MODEL FOR PKI INTEROPERABILITY IN SERBIA

Radomir I. Prodanović[a], *Ivan* B. Vulić[b]
[a] Serbian Armed Forces, General Staff,
Department of Telecommunications and IT (J-6),
Centre for Applied Mathematics and Electronics,
Belgrade, Republic of Serbia,
e-mail: radomir.prodanovic@vs.rs,
ORCID iD: http://orcid.org/0000-0002-2067-2758
[b] Ministry of Defence of the Republic of Serbia,
Military Intelligence Agency, Belgrade, Republic of Serbia
e-mail: ivan.vulic@vs.rs,
ORCID iD: http://orcid.org/0000-0002-5161-5422

https://dx.doi.org/10.5937/vojtehg65-11041

FIELD: IT
ARTICLE TYPE: Professional Paper
ARTICLE LANGUAGE: English

Abstract:

The increasing use of electronic services that use electronic certificates and the increasing implementation of public key infrastructures require their interconnection and interoperability. In this paper, the authors analyze the models for interoperability between various PKI domains and their possible application in achieving interoperability of the public key infrastructures in the Republic of Serbia. The implementation of the interoperability of the existing models is discussed from the following aspects: scalability, processing of certification paths, implementing policies, the points of failure and the possibilities of re-establishing trust. We proposed a conceptual model based on the Bridge Certification Authority trust model. This model can provide the establishment of the interoperability of both the existing and new national PKI domains, their interconnection as well as their connection with foreign PKI domains. The model was extended with the Validation Authority that provides more efficient processing of the certification path.

Key words: *model, interoperability, PKI, certification authority, certificate.*

Introduction

The companies use the Internet for global business, which means that their information resources are distributed in more places. Therefore, di-

scussions about the elimination of security risks should consider distributed security architecture. The Public Key Infrastructure (PKI) technology is applied in distributed security architecture (Pfleeger, Pfleeger, 2006).

Companies can use electronic certificates (hereinafter: certificates) for electronic services which are issued by different certification authorities from different PKI domains. In order to ensure the functioning of electronic services which use PKI certificates from different domains, there should be a mutual link between them, i.e. it is necessary to establish interoperability for common work of two or more PKI domains.

The main problem with the connection of certification authorities from different PKI domains is certification path discovering and processing, as well as the validation of the user certificate. This problem is overcome by using an appropriate interoperability model.

In the Republic of Serbia (hereinafter: R. Serbia) there are more independent certification authorities which issue electronic certificates and (or) qualified certificates. While researching the Certificate Policies and the Certification Practice Statements of the accredited certification authorities, together with the data from the official websites of the certification authorities in R. Serbia, we have concluded that there is neither connection nor any form of interoperability between the PKI architectures of the authorities whose certifications are registered or recorded. Also, there is no PKI interoperability with other countries.

One form of the distribution trust through the Windows operating system has been achieved by the Serbian Post Certification Authority which became a member of the Microsoft's "Windows Root Certificate" program in September 2009.

The paper (Pavlović, 2007) proposes a possible way for realizing the national PKI. This solution is based on the existence of the Central Root Certification Authority which signs government certification authorities and on the existence of the Bridge Certification Authority through which the government PKI architecture is linked with PKI architectures of non-government organizations (NGOs) and PKI architectures of other countries. Today, this approach would cause numerous problems in the existing government PKI architectures. The authors (Prodanović, Vulić, 2011) propose to form a Bridge Certification Authority which would create a relation of trust with current and future governmental and NGOs PKI architectures, as well as with PKI architectures of other countries. This approach does not require the re-establishment of PKI architectures but the exchange of cross-certificates and the definition of certificate constraints. The problem of this solution is the complexity of processing the certification path.

The proposed PKI interoperability model is aimed to contribute to the realization of the connection of the existing PKI domains, future PKI domains, their interconnection, and their connection with PKI domains of other countries. The model also proposes a mechanism for processing certification paths.

The paper explains PKI, then considers the types of PKI interoperability models and, finally, it analyzes possibilities of applying the described models on the PKI of R. Serbia. A conceptual model of the R. Serbia PKI interoperability is proposed, followed by the conclusion.

Public Key Infrastructure

Since the Internet and intranet are distributed environments, it can be said that PKI with its capabilities represents modern security architecture to protect and securely distribute information in distributed environment.

PKI is a complex system that consists of hardware, software, people, policies and procedures necessary for the creation, management, distribution, use, PKI storage and revocation of electronic certificates and public key cryptography management (Adams, Lloyd, 2003, pp.11-15).

PKI enables the establishment of connections between public keys and entities (in the form of certificates), checks the connections by other entities and enables services necessary for key management in distributed systems.

