FAILURE POINTS IN THE PKI ARCHITECTURE

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/vojtehg65-11144

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

Abstract:

Over the last 20 years, the PKI architecture has found its vast application, especially in the fields which require the establishment of a security infrastructure. Given that the purpose of this architecture is to be used for achieving higher security standards, its smooth operation has to be one of the main requirements for its implementation. Its complexity is mirrored in the numerous implementations that the PKI has had so far. For all the reasons mentioned above, it is of great importance to consider potential failure points of such a structure. Due to the complexity of these structures, this paper will present only a basic review of such stress points, without providing details on specific applications and types of implementations. The significance of failure points will be explained by examining the common features of the PKI architectures and the occurrence of failure points in these structures, and where possible, an overview of suggestions for preventing such failures will be provided.

Key words: smart cards, cryptography, HSM, PKI, security, failure, architecture.

Introduction

PKI stands for Public Key Infrastructure, and as such it represents infrastructure based on the use of public key cryptography. The idea to use asymmetric cryptographic algorithms in user authentication protocols, and other services that the PKI enables, preceded the formation of this infrastructure.

The use of asymmetric algorithms means that a key pair will be generated, the private one and the public one. Intuitively, it may be concluded that it is an imperative to keep the private key a secret, while the public key should be in some way announced to those who participate in the communication, and all that in such a manner that it is unequivocally clear who the participant is and that the key linked to them really belongs to that participant. This leads to the introduction of certificates as a means of binding entity with its public key, and to the development of the PKI architecture which is therefore used to manage these certificates and to guarantee their validity.

A failure is a very important concept in technology, and its importance becomes more apparent with the development of faster and more powerful computer systems. Whether they are considered from the security of private data standpoint, or from the standpoint of material and physical security, the study of ways they could be classified and processed in various fields of technology is important. The study of failures in complex systems, as the PKI architecture may be, is especially interesting. In the case of such complex systems, it is advisable to try to prevent faults and make fault – tolerant systems.

The Concept of Faults

Reliability is often presented by contemporary technical systems as a wanted quality in front of system designers. The definition of reliability can be given as a probability of the system to perform its intended task successfully, within a certain trust scope and within specified performance boundaries, while being utilized in the proper manner and for the intended purpose, under the specified load, and taking into account the previous system utilization time (Ramović, 2005). Therefore, it is clear that the concept of reliability is complex and at the same time, intertwined with the concept of faults.

When a system deviates from its specified behavior, it is said that a failure has occurred. A failure is caused by an error, which would be an

invalid system state, and it is an external manifestation of the said errors occurring within the system. Faults are the root cause of errors.

There are many ways of classifying faults in the systems, depending on the observation scope, where the said concepts can be observed at the level of a component within the system, as well as at the system level. It is clear that by observing such concepts at the component level as a part of a complex system, one arrives at very intricate definitions of reliability and fault, especially considering mutual dependency of system components. Also, there are a lot of criteria by which faults can be classified and some of those are given in Table 1.

Table 1 – Fault types arranged by classification methods, taken from (Ramović, 2005)
Таблица 1 – Виды сбоев по методам классификации, согласно (Ramović, 2005)
Табела 1 – Врсте отказа по методама класификације (Ramović, 2005)

Classification criteria	Fault type
By the type of state change	Unexpected fault
	Gradual fault
By relationship with other faults	Independent fault
	Depended fault
By possibility of utilization after fault occurrence	Complete fault
	Partial fault
By elimination period	Permanent fault
	Intermittent fault
By external manifestation	Apparent fault
	Suppressed fault
By the cause of fault	Design fault
	Technological fault
	Operational fault
By the nature of fault	Natural fault
	Artificial fault
By the time of occurrence	Fault during testing period
	Fault in the preparation period
	Normal exploitation fault
	Near end exploitation period fault
By fault intensity	Random fault
	System fault

It is not possible to apply all the classification methods to every system, nor to all parts of it, but it is clear that some of these classification methods are, because of their nature, more relevant for consideration.

For the purposes of this paper, a classification method from the standpoint of possibility of utilization after occurrence of a fault makes an interesting topic. Within this method, there are the concepts of a complete and a partial fault, where it is intuitively clear that the system is rendered non-usable after the occurrence of a complete fault, while the system is still somewhat usable after the occurrence of a partial fault.

