A SURVEY OF PKI ARCHITECTURE

Radomir Prodanović[1]
Ivan Vulić[2]
Ivan Tot[3]

DOI: https://doi.org/10.31410/ERAZ.S.P.2019.169

Abstract: *PKI architecture is base of e-business security in an insecure Internet environment for a geographically distributed organization. Choosing an adequate PKI architecture is a real challenge. Each PKI architecture has its advantages and disadvantages which should be taken into consideration before choosing the one. Therefore, authors in this paper give description and comparative analysis of the basic PKI architectures. This analysis has two aspects: first, comparison of advantages and disadvantages, and second, aspect of parameters chosen by the authors. Chosen parameters are: trust, certification path, scalability, flexibility and failure.*

Keywords: *PKI architecture, certification authority, trust, scalability, certification path.*

1. INTRODUCTION

Rapid development of Internet and information technologies has encouraged many companies to switch to a new form of business: e-business. Many companies today develop systems of e-business in order to strengthen its competitive position and adapt to the new models of business.

Companies intend to make profit from the investments in information technologies, e.g. more efficient business and management, by transition to e-business. However, e-business has its risks and information security is a major one in e-business. This risk is one of the main causes why some companies hesitate to fully adopt e-business.

Since companies make transactions via Internet on the global level, their information resources are distributed to the many locations. When we talk about reducing or removing security risks, we have to consider distributed security architecture. Technology which is used in distributed security architecture is public key cryptography. This cryptography is applicable through Public Key Infrastructure (PKI) [1].

The members in communication may get certificates from different certification authorities (CAs), depending on the organization to which they give its trust. In order for these members to trust each other, establishment of mutual trust requires establishing trust relationship between different CAs. In this way the PKI architecture is building up. PKI architecture depends on number of certification authorities, their locations and trust relationship between CAs.

Selecting the best PKI architecture is not a simple task. One of the reasons is non-existence of hard obligatory rules for choosing PKI architecture, and there isn't PKI architecture which provides the solution for all situations. However, the designers need to know all capabilities of the

[1] Centre for Applied Mathematics and Electronics, Serbian Armed Forces, Vojvode Stepe 445, 11000 Belgrade, Serbia
[2] Military Technical Academy, University of Defense, Pavla Jurišića Šturma 1, Belgrade, Serbia
[3] Military Technical Academy, University of Defense, Pavla Jurišića Šturma 1, Belgrade, Serbia

PKI architectures in order to make the best possible PKI architecture. Some authors are trying to define rules for selection PKI architecture or appropriate commercial Certification Service Providers [2], [3] to make selection of PKI architecture as easier as possible. Also, very important part of selection a PKI architecture is identifying historical development and problems of the real PKI architectures (for example EuroPKI) [4]. Authors consider that an organization at first need to be inform of advantages and disadvantages of the basic PKI architectures before starts deeper analyze which includes certification practices, services and applications. Authors in this paper give an overview of the basic PKI architectures and two comparative analysis for the purpose of identifying advantages and disadvantages of these PKI architectures.

In Section 2, the authors show review and description of fundamental PKI architectures. Section 3 shows comparative analysis of the PKI architectures. The first analysis shows advantages and disadvantages of the PKI architectures. The second is based on parameters chosen by authors. The authors chose such parameters which enable easy selection of the most appropriate PKI architecture. The conclusion is given in Section 4.

2. FUNDAMENTAL PKI ARCHITECTURES

There are more PKI architectures, but all of them can be classified in one of the next fundamental architectures [5]-[8]:

- Simple PKI architecture,
- Enterprise PKI architecture,
- Hybrid PKI architecture.

2.1. Simple PKI Architecture

Single CA Architecture. The single CA is most common in practice. It provides services to all entities in PKI environment (issuing certificates, publishing them in public directory, issuing certificate revocation lists (CRL), etc.). All entities trust only to one CA in this PKI architecture.

Single CA architecture is suitable for small organizations with limited number of users but not for organizations with fast development because it does not allow adding new CAs.

Basic Trust List Architecture. CAs do not establish a relationship between them in this model, so there are no certification paths. The entities establish relationship to CAs from trust list which is in possession of the entities.

