UDC 004.41.5

Simulation Analysis of Protected B2B e-Commerce Processes

Zoran V. Živković[1] and Milorad J. Stanojević[2]

[1] The Institute of Applied Mathematics and Electronics, Kneza Miloša 37,
11000 Belgrade, Serbia and Montenegro
ezoran@beotel.yu
[2] Faculty of Transport and Traffic Engineering, Vojvode Stepe 305,
11000 Belgrade, Serbia and Montenegro
milorad@sf.bg.ac.yu

Abstract. In this paper a simulation analysis of certain trust models (complex *PKI* architectures) with regard to the security support of *B2B* applications on the Internet is presented. The objective of such an analysis has been the choice of the most efficient *PKI* architecture and a solution of the cryptographic interoperability problem. A simulation model of protected *B2B* e-commerce has also been presented, based on the chosen *PKI* architecture. This paper has shown the significance of the up-to-date cryptographic mechanisms: digital signature and digital certificate to deliver the main security services based on *PKI*.

1. Introduction

The security of Internet electronic transactions is one of the key factors needed for further e-business development. Online commerce processes demonstrate particular sensitivity to security problems. Development of Internet local networks has brought about an increase in security risks and threats that may jeopardize supply and demand, especially payment procedures in on-line commerce. Hence, customers and traders are often preoccupied with the problem of electronic transactions security.

Various cryptographic techniques have been adopted, in addition to physical technical and organizational protection measures to solve this problem. They are based on modern cryptographic systems and mechanisms. By skillfully combining available cryptographic systems and mechanisms it is possible to build an adequate cryptographic architecture and offer several basic security services: *confidentiality (privacy), authentication, check on the integrity and non-repudiation of the electronic transactions activities* [10].

An efficient and integral application of the above-mentioned security services can be achieved by using a technology based on the Public Key Infrastructure (*PKI)*. Besides, it enables digital signing for sensitive electronic transactions and their exchange with a signatory digital certificate. However, in *PKI* services and certifications, the traditional bilateral communication model is assigned to an independent trusting party, (Certification Authority, *CA*), which represents a *PKI* basic component. There is an additional complexity in the standard communication model due to the need for validation of a user's certificate status. With this objective in mind, the introduction of a required validation authority (VA), as the *PKI* additional component, is necessary. An increasing number of users with certificates and diversity of their business interests may override capabilities of a single *CA*. Therefore, a greater number of CA_s is being set up and they represent the trust points for users' communities. Mutual businesses interests of the users from different *CA* domains form complex PKI_s with more complex structures than one *CA*. The main problem of such structures relates to the arrangement of the trust relationship between particular CA_s within *PKI*, known as the *cryptographic interoperability.* To solve this problem there are three main trust models: *hierarchical, mesh* and *bridge trust models* and their possible combinations.

A general aspect of individual trust models has been presented in [4], [8], and [9]. The second analysis approach has been based on simulation modeling and it gives specific information on the choice of a more efficient trust model and the solution of the cryptographic interoperability problem. This approach has been used in [11], [12], and [14].

A simulation modeling approach in the analysis of the cryptographic interoperability problem has also been presented in this paper. Two trust models have been analyzed: hierarchical and bridge, in electronic payments for Business-to-Business *(B2B)* applications. A comparative analysis of the presented models has determined the choice of the most efficient model. The simulation model of the protected *B2B* electronic commerce on the basis of the selected trust model has also been presented. The simulation models have been developed in simulation language *GPSS/H* [6]. The obtained results show the efficiency of the selected trust model essential functions: *cross-certification* and *validation of the certification paths.*

2. The Protected B2B Electronic Commerce

Internet technology has been instrumental in transforming traditional forms of selling goods and services into electronic ones. Electronic commerce has become an efficient method of regulating supply and demand. Business-to-Business applications represent currently a dominant form of on-line electronic commerce. Economic interests of organizations and dynamic relationships in their contacts with business partners have shown that the model *B2B* of electronic commerce contributes to an increased production, lower costs in business processes and an efficient surplus product management. Business relationships among business partners can be frequently disrupted and then reestablished, primarily because of economic interests. In this respect *B2B* offers extraordinary support. On the other hand, besides the obvious advantages, this application represents a source of sensitive information, continuously confronted with security risks, threats and attacks [8].