PKI provides a trusted environment for the transmission of information in distributed systems by providing:

- Authenticity of the parties to the communication - the participants in the communication are checked,
- Message integrity - guarantees that messages have not been changed during transmission,
- Non-repudiation of sending and receiving - the participants in communication cannot deny sending or receiving messages,
- Confidentiality of the message - the message content can be found out only by the entity to whom a message is intended.

Today, PKI is applied in many applications and protocols such as Secure Sockets Layer (SSL), Secure Multipurpose Internet Mail Extensions (S/MIME), IP Security (IPSec), Secure Electronic Transactions (SET) and Pretty Good Privacy (PGP).

The OASIS Research (2003) has shown that PKI is mostly applied to: electronic signatures, web servers (SSL), protection of e-mail and web

services, virtual private networks (VPN), e-commerce, protection of wireless networks (Wi-Fi), code protection and network authentication.

Due to growing needs of financial institutions, companies, government agencies, health and other organizations to use the Internet for their business, information security has become an essential as well as a more complex element of security operations. Not only do organizations have to protect their information and maintain trust with partners but also they have to comply with the government and other standards which relate to the security of operations.

The Components of PKI Architecture

The PKI architecture model is composed of five components specified in (Arsenault, Turner, 2003): the certification authority, the registration authority, PKI Repositories, archives, end entities and their mutual relationships. The PKI architecture model, its functional components and their interconnection are shown in Figure 1.

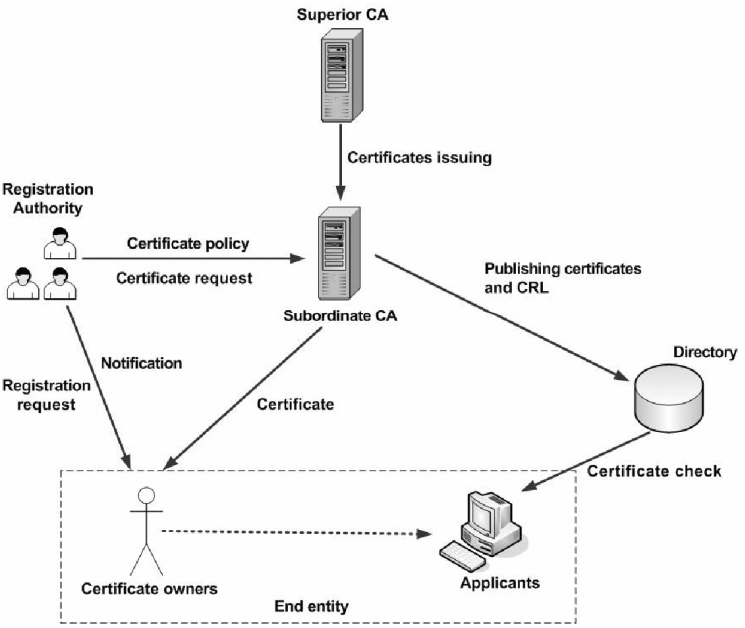

Figure 1 – The relationship between the PKI components
Рис. 1 – Иерархическая архитектура PKI
Слика 1 – Међусобни однос компоненти PKI

The Certification Authority (CA) is a collection of computer hardware, software and human resources. It is responsible for issuing certificates

(created and signed), managing information on the status of certificates and Certificate Revocation Lists (CRLs), publishing certificates and CRLs, and managing archives of expired certificates. The CA can delegate responsibilities to other infrastructure components. It most often works together with the registration authority which is responsible for the identification of entities applying for the issuance of certificates (Prodanović, 2007), (Prodanović, Petrović, 2006).

The Registration Authority (RA) (Sheehy, et al, 2011) is a confidential representative of the CA responsible for verifying the identity of an applicant for a certificate. In addition, the RA can perform other functions which the CA has conveyed to it such as providing reports of revoked certificates, generating key pairs or archiving keys. The RA cannot issue certificates or generate CRLs.

The PKI repository provides storage of certificates and information about their status. The PKI database must fulfill the following requirements: a simple and standardized approach, modern way of data storage, built-in protection, data management and the possibility of storing similar data. The database is implemented as a directory according to standard X.500. The directory stores and distributes certificates and manages their changes. PKI applications access the directory through the LDAP (Lightweight Directory Access Protocol) (Johner, et al, 2000) protocol which is a customized version of the DAP (Directory Access Protocol) protocol.

Archives. The archives contain stored CA certificates for a longer period of time. Archives must guarantee that certificates have not been and will not be changed while they are in the archives. Before the certificate issued by the CA is stored to the archives, it is necessary to determine whether the certificate comes from the CA and whether it is valid. The certificates are stored in the archives so that some signatures of older documents could be verified.