There are various interpretations of trust lists because there is no single way for defining or formalizing these lists. It can be interpreted as a certificate list (for example, a certificate storage used by a web browser) or as a signed list that can contain any confidential information (certificate hash or file names) in the case of a Microsoft Certificate (Certificate Trust List, CTL) [9]. In [10], a trust list is defined as a signed set of certificates with information defining the characteristics and constraints of trust. User trust list is the most used PKI architecture since it has been extended through operating systems and web applications. Trust list with vital information in this architecture is maintained by every user himself and that can cause additional problems.

This architecture, in essence, consists of several independent CAs, i.e. from several single CA architectures, so compromising one CA does not affect all architectures.

2.2. Enterprise PKI Architecture

Several single CAs establish trust relationship with each other and build growing PKI architectures. CAs can make such relations where some CAs are superior or subordinate to others or equal (peer to peer) CAs. Every organizational structure in theory can be realized over hierarchical PKI and mesh PKI.

Hierarchical PKI Architecture. This architecture is mostly implemented in hierarchical organization because it follows hierarchical development of organization. This PKI architecture is built on one-way trust relationships between superior and subordinate CA, as on Figure 1. There is one CA (root CA) at the top of the hierarchy that all users trust [11]. The CA distributes public key to every entity and initiates trust to PKI. But this trust is having a bad side as it is now root CA is weakest point of this architecture. Overall architecture becomes useless and unsecure if it gets compromised.

The superior CA (root CA) issues certificates only to subordinate CAs, but the subordinate CA issues certificates to its subordinate CAs and to end entities. In that way CA can delegate added functions or limit some functions to subordinate CA. The certification path is short, and the longest one is equal to sum of subordinate CAs's certificates plus end entity's certificate.

This architecture is scalable enough, because it can simply follow the changes in growing organization [12]. This architecture during the expansion establishes trust relationships between root CA and new CAs or between subordinate CAs and new CA.

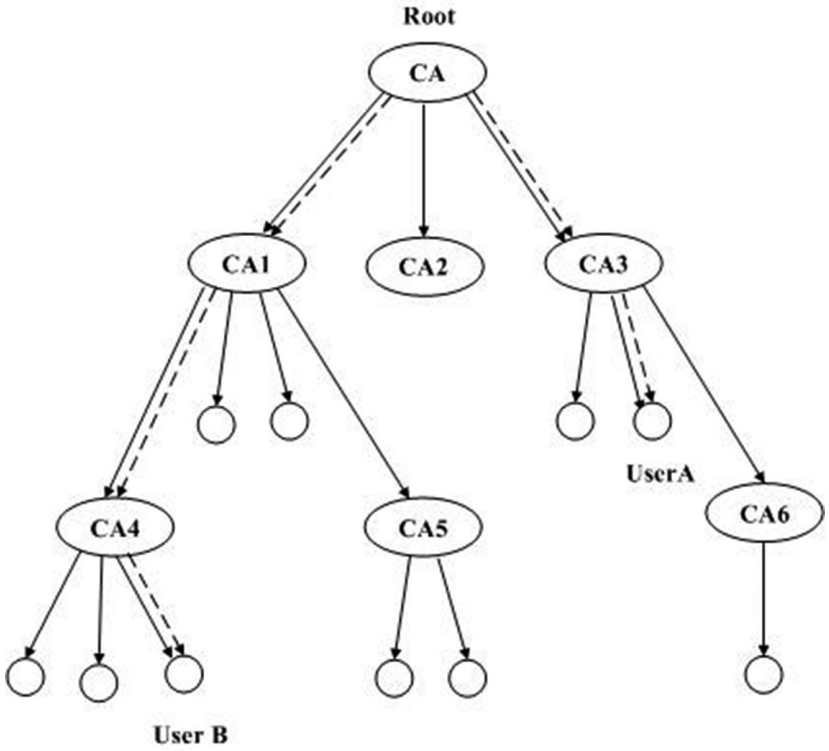

Figure 1: Hierarchical PKI architecture

Mesh PKI Architecture. The CAs provide PKI services and establish peer-to-peer relationships in the mesh PKI architecture. This architecture is, usually, alternative to hierarchical model because of its advantages [12], [13].