There are several methods to protect local systems used in *B2B* applications. One of them is the introduction of firewalls protecting the local systems from hackers and similar outside sources. A more secure protection method has been based on a cryptographic mechanism of enciphering all information stored in a local system and their deciphering by authorized users in the work process. This method is of paramount importance for secure communication since it enables enciphered transmission of data through *cryptographic tunnels* on the Internet. By using a cryptographic tunnel technique, virtual private networks (*VPN*) can be developed to maintain privacy in the course of communication.

Further development of on-line electronic transactions security has led to the establishment of electronic commerce protection at the application level. It is based on the cryptographic mechanisms and protocols by which *privacy, authentication, integrity* and *non-repudiation* in a network environment have been established. The best known standard solutions of this type are: Secure Sockets Layer protocol (*SSL*), Private Communication Technology protocol (*PCT*), Transport Secure Layer protocol (*TSL*), Secure Hypertext Transport Protocol (*S-HTTP*), Secure Electronic Transactions (*SET*) and others [7].

Modern cryptography consists of a variety of different cryptographic algorithms and systems, which can be used to create adequate cryptographic mechanisms and protocols, aimed at the support of the above security services [2]. In order to maintain privacy in a communication channel between the client and server, in terms of greater security and work speed, the enciphering and deciphering mechanisms with symmetrical properties have been recommended: Data Encryption Standard (*DES*), Advanced Encryption Standard (*AES*) and others. For the *B2B* subjects (entities), besides privacy in communication, of great importance are the matters concerning validity of subject identity/transaction origin, validity of transaction integrity and inability of repudiation of electronic transactions exchange. The digital signature and the digital certificate represent cryptographic mechanisms, based on the asymmetric cryptosystem properties, which support the above services in a secure way. In practice, the digital signature of electronic transactions is required from the sending party and the digital signature verification from the receiving party (relying party), whereby the digital certificate of the transaction signatory is used [7].

The degree of a relying party trust is based, besides the above mentioned factors, on the certificate validity. For significant financial transactions, the certificate validity has a key role. The digital certificates are issued with a limited validity period (e.g. from 2 to 5 years). However, the certificate validity period may expire even before the agreed period (loss of the certificate, name changes, compromising of a key, etc.). In such cases they are reported invalid and are entered into the certificate revocation list (*CRL*). A possibility of manipulating invalid certificates represents an additional security risk. Hence any security system based on certificates, without certificate status validation is in itself incomplete and insecure. In this respect an additional function of certificate validation status is needed, in order to secure the *overall trust* regardless of an application, *CA* or the physical location of users [7].

The above mechanisms for secure exchange of electronic transactions function efficiently within a modern technology based on a public key infrastructure (*PKI*). In essence, a *PKI* represents a group of hardware, software, people, policies and procedures necessary for generation, management, storage, distribution and revocation of certificates [5].

The main functions of protected *B2B* electronic commerce can be presented by a simplified model as shown in Fig. 1.

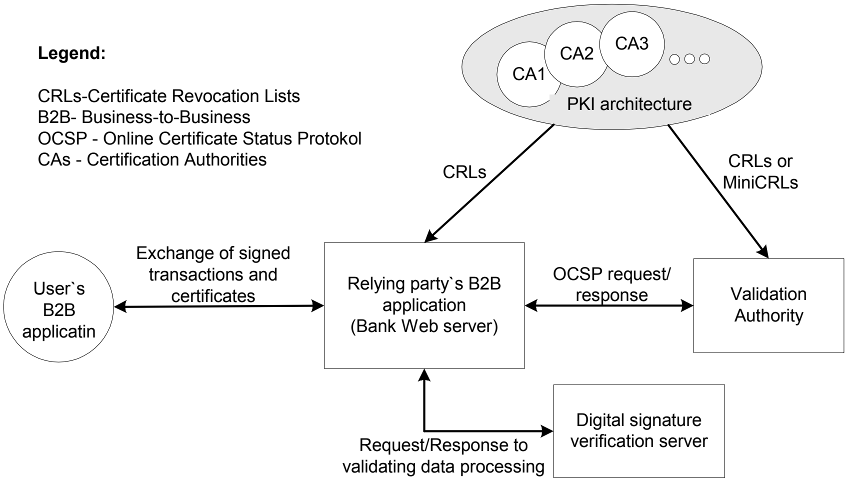
Legend:
CRLs-Certificate Revocation Lists
B2B- Business-to-Business
OCSP - Online Certificate Status Protokol
CAs - Certification Authorities
CA1
CA2
CA3
PKI architecture
CRLs
CRLs or MiniCRLs
Exchange of signed transactions and certificates
User`s B2B applicatin
Relying party`s B2B application (Bank Web server)
OCSP request/ response
Validation Authority
Digital signature verification server
Request/Response to validating data processing