End Entity (End-Entity, EE) is defined as a user of PKI certificates and (or) end user of a system that is the subject of the certificate (Arsenault, Turner, 2003). In other words, in the PKI system, the end entity is a general term for a subject that uses any services or functionality of the PKI system and it can be the owner of a certificate (individuals, organizations or other entities) or the applicant (may be an application, service, CA, etc.) for a certificate or a CRL. The term PKI users is often used and it refers to organizations or individuals that use PKI, but do not issue certificates. They rely on other companies that publish certificates and verify certificates of other entities in the business.

Certificate. The purpose of the certificate is to establish a link between an identified (notified) entity and the public key, indirectly with the core-

sponding private key of the entity. This is accomplished when the CA uses its private key for signing the certificate, so that the certificate can be later verified by any entity which has the public key of the CA. The latest version of X.509 standard for the certificate structure published in 2000 defines a new set of additional certificate extensions. However, this set of extensions does not require the issuance of a new version of the certificate because these extensions can be included in version v3 which is specified by the IETF (Cooper, et al, 2008).

The Interoperability of PKIs

There is an increasing growth in requirements for the interoperability of PKIs. The full potential of PKI-based electronic services can be achieved only if large organizations provide certificates for e-business and if there is interoperability between PKIs.

In order to establish PKI interoperability, it is necessary to establish two processes of interoperability, namely:

- Political or contractual process of establishing mutual recognition. This process is necessary to determine whether the participants of interoperability comply with certain technical, security and management requirements for interoperability, prior to proceeding with the implementation of technical interoperability.
- The technical solution for the transfer of mutual recognition. This solution is used in order to transfer enough information on participant's status of interoperability so that the recipient of the certificate can automatically decide whether to accept or not a certificate from another PKI domain.

The policy of PKI interoperability involves determining the trusted PKI domain having the required level of security. Technical PKI interoperability includes processing certification paths through different PKI domains in order to discover certification paths and determine the validity of the certificate.

Interoperability can be perceived through three categories: interoperability between applications, between the components and between PKI domains (PKI Forum, 2001).

Interoperability between applications allows different PKI applications to be interoperable with one another, regardless of who has produced them. When manufacturers develop applications, in order to achieve interoperability of the PKI environment, they consider ways for storing credentials as well as the compatibility between different files and message formats (eg. the size of keys and algorithms should be compatible between different applications) and the communication between different applications.

Interoperability between components enables numerous PKI components to work together in order to get an overall functionality of the PKI solution. This interoperability is important because errors in the communication between the components cause the interruption of PKI functionality. In order to preserve interoperability between PKI components during development, it is necessary to use common protocols and message formats for communication between various components such as the CA, the RA and clients. The standards that ensure interoperability between components are: Public Key Infrastructure standard X.509 Certificate Management Protocol (PKIX-CMP) and Public Key Infrastructure standard X.509 Certificate Request Message Format (PKIX-CRMF). Also, it is necessary to use the most common mechanisms for providing information about the revoked certificates, such as the Online Certificate Status Protocol (OCSP) and the Certificate Revocation List (CRL). No less important in terms of interoperability is the implementation of authentication methods and cryptographic algorithms.

Interdomain interoperability focuses on establishing relations of trust between different PKI domains. This interoperability, besides characteristic problems, includes problems that stem from the interoperability of applications or components. Besides that, keeping in mind the technological solutions associated with these issues, this interoperability requires the existence of questions to the answers related to policies. When considering this type of interoperability, it is necessary to consider the availability of the public key between the domain and the general policies of the PKI domain. In addition, each domain should remain faithful to the set of policies that govern its certification process. The most important aspect of this interoperability is the support to cross-certification between CAs. The cross-certification can be implemented using a PKIX-CMP and other PKCS standards such as PKCS # 7 and PKCS # 10.

Models of PKI interoperability

The obvious approach to solving PKI interoperability is the existence of a central CA, or a point of trust. The hierarchical model includes a centralized control and unanimous support. There are other solutions that are more flexible, such as (Connolly et al, 2005): cross-certification model, cross-recognition model, bridge model and certificate trust list model.

A single (root) CA model is based on the existence of a CA which issues certificates to all users who trust it and thus realizes the trust in their mutual transactions. This model is sensitive to an increase in number of

users, which causes technical and administrative overhead of PKI schemes at the state level; it also causes the multiplicity of requirements that a CA cannot fulfill or a refusal to accept a CA, thus causing the CA security breach which affects all users.

Strict hierarchy model. This model extends the model with a single CA and allows specialization between CAs. With this model, users need to be persuaded to trust the root CA, even if it does not directly issue certificates. In this model, the root CA is a critical point of security. Compromising the root CA causes the failure of the whole PKI. In addition, the problem may be that the root CA, by its policies, imposes restrictions on subordinate CAs. This model does not have the problem of interoperability and it is suitable for use in centralized systems.