The network PKI architecture builds bidirectional trust relationships between equal CAs on peer-to-peer basis, by issuing CA certificates to each other, as on Figure 2. The CA may restrict trust by issuing certificates with restrictions contained in the certificate, such as: name constraints, policy constraints and path-length constraints [14].

There are many trust points, so compromising any of them does not affect architecture functioning. The compromised CA recovers trust by revoking all issued certificates and issuing new certificates.

The certification path construction is more complex than in hierarchical PKI architecture. There is not established path from certificate end entities to the trust point. The certification path construction is difficult because there are many path options and some of the certification paths lead to useless dead ends. The maximum length of a certification path in a mesh PKI is equal to the number of CAs in the PKI.

Mesh PKI architecture can be extended by simple addition of new CAs and establishing trust relationships with them. Scalability of this architecture is not generally good despite simplicity of growth. The causes of bad scalability are complexity of certificates, discovering and verification of a certification path.

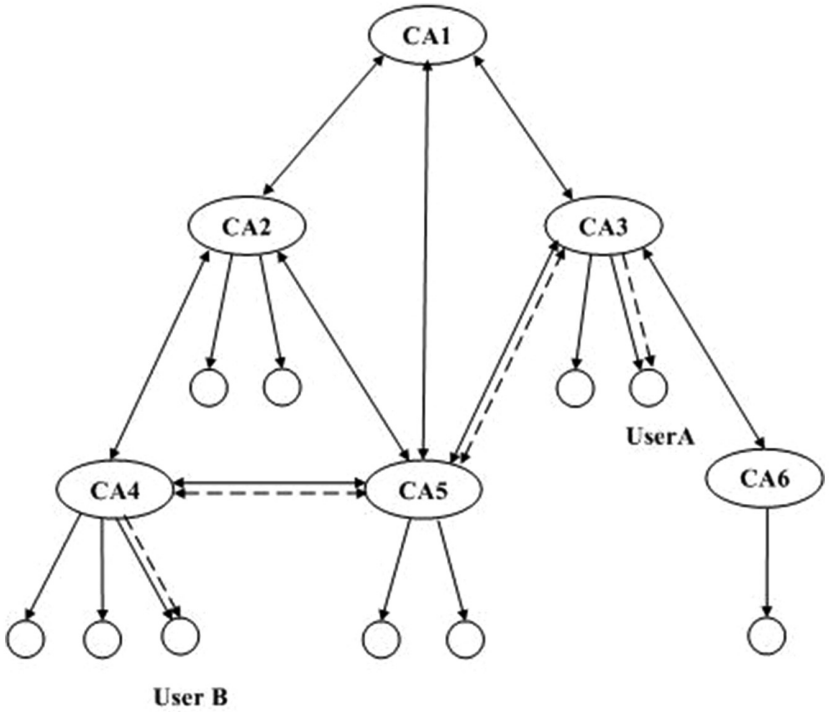

Figure 2: Mesh PKI architecture

2.3. Hybrid PKI Architecture

Many organizations use electronic communication with other organizations in order to extend their business. The organization which has hierarchical PKI architecture can have problems in communication with mash PKI architecture other organization. In this situation PKI needs to implement solution which will enable safe communication between users in different PKI architectures. The solution is a hybrid PKI architecture which allows organizations with different PKI architectures to establish safe environment for secure exchange of information.

There are three type of hybrid architecture:

- Extended Trust List Architecture,
- Cross-certified PKI Architecture,
- Bridge Certification Authority Architecture.

Extended Trust List Architecture. End entities, not CAs, in this architecture establish trust relationships through maintenance of the trust list. It contains many trust points to which end entities trust, as it shows in Figure 3.

This architecture can establish trust to hierarchical and mesh PKI architecture. The entries in this trust list contain root CA from hierarchical and some CAs from mesh architecture. The complexity of the certification path construction depends on the architectures connecting to each other.

