) until numbers of subscribers grow larger. Hence status of subscriber's certificate is only provided by CRL without OCSP (Prov. 4.9.9, 4.10.1, 7.3.1, 7.3.2). The CRL for subscribers' certificate must be updated and published at least once a day. The maximum time of the CRL is 10 days (Prov. 4.9.6, 4.9.7, 4.9.8).
- After issuance stage, Sub-CA should not modify its subscriber's certificate (Prov. 4.8) with or without request from the respective subscriber. This policy aims to ensure certificate's integrity. If there is any amendment on the identity of a subscriber's certificate, Sub-CA will revoke his current certificate and issue a new one. Detail current certificate revocation mechanism stipulated in related provisions below.
- Revocation for a subscriber's certificate will be delivered based on these circumstances (Prov. 4.9.1): [a] Identifying information or affiliation components of any names in the certificate becomes invalid; [b] Any information in the subscriber's certificate becomes invalid; [c] There is a reason to believe that the private key has been compromised; [d] Direct request from the subscriber; or [e] Subscriber has been died. This revocation mechanism can involves RA depends on the related participant in the certification practice.
- Sub-CA's data center and data recovery center must be in Indonesia [1]. CP and CPS only unveil premises address without disclosure complete location (Prov. 5.1.1, 5.7.4). For required assessment, Sub-CA can provide open-access to necessary external auditor or Root CA.
- Other standards acquired in Sub-CA refer to standards of Root CA as shown in Table 1.

6.3. Human Resource Requirements for Sub-CA's CP and CPS

Human resource in this section depicts the personnel aspects of a Sub-CA. A Sub-CA needs to consider international best-practice and national regulations in establishing human resource, availability and competence. While waiting for further instruction from MCIT regarding the human resource requirement aspect, Sub-CA need to review how the human resource will be managed.

Roles and responsibilities of each personnel need to be established. As a baseline, Sub-CA should establish the following roles (Prov. 5.2.1): system administrator, operator, registration officer, and auditor [4]. Sub-CA may add more professionals to support their business activities but should ensure the segregation of duties among personnel which should be informed in CP and CPS (Prov. 5.2.3, 5.2.4). Sub-CA also needs to describe minimum allocated personnel for each role (Prov. 5.2.2).

Sub-CAs must comply with national competency standard (SKKNI) and declare the compliance through CP and CPS (Prov. 5.3.1, 5.3.2, 5.3.3, 5.3.4). Sub-CA describes explicitly that SKKNI in information security has been referred in building the standard competency of its personnel.

Following the regulation on information security in *SMPI* [11], Sub-CAs with strategic classification must also implement ISO/IEC 27001 in its system. As consequence, Sub-CA should also build the competencies of its personnel on ISO/IEC 27001 (Prov. 5.3.1, 5.3.2, 5.3.3, and 5.3.4) [4]. Sub-CA in a specific sector, such as banking, procurement, immigration, should also responsible to acquire competencies in the respective sector.

Sub-CA should also build the non-technical capacity of its personnel. Sub-CA's personnel should aware the national regulations on information security, such as *UU-ITE*, *PP-PSTE*, and *SMPI* [4]. The personnel of Sub-CA must also be Indonesian citizen and therefore background checking of personnel is a mandatory (Prov. 5.3.1, 5.3.2).

7. RECOMMENDATION FOR FUTURE IMPROVEMENT

This section proposes several recommendations for INPKI improvement that requires information security enhancement of Root CA and Sub-CA in several aspects. First recommendation is differentiation of subscribers' certificate issued by Sub-CA. Certificates need to be classified based on its type, usage, and technical requirement. As example, certificates for enterprise usage should have stringent requirement compared to certificates for personal usage. Certificate for high risk digital business, such as taxation and banking, also entail higher security requirement. This concept actually has been performing by National Crypto Agency [17] in certification practice and its life-cycle. National Crypto Agency determines the standardization that called as Level of Assurance Level of Assurance (LoA). They have classified certificate into four levels. Each level has different type and usage of certificate which the higher level has more complex requirement. This exploration proposes this concept to be established in INPKI by all Sub-CA.

In our analysis, MCIT as Root CA should determine the type of certificate that officially recognized in INPKI, then specifies the scope of usage and authorized subscriber. MCIT can develop analysis that summarize feasibility study and risk management for each certificate type. Based on the analysis result, MCIT should decide the minimum requirement for Sub-CA to issue them. Afterwards, MCIT establish the classification or level that cover all recognized certificates. Based on it, Sub-CA can review which level for certificate that will be issued and implements the minimum allowed requirement. Each Sub-CA should proclaim which level for its certification practice in the CP and CPS.

8. CONCLUSION

This section summarizes the exploration study of CP and CPS for CA in Indonesia. As a strategy to secure digital business in Indonesia, MCIT has established Indonesia National PKI (INPKI) with hierarchical model. It involves MCIT as Root CA, several Sub-CAs that organized by Root CA, Registration Authority, and subscriber. To raise its trustworthiness, Root CA and Sub-CA should deliver their CP and CPS as declaration of certification practice.