Cross-certification (mash) model. In this model, CAs establish relations of trust according to whether they trust each other. The user can trust an unknown CA across the certification path that leads to a local trusted CA. However, the establishment of interoperability across the network certification is technically and logistically challenging. Interoperability is not easily achievable between two CAs only by co-ordinating their policies and technical systems. The problem of interoperability is complicated as the number of cross-certifications grows even faster. The very nature of this model, where CAs are not familiar to each other, is not an ideal approach to establishing a multinational PKI. This model is most suitable for two or three related CAs which are required to interoperate with each other.

Bridge CA model. This model implies the existence of a central CA that achieves a bidirectional trust relationship with one CA of each PKI. It represents a communication channel between the CAs that it connects, i.e. interoperability is accomplished through it. This combines the aspects of the root model and the mash model. The bridge CA model provides simpler administration because it is required to establish only one pair of cross-certifications with each CA rather than n^2 certifications (n is the number of CAs) in a complete mash model. This model does not impose as strict technical requirements as the mash model. With its policy, the bridge model sets minimum requirements for connecting PKIs. The model is focused on the tasks of providing interoperability and that helps to centralize the management of interoperability problems in one organ that can develop and promote best practices. This model allows the connection of different models into one.

Cross-recognition model. In this model, a particular CA or PKI domain agrees to admit other CA or the PKI domain before a lower level of technical solutions is built. This means that the user from one PKI domain can use the information of the authority in the other PKI domain for authentica-

tion and vice versa. This model requires a close cooperation between the CAs at the administrative level or the existence of an agency for accreditation at the higher level. Cross-recognition allows formal and reciprocal recognition by the competent PKI authorities (top trust point) of the new PKI domain to impose, manage and enforce PKI trust standards and processes for accepting trust certificates in recognized fields. This allows that the users of one PKI domain can rely on the certificates issued by another domain for use in certain applications within the limits of accredited certification policy. This model does not guarantee the status and reliability of foreign certificates. Cross-recognition differs from cross-certification because there is no mutual recognition between CAs. The reason is that the model of recognition is based on the concept of an independent CA, which is licensed and accredited in order to achieve mutual recognition of CAs. The model of recognition avoids some of the technical interoperability issues.

Certificate trust list model. This model involves a list of CAs from trusted certification authorities. The list is electronically signed to ensure its integrity. These lists are simple and provide confidential communications. In this way, they avoid a need for a complex cross-certification process. These lists have led to the web model that represents the most widespread PKI interoperability across web browsers. The essence of this model is that the certificate user trusts the issuer of the certificate trust list, and therefore believes CAs in the list.

Accreditation certificate model. This model was proposed by the Australian Government during the development of Australia's PKI (Lloyd et al, 2001), (Australian Government, 2009). The model introduces the accreditation certificate which confirms that the CA is accredited by the Australian Government. In essence, each accredited CA has a public key signed by the accreditation body of Australia. The process of signing provides security to users that the CA is accredited. As long as users trust the accreditation authoritity, they will recognize each accredited CA as trusted. This model is similar to the concept of the strict hierarchy model. However, each accredited CA may have its own unique CP and CPS and nothing prevents them from having only a signed public key which is not allowed in the model of strict hierarchy.

Analysis of the Existing PKI Interoperability Models

Each of the above mentioned models of interoperability has its good and bad sides. Not all models can solve the problem of the interoperability of already established PKIs. Such models require that interoperability be

designed first, and then PKI architecture be established. Some models are rigid because they enable only interoperability of CAs in the hierarchy, while others overcome this by establishing cross-relations of trust which complicate the processing of certification paths. Some models implement the policy only through the acceptance of contracts, while others can implement it through certificates. On the other hand, some models are not suitable for international interoperability.

In order to establish the most favorable model of trust for the establishment of interoperability, the models were evaluated from the point of scalability, processing of certification paths, application of policies, point of failure, re-establishment of trust and the possibility of establishing the interoperability of the existing with new national PKI domains and their connecting with international PKI domains.

The single CA model cannot be applied to solve interoperability problems because it would involve only one CA to issue certificates for all PKI users, and it is necessary to have at least two PKI domains in order to achieve interoperability. The introduction of this model of trust aimed at reducing the number of PKI domains in order to solve the interoperability is not a good solution because this model is not scalable. Furthermore, it is technically and administratively demanding at the state level and cannot meet all the requirements of users and organizations. A good feature of this model is a rapid discovery of a certification path and validation. Generally speaking, this model can achieve neither interoperability between the existing PKI domains and the new PKI domains nor their interoperability with international PKI domains.

The strict hierarchy model can be used to connect the existing PKI domains although this model connects multiple certification authorities. This model could have achieved the PKI interoperability in the PKI domain of R. Serbia before the existing PKI domains were formed, by forming a national root certification authority from which the existing and new PKI domains or subdomains would have stemmed. In this way, centralized policies would have been applied and certification paths would have been faster discovered and validated. However, as mentioned before, this model cannot be applied to connect the existing PKI domains, or for connecting with international PKI domains. The problem of this model is the security of the root CA because jeopardizing its security would cause failure of all PKIs in the state. The introduction of a centralized root CA separately for the government domain and separately for the commercial domain would enable faster discovering and validation of certification paths between PKI domains which would be connected by some other model.

