OIC-CERT Journal of Cyber Security
Volume 2, Issue 1 (February 2020)
31 – 42

Digital Certificate's Level of Assurance Development with Information Value and Sensitivity Measurement

Nikson Badua Putra[1], and Arry A. Arman[2]
[1] Government CSIRT, Badan Siber dan Sandi Negara, Jakarta, Indonesia
[2] Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Bandung, Indonesia
[1]**nikson.badua@bssn.go.id,** [2]**arry.arman@yahoo.com**

ARTICLE INFO

Article History
Received 28 Jul 2019
Received in revised form 15 Aug 2019
Accepted 25 Sep 2019

Keywords:
the level of assurance, digital certificates, information sensitivity, synthesize, AHP

ABSTRACT

This paper presents the research to develop the digital certificate's level of assurance. The level of assurance (LoA) in this paper is a level of assurance which reflects the authenticity degree of digital certificate's ownership. This LoA has a three-level, which define in four LoA standards such as ISO 29115: 2013, NIST SP 800-63-3, STORK, and KANTARA. From the previous researches and initial interview with digital certificate provider from Indonesia Government, this research concludes that information sensitivity measurement should be assessed to select the appropriate LoA. The related works and standards so far were not given any solution to this problem. This paper tries to solve it by offering LoA and its determination guidance model. This solution is achieved by synthesizing the four LoA along with information value and sensitivity measurement, which indicators determined by prioritization with the analytical hierarchy process (AHP). The proposed model-simulated and discussed so the information sensitivity measurement might assist in getting the suitable LoA level of the sensitive information been protected by a digital certificate.

I. INTRODUCTION

A Certificate Authority provides digital certificate services with a Level of Assurance for each level; one may have three levels as described below [NIST SP 800-63-3]:

- Level 3: High assurance of the authenticity and ownership of the digital certificate
- Level 2: Medium assurance of the authenticity and ownership of the digital certificate
- Level 1: Low assurance of the authenticity and ownership of the digital certificate

This level of assurance reflects authenticity degree of digital certificate's ownership that includes [3]:

- assurance degree in identity's checking or the entity that the certificate is issued; and
- assurance degree that the person uses the certificate is indeed the person that has the correct certificate. If the level is higher, so the degree of confidence in the ownership of electronic certificates to the owner is higher.

Because this level of assurance describes the degree of trust or the degree of confidence in an electronic system uses electronic certificates as the identity of a legal entity accordingly by using electronic certificates. The provider of electronic certificates directly gives the guarantee of trust and confidence, so this study does not discuss the trust and confidence of the

ISSN 2636-9680
eISSN 2682-9266

digital certificate being assured or not assured.

The selection of this level of assurance should base on risk assessment of digital transactions or services in the authentication of the entity. By mapping the impact level to the level of assurance, the entity of the digital transactions or services may determine the level of assurance that they needed, can use the digital services or do the electronic transactions, and ensure their identity's safety. An example of the assessment of the level of impact can be seen in **TABLE 1** [1].

TABLE 1: Potential impact at each level of assurance [1]

Potential impact	Level of Assurance		
	1	2	3
Impact on standing, reputation, status	Low	Med	High
Money loss or agency accountability	Low	Med	High
Impact on organization capability or asset, and public concern	N/A	Low/Med	High
Illegal sensitive information disclosure	N/A	Low/Med	High
Personal physical damage	N/A	Low	Med High
Law and regulation violations	N/A	Low/Med	High

As concluded in NIST SP 800-30 Guide for Conducting Risk Assessments [2], for each risk that analyzed, the appropriate control is needed to be able to respond to the risk. Digital signatures are present as one of the cryptographic controls that can be applied against the security risk in information systems as described in ISO/IEC 27001:2013 Information Security Management Systems.

