Application of a Generalized Fuzzy Model in PKI Architecture Determination

Radomir Prodanović*, Ivan Vulić **, Dušan Bogićević**
* Centre for Applied Mathematics and Electronics, Serbian Armed Forces, Belgrade, Serbia
** Military Academy, University of Defence, Belgrade, Serbia
radomir.prodanovic@vs.rs, ivan.vulic@mod.gov.rs, dusan.bogicevic@vs.rs

***Abstract*— It is difficult to decide what the best PKI architecture is to be applied due to unspecified determination parameters. The PKI architecture content and a comparative analysis of advantages and disadvantages are not sufficient for the appropriate determination of PKI as it is founded on subjective criteria. Subjectivity in interpretation of the PKI quality contributes to non-specificity of input data. The objective of the research is to obtain an efficient working framework for the application of the natural linguistic in determination of PKI architecture by using the fuzzy logic. In order to reduce the subjectivity in determining the appropriate PKI architecture, the authors propose the working framework based on selected parameters and fuzzy logic. For PKI architecture determination purposes, the authors use the value of a global limitation fulfillment for each architecture obtained by the Generalized Prioritized Fuzzy Constraint Satisfaction Problem.**

I. INTRODUCTION

Permanently increasing needs for security of electronic transactions makes PKI a key infrastructure for safeguarding integrity, authenticity and non-repudiation of transaction between entities. Organizations and users use an electronic certificate as a PKI product for the purpose of realization of safe transactions. There are several PKI architectures in literature, like hierarchical, mesh and bridge architecture. Differences between these architectures or their inter-relations contribute to end entities having an issue to determine the best architecture to suit their needs.

End user may make a determination on the appropriate PKI architecture based on the advantages and disadvantages of the PKI architecture. However, is it possible to make a right decision on an appropriate PKI architecture for business operations based only on the analysis of advantages and disadvantages? It has to be considered that organizations or users are not familiar with the characteristics of different PKI architectures, as well as what are the criteria for making determination on the best architecture.

Complexity and diversity of PKI architecture, their increased use in safeguarding the parties in electronic transactions, are the key to motivate the authors to research PKI architecture in order to create a framework for determination of an architecture that is acceptable for the organizations and users. The authors are of the opinion that it is necessary to set the appropriate criteria for determination of the most appropriate architecture, as well as the appropriate process for making the most effective decision.

The selection of the most appropriate PKI architecture is not a simple task. It requires one to be familiar with several different PKI architectures which is not a simple task for a decision maker. Knowledge on PKI architecture advantages and disadvantages is not sufficient to enable determination on the best choice of architecture. On the other hand, design of PKI architecture is an expensive investment that would facilitate the process of determination. Selected appropriate architecture must be of a good quality in order to escape rejection after some time upon realization that it was not the most appropriate choice.

The issue of selection of an appropriate PKI architecture originates from the lack of parameters, criteria and procedures for selection that may be utilized. The authors emphasize the issue as the key cause for failure of PKI projects or for their inefficiency in their lifetime.

Authors of other papers do not examine how to select the most appropriate architecture but, instead, briefly describe types of PKI architecture briefly reviewing their advantages and disadvantages. In the paper "A Survey of PKI Architecture", the authors conducted a comparative analysis of PKI architectures on the basis of their advantages and disadvantages, as well as a comparative analysis based on the selected parameters. The authors did not find the proposed solutions for the PKI architecture determination while searching databases available on the internet.

The proposed solution enables the selection of the most suitable PKI architecture. Rest of the paper includes: the second section describes the applied methodology; section three describes proposed solution for determining the most suitable PKI architecture based on generalized fuzzy model and section four provides a conclusion.

II. METHODOLOGY

A. Systematization of PKI

There are several PKI architectures, but all of them can be classified into one of the following architectures [1-4]:

- Simple CA Architecture (Single CA Architecture, Basic Trust List Architecture),
- Enterprise PKI Architecture (Hierarchical PKI Architecture, Mesh PKI Architecture),
- Hybrid PKI Architecture (Extended Trust List Architecture, Cross-certified PKI Architecture, Bridge Certification Authority Architecture).

A single CA (Certification Authority) has one certification authority that provides PKI services to all users.

Copyright 2020 by Information Society of Serbia - ISOS, Serbia | Creative Commons License: CC BY-NC-ND

A Basic trust list is the widespread PKI architecture because it is extended through operating systems and web applications. End users can modify this list by adding or deleting a CA. This model is not technically complex, however, users do not have the way or skill to properly maintain their trust because they do not know whether adding or deleting a CA from the list can cause a security risk.