The cross-certification model can be applied for the establishment of interoperability, but only between two or three PKI domains. Connecting multiple PKI domains represents a technical and administrative challenge; furthermore, it does not solve the problem of interoperability with international PKIs. Establishing more cross-certifications would lead to the problem of coordination of certification policies and to the problems in the process of discovering and validation of certification paths.

The cross-recognition model can be used to establish interoperability between the PKI domains in R. Serbia. The PKI domains would agree to mutually recognize the certification authorities before they build a technical solution. This requires a close cooperation between the PKIs or the existence of accreditation agencies, which currently is not the case (there is an organizational unit in the Ministry of Trade, Tourism and Telecommunications that works on the CA certification for entering the Register of Certification Authorities issuing qualified certificates). The recognition allows formal and reciprocal recognition of new PKI domains by the competent PKI authority (top trust point). Trust is achieved by accepting the standards, policies and processes for the acceptance of appropriate trust certificates in the identified fields. This way of trust enables the users of one PKI domain to rely on the certificates of another domain for use in specific applications within the accredited certification policy. This model can be used as a temporary solution for the formal interoperability of the existing PKI, until establishing a model that will enable the connection of all existing, new and international PKIs.

The certificate trust list model is a potential model for interoperability that could be applied. In order for users to trust the certification authorities in the trust list, it is necessary that each item in the list and the list itself are signed by a trusted authority in whom all users trust. The problems of this model are the growth of the trust list, non-existence of central administration and implementation of validation process within an organization, list update and its maintenance. The lack of scalability, the loss of central administration, policy enforcement and additional operating costs related to the access to the list reduce the use of this model for resolving the trust across multiple PKI domains in R. Serbia and the trust with international PKI domains.

The accreditation certificate model includes the introduction of an accreditation CA that will sign other CA certificates. In this way, users who believe the accreditation authority also believe the users from other PKI domain CAs to which the accreditation authority signed certificates. This model can create trust between the PKI domains in R. Serbia by forming the accreditation CA that would sign the keys of all root CAs thus achieving interoperability with the harmonization of policies and technical issues regarding discovering and validation of certification paths. Also, the accre-

ditation CA would sign a CA certificate to newly added PKI domains. This approach is possible because this model allows each accredited CA can have its own unique CP and CPS. In addition, nothing prevents the CA from having a self-signed public key. However, this model does not solve the problem of interoperability with international PKI domains.

The bridge model is designed with the aim of connecting multiple PKI domains. This model helps to centralize the management of interoperability problems in a single body that can develop and promote best practices. It allows the connection of different PKI architectures, including bridge architecture, so that all architectures merge into one thus enabling interoperability. The model is scalable because it allows adding both the existing and new PKIs, reduces the number of cross-certificates and makes it easier to discover and validate certification paths better than the mash model. In addition, policies can be implemented through certificates, connection with international PKIs is possible, and the bridge model failure does not affect internal operability within individual PKI domains. The problem may occur with a large number of PKI domains which complicates the process of discovering and validation of certification paths. This model is most acceptable for the establishment of interoperability between national PKIs in R. Serbia and their interoperability with international PKIs.

Proposed PKI Interoperability Model for the Republic of Serbia

There are six accredited certification authorities (governmental and non-governmental) which issue qualified certificates in R. Serbia or six PKI domains between which it is necessary to establish PKI interoperability. All certification authorities are based on a hierarchical PKI architecture with a root CA as the top point of trust and one or more subordinate CAs.

When choosing a model of interoperability, the following has been taken into consideration:

- processing certification paths, i.e. its discovery and validation from the end user to the point of trust,
- determining the properties of the certificate from certificate policy, and
- determining whether the certificate is trusted for the intended purpose.

This chapter gives a conceptual proposal of the multidomain PKI interoperability in R. Serbia, which includes the realization of the:

- interoperability between the existing accredited PKI domains,

- interoperability between newly established PKI domains in the governmental and public sectors, and
- interoperability of the PKI domains in R. Serbia with international PKI domains.

The proposed model of the interoperability of PKIs in R. Serbia, Figure 2, is based on the bridge model that enables interoperability between the existing (enrolled in the Register[1]) and new PKI domains of different architectures (hierarchicals, mashs, bridges) as well as their connection with international PKI domains. The basic model has been extended with the validation authority that allows faster processing of certification paths. As an integral part of the national PKI infrastructure, an accreditation body that determines the general certification policy of the PKI in R. Serbia is introduced. The introduction of an accreditation body is initiated by the fact that governmental and public PKIs have been established without a clear global policy on PKIs in R. Serbia. This model allows the implementation of a clear PKI policy for all PKI domains.