Previous research, as in [3], recommends that Guideline in determining the Level of Assurance should be there to build the certificate policy with its description in the Introduction section in the certificate policy. This recommendation is because of the LoA impacts, ie, 1) mechanism of registration verification; 2) the protection of crypto-key; and 3) certificate management and protection in Certificate Authority. Another research [4], investigated the previous efforts in defining the Level of Assurance. From their investigation, they found that the LoA may assist in getting the proper access control of the sensitive resources, for example is the information. From this research, the results find that the Level of Assurance which measures the information's sensitivity is required. Another study [5] has seen the differences of ISO/IEC, NIST, STORK, and KANTARA approaches with their historical order linked to each other, their summary of the four LoA then may be used later in the synthesis of these four LoA approaches.

However, the selection criteria of digital certificate's assurance level by considering the sensitivity of the information or data that transmitted secured by a digital certificate has not found. Therefore, this study will carry out the analysis and design of these required criteria. One research [6] found to apply the information's sensitivity measurement to help determine the Level of Assurance. This research provides the quantitative classification of information method by calculating the information value and information sensitivity.

This research carried out by analysis and synthesis on the four LoA standards, weighing the LoA criteria indicator with Analytic Hierarchy Process (AHP), and then simulate and discuss the results of the proposed LoA selection criteria.

II. LOA DEVELOPMENT

As described in the previous section that improved LoA is developed by analyzing and synthesizing the current four LoA standards with a gap analysis of the indicators and each level characteristics, later then the indicator's weighting is analyzed with AHP and combine it with information's sensitivity measurement to achieve the design of the improved LoA.

A. Analyze and synthesis of ISO 29115:2013, NIST SP 800-63-3, STORK, KANTARA, Information's Classification

The synthesis

In this subsection, the synthesis carried out on the four LoA and information classification indicators based on [6], comparing the linkage of impact characteristics and information classification's characteristics which describes in **TABLE 2-8**. A two-way arrow illustrates a powerful link between NIST, ISO, and KANTARA which can be used to construct the criteria of the indicator. While the straight-line sign on the indicator illustrates that the two do not have interrelations on the indicator.

TABLE 2: LOA Indicator Characteristics Synthesis

Indicator Characteristics	Level of Assurance			
	NIST	ISO, KANTARA	STORK	Info Class
1. Impact on standing, reputation, status	↔	↔	—	—
2. Money loss or agency accountability	↔	↔	—	—
3. Impact on organization capability or asset, and public concern	↔	↔	—	—
4. Illegal sensitive information disclosure	↔	↔	—	—
5. Personal physical damage	↔	↔	—	—
6. Law and regulation violations	↔	↔	—	—
7. Access to private data consideration	↔	—	—	—
8. Federated systems consideration	↔	—	—	—
9. Information's reliability	—	—	—	↔
10. Information's increment	—	—	—	↔
11. Information's timeliness	—	—	—	↔
12. Information's availability	—	—	—	↔
13. Information's users' ability	—	—	—	↔
14. Opportunity costs	—	—	—	↔
15. Degree of dependence	—	—	—	↔
16. Regeneration costs	—	—	—	↔
17. Regeneration time	—	—	—	↔

The table above illustrates the synthesis process for determining the LoA indicators. The 2-way arrow represents a deep connection, while the straight lines represent the lack of linkage. For example, the two arrows on the indicator "impact on standing, reputation, status" in the column of NIST, ISO, KANTARA illustrates that this indicator has a significant linkage on the NIST, ISO, and KANTARA. The straight line on the same indicator in the STORK, and the Info Class column describes the lack of linkages between STORK and Class Info on this indicator.

ISSN 2636-9680
eISSN 2682-9266

From the table, NIST has the most accurate indicator, besides that ISO has the same indicator as NIST. Information classification indicator doesn't match four LoA, so the result is the information classification indicator along with impact indicator from four LoA to develop the improved LoA based on this synthesis.

Next step is analyzing the characteristic of each LoA level as described below to determine the number of the LoA and the detailed characteristics.