Fig. 1. Protected *B2B* e-commerce

A commerce bank delivers financial services to the users (organizations) in a process of *B2B* electronic commerce. In order to enhance the security of electronic transactions the bank considers an appropriate *PKI* architecture. The certified users aided by the bank Web server make their choice of the transaction type (purchase/selling, the number of stocks, price per stock and other options). The bank Web server requests each transaction to be digitally signed and presented with the user's digital certificate. The validation authority task is primarily to verify the certificate digital signature and subsequently to validate its status and finally it is possible to verify the digital signature of the transactions itself. A validation procedure in the application of the relying party is performed by an additional server for digital signatures verification (Fig. 1) [7].

3. Complex Public Key Infrastructures

There are a number of factors that play a role in selection of an appropriate *PKI* architecture to support a given application (Fig. 1). Political and economic interests of some users` communities represent only starting points for selection of an appropriate *PKI* architecture. Besides, a growing number of *PKI* users may additionally increase the complexity of a *PKI* architecture: lengthening of *PKI* paths, increasing the number of certificates, overloading of the certificate status validation system and so on.

In a given model (Fig. 1) the financial institution management introduces a protected *B2B* application with a number of users ranging from several thousands to several dozen thousands. The topology of the discussed *PKI* architecture is to a great extent affected by the geographical distribution of potential *PKI* users. Given the specific conditions, the protected *B2B* application exceeds the *PKI* architecture possibilities with a uniform *CA*. That is why more complex *PKI* architectures are being considered: hierarchical, mesh and bridge architectures [8], [9].

We will consider a hierarchical *PKI* architecture that contains one root *CA* and ten subordinate CA_s (Fig. 2).

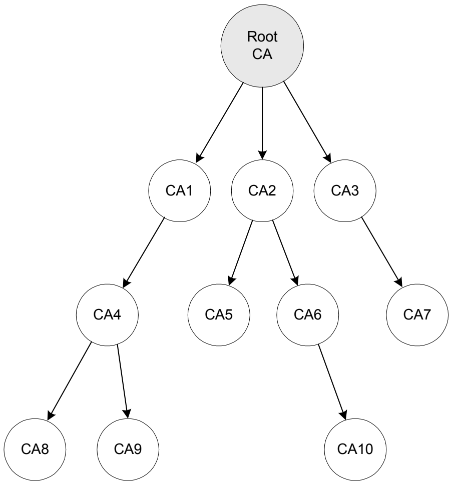

Fig. 2. Evaluated hierarchical *PKI*

In the reviewed hierarchical *PKI* architecture all users have trust in the root *CA*. The trust relationship has been defined unilaterally, from root *CA* to the end user. The end users obtain certificates from their CA_s (CA_1, CA_2,..., CA_{10}) while at the same time they obtain certificates from the root *CA* (cross certificates). The certification paths always start with the public key of the root

CA. The longest path equals the tree depth plus one. The principal weakness of this architecture lies in the fact that the central trust comes from just one point. Thus, bearing this in mind, compromising of the root *CA* leads to compromising of the entire *PKI* [8], [9].