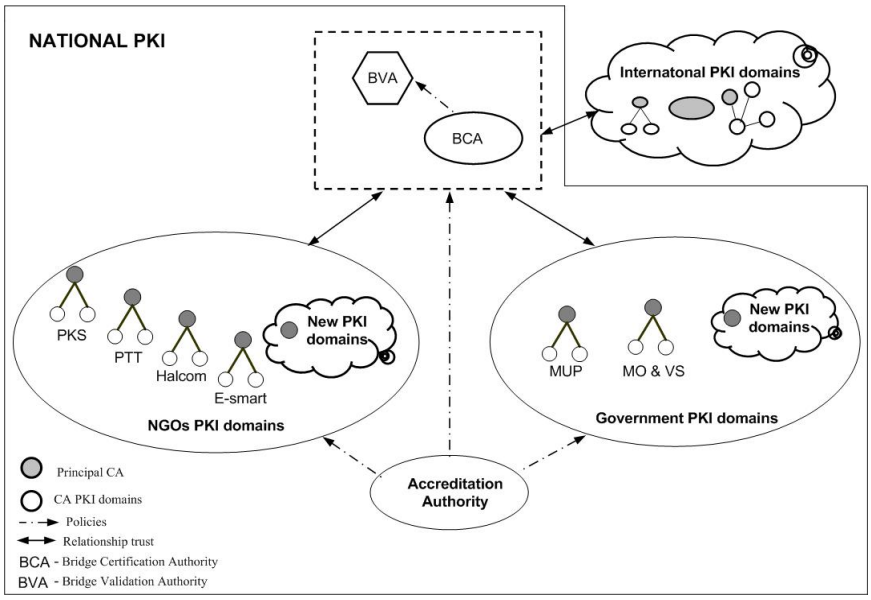

Figure 2 – The proposed model of PKI interoperabilty in the Republic of Serbia
Рис. 2 – Предлагаемая модель ПКИ взаимодействия и доверия в Республике Сербия
Слика 2 – Предложени модел PKI интероперабилности Републике Србије

[1] The Register of certification authorities for issuing electronic certificates, http://epotpis.mtt.gov.rs/elektronski-potpis/

This concept allows the connection of PKI domains which enable electronic business between citizens, the state, government administration, local administration and local government, businesses, health, culture and other scopes that require the safe exchange of distributed and security sensitive data.

The bridge PKI mode i.e. the bridge CA achieves relations of trust between different PKI domains. The trust is achieved by establishing peer-to-peer relations of trust with the CAs of different PKI domains. The trust with governmental and non-governmental root CAs is achieved via the existing PKI domains.

The policy of the bridge CA defines the interoperability mechanism to ensure trust over different PKI domains. A successful cross-certification confirms that an applying PKI operates in accordance with the standards, guidelines and practices of policy issued by the authority of interoperability. The Memorandum of Cross-Certification (formally describing the conditions of cross-certification) is signed between the bridge CA and an applying PKI.

One of the main advantages of using the bridge CA trust model is to provide centralized management and automated enforcement of a validation policy. The path of trust is built by cross-certification between PKI domains and the bridge CA. The policy of certificate validation may limit the scope of trust through the established cross-certification. The application of this policy to certificates at the time of transactions allows security and trust of business processes between PKI domains.

Validation policies include specific rules and parameters to be used during the validation of certificates. In this model, validation policies are implemented through the use of policy and (or) limitations specified in cross-certificates. Constraint policies are used to restrict the use of certificates based on the policies under which the certificate was issued.

When PKI domains enter the bridge interoperability model, in addition to the establishment of relations of trust and the acceptance of policies, a contract on the implemented validation policies is concluded. New PKI domains may limit the relations of trust with other PKI domains and their subdomains, as well as to exclude certain subdomains. This is done by specifying a list of names (i.e. X.500 characteristic names) of all subdomains in the "name constraint" extension of cross-certificates. There is an option to include or exclude specific names or subgroup names (for example, all of abc.gov addresses) via this mechanism.

The proposed model allows automated discovering and validation of certification paths, including the application of restrictions. The accepted validation policy is implemented in the extension of cross-certificate after

codification. In this way, an automatic validation process is enabled for all future transactions.

In the existing PKI trust models, a construction of the trust path is a simple process because they are all based on a hierarchical architecture. However, the process of discovering certification paths via the bridge CA becomes a complex process due to cross-certificates. The main problem is in the processing of certification paths which can be time-consuming for applications using PKI in their work. This problem could be solved by applying a protocol for simple certificate validation, named SCVP (Server-based Certificate Validation Protocol) (Freeman, et al, 2007).