TABLE 3: LEVEL 1 Characteristics Synthesis

Characteristics	ISO, KANTARA	NIST 800-63-3	STORK
Usage	◄———	———►	———
Assurance on the identity which is claimed or asserted	◄———	———►	———
Authentication method	———	◄———	———
Credential strength	———	◄———	———
Authentication protocol	———	◄———	———
Attack that prevented	———	———	———
Security of the credentials	———	◄———	———

From the synthesis above, for usage and assurance characteristics, ISO; KANTARA; and NIST have the strong bond to build the Level 1 LoA, while on four other characteristics only NIST that have the details. And for characteristic, which is the attack that desired to prevent, all of the standards do not have the details.

TABLE 4: LEVEL 2 Characteristics Synthesis

Characteristics	ISO, KANTARA	NIST 800-63-3	STORK
Usage for	◄———	———►	———
Assurance on the identity which is claimed or asserted	◄———	———►	———
Authentication method	◄———	———►	———
Credential strength	———	◄———	———►
Authentication protocol	◄———	———►	———
Attack that prevented	◄———	———►	———
Security of the credentials	◄———	———►	———

From the synthesis of level 2, the characteristic of usage and assurance from NIST, ISO, and KANTARA obtained, which have a strong bond with each other. The authentication method and authentication protocol characteristic obtained from all of the four standards. Credential strength characteristic from NIST and STORK, attack characteristics from ISO, KANTARA, and NIST, the security of the credentials characteristic from ISO, KANTARA, and NIST.

TABLE 5: LEVEL 3 Characteristics Synthesis

Characteristics	ISO, KANTARA	NIST 800-63-3	STORK
Usage for	◄———	———	———►
Assurance on the identity which is claimed or asserted	◄———	———	———►
Authentication method	◄———	———	———►
Credential strength	———	◄———	———►
Authentication protocol	◄———	———	———
Attack that prevented	———	———	◄———
Security of the credentials	———	◄———	———

All of the standards have a strong bond in usage, assurance, and authentication method characteristics, but only NIST that has high impact mitigation, while the others just substantial impact mitigation usage. Besides that, only NIST have difference details about assurance, which is a very high measurement, and authentication method which uses two separate authentication factor. In credential strength characteristic, NIST and STORK have a strong bond, but only NIST have a requirement which is hardware-based authenticator which resistant to verification forgery. And last for level 3 analysis, only NIST has a strong bond with the security of the credentials characteristics.

TABLE 6: LEVEL 4 Characteristics Synthesis

Characteristic	*ISO, KANTARA*	*STORK*	*NIST 800-63-3*
Usage for	◄———	———►	———
Assurance on the identity which is claimed or asserted	◄———	———►	———
Authentication method	◄———	———►	———
Credential strength	◄———	———►	———
Authentication protocol	◄———	———►	———
Attack that prevented	◄———	———►	———
Security of the credentials	◄———	———►	———

To get the characteristic of level 4, only the NIST standard which not has bonded with all of the characteristic, because NIST SP 800-63-3 doesn't have level 4.

Results of the synthesis

The result of the synthesis achieved by analysis in the previous subsection describes below. First, define the low, medium, and high levels of indicators.