The Extended Trust List generates a certificate cache in order to eliminate such problems. This cache contains all the possible certification paths. Path mechanism can refer to the cache and search for the appropriate path instead of constructing a certification path. Every certification path has path value based on the complexity of the certification path.

This architecture can be easily extended by adding more CAs from different PKI architectures to user trust lists. Trust list maintenance and problems are the same as in Trust List architecture.

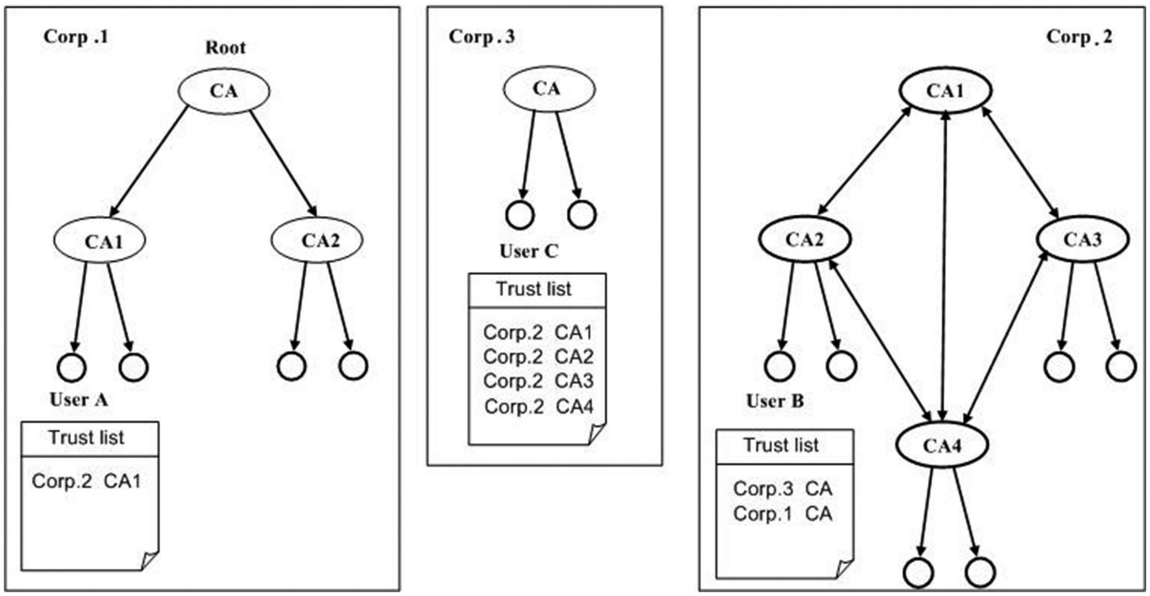

Figure 3: Extended Trust List architecture

Extended Trust List architecture does not have a trust point which crashes the whole architecture. We consider these failure points from the aspect of entities functionality which establishes trust with other PKI architectures. The first failure point is trust list. The entity will not trust any CA or architecture when trust list fail. The second failure point is failed certificate cache mechanism and certification paths searching.

When CA is a failure point, it will recover itself by suspending issued certificates, generating new public key and issuing new certificates. The solution when the trust list fails is a creation of a new trust list and recovering of the cache and search mechanisms.

Cross-Certified Enterprise PKI. The peer to peer trust relationships in this architecture are established between same or different organization architecture [15]. Trust relationship established with cross-certification can be restricted by defining restrictions in one or more cross-certificate pair extensions.

This architecture enables adding one or more new PKI architectures by simple establishment of cross-certification pair. The root CA or any subordinate CAs in hierarchical architecture can establish peer-to-peer trust relationship to any CAs from mash architecture, to CA from single CA architecture or to other hierarchical architecture. Likewise, mash architecture and single CA architecture can establish trust relationship to one or more same or different architectures. The Figure 4 shows peer to peer trust relationship and certification path by double lines between Enterprise PKI architectures.