Also, it is important to consider the ways of determining the scope of a failure and the consequences of its occurrence, as well as the ways of achieving recovery after a failure in the architecture.

The PKI Architecture

As mentioned previously, when speaking of the PKI architecture, several different types of architecture, depending of their intended use, may be considered; however, it is obvious that they all have some common features.

Since it is the architecture intended for the purpose of establishing security, it is apparent that the use of cryptographic techniques achieved through the specialized hardware and software will be needed. The PKI architecture is inherently based on the use of certificates, their generation and application in order to enable different services based on this architecture. Besides the cryptographic part of it, this architecture also requires an extensive use of various hardware and software resources, namely servers, computer networks and application software.

Broadly speaking, the PKI architecture is based on the existence of one or more trusted authorities with their policies and protocols, which enable certain services distinctive for the PKI (Adams, Lloyd, 2003), (Chokani, 2003).

These trusted authorities are called certification authorities. They are responsible for establishing trust policies, and for the issuance and management of certificates, which then enable the use of various services, i.e. services of authentication, digital signing and non-repudiation. The only self-signed certificates are those that belong to the certificate authority, while user certificates are signed by the certification authority and as such, are considered to be a valid confirmation that the key given in the certificate really belongs to the owner of the said certificate, as long as there is no breach of trust established in the certification authority.

In the PKI architecture, beside certification authorities and depending on the application of the said architecture, there may be one or more registration authorities, which have the role of collecting the relevant user data which will be later displayed in the certificate, and in establishing indirect connection between the certification authority and its end users.

Architecture Types and Failure Points in Them

Generally speaking, there are several basic PKI architecture types, and they are hierarchical, distributed trust architecture, web architecture, mash architecture and bridge architecture.

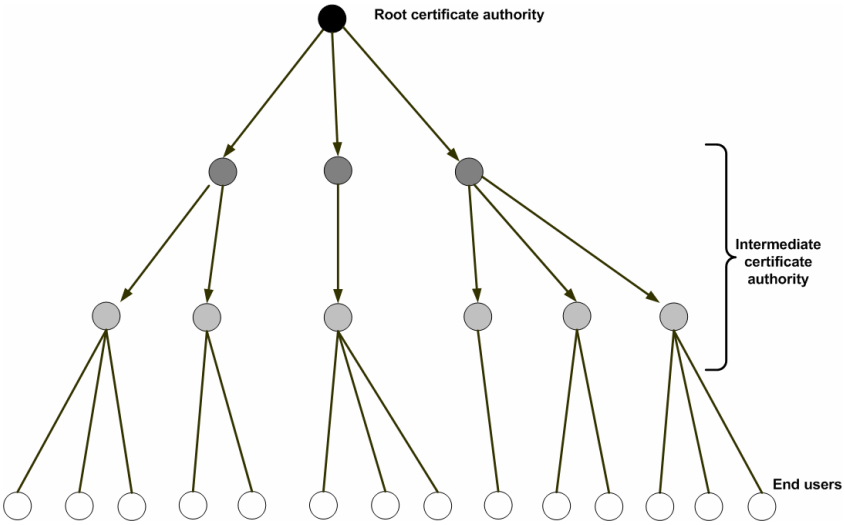

Figure 1 – Hierarchical PKI architecture
Рис. 1 – Иерархическая архитектура PKI
Слика 1 – Хијерархијска PKI архитектура

The hierarchical architecture, shown in Figure 1, requires the existence of a Root certificate authority in the top of the hierarchy, and one or more certificate authorities called the Intermediate certificate authorities which issue end user certificates. End users are at the lowest level of this hierarchy. This type of architecture is often used in the business organizations and in the cases when achieving a high level of scalability is necessary. In the case of this architecture, the Root certificate authority will sign only certificates of those who are at the level below it, while the certificates of end users will be signed by the Intermediate certificate authority at the level above them.

Being that the Root certificate authority is the basic trust point in the whole hierarchy, it being compromised will lead to the failure of the whole structure, while compromising the Intermediate certificate authority will cause only a partial failure within the structure.

In case of a failure of the Intermediate certificate authority, recovery is achieved by revoking all valid certificates this body has issued and by

establishing a new Intermediate certificate authority which will reissue certificates for end users of the previous Intermediate certificate authority. It is possible for the Root certificate authority to issue certificates for end users directly, without having any intermediate body, but it is not advisable to do so because the failure of such certificate authority simultaneously means the failure of the whole architecture.