ISSN 2636-9680
eISSN 2682-9266

TABLE 7: Synthesis Results of Indicator Characteristics

Indicator Characteristic	*Low*	*Medium*	*High*
Impact on standing, reputation, status	Impact on standing, reputation, status occur in short or limited term.	Impact on standing, reputation, status occur in short or long limited term.	Impact on standing, reputation, status occur in the long term severe and affect many parties.
Money loss or agency accountability	Financial loss or agency accountability, not significant/ not so serious.	Financial loss or agency accountability is significant/ serious.	Financial loss or agency accountability is severe at a catastrophic level.
Impact on organization capability or asset, and public concern	Declining organizational capabilities, increasing the time spent by the organization to perform tasks and functions at recognizable levels, low damage to organizational assets or the public interest.	Declining organizational capabilities, increasing the time spent by the organization to complete tasks and services, and damage to organizational assets or public interest at a significant level.	Declining organizational capabilities, increasing the time spent by the organization to perform tasks and functions, and damage to organizational assets or public interest at a very high level.
Illegal sensitive information disclosure	Disclosure of confidential personal/government/trade information on low-level secrecy impacts, in short, and limited scope and time.	Disclosure of sensitive personal/government/trade information on medium-level secrecy impacts.	Disclosure of sensitive personal/government/trade information on high-level secrecy impacts.
Personal physical damage	Injuries at a mild level, and do not require medical action.	Injuries at a mild level, and need medical action.	Severe injury or death, caused by a service access error.
Law and regulation violations	A violation caused by service access error with the possibility of not being subject to law enforcement.	A violation caused by service access error with the possibility of being subject to law enforcement such as KUHP, KUHAP, UU ITE.	A violation caused by service access error which is of particular interest in law enforcement such as corruption, terrorism, drugs.
Private data access	It doesn't need private information to do the transaction.	Information System Services makes personal data accessible.	
Information's reliability	The information does not describe the actual situation, and information may be obscured or misdirected, information may lose the minimum requirements, and may lose the content of the information.	The information describes some of the actual situations; information's correctness may be obscured or partially deviated; information may lose the minimum requirements/part of the main contents.	The information describes the actual situation; information's correctness should not be obscured or deviated; the information should not lose the minimum requirements/part of the main contents at all.
Information's increment	Information system service users do not obtain new information or benefits from information system services.	Information system users gain some new information or benefits from information systems services.	Users of information systems get a lot of new information or benefits from information systems services.
Information's timeliness	Information in information systems services doesn't have expired time.	Information in information systems services has relatively long expired time.	Information in information systems services has relatively short expired time.

Indicator Characteristic	*Low*	*Medium*	*High*
Information's availability	No difficulty is found/doesn't need to pay attention to the difficulty in creating, processing, storing, and entering information in information systems service.	Find some difficulty in creating, processing, storing, and entering information in information systems service.	Find many difficulties in creating, processing, storing, and entering information in information systems service.
Information's users' ability	Information system service users do not easily understand and use information obtained from information system service.	Information system service users can understand and use some of the information obtained from information system service.	Information system service users easily understand and use all of the information obtained from information system service.
Opportunity costs	There is no or very little interest in any particular party in using the information on the Information System Service.	There are several interests of certain parties in using the information on Information Systems Service.	There are many interests of certain parties in using the information on Information Systems Service.
Degree of dependence	Loss of access control of the information systems services does not or slightly affect/harm the owner of the information.	Loss of access control of the information systems services affects/harm the owner of the information on the middle level.	Loss of access control of the information systems services affects/harms the owner of the information on the high or entire level.
Regeneration costs	Only a small amount of cost is required to correct any missing, damaged, or leaked information in the Information System service.	Only a medium amount of cost to correct any missing, damaged or leaked information in the Information System service.	Needed many costs to correct any missing, damaged or leaked information in the Information System service.
Regeneration time	It doesn't need time to correct any missing, damaged or leaked information in the Information System service.	Needed a short time to correct any missing, damaged, or leaked information in the Information System service.	Needed a long time to correct any missing, damaged, or leaked information in the Information System service.

Next, the synthesis results of LoA level characteristics illustrate in **TABLE 8**.

TABLE 8: Level Characteristics Determination

Level Characteristic	*Level 1*	*Level 2*	*Level 3*
Usage	Minimum risk authentication errors, low impact identity abuse, information sensitivity has little/no value.	Medium-risk authentication errors, medium-impact identity abuse, information sensitivity has moderate value.	High-risk authentication errors, identity abuse, have a substantial impact; information sensitivity has a high value.
Assurance on the identity which is claimed or asserted	The claimant controls an authenticator registered to the subscriber	Verify identity which is claimed with identity in the real world, whether remote or physical presence.	High, verification of identities recognized by the government needs a physical presence.
Authentication method	*Single-factor authentication.*	Ownership proof and separate multi-factor authentication controls.	