Hierarchical PKI architecture is built on one-way trust relationships between the superior and the subordinate CA. At the top of the hierarchy is one CA (root CA) that all users trust [5]. Root CA issues certificates only to subordinate CAs while they issue certificates to both their subordinate CAs and users. The root CA public key is distributed to all users and thus initiates trust in the PKI.

Mash PKI architecture builds bidirectional peer-to-peer relationships between peer CAs by issuing certificates to each other. This architecture is a common alternative to the hierarchical model due to its advantages [6,7]. The mash architecture can be divided into: full mash architecture (each CA establishes a trust relationships with other CAs) and partial mash architecture (the CA does not establish a trust relationships with all other CAs).

Extended Trust List architecture uses a trust list to connect multiple identical or different PKI architectures. Trust lists have been criticized for not having a clear criterion for entering trust points in the list.

Cross-certified PKI architecture enables the connection of several different PKI architectures by establishing a cross-certified trust relationship. Entities of one PKI architecture can confirm the existence of entities whose certificate is from another PKI architecture. Different users construct different paths for the same end-entity certificate in this architecture.

Bridge CA architecture connects different PKI architectures regardless of the architecture, by introducing a new CA (bridge CA) that establishes peer-to-peer trust relationships with the CAs of other PKI architectures.

B. PKI architectures analysis

Single CA architecture is the simplest to implement from all described PKI architectures in this paper. This architecture does not have possibility of extension by establishing trust relationships to other CAs. Certification path processing is much faster as a result. This architecture, however, has single trust point which violating the whole architecture. It is closed architecture because trust relationships exist only between its entities. This architecture is suitable for small organizations.

The Basic Trust List architecture resolves problem of closed architecture. It introduces trust list on end entities side of different PKI architectures. The end entity manages the trust list. On the one hand, it is good because end entity determines other entities with which will establish secure communication. On the other hand, there is a problem of maintaining and managing the trust list. This architecture is suitable for establishing small number of the trust relationships between different PKIs.

The Hierarchical architecture is suitable for organization with hierarchical structure because it can follow their development. It has automated trust check mechanism. This mechanism is built in certification path processing process, so the end entity does not have to update trust list. The trust depends on root CA's private key which represents failure point. Compromising this point causes failure of the whole architecture. It is a big problem with this architecture. The hierarchical architecture has more scalability then single CA and trust list architectures because it can easily follow expansion of the organization. It is not flexible, however, because there is one failure point.

The mesh architecture is more flexible then hierarchical architecture because it has more failure points. Compromising any of trust point can not cause PKI architecture crash. Scalability of this architecture is diminished because numerous trust relationships between CAs complicate certification path processing. The discovering of the certification paths is more complex then in hierarchical architecture because there are more certification paths to an end entity. The consequences of bigger number of certification paths are bidirectional trust relationships. Constraints in this architecture are bidirectional, while these are unidirectional in hierarchical architecture.

The hybrid PKI architectures are the result of necessity of communication between organizations with different PKI architectures. Hybrid PKI architectures produce environment for secure information exchange between organizations.

The Extended Trust List architecture is similar to Basic Trust List architecture. This architecture, however, is more complex because it establishes trust relationship between different PKI architectures. End entity certificates can not reveal to which architectures certificate belongs. It creates more problems in defining initial point of certification path. This architecture can be easily expanded but it causes problems with trust list maintenance. This is the reason for bad scalability. The extended trust list architecture does not have single failure point which will cause crash of the whole architecture. Compromising CA in users trust list will prevent users from establishing relationship with users of that particular CA, but will leave communications with users of other CAs intact. The biggest problem is situation when trust list and mechanism for generation of a certificate cache fail. Users will not be able to communicate with users of other PKIs in this situation.

The Cross-certified Enterprise PKI architecture resolves the Extended Trust list architectures problems. This architecture establishes trust relationships between a numbers of different PKI architectures. Establishing trust relationships by cross-certified pair to several CAs produce more certification paths from user to end entity and make this architecture more flexible. Compromising CA with established trust relationships to other PKI architectures does not affect secure communication between users of other architectures. Increasing the number of relationships between CAs causes complicate discovering and processing of certification path which affects to limited scalability.