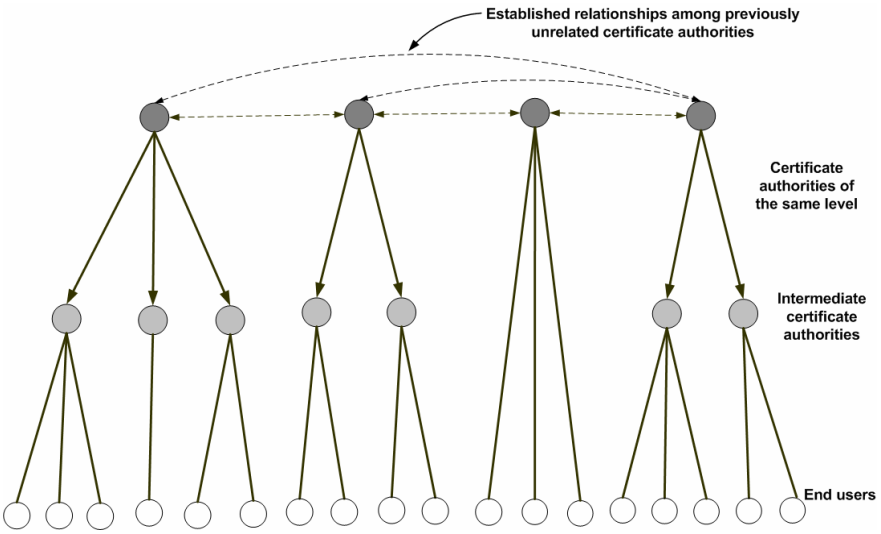

Figure 2 – Distributed trust PKI architecture
Рис. 2 – PKI архитектура распределенного доверия
Слика 2 – PKI архитектура дистрибуираног поверења

The distributed trust PKI architecture is the second type of the PKI architecture. As shown in Figure 2, in this type of architecture, a bidirectional relation of trust interoperability is achieved among several certification authorities. This way, several certification authorities established for different purposes and for different end users, are bound in a trust chain in order to enable some common service or a faster mutual authentication, and all that without the need for issuing multiple certificates. Depending on the way of establishing trust relations within the certification authorities in this architecture (Adams, Lloyd, 2003), a failure of a single certification authority will naturally affect its end users, but it will have only limited or none at all influence on the end users of other certificate authorities. What complicate things in this type of architecture are different models of establishing trust relations among the certificate authorities within the architecture.

After the failure of a certificate authority in this type of architecture, recovery can be achieved by revoking all valid certificates this authority has issued, breaking the trust relation this authority has had with other authorities, reestablishing this authority and broken trust relations by reissuance of all the revoked certificates.

The Web PKI architecture, shown in Figure 3, is used within web browsers, where there are preinstalled certificates of the Intermediate and Root certificate authorities whose certificates will be trusted by the browser. Compared to the other types of the PKI architectures, this is considered to be the easiest and simplest for use, but it is also the most susceptible to security problems (Adams, Lloyd, 2003). The biggest problem with this architecture lies within its users not being informed enough about the meaning of having preinstalled certificates in their browser and the way they can affect their safety.

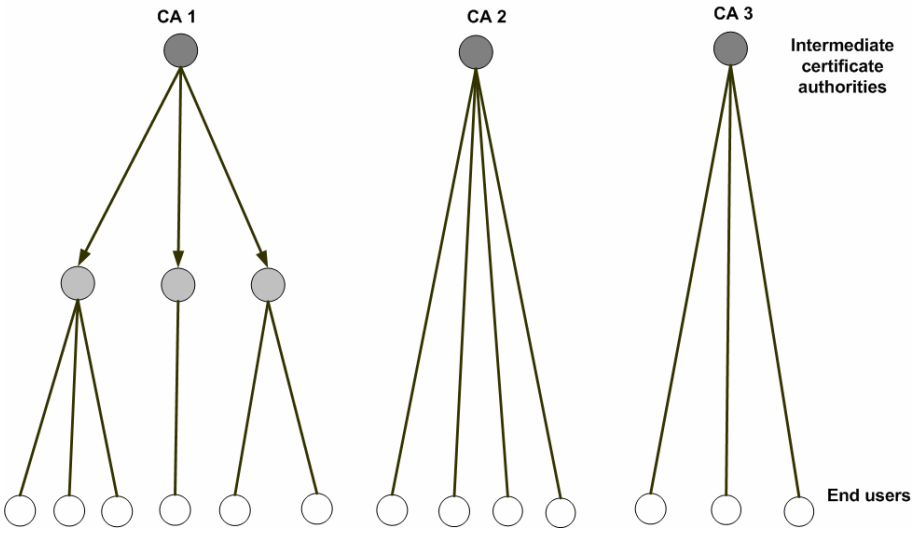

Figure 3 – Web PKI architecture
Рис. 3 – Архитектура Веб PKI
Слика 3 – Веб PKI архитектура