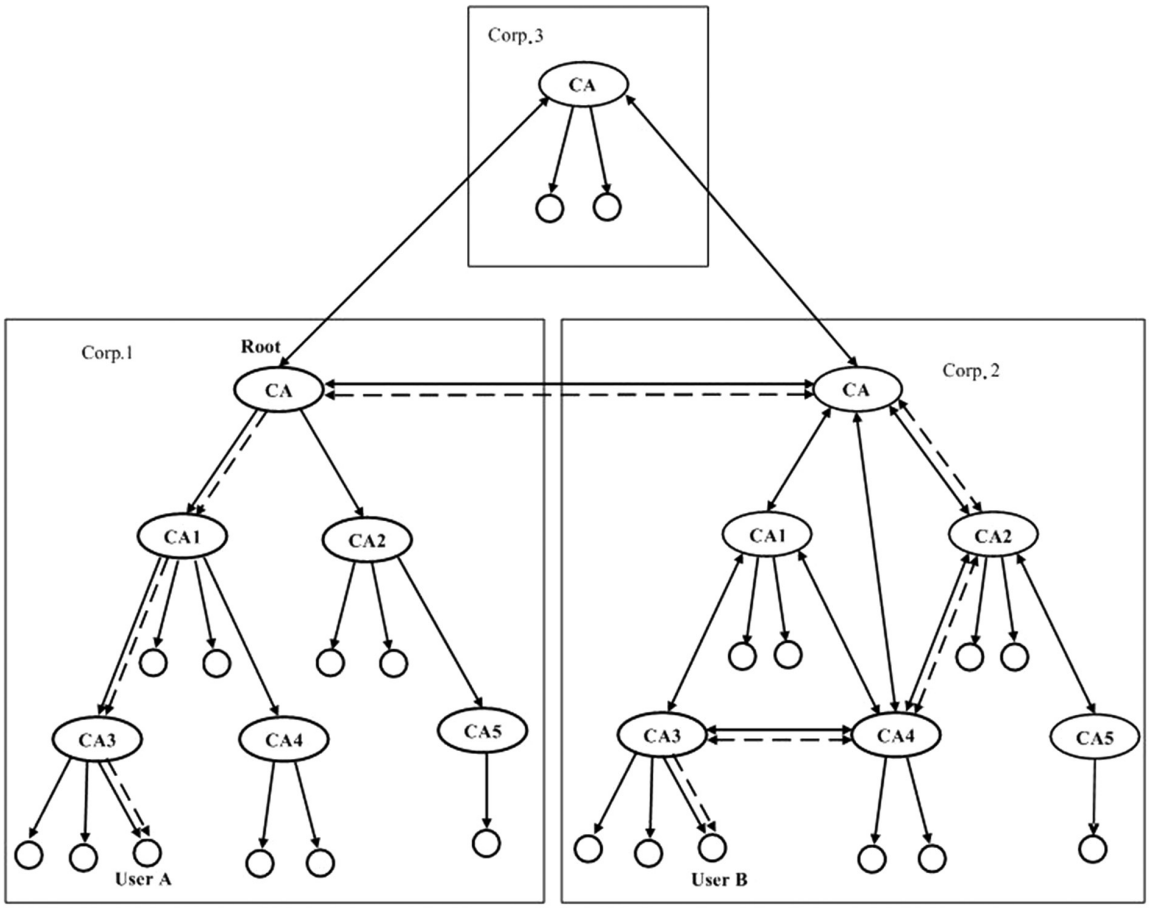

Figure 4: Cross-Certified Enterprise PKI architecture

When CAs from different architectures establish trust relationships with cross-certificates, then their entities can confirm existence of other entities. It enables secure communication between all users in PKI architecture. Different users construct different certification paths for the same end entity certificate in Cross-certified PKI architecture. The certification path begins at the trust point. Construction method depends of native architectures between which trust relations are established.

Failure of root CA, subordinate CA or CA in mesh PKI architecture will cause whole or partial architecture failure when we consider Cross-certified architecture. The compromised CA will recover in the way that was described earlier in this paper in the Section on Enterprise PKI Architecture. New CA can establish trust relationship to CA from other PKI Architectures.

This type of architecture is not applicable for connecting more enterprise architectures, so we can say that its scalability is restricted.