The Bridge CA architecture is developed to increase scalability and flexibility of Hybrid PKI architectures, reduce number of cross-certified and certification paths and enable simple extension of architecture. The Bridge CA architecture has shorter trust path then mash PKI with same number of CAs. The mechanism for discovering certification path is more complex then for hierarchical architecture, and certification path is approximately twice

as long. Every Principal CA (hierarchical root CA or mash architecture CA) in Bridge CA architecture establishes one trust relationship with Bridge CA. The mash cross-certified architecture establishes n^2 trust relationships between CAs, while this architecture establishes n trust relationships. The Bridge CA does not have function of superior CA over PKI architectures to which makes cross certificates.

C. Comparative analysis based on selected parameters

The authors selected some parameters and made comparison of PKI architectures in second aspect of comparative analysis. The authors selected next parameters:

- Trust. Authors consider this parameter through a trust point and a trust relationship establishing in architecture. The trust point is a point, or CA, from which the certificate user begins validating the certification path. A trust relationship is a link between the user's certificate and the CA to which the user trusts, assuming that the CA has issued the appropriate valid certificate [8].
- Certification path. The certification path is a chain of certificates achieved through trust relationships between certification authorities, in order to determine whether the certificate being checked is signed by its publisher.
- Scalability. Scalability is the ability of the PKI architecture to expand by adding new CAs or new PKIs, or reduce by excluding one or more CAs from the PKI architecture, or by excluding one or more PKI architectures.
- Flexibility. This parameter shows the ability of the PKI architecture to adapt to failure and expansion of the architecture.
- Failure. The failure point is the weakest point in the PKI architecture whose dysfunction is questioning the work of the part or the entire PKI architecture. The failure point in PKI architecture is CA with compromised private key. Failure recovery is a process of re-establishing trust in the PKI architecture [9].

A detailed analysis of the advantages and disadvantages of PKI architectures, as well as a comparative analysis based on selected parameters is given in the paper [10].

D. Determining values and constraints for linguistic variables

The selected parameters represent linguistic variables that can have any of the following values: small, medium, medium, large, extremely large. These are expressions of linguistic variables and are expressed by fuzzy sets over the universal set $U \subset R+$ which is also called the working domain. This approach aims to map the expressions of linguistic variables into numerical values in order to determine the membership degre. The max value of the membership function is taken when the expression intervals overlap.

The membership function determines the degree of the convenience of given limitations with the corresponding influence on the complexity of the architecture.

The linguistic variable "trust" is defined on the universal set U = [0, 22]. The x-axis will represent the numerical values of the expressions that represent the impact on the complexity of the architecture. Trust will be represented by triangular numbers that will represent values such as: small, slightly higher, medium, medium-large, large, and extra large.

TABLE I. TABLE FOR DETERMINING THE IMPACT OF COMPLEXITY FOR THE VARIABLE "TRUST"

Trust	Values	Limitation
Trust in CA without trust relations. (1)	small	1-5
Trust in CA from trust list. (2)	slightly higher	3- 7
Trust in one point of PKI architecture (root CA). (3)	medium	5-10
Trust in multiple CA PKIs with bidirectional and unitary relations of trust. (4)	large	8-15
Trust in multiple CA PKIs with bidirectional trust relations. (5)	large	13- 22
Trust CAs from the trust list of different PKIs. (6)	medium	8-13
Trust between different PKI architectures by establishing a peer to peer relationship of trust. (7)	large	15- 20
Trust between different PKIs through intermediaries (Bridge CA). (8)	medium-large	13-22

Additional parameters for trust consideration:

- more points of trust in the trust list affect the complexity of the architecture;
- bidirectional relations of trust complicate the PKI architecture;
- trust relations between peer to peer CA are more complex than relations in hierarchical PKI;

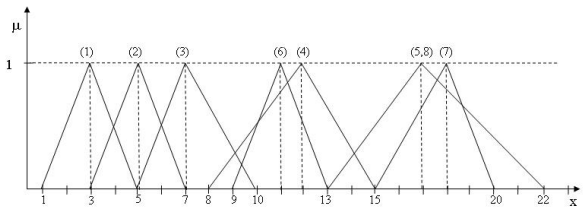

Figure 1. The value of the linguistic variable "Trust"

Linguistic variable "certification path" is defined on the universal set U = [1,30]. The x-axis will represent the numerical values of the expressions that represent the impact on the complexity of the architecture. Certification path is represented by triangular numbers (part and sigma) that will represent values such as: small, medium, medium-large, large and extra large.