The emerging issue that threatens the INPKI is the low proficiency in formulating appropriate, adequate, and sufficient content of CP and CPS. This research has explored, provided more insight, and criticized the content of the proposed CP and CPS based on necessary international standards (such as ITU X.500, PKCS #10, and RFC 5280) and related national regulation (especially *UU-ITE*, *PP-PSTE*, and *SMPI*). Using qualitative approaches in FGD technique and literature reviews as methods, this research offers more accurate discussion to enhance the quality of proposed CP and CPS.

This research also explores the analysis of Root CA's and Sub-CA's CP and CPS using three aspects: governance; technical; and human resource requirements. Governance aspect portrays hierarchical relationship in INPKI, such as how Root CA interacts with Sub-CA. Technical requirement establishes adequate standard actualized in certification practice. Human resource in this exploration portrays personnel's profile that should be confirmed by CA's personnel. In case of Root CA, this research has revised the suitability of its CP and CPS using WebTrust Disclosure Criteria. There are 40 criteria have been mapped successfully into related provisions in Root CA's CP and CPS. To improve implementation of INPKI, this research also follows the Level of Assurance as initiated by National Crypto Agency. As implication, MCIT should classify the type of certificate and formulate necessary requirement, such as identifying the subscriber.

9. FUTURE RESEARCH

For further research, this exploration suggests the adaptation of CP and CPS in specific sector. It will consider more complex regulation since eash sector requires specific regulations that stipulated in CP and CPS. CA should customize its certification practice based on thematic business process and specific IT documentation framework. As illustration, a CA for taxation service should accommodate the financial affairs and required techonology as instructed by Ministry of Finance and Financial Service Authority. To promote this expansion plan, MCIT as Root CA Indonesia should consolidate related ministries or government agencies to establish implementation plan based on respective sector. This consolidation becomes strategy of INPKI adaptation to enlarge its usability in various environments. Therefore, INPKI will contribute to the ICT development in Indonesia through Indonesian citizen's information protection.

ACKNOWLEDGMENT

This research was supported by Universitas Indonesia under PITTA Grant 2018 "Risk Evaluation and Improvement Strategies for Platform-Based Startup Business" (No: 1899/UN2.R3.1/HKP.05.00/2018). We gratefully thank Faculty of Computer Science and Directorate of Research and Community Engagement, Universitas Indonesia.

REFERENCES:

[1] Government Regulation of Republic of Indonesia No.82 year 2012, "Electronic System and Transaction Authority", 15 Oct. 2012.

[2] R. Hunt, "Technological Infrastructure for PKI and Digital Certification", *Journal of Computer Communication* 24, 2001, pp. 1460-1471.

[3] A. Gandhi, Y.G. Sucahyo, T. Sirait, "Certificate Policy and Certification Practice Statement for Root CA Indonesia", *Proceedings of 2nd International Conference on Science in Information Technology*, 2016, pp. 312-317.

[4] A. Gandhi, Y.G. Sucahyo, T. Sirait, "Formulation of Certificate Policy and Certification Practice Statement Framework for Subordinate Certification Authorities Indonesia", *Proceedings of 3rd International Conference on Information Science and Security*, 2016, pp 32-36.

[5] A. M. Al-Khouri, "PKI in Government Identity Management Systems*", International Journal of Network Security & Its Applications*, Vol.3, No.3, 2011.

[6] S. Choudhury, K. Bhatnagar, W. Haque, "Public Key Infrastructure Implementation and Design", M&T Books, New York, 2002.

[7] S. Koga, K. Sakurai, "A merging method of certification authorities without using cross-certifications", *Proceedings of International Conference on Advanced Information Networking and Application*, 2004, pp. 174-177.

[8] Law of Republic of Indonesia No. 11 year 2008, "Electronic Information and Transaction", 21 Apr. 2008.

[9] S. Chokani, W. Ford, R.V. Sabett, C.R. Merrill, S.S. Wu, "RFC 3647 - Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework", the Internet Society, 2003.

[10] AICPA/CICA PKI Assurance Task Force, “Trust Service Principles and Criteria for Certification Authorities Version 2.0”, Canadian Institute of Chartered Accountants, 2011.

[11] Regulation of Minister of Communication and Information Technology, Republic of Indonesia No. 4 year 2016, “Information security management system”, 8 Apr. 2016.

[12] National Center for Digital Certification, Kingdom of Saudi Arabia, “NCDC Government-CA Certificate Policy Version 2.7”, 2015.

[13] Ministry of Interior Qatar, “Infrastructure CA Certification Practice Statement Version 1.2”, 2014.

[14] Ministry of Interior Qatar, “Citizen and Resident CA Certification Practice Statement Version 1.2”, 2014.

[15] Department of Science and Technology, Republic of Philippine, “Philippine National PKI Certificate Policy Version 1.0”, 2013.

[16] Regulation of Ministry of Manpower, Republic of Indonesia No. 55 year 2015, “National Competency Standard in Information Security”, 24 Feb. 2015.