ISSN 2636-9680
eISSN 2682-9266

Level Characteristic	*Level 1*	*Level 2*	*Level 3*
Credential strength	Secured only with non-cryptographic general authentication.	Crypto, authentication of key ownership secures the credential is secured.	Only hardware-based authenticator resistant to verifier forgery is allowed.
Authentication protocol	*Secure authentication protocol.*	*Secure authentication protocol.*	*Secure authentication protocol* cryptographic.
Attack that prevented	There are no specific requirements; minimal guarantee.	*Eavesdropping*, *online guessing attack.*	Protection focus on counterfeiting verifier forgery and MITM attacks.
Security of the credentials	No crypto method.	Encrypted using approved cryptography so that only RP (relying party) can decrypt it.	Cryptographically protected, the identity claim controller controls tied to the subscriber account.

B. Prioritization the LoA indicator with analytical hierarchy process

AHP is a measurement theory using pairwise comparisons which depends on expert judgment to obtain priority scales [7]. In this study, the AHP approach is carried out as a fair comparison on each LoA indicator which has synthesized, which aim that each indicator has weight, to develop the improved LoA. Furthermore, the analysis of flow chart determination of the assurance level uses this weight, which indicators are prioritized to be calculated compared to other indicators. This comparison is a person's subjective assessment of criteria based on several considerations. The AHP model uses individual perception, which is considered "expert" as the primary input. The "expert" criteria here refers to the individual who understands the problems correctly, feels the consequences of a problem or has an interest in the issue [8]. According to [6], the weights of utility and cost factors in information value measurement along with the comparison of pairs of sensitivity factors of the information can be obtained by asking expert opinions and then using the AHP method to calculate them. In this study, the assessment or weighting of AHP is carried out by the developer of the information systems which are secured by the digital certificate.

Some indicator variables to determine LoA are compared using pairwise comparisons matrices; that is, the comparison matrix contains the preference level of several alternatives for each criterion. The scale of preference used is a scale of 1 which shows the lowest importance level up to a range of 9 which shows the extreme importance. The comparison stage in AHP begins by comparing each alternative per criterion. The results of the AHP analysis for selecting the order of the flowchart improved LoA illustrates in **Fig. 1**.

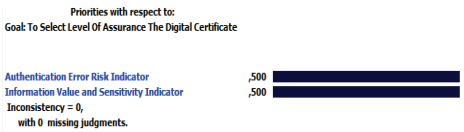

Fig. 1: AHP of Authentication and Information Sensitivity Indicator.

From **Fig. 1**, the authentication error indicator, with information value and sensitivity indicator, has equal relative importance, whose goal is to determine the LoA. The next step, selecting the priority order between six indicators in the authentication error risk indicator using AHP analysis as describes in **Fig. 2**.

ISSN 2636-9680
eISSN 2682-9266

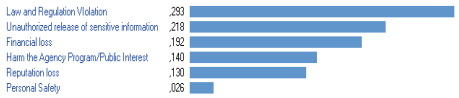

Fig. 2: AHP of Authentication Error Risk Sub Indicator

Concluded from **Fig. 2** that the relative importance between authentication error risk sub-indicator:

1. Law and regulation violation
2. Unauthorized release of sensitive information
3. Financial loss
4. Harm the agency program/public interest
5. Reputation loss
6. Personal safety

Finally, the final relative importance between all indicator orders from the top importance shows in Fig 3.

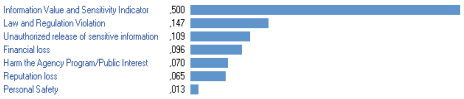

Fig. 3: AHP of All Indicator and Sub Indicator

C. Design of the improved LoA determination guidance

The design of the improved LoA determination guidance achieved by designing the flowchart matrix from the prioritization indicator resulted in the previous subsection. This flowchart, motivated by the measurement of information sensitivity needs to determine the desired LoA. The designed diagram illustrates in **Fig. 4**.