The SCVP standard defines two accesses of delegating discovering the path of trust. In the first approach, Delegate Path Discovery, the client delegates the task of discovering the certification paths to the SCVP server, but not the task of its validation. In the second approach, Delegate Path Validation, the client delegates the task of constructiing a valid certification path and the task of validating, i.e. confirming that the public key contained in the certificate profile can be used for its purpose. Both approaches relieve the user application of the problem of discovering and validating certification paths through centralized validation policy.

A crucial factor in the development of any PKI is to achieve scalability to be able to meet the needs of more users. PKIs in R. Serbia are based on a hierarchical architecture, and considering that this type of arhitecture is scalable and the easiest to implement, it is expected to witness an increase in the number of PKI domains, users, and, consequently, certificates. An increased pressure from the state on all levels of government to use the services of e-government and e-commerce will result in a large number of transactions. This leads to a need to build validation systems because the authentication and verification of trust of paths, as a part of the confirmation of each transaction, must be automated, scalable and secure.

The system for discovering and validating certification paths of the proposed model has to satisfy the following requirements:

- High performance - the system has to provide quick answers to the application's request so that users do not notice that the validation process has started,
- High availability - the system must be available when the end user wants to use it,
- Scalable - increasing the number of users and PKI domains should have a minimal impact on performance, availability and security,

- Security - the system must ensure public confidence in the security of information exchanged in transactions using the certificate,
- Interoperable - a system must be based on open standards to ensure interoperability with all applications in accordance with appropriate standards,
- Low risk - the system must be based on technology that has been proven to work in realistic operational scenarios of equal or larger size.

The proposed model has the following advantages over the other models:

- Centralized management and automatic implementation of validation policy,
- Automation of processing certification paths of trust between domains, including the application of restrictions,
- Automatic validation process for all subsequent transactions without the need for any transaction, especially considering the terms of the contract,
- Expansion of the national PKI by new governmental and non-governmental PKI architectures is simple, it does not complicate the process of discovering certification paths and it is transparent to users,
- Breach of security of individual PKI domains does not affect the functionality of the entire national PKI,
- There are restrictions to the failure of the national PKI in the event of compromising one private key, since more keys of the bridge CA can be used to establish relations of trust.

Conclusion

PKI interoperability is necessary for the establishment of a national PKI in securing electronic services that use certificates on a national and global level. Depending on their advantages and disadvantages, the existing PKI interoperability models, can be used, to a greater or lesser extent, as standalone or in a combination with other models for the realization of PKI interoperability. When considering the introduction of PKI in the country, the need for interoperability should be addressed first, then the criteria should be established followed by the development of PKI interoperability policies. The proposed PKI interoperability model provides

a good basis for the improvement of the national PKI and for the connection with international PKIs.

Further research should be carried out in the direction of organizational solutions of the PKI interoperability in R. Serbia and concrete technical solutions arising from the proposed model, such as the mechanism for processing certification paths and software of the bridge certification authority.

References

Adams, C., & Lloyd, S., 2003. *Understanding PKI: Concepts, standards, and deployment considerations*, Addison-Wesley Professional, pp.11-15.

Arsenault, A., & Turner, S., 2003. Internet Draft PKIX: Internet X. 509 Public Key Infrastructure: Roadmap, PKIX Working Group.

Australian Government, 2009. *Gatekeeper PKI Framework*. Department of Finance and Deregulation. Available at: https://www.finance.gov.au/ sites/default/files/Certification_Authority_Accreditation_Criteria.pdf.
Accessed: 17 May 2016.

Connolly, C., van Dijk, P., Vierboom, F., Wilson, S., 2005. *PKI Interoperability Models*, Galexia.

Cooper, D., Santesson, S., Farrell, S., et. al., 2008. Internet X. 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 5280.

Freeman, T., Housley, R., Malpani, A., et al, 2007. *Server-Based Certificate Validation Protocol*, Network Work Group, RFC 5055.

Johner, H., Fujiwara, S., Yeung, A.S., et al, 2000. *Deploying a Public Key Infrastructure*, IBM Redbooks, SG24-5512-00. Available at: http://www.ibm.com/redbooks. Accessed: 17 May 2015.

Lloyd, S., Fillingham, D., et al, 2001. *CA-CA Interoperability,* White Paper. PKI Forum. Available at: http://www.oasis-pki.org/pdfs/ca-ca_interop.pdf, Accessed: 17 May 2016.

- OASIS, 2003. *Survey on Obstracles to PKI Deployment and Usage, version 1.0*. Available at: http://people.cs.vt.edu/~kafura/cs6204/ Readings/Authentication/PKIObstaclesSurveyReport.pdf. Accessed: 17 May 2016.

Pavlović, G., 2007. [Internet]. Available at: http://www.telekomunikacije.rs/archive/first_issue/g_pavlovic:_implementacija_ elektronskog_ potpisa_u_srbiji.119.html. Accessed: 25 May 2016.