Additional parameters for considering the certification path:

- increasing the number of certification authorities increases the complexity in the discovering and validation of the certification path;
- The introduction of restrictions in certificates affects the speed of the certification path validation;
- Peer to peer relationships between CAs are complicating the construction and validation of the certification path. The complexity is greater if bidirectional relations of trust are used.

TABLE II. TABLE FOR DETERMINING THE IMPACT OF COMPLEXITY FOR THE VARIABLE "CERTIFICATION PATH"

Certification path	Values	Limitation
The length of the certification path is one certificate, simple construction and validation. (1)	small	1-5
Certification path of more certificates of subordinate CA, simple construction, and validation depends on the length and limitations. (2)	medium	4-10
Certification path of more certificates of peer to peer CAs, complex construction, and validation depends on the type of relations, length and limitations of the certificate. (3)	medium-large	8-15
The PKI architecture trust over the trust list, the complexity of the construction and the validation depend on the PKI architectures are connected. (4)	large	14-20
The trust relationship between two CAs of different PKI architectures, the complexity of construction and validation depend on the PKI architectures and trust relationship between CAs through which the architectures are connected. (5)	very large	19 and more

- Connecting PKI architectures via trust lists - connecting multiple PKI complicates the certification path determination mechanism. The complexity also depends on the certification paths of the PKI architectures that are connected.
- The certification path is complicated when more PKI architectures are connected through its CA by establishing a trust relationship. Complexity of the entire certification path depends on the types of PKIs that are connected (more network, more hierarchical architectures, or combined).
- The certification path for PKI architectures that are connected through an intermediary depends on the achieved relationship of trust with the intermediary and the type of PKI architectures that are connected.

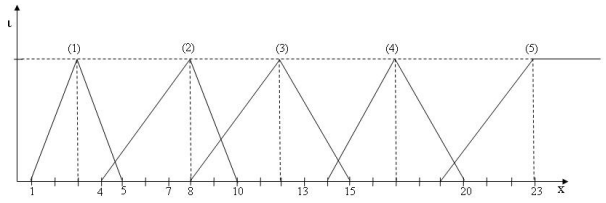

Figure 2. Value of the linguistic variable "certification path"

The linguistic variable "scalability" is defined on the universal set U = [1,11]. The x-axis represents the numerical values of expressions that represent the impact on the complexity of the architecture. Scalability is represented by triangular and sigma numbers that represent values such as: small, medium and large.

TABLE III. TABLE FOR DETERMINING THE IMPACT OF COMPLEXITY FOR VARIABLE "SCALABILITY"

Scalability	Values	Limitation
There is no possibility of expansion or it slightly affects the architecture.	small	1-9
Simple extension of architecture that has less impact on architecture.	medium	7-14
The addition of certification authorities significantly affect the architecture functioning.	large	12 and more

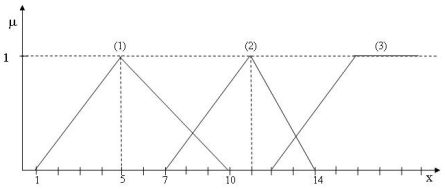

Figure 3. Value of the linguistic variable "scalability"

The linguistic variable "flexibility" is defined on the universal set U = [1,20]. The x-axis represents the numerical values of the expressions that represent the impact on the complexity of the architecture. The flexibility is represented by triangular, trapezoidal and sigma numbers that represent the values: small, medium and large.

TABLE IV. TABLE FOR DETERMINING THE IMPACT OF COMPLEXITY FOR VARIABLE "FLEXIBILITY"

Flexibility	Values	Limitation
The architecture is flexible and recovers quickly after failure.	small	1-10
The architecture is less flexible because it takes more time to recover.	medium	7-15
The architecture is less flexible because a lot of CAs and trust relations need to be established.	large	12 and more

Additional parameters for flexibility considering:

- The architecture is more flexible if a smaller number of users are left without service during failure or it is necessary to re-establish fewer certification authorities;
- Architecture is more flexible if it is necessary to establish a smaller number of trust relations.

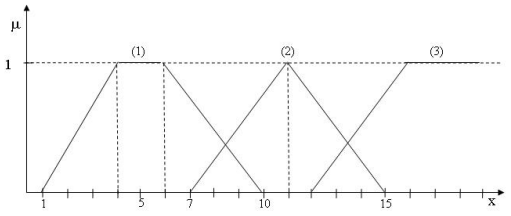

Figure 4. Value of the linguistic variable "flexibility"

The linguistic variable "failure" is defined on the universal set U = [1,20]. The x-axis represents the numerical values of the expressions that represent the impact on the complexity of the architecture. The failure will be represented by triangular and trapezoidal numbers that represent the values: small, medium and large.