The second solution to the cryptographic interoperability problem is based on the establishment of the peer-to-peer trust relationship between CA_s. These PKI_s are called mesh PKI_s [8], [9]. With these PKI_s there is no uniform trust point; each *CA* is a trust point for its users. The peer-to-peer relationships between CA_s have been regulated by mutual issuance of cross certificates. In case of ones CA being compromised there is no danger of compromising the entire *PKI*. The principal weakness of the mesh *PKI* architecture lies in the fact that there should be a large number of certificates between CA_s (cross certificates). This problem is known under the name *N*-squared *(N^2)* problem. *N* CA_s require *N(N-1)/2* cross certificates. For example, for 300 CA_s we need 44850 certificates between all CA_s [7].

A significantly more practical solution can be obtained in a case when in a mesh *PKI* one *CA* is pronounced a central (bridge), and all others are being cross certificated with it. In this way we obtain a bridge *PKI* architecture, whereby, among other things, the problem of a large number of certificates is being solved; for 300 CA_s it is necessary to have only 300 cross certificates, or generally *N* cross certificates (Fig. 3) [7].

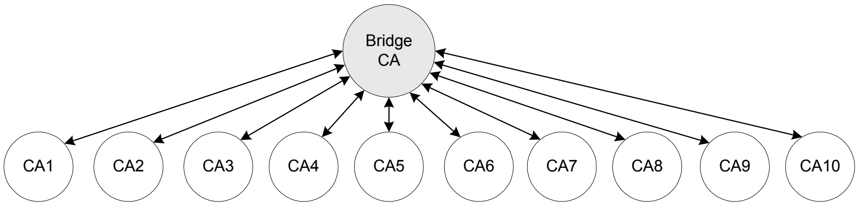

Fig. 3. Evaluated *BCA PKI*

The bridge *CA* represents the “trust bridge” between individual users within different CA_s, not the trusting point. It establishes the peer-to-peer relationships with all CA_s based on the mutual issuance of cross certificates. In contrast to the mesh *PKI* architecture, the bridge *PKI* architecture features shorter certificate paths, and their identification is simpler [8].

4. Simulation Analysis of the Trust Model in Public Key Complex Infrastructures

In this paper we consider one of possible approaches to the problem of selecting a suitable *PKI* architecture for a given application (in our case *B2B*). The analysis is based on the previously described properties of *PKI* architectures [11]. *The number of validated certificates in a time unit* has been adopted as the selection criterion. The two trust models have been analyzed: hierarchical and bridge (Figs. 2 and 3). The simulation model is developed under the following assumptions:

- given hierarchical trust model with root *CA* and ten subordinate *CA*$_s$, (see Fig. 2);
- given *BCA* trust model with one *BCA* and ten peer-to-peer *CA*$_s$, (see Fig. 3);
- the number of requests for certificate validation: 1, 2, 3, 4 and 5 requests/s;
- the digital signature verification time: 40 ± 5 ms;
- type of status certificate validation: *CRL*;
- the issuance policy *CRL*$_S$: one *CRL* per day.

The certificate validation server in the application of the relying party has been modeled as the queuing system [12]. The users initiate signed transactions with their own certificates issued by their *CA*$_s$, according to Poison's distribution with different frequencies of requests for certificate validation (1, 2, 3, 4, 5 requests/s). In both trust models the following validation procedures have been analyzed (figure 6):

- the certificate chain verification on individual certification paths;
- down-loading of *CRL*$_s$ from individual *CA*$_s$ in accordance with the proclaimed policy;
- the *CRL*$_s$ digital signature verification;
- searching of *CRL*$_s$.

Simulation lasted 24 hours, with 1 ms time unit. On the basis of the obtained results the following conclusions can be drawn can be concluded:

- in the hierarchical trust model (Fig. 4) the total number of 86659/173698/261008/347339/417565 has been validated with the request frequency of 1/2/3/4/5 requests/s respectively. Out of this number, in the time period of 100 ms 23392/46800/70424/86027/87810 certificates have been validated; in the time period of 200 ms 23614/51215/83963/118382/144113 certificates have been validated; in the time period of 250 ms 1/3/4/5/4 certificates have been validated and in the time period of 300 ms 0/1/2/3/5 certificates have been validated (Fig. 4);