PKI Forum, 2001. *PKI Interoperability Framework*, PKI Forum. Available at: http://www.oasis-pki.org/pdfs/PKIInteroperabilityFramework.pdf.
Accessed: 14 October 2014.

Pfleeger, C.P., & Pfleeger, S.L., 2006. *Security in Computing, 4th ed*, Prentice Hall.

Prodanović, R., 2007. Ugrožavanje bezbednosti u elektronskom poslovanju. In: *Simpozijum YU INFO 2007*, Kopaonik, March 11.

Prodanović, R., & Petrović, M., 2006. Digitalni sertifikat - nosilac zaštite u elektronskom poslovanju. In: *SymOrg*, Zlatibor, June 07.

Prodanović, R., & Vulić, I., 2011. A Proposal for the Solution of the Public Key Infrastructure of the Republic of Serbia. In: *4th International Scientific Conference on Defensive Technologies OTEH*, Belgrade, October 06.

Sheehy, E.D., Greene, M., Lundin, M., Ward, J., 2011. *Trust Service Principles and Criteria for Certification Authorities, Version 2.0*., Canadian Institute of Chartered Accountants.

МОДЕЛЬ ДОВЕРИЯ И АРХЕТЕКТУРА
PKI В РЕСПУБЛИКЕ СЕРБИЯ

Радомир И. Проданович[а], *Иван* Б. Вулич[б]
[а] Вооруженные силы Республики Сербия, Генштаб,
Управление телекоммуникаций и информатики (J-6)
Центр прикладной математики и электроники, г. Белград,
Республика Сербия
[б] Министерство обороны Республики Сербия,
Военно-разведывательное агентство, г. Белград, Республика Сербия

ОБЛАСТЬ: информационные технологии
ВИД СТАТЬИ: профессиональная статья
ЯЗЫК СТАТЬИ: английский

Резюме:

Применение электронного сервиса, использующего цифровые сертификаты увеличивается с каждым днем, увеличивается также и количество внедренных инфраструктур открытых ключей, в связи с чем появилось необходимость в их объединении и взаимодействии. В данной статье представлены результаты проведенного анализа модели взаимодействия между различными доменами инфраструктуры открытых ключей и возможность их применения в осуществлении взаимодействия инфраструктур открытых ключей в Республике Сербия.

Применение существующих моделей взаимодействия рассматривается с точки зрения масштабируемости, обработки сертификационного маршрута, применения политики, точки отказа и возможности установления новых доверительных отношений. Разработана концептуальная модель, основанная на мостовой модели доверия. Данная модель обеспечивает взаимодействие существующих и новых национальных PKI (Public Key Infrastructure) доменов их соединение, а также подключение к зарубежным PKI доменам. Модель

расширена валидационным авторитетом, который обеспечивает эффективную обработку сертификационного пути.

Ключевые слова: сертификат, PKI системы, домены, доверие, модели, инфраструктура.

МОДЕЛ ЗА PKI ИНТЕРОПЕРАБИЛНОСТ У РЕПУБЛИЦИ СРБИЈИ

Радомир И. Продановић[а], *Иван* Б. Вулић[б]
[а] Војска Србије, Генералштаб, Управа за телекомуникације и информатику (J-6),
Центар за примењену математику и електронику, Београд, Република Србија
[б] Министарство одбране Републике Србије,
Војнообавештајна агенција, Београд, Република Србија

ОБЛАСТ: информационе технологије
ВРСТА ЧЛАНКА: стручни чланак
ЈЕЗИК ЧЛАНКА: енглески

Сажетак:

Све већа примена електронских сервиса који користе електронске сертификате и све више имплементираних инфраструктура јавних кључева условили су потребу за њиховим међусобним повезивањем, односно остваривањем интероперабилности. У овом раду извршена је анализа модела за интероперабилност између различитх домена инфраструктуре јавних кључева и њихова могућа примена у остваривању интероперабилности инфраструктура јавних кључева у Републици Србији. Примена постојећих модела интероперабилности сагледана је са аспекта скалабилности, обраде сертификационе стазе, примене политика, тачке отказа и могућности поновног успостављања поверења. Предложен је концептуални модел заснован на мостовном моделу поверења. Овај модел обезбеђује успоставу интероперабилности постојећих, нових националних PKI (Public Key Infrastructure) домена, њихово међусобно повезивање, као и повезивање са иностраним PKI доменима. Модел је проширен валидационим ауторитетом који обезбеђује ефикаснију обраду сертификационе стазе.

Кључне речи: сертификат, PKI системи, домени, интероперабилност, модели, инфраструктура.

Paper received on / Дата получения работы / Датум пријема чланка: 30.05.2016.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 20.12.2016.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 22.12.2016.