2.4. Bridge Certification Authority Architecture

The Bridge Certification Authority Architecture (Bridge CA architecture) is introduced by U.S. Federal Government in order to simplify connection of the PKI architectures by cross-certified pairs [12], [15]. This architecture connects different PKI architectures by introducing new CA (bridge CA) which establishes relations between PKIs.

The Bridge CA is not trust point and does not issue digital certificates to users. The users of Bridge CA consider it as mediator between different PKI architectures. The enterprise architecture establishes trust relationship to bridge CA (Principal CA) via root CA or some CA from mesh architecture. The new CA or Enterprise PKI architectures can be easily added by establishing peer-to-peer trust relationships. Every expansion is transparent for users because trust point is not changing. Figure 5 shows Bridge CA which establishing trust relations to three PKIs, Comp.1., Comp.2. and Comp.3.

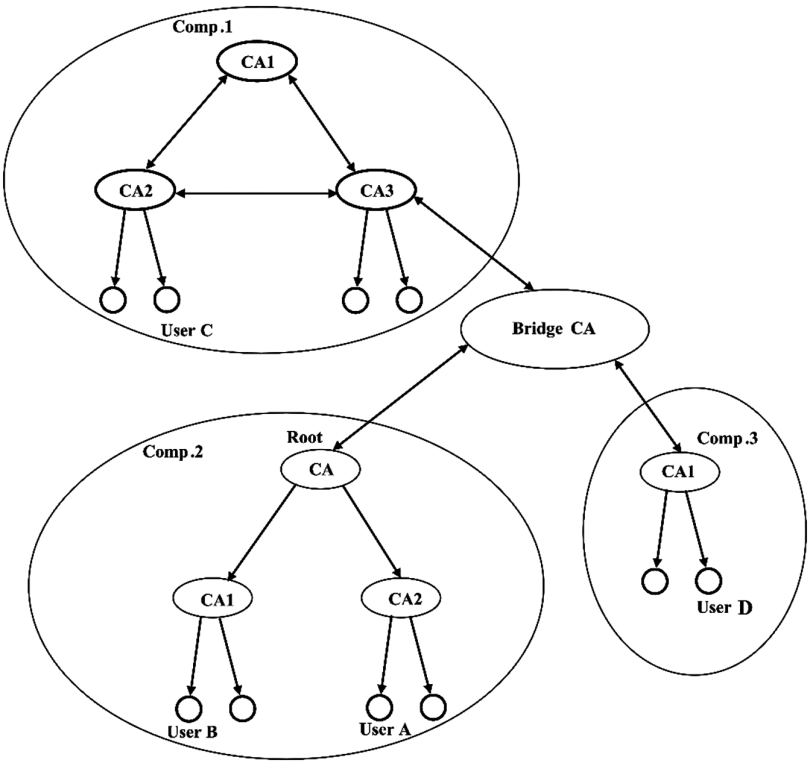

Figure 5: The Bridge PKI architecture

The bridge CA can be compromised entirely or partially. The former refers to compromising of all private keys for which bridge CA is signed certificates issued for Principal CAs. Compromising Principal CA in this architecture will disable Enterprise PKI architecture to establish secure communication to other PKI architectures. If Principal CA uses only one private key for signing certificates, compromising that key causes complete bridge CA architecture failure. Also, the hardware and software failure can cause complete PKI architecture failure. The re-establishing trust relationships with each Principal CA Enterprise PKI of architecture establishes trust between different or same architectures.

The users know path to the bridge CA, and they only need to determine the path from the bridge CA to the entity certificate. Depending of certification chain length, however, processing can be complicated because of requirements in the certificates, i.e. policy and name constraints, certificate status, policy mappings.

This architecture expands by adding new Enterprise PKI architectures. The Bridge CA architectures have to establish mutual relationships, but this is followed by many technical and operative problems, as described in [16].

3. THE COMPARATIVE ANALYSIS OF PKI ARCHITECTURES

There are technical and policy problems in building PKI in practice. The organization have to choose architecture which best fulfils its requirements. Combination of different architectures can develop the optimal PKI architecture.

In this section, the authors make comparative analysis through advantages and disadvantages aspect of PKI architectures and aspect of selected parameters. Through the first aspect of comparative analysis, Table 1, the authors show advantages and disadvantages of PKI architectures. 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 [17].
- 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 [18].