[17] M. E. Aziz, S. Yazid, “Certificate Policy Analysis and Formulation of the Government Public Key Infrastructure using SSM”, *Proceedings of International Conference Advance Computer Science and Information Systems*, 2016.

APPENDIX A:

Table 2: Coverage Root CA's CP and CPS on WebTrust Disclosure Criteria, improved from [3].

No	Disclosure Criteria	Related Provisions in CP and CPS	Note
	General		
1	Identification of each CP and CPS for which the CA issues certificates	1.2	-
2	Community and applicability	1.3.1.1, 1.3.1.2, 1.3.2, 1.3.3, 1.3.4, 1.3.5.1	-
3	Contact details and administrative provisions	1.5.1, 1.5.2, 9.10.1, 9.10.2	-
4	Any applicable provisions regarding apportionment of liability	5.2.4, 9.8	-
5	Financial responsibility	9.2.1, 9.2.2, 9.2.3	-
6	Interpretation and enforcement	9.10.3, 9.11, 9.13, 9.14, 9.15, 9.16.3	-
7	Fees	9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5	-
8	Publication and repository requirements	2.1, 2.2, 2.3, 2.4	-
9	Compliance audit requirements	8.1, 8.2, 8.3, 8.4, 8.5, 8.6	-
10	Description of the conditions for applicability of certificates issued by the CA that reference a specific CP	1.4.1, 1.4.2	-
11	CA and/or RA obligations	1.3.1.1	r/v
12	RA obligations	-	n/p, r/v
13	Repository obligations	2.1, 2.2, 2.3	-
14	Subscriber obligations	1.3.1.2	r/v
15	Relying party obligations	1.3.4	-
16	Any applicable reliance or financial limits for certificate usage	-	n/p
	Key Life Cycle Management		
17	CA key pair generation	5.7.2, 5.7.3, 6.1.1, 6.1.5, 6.1.7, 6.3.2	r/v
18	CA private key protection	6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10, 6.2.11	r/v
19	Whether the CA provides subscriber key management services and a description of the services provided	4.3.1, 4.3.2, 4.4.1, 4.5.1, 4.6.1, 4.7.1, 6.1.1, 6.1.5, 6.1.7, 6.3.2, 6.4.1, 6.4.2, 7.1	r/v
20	CA public key distribution	6.1.2, 6.1.3, 6.1.4	r/v
21	Key changeover	5.6	-
22	Subscriber key pair generation	4.5.1, 6.1.1, 6.1.5, 6.1.7, 6.3.2, 6.4.1, 6.4.2, 7.1	r/v
23	Subscriber private key protection	6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.2.5, 6.2.6, 6.2.7, 6.2.8, 6.2.9, 6.2.10, 6.2.11, 6.4.2	r/v
	Certificate Life Cycle Management		
24	Whether certificate suspension is supported	4.9.13	r/v
25	Initial registration	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6, 3.2.1, 3.2.2, 3.2.3, 3.2.5, 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3, 4.3.1, 6.1.2, 6.1.3	-
26	Registration requirements where external RA are used	-	n/p, r/v
27	Certificate renewal	4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.3.2, 4.4.2, 9.1.1	-
28	Routine rekey	3.3.1	-
29	Rekey after revocation or expiration	3.3.2	-
30	Certificate issuance	4.3.1, 4.3.2, 4.6.4, 4.6.7, 4.7.4, 4.7.7, 6.3.2, 9.1.1	r/v
31	Certificate acceptance	4.4.1, 4.4.2, 4.4.3, 4.6.5	-

No	Disclosure Criteria	Related Provisions in CP and CPS	Note
32	Certificate distribution	4.3.1, 4.3.2, 4.4.1, 4.4.2, 4.4.3, 4.5.1, 4.5.2	-
33	Certificate revocation	4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.9.5, 4.9.6, 4.9.7, 4.9.8	r/v
34	Certificate suspension	-	n/p, r/v
35	Provision of certificate status information	1.3.4, 4.5.2, 4.9.6, 4.9.7, 4.9.8, 4.9.10, 4.10.1, 4.10.2, 5.5.1, 5.5.2, 5.7.2, 5.7.3, 9.12.2	-
36	Certificate profile	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.1.5, 3.1.6 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5, 7.1.6, 7.1.7, 7.1.8, 7.1.9	r/v
37	CRL profile	7.2.1, 7.2.2	-
38	Integrated circuit card (ICC) life-cycle management	-	n/p
	CA Environmental Controls		
39	CPS and CP administration	1.5.3, 1.5.4, 9.12.1, 9.10.1, 9.10.2, 9.12.1, 9.12.2	r/v
40	CA termination	5.8	-
41	Confidentiality	9.3, 9.4	r/v
42	Intellectual property rights	9.5	-
43	Physical security controls	5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8	-
44	Business continuity management controls	4.9.12, 5.7.4	r/v
45	Event logging	5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.5.1, 5.5.2, 5.5.3, 5.5.4	r/v

n/p	=	there is no related provision or not performed
r/v	=	revision to the previous mapping in [3]