TABLE V. TABLE FOR DETERMINING THE IMPACT OF COMPLEXITY FOR VARIABLE "FAILURE"

Failure	Values	Limitation
Partial loss of trust, users inability to communicate with part of the same architecture.	small	1-10
Users inability of other architectures to communicate with users of the failured CA architecture.	medium	6-15
Failure of the whole architecture.	large	13 and more

Additional parameters for failure considering:

- The severity of the trust partial loss depends on the number of users who lost the service and the number of CAs who lost trust;

- The failure is more severe if a large number of PKI architectures have lost trust or a larger number of users have lost a service that depends on the failed PKI.

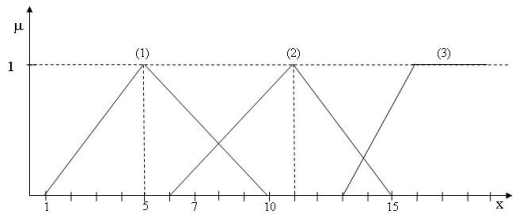

Figure 5. Value of the linguistic variable "failure"

III. APPLIED GENERALIZED PRIORITIZED FUZZY CONSTRAINT SATISFACTION PROBLEM

Authors analyzed PKI architectures and selected the characteristic parameters for all architectures in order to solve the problem of selecting the best PKI architecture. The following parameters were selected for decision-making purposes: trust, certification path, scalability, flexibility and failure. The selected parameters are linguistic variables for which the authors specify domains and a set of constraints.

The application of the model is carried out through three phases: the preparatory phase, the calculation phase and the decision-making phase.

In the preparatory phase are selected the parameters for choosing PKI architecture. At least three of the five parameters have to be selected. Parameters are linguistic variables that are converted into numerical values using impact tables. The domain of the variable is defined in the previous chapter. Constraints are fuzzy subsets of the corresponding domains and are shown in Tables 1-5.

Each constraint is then modeled as a characteristic membership function, as shown in Figures 1 to 5. The membership function of triangular fuzzy numbers is calculated by formula 1), trapezoidal by formula 2) and sigma fuzzy numbers by formula 3). Figure 7 shows previously mentioned fuzzy functions.

$$\mu(x)=\begin{cases} 1-(a-x)/b & a-b\le x<a \\ 1-(x-a)/c & a\le x\le a+c \\ 0 & otherwise \end{cases} \quad 1)$$

$$\mu(x)=\begin{cases} 1-(a-x)/c & a-c\le x<a \\ 1 & a\le x<b \\ 1-(x-b)/d & b\le x\le b+d \\ 0 & otherwise \end{cases} \quad 2)$$

$$\mu(x)=\begin{cases} 1-(a-x)/b & a-b\le x\le a \\ 1 & x>a \\ 0 & otherwise \end{cases} \quad 3)$$

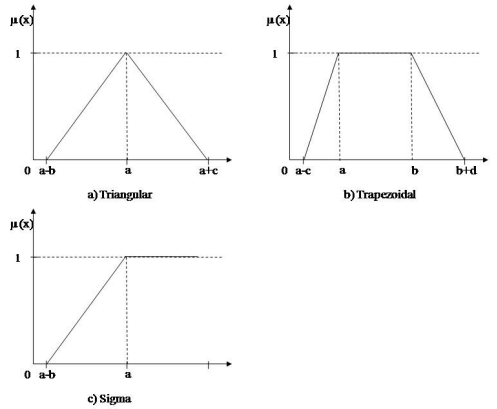

Figure 6. Triangular, trapezoidal and sigma fuzzy functions

The criteria for selecting a PKI are then determined (for example: trust, medium (7); certification path, medium large (10); scalability, small (7); flexibility, large (13); failure, small (6)) and priorities (for example: trust, 0.7; certification path, 0.8; scalability low, 0.4; flexibility, 0.7; failure, 0.8).