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.

Table 1: The comparative analysis of advantages and disadvantages of PKI architectures

Architecture	Advantages	Disadvantages
Simple CA Architecture		
Single CA Architecture	Simple architecture, Ease implementation, Simple certification path processing, Suitable for small organizations with a limited number of users.	Non scalable, Crush of the whole architecture when CA is compromised, Does not establish trust Relationship to other CAs.
Trust List Architecture	Enables secure communication between different single CA architectures, Enables architecture extending, Simple establishing trust.	Does not exchange certificate between CAs, Growth of architecture can cause its complexity, There are problems with trust list management
Enterprise PKI Architecture		
Hierarchical Architecture	Adjustable within hierarchical organization structure, Simple discovering and processing of certification path The certification paths are short.	There cannot be one CA on the World, The organizations do not have to have hierarchical structure, Compromising of the root CA causes compromising of the whole architecture.
Mash Architecture	Flexible architecture, The users trust CA that issued certificate, no matter where the CA is in PKI architecture, Direct making a cross certificate pair. It accelerates certificate path construction, The recovery procedure is simple because of small number of users.	The certification path construction is complex, There are useless dead ends or endless loops of certificates, Bad scalability because increased number of CAs causes performance degradation, The certification policy causes more complex certificates and certification path processing.
Hybrid PKI Architecture		
Extended Trust Architecture	Simple establishing trust between organizations with different PKI architectures, Simple architecture extension, Users have full control of trust list.	Certificate end entity does not define to which architectures that certificate belongs, There are problems in discovering certification path initial point, Architecture can become more complex in time, There are problems in trust list management.
Cross-Certified Enterprise Architecture	It can consist of same or different Enterprise PKI architectures, Simple adding new PKI architectures, Secure communication between entities from different architectures, Trust relationship between PKI architectures can be required	Limited scalability, Complex certification path, depend on native PKI architecture.
Bridge CA Architecture	Removing disadvantages of hierarchical and mash architecture, Simple architecture extension. It is transparent to users, Reliable after compromising of keys, Simple certification path processing, It is very scalable architecture because adding new certificate does not complicate certification path.	Bridge CA compromise causes crash of the whole architecture, Discovering certification path is more difficult than in hierarchical architecture, Certification path length is approximately double then in hierarchical architecture, More problems in connecting bridge CA architectures.

Table 2a: The comparative analysis of PKI architectures based on selected parameters

		Architecture			
Parameter		Single CA	Basic Trust List	Hierarchical PKI	Mash
Trust	Trust Anchor	Single CA	Single CA	Root CA	Any CA in architecture
	Trust relationship	-	Trust list	Unidirectional	Bidirectional
Certification path	Certification path	One certificate	One certificate	Sum of subordinate CAs certificates plus end entity certificates	Sum of all CAs certificates on selected path plus end entity certificates
	Certification path Construction	-	Simple	Simple	Complex
Scalability		Bad	Bad	Good	Bad
Flexibility		Bad	Bad	Bad	Good
Failure	Failure point	Single CA	No failure point	Root CA	No failure point
	Recovery after compromise	Simple	Simple	Medium complex	Simple

Table 2b: Continued Table 2a.

		Architecture		
Parameter		General Extended Trust	Cross-Certified Enterprise	Bridge CA
Trust	Trust Anchor	Any CAs	Trust point of PKI architectures	Trust point of PKI architectures
	Trust relationship	Trust list	Unidirectional and bidirectional	Unidirectional and bidirectional
Certification path	Certification path	One certificate	Sum of the longest certification path certificates of PKI architectures to which end entities belong	Sum of the longest certification path certificates of PKI architectures to which end entities belong plus bridge CA certificate
	Construct Certification path	-	Complex	Medium complex
Scalability		Bad	Bad	Good
Flexibility		Good	The best	The best
Failure	Failure Point	Any CA in architecture and trust list	Characteristic point of architecture failures that establishing trust relationship	Bridge CA and characteristic point of architecture failures that establish trust relationship
	Recovery after compromise	Depending on complexity	Simple/complex	Simple

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 cannot 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 than 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 cannot 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 number 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 than 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.