ISSN 2636-9680
eISSN 2682-9266

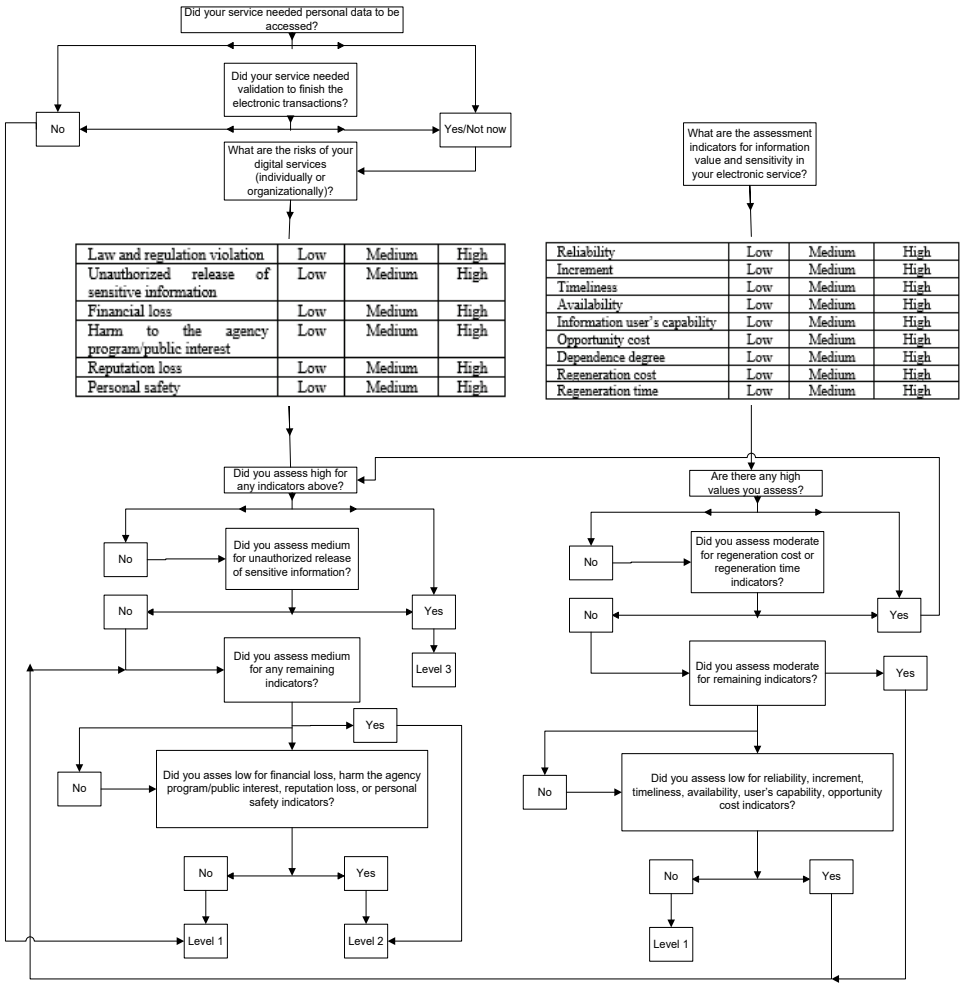

Fig. 4: Improved LoA Determination Flowchart

III. SIMULATION AND DISCUSSION

In this section, the same expert in AHP analysis simulating the improved LoA determination flowchart model. The simulation gives Level 3 LoA. The result of this simulation because the expert chooses the high rate for information indicators on the right side, and authentication error risk indicators on the left side, especially for dependence degree which reflects the high sensitivity of information, and high rate for financial loss indicator which indicates the agency accountability impact because the authentication risk error. The expert's digital service provides electronic processing of disbursement requests of the supported fund's cost for the infrastructure project from the executor bank. The digital signature implementation for these services is desired to assure the service's access control and the authenticity transmitted data. More advanced, this service very dependent on access account and its credential information, which to control the information and data being processed in the service, because these data and information have a high sensitivity which is private data of the debtors.