Because this architecture may have an extremely large number of end users, a simple revocation may not be the solution for the case of compromising a key within the certificate, because some browsers do not have a built-in function for checking the revocation list. This means that the user of a browser must be somehow informed of certificate compromising, and that he himself must remove that certificate from the list of trusted certificates in his browser.

The main characteristic of this architecture is that the user decides what certificates he will trust. The Mash PKI architecture (Figure 4) establishes bidirectional peer-to-peer trust relationships in a way that CAs issue certificates to each other (Adams, Lloyd, 2003).

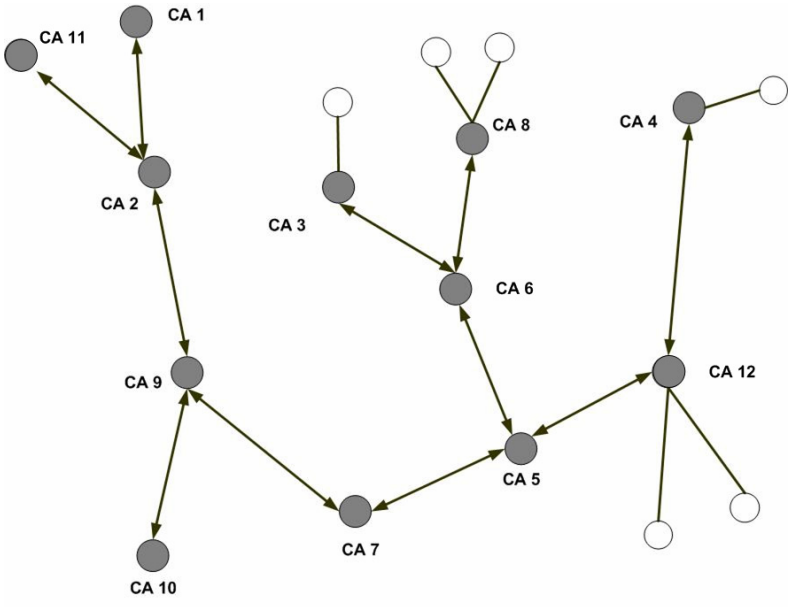

Figure 4 – Mash PKI architecture
Рис. 4 – Сетевая PKI архитектура
Слика 4 – Мрежна PKI архитектура

In this architecture, there are more trust points so compromising any of them wil not influence the functionality of the architecture. In case of compromising one CA, the entities of the other CAs continue to comunicate with the rest of the entities if there is a valid certification path. The compromised CA can be trustful again in the next case: all the certificates issued by this CA have to be revoked, and than the CA issues new certificates signed by a new public key. The CA issues new certificates for the users and the other CAs with whom it establishes relationships.

The last type of the PKI architecture to be mentioned in this paper is the Bridge PKI architecture, shown in Figure 5. The Bridge PKI architecture connects different PKI architectures regardless of architecture, in a way that it introduces a new CA (bridge CA) which establishes peer-to-peer trust relationships with the CAs of the other PKI architectures (Moses, 2003). In the case of a hierarhical PKI architecture, a trust

relationship is established with the root CA, and in the case of a mash PKI architecture with any of CAs.

In this type of the architecture, a compromising CA which establishes trust relationships will influence the abillity of that PKI architecture to achieve secure communication with the other PKI architecture.