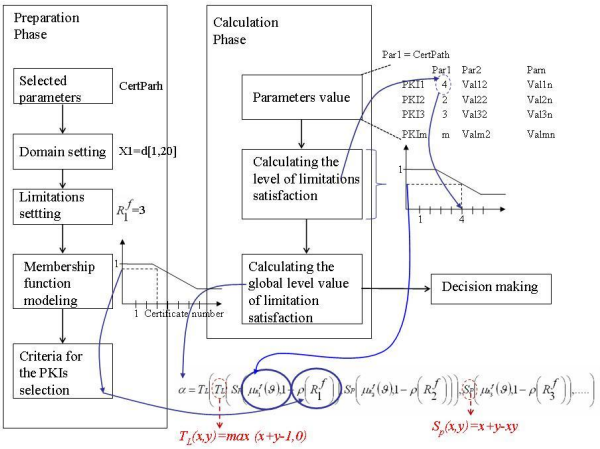

Figure 7. GPFCSP application process

The calculation phase is performed as follows:

- The degree of constraint satisfaction is calculated for each constraint for each PKI architecture. The degree of constraint satisfaction is calculated as a cross-section of the parameters given values and the listed belonging functions of parameter given constraints (as an example for PKI1, Par1, the degree of satisfaction is 0.7), Figure 7;

- Calculating the value of the constraint global satisfaction for each PKI architecture is performed by application of Generalized Prioritized Fuzzy Constraint Satisfaction Problem (GPFCSP) [11].

Formula for calculation of global level of limitation satisfaction for three is given by the formula (4)

$$\alpha = T_L\left(\begin{array}{l} T_L\left(S_P\left(\mu_{R_1^f}(\vartheta), 1-\rho\left(R_1^f\right)\right), S_P\left(\mu_{R_2^f}(\vartheta), 1-\rho\left(R_2^f\right)\right)\right), \\ S_P\left(\mu_{R_3^f}(\vartheta), 1-\rho\left(R_3^f\right)\right) \end{array}\right) \quad (4)$$

Whereas SP(x,y) t-conorm, TL(x,y) t-norm and the following equations are applicable:

$$S_p(x, y) = x+y-xy \quad (5)$$

$$T_L(x, y) = max\ (x+y-1, 0) \quad (6)$$

Based on the obtained results for each considered PKI, a decision is made on the selection of the most suitable architecture. If alpha has a value closer to number 1, it means that the architecture is more complex.

IV. CONCLUSION

A systematic approach in considering PKI architectures and the application of a generalized fuzzy model reduce subjectivity in making a decision on the choice of PKI architecture. It is important to choose the most suitable PKI architecture to reduce costs, and make the best use of the chosen PKI architecture.

The proposed solution can also be used to assess the choice of PKI architecture to be built, as well as to select ready-made solutions.

REFERENCES

[1] J. Linn, "Trust Models and Management in Public-Key Infrastructures". RSA Laboratories, (2000) [Online]. Available: http://www.rsasecurity.com/rsalabs/.

[2] T. W. Polk, N. E. Hastings, "Bridge Certification Authorities: Connecting B2B Public Key Infrastructures". National Institute of Standards and Technology, 2000

[3] R. Perlman, "An Overview of PKI Trust Models". IEEE Network, Vol. 13, 38-43.,1999.

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

[5] T. Moses, "PKI trust models. Draft", 2003. [Online]. Available: http://www.it-c.dk /courses/ DSK/F2003/ PKI_Trust_models.pdf

[6] W. E. Burr, *Public Key Infrastructure (PKI) technical Specification: Part A –Technical Concept of Operations*. National Institute of Standards and Technology Working Draft, 1998

[7] C. Adams, S. Lloyd, "Understanding PKI: Concepts, Standards, and Deployment Considerations". Second Edition Addison Wesley, 2002.

[8] R. Shirey, *Internet Security Glossary*, Version 2, RFC 4949, IETF, 2007.

[9] R. Prodanović, I. Vulić, "Failure Points in the PKI Architecture", Vojnotehnički glasnik/Military Technical Courier, Vol 65, Issue 3, pp. 771-784, 2017.

[10] R. Prodanovic, I. Vulic, and I. Tot, "A Survey of PKI Architecture". Selected Papers / Fifth International Scientific Conference ERAZ 2019, Knowledge Based Sustainable Development, Budapest, Hungary, 2019. doi: 10.31410/ERAZ.S.P.2019.169.

[11] A.Takači, "Towards Priority Based Logics", Proceedings of the 11th International Conference on Information Processing and Management of Uncertainty in Knowledge-Based Systems (IPMU 2006), Paris, France, 2006, pp. 651-657.