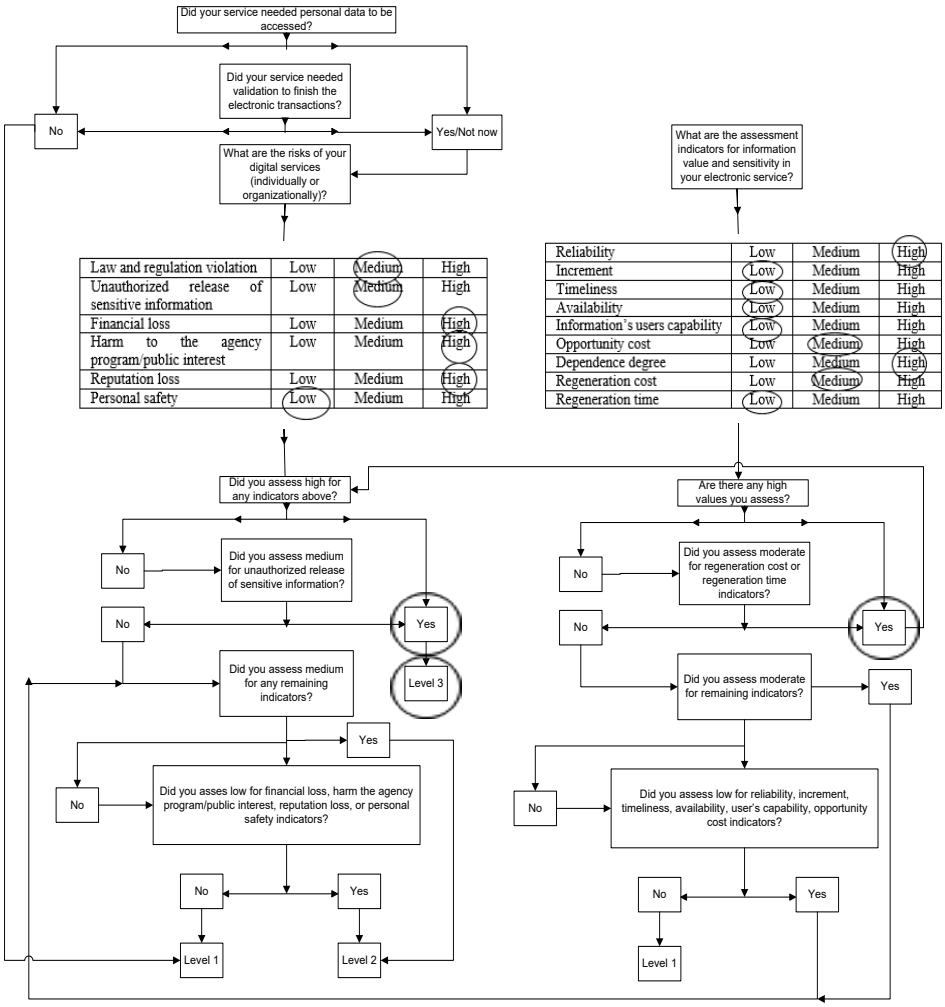

Fig. 5: Simulation Improved LoA Determination Flowchart

IV. CONCLUSION

This research proposes a model of Digital Certificate LoA and its determination guidance that improved by the synthesis of four current LoA standards and information value and sensitivity measurement. Concluded from the simulation and discussion with the expert of a digital service that being protected by a digital signature, this proposed model may assist in getting the suitable LoA level of the sensitive information being protected by a digital certificate which reflects in information value and sensitivity measurement assessed before the impact of authentication error risk.

V. REFERENCES

[1] M. E. Garcia and J. L. Fenton, "Digital identity guidelines."

[2] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," no. September, 2012.

[3] M. Endhy Aziz, "Certificate policy analysis and formulation of the

ISSN 2636-9680
eISSN 2682-9266

government public key infrastructure using SSM," Universitas Indonesia, 2016.

[4] A. Nenadic, N. Zhang, L. Yao, and T. Morrow, "Levels of authentication assurance : An investigation," pp. 155–158, 2007.

[5] T. Born and M. Peyrard, "Levels of Assurance," pp. 1–16.

[6] I. Sensitivity, "Supply chain information classification," 2007.

[7] T. L. Saaty, "Decision making with the analytic hierarchy process," vol. 1, no. 1, 2008.

[8] E. Helmud and S. Informasi, "Pemilihan paket internet android pada operator telepon gsm menggunakan metode analytical hierarchy process (AHP)," vol. 8, no. 1, pp. 918–927, 2016.