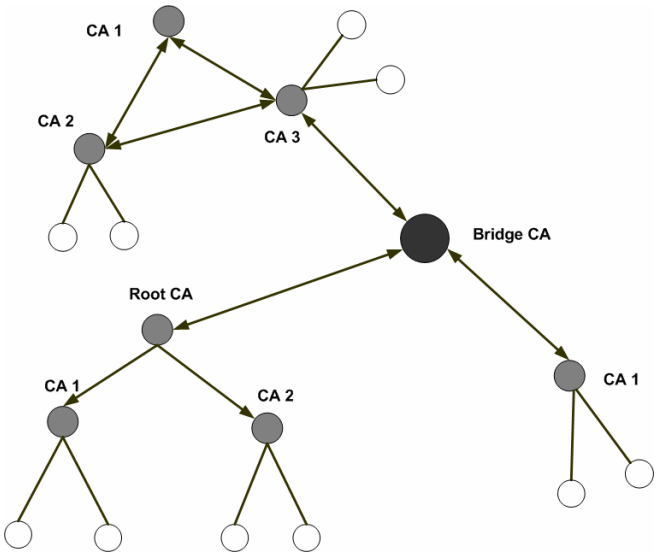

Figure 5 – Bridge PKI architecture
Рис. 5 – Мостовая PKI архитектура
Слика 5 – Мостовна PKI архитектура

The Bridge CA can be compromised completely or partially. Completely compromising means compromising all of the private keys which the bridge CA used for signing certificates issued for the CAs by which trust was established. If the bridge CA uses only one private key for signing certificates by which it establishes a trust relationship, than compromising that key causes a collapse of the whole bridge PKI architecture. Compromising a single private key means only losing the trust with that particular architecture, while the trust between the rest of the architectures stil exists.

Reestablishment of the trust in the case of compromising CA which establishes trust relationships can be accomplished in the way characteristic for the PKI architecture to which that CA belongs. Furthermore, the CA which establishes trust has to revoke a certificate issued by the Bridge CA and to reestablish a new trust relationship with that CA. Reestablishing a trust relationship with the Bridge CA can be accomplished by exchanging certificates.

Cryptographic methods and their failure

PKI architectures use various cryptographic algorithms and techniques for the realization of those algorithms within the protocols they are used in. As previously mentioned, the core of the PKI architecture is based on the implementation of the public key algorithms (Schneier, 1996). It is an accepted practice for one certificate authority to use one public key algorithm while keeping track of the attempts to break that algorithm. Algorithm vulnerability makes the whole architecture which is based on it vulnerable; therefore, hardware devices used for the implementation of cryptographic functions, depending on their price and quality, offer more than one algorithm and several key size options for each of them, their periodic renewal, assuring limited influence in case of accidental or deliberate compromising of any of the keys positioned higher in the hierarchy.

Besides the asymmetric cryptographic algorithms, various hash functions are used in these architectures.

A failure caused by any of these algorithms or functions having been broken, even if the break did not happen within the used system, means the security violation of every PKI system that uses them, and thus represents a critical type of a failure. Recovery after this kind of failure would require the revocation of all certificate authorities within the PKI architecture, the revocation of all certificates issued by it and a new architecture based on more stringent algorithms or longer keys being established.

Hardware cryptographic modules and their failure

HSM (*Hardware Security Module*) are devices characteristic for their use in the PKI architecture, although they are not required for its implementation. In the PKI architecture, these devices enable a safe implementation of cryptographic operations in the process of key generation, certificate signing, while at the same time they provide a safety mechanism against an unauthorized access to it. This mechanism automatically destroys data in the HSM device. It could be argued that the PKI architecture is secure if its keys are secure, and HSM devices provide that security.

All cryptographic operations and key management are stopped as a result of this device failing. This leads to the failure of a certification authority that uses this HSM device. It is often the case that several

certificate authorities are established on the basis of only one HSM device having several slots designated to each certificate authority in the hierarchy, which means that the failure of this device would lead to a failure of the whole architecture. These failures could be classified as temporary, from the standpoint of time needed for recovery from them. It is advisable to have another HSM device ready to be implemented in the structure. This, in turn, requires the existence of specialized procedures for handling these devices and making back up data from them (Souza et. al, 2007). Since these procedures are often treated as internal and thus kept secret, there are not many sources providing more details about them. Because of their value within the PKI architecture, it is clear that these devices are very valuable for the whole PKI architecture and they should be given greater attention which goes beyond the scope of this paper.

Smart cards, as hardware elements enabling data storage and safe execution of cryptographic functions, and by their relatively simple design and application methods, have been vastly implemented among different PKI architectures.

The application of these devices provides double authentication by means of “something you have”, which would be the card itself in this case, and by means of “something you know”, which would be the PIN code that enables card access.