4. CONCLUSION

Selecting suitable PKI architecture is not simple task. Implementation of PKI into a corporation is a solution that requires adjusting the organization's business, educating employees, and financial investing. It is necessary to consider the needs of the business, as well as the advantages and disadvantages of PKI architecture in order to choose the best PKI architecture. It depends on more factors, like scalability, flexibility, trust point, trust relationships, compromise CA recovering, certification path processing. Also, there is a need for identifying advantages and disadvantages of every architecture which can be applied as a solution.

The selected parameters describe the architecture more closely and give an insight into its functionality. If PKI-based services speed is essential for an organization it is important to choose an architecture that will not have a long certification path and complex constraints. Organizations can quickly grow and incorporate with other organizations, and it is therefore necessary to consider the scalability and flexibility parameters in order to reduce the cost of adapting to another architecture. One of the organization goals is safe business that can be achieved only if chosen PKI architecture can be quickly recovered in the event of a cancellation.

New solutions for PKI architectures should be in simplicity, in establishing trust between different PKI architectures and in increasing scalability and flexibility.

REFERENCES

[1] Pfleeger, C.P., Pfleeger, S.L., Margulies, M. (2015) *Security in Computing*, 5th Edition Prentice Hall.
[2] Casola, V., Mazzeo, A., Mazzocca, N., Rak, M. (2005) An Innovative Policy-Based Cross Certification Methodology for Public Key Infrastructures. EuroPKI 2005, pp. 100-117.
[3] Lopez, J., Oppliger, R., Pernul, G. (2005) Classifying Public Key Certificates. EuroPKI 2005: pp. 135-143.
[4] Lioy, A., Marian, M., Moltchanova, N., Pala, M. (2006) PKI past, present and future, Int. Journal of Information Security, pp. 18-29.
[5] Linn, J. (2000) Trust Models and Management in Public-Key Infrastructures. RSA Laboratories,
[6] Polk, W. T., Hastings, N. E. (2000) Bridge Certification Authorities: Connecting B2B Public Key Infrastructures. National Institute of Standards and Technology.
[7] Perlman, R. (1999) An Overview of PKI Trust Models, IEEE Network, Vol. 13, pp. 38-43.
[8] Choudhury, S., Bhatnagar, K., Haque, W (2002) *Public Key Infrastructure Implementation and Desig*n, John Wiley & Sons, Inc. New York.
[9] Microsoft, (2016) Certificate Trust List Overview. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/aa376545%28v= vs.85%29.aspx
[10] Certipost, (2004) Trust List Usage Recommendations for a European IDABridge/Gateway CA Pilot for Public Administrations. IDA PKI II / EBGCA /WP1.2
[11] Moses, T. (2003). PKI trust models. Draft, [Online]. Available: http://www.it-c.dk /courses/ DSK/F2003/ PKI_Trust_models.pdf
[12] Burr, W. E. (1998) Public Key Infrastructure (PKI) technical Specification: Part A –Technical Concept of Operations. National Institute of Standards and Technology Working Draft.
[13] Adams, C., Lloyd, S. (2002) *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Second Edition Addison Wesley.

[14] Santesson, S., Farrell, S., Boeyen R., Housley, S., Polk, W. (2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Network Working Group Request for Comments, IETF RFC 5280.
[15] Turnbull, J. (2001) Cross-Certification and PKI Policy Networking. Version: 2.0, Entrust. [Online]. Available: https://www.researchgate.net/publication/245817335_Cross-Certification_and_PKI_Policy_Networking
[16] Author unknown (2002) A bridge CA for Europe's Public Administrations. Feasibility study, European Commission - Enterprise DG, Public Key Infrastructure for Closed User Groups Project.
[17] Shirey, R. (2007) Internet Security Glossary, Version 2, RFC 4949, IETF.
[18] Prodanović, R. I., Vulić, I.B. (2017) Failure Points in the PKI Architecture, Vojnotehnički glasnik/Military Technical Courier, Vol 65, Issue 3, pp. 771-784.