Thus, card access is enabled only by the PIN code known only to the owner of the card, which makes contents of the card and its features limited within the architecture, establishing a higher security level at the same time. It is possible to limit the number of incorrectly typed PIN codes, after which the access to the card will be blocked. This failure is only temporary and it is limited only to the card itself and to the scope of privileges the card holder has.

Failures of these devices caused by minor mechanical damage, when the card is somewhat or completely rendered unusable, are problematic because there could still be some possibility for someone to access the chip content, which is one of the reasons why the smart card validity period is limited and why it is a requirement for their users to return them to the certificate or registration authority for disposal in case of a mechanical damage or card validity expiration.

Failures of individual end user smart cards can be considered to have only minor consequences if the established procedures of smart card handling have been followed after the occurrence of failure.

Conclusion

The PKI architectures can be extremely complex, containing a large number of specialized, as well as general hardware and software components, complicated and expensive for implementation. At the same time, they enable extremely important services such as authentication, integrity, privacy and non-repudiation.

Because of their intricacy and various implementations, a thorough analysis of their failure points is required, as well as the establishment of methods and algorithms for overcoming such failures. This analysis could be conducted by already established methods for the evaluation and simulation of stressful points within the architecture, or by implementing some new methods specifically tailored for this architecture's requirements.

References

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

Chokani, S., Ford, W., Sabett, R., Merrill, C., & Wu, S., 2003. *Internet X. 509 Public Key Infrastructur Certificate Policy and Certification Practices Framework, RFC 3647*.

Moses, T., 2003. *PKI trust models*. Draft. Available at: http://automedicbilling.com/CalculateSavings/PKI_Trust_models.pdf. Accessed: 17 May2016.

Ramović, R., 2005. *Pouzdanost sistema elektronskih, telekomunikacionih i informacionih* Beograd: Katedra za mikroelektroniku i tehničku fiziku (in Serbian).

Schneier, B., 1996. *Applied Cryptography*. John Wiley & Sons.

Souza, T.C.S., Martina, J.E., & Custodio, R.F., 2007. *Audit and backup procedures for Hardware Security Modules, White paper*.

ТОЧКИ ОТКАЗА В PKI АРХИТЕКТУРЕ

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:

За последних двадцать лет, архитектура PKI стала широко применяться, особенно в областях, требующих создания инфраструктуры безопасности. Учитывая, что цель создания такой архитектуры заключается в обеспечении безопасности систем, главными задачами при внедрении архитектуры PKI являются бесперебойная работа и взаимодействие с другими компонентами комплектной структуры. Из вышеизложенного следует, что прогноз потенциальных точек отказа представляет собой исключительно важный фактор. В связи с ограничением объема статьи, и так как речь идет о значительно сложных инфраструктурах, в данной работе представлен лишь общий обзор главных потенциальных точек отказа, без подробного объяснения характеристик по каждому отдельному виду внедрения архитектуры. В статье исследуются общие характеристики PKI архитектур, на основании которых трактуется значение возможных отказов и предлагаются мероприятия по предупреждению и преодолению данного рода проблемы.

Ключевые слова: смарт-карты, криптография, HSM, PK, безопасность, отказ, архитектура.

ТАЧКЕ ОТКАЗА У PKI АРХИТЕКТУРИ

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:

Током последњих 20 година PKI архитектура нашла је широку примену, посебно у областима које су захтевале успостављање сигурносне инфраструктуре. С обзиром на то да се користи ради сигурности јасно је да је њен несметан рад један од основних

захтева који се поставља при њеној имплементацији, а већ самим увидом у бројне типове архитектура и различите имплементације увиђа се њена комплексност. Због тога је разматрање потенцијалних тачака отказа од велике важности. Како се ради о врло сложеним инфраструктурама, овај рад даће само основни преглед тачака које могу бити тачке отказа, без детаља који су карактеристични за поједине примене и типове имплементација.Тражиће се заједничке карактеристике PKI архитектура и на њима објашњавати значај отказа који се могу десити, а тамо где је могуће биће наведени и предлози за њихово превазилажење.

Кључне речи: смарт картице, криптографија, HSM, PK, безбедност, отказ, архитектура.

Paper received on / Дата получения работы / Датум пријема чланка: 14.06.2016.
Manuscript corrections submitted on / Дата получения исправленной версии работы / Датум достављања исправки рукописа: 16.08.2016.
Paper accepted for publishing on / Дата окончательного согласования работы / Датум коначног прихватања чланка за објављивање: 18.08.2016.