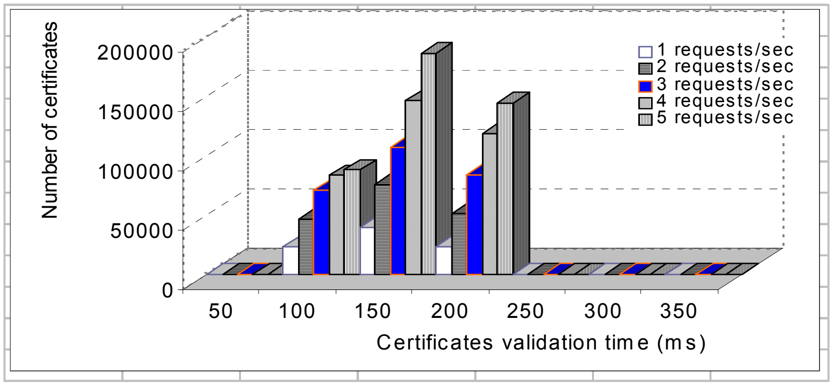

Fig. 4. Distribution of the total validation time in a hierarchical *PKI*

- in the bridge trust model (Fig. 5) a total of 86659/173698/261008/347339/417565 certificates have been validated with the request frequency of 1/2/3/4/5 respectively. Out of this number, in the time period of 100 ms, 86656/173688/260996/309195/324780 certificates have been validated; in the time period of 150 ms 3/1/3/38132/92777 certificates have been validated; in the time period of 200 ms 0/9/9/7/2 certificates have been validated and in the time period of 250 ms 0/0/0/5/6 certificates have been validated (Fig. 5);

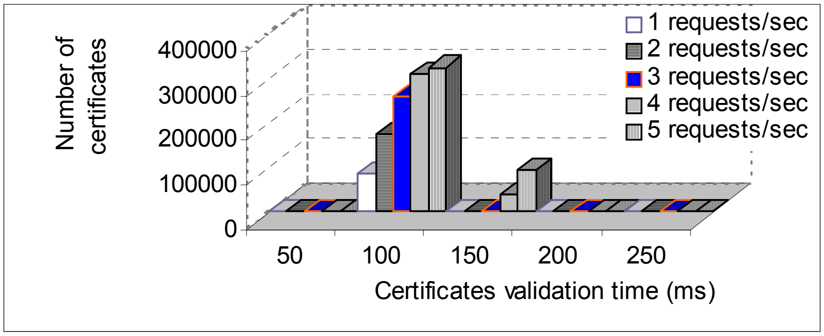

Fig. 5. Distribution of the total validation times in bridge *PKI*

- obtained results show that the largest number of certifications have been validated in the shortest time in the bridge trust model (Fig. 5), while in the hierarchical trust model this procedure lasted longer (Fig. 4).

In given simulation models there are a larger number of random variables. The random value generation can be carried out by using modifications in the interval form, i.e. spreading (uniform distribution). However, when applying simulation language *GPSS/H,* the problem of transparency occurs, which has been taken care of by using different strings of random number generators with all types of initial values. Because of this the changes occurring in one part of a model do not affect the performance of other parts of the model, since the sources of randomness in the model are statistically independent [1].

In this paper the experimentation has been made with the models with the aim of testing the effects of random variables variability according to the experiment plan. Six independent realizations of each model have been assumed by the experiment plan. In each realization care was taken of the statistical independence by using different, independent strings of random numbers for each of the random variables. The obtained results represent mean values of all six realizations, which yield more trustworthy simulation results, shown in the histograms in Figs. 4 and 5.

5. The Simulation Model of Protected B2B Electronic Commerce

In publicly accessible literature the standard methods for overall functionality analysis in this domain have not been reported. An approach to the analysis of the functioning of protected *B2B* application based on the simulation modeling has been presented in [13]. In this paper we applied a simulation procedure based on experimenting with a real system computer model. The objective is to gather information so that the efficiency of a particular *PKI* architecture when protecting *B2B* electronic commerce can be analyzed.

In the given model, the validation process has been analyzed which, apart from validation procedures mentioned in Section 4, also comprises digital verification signatures in the transactions themselves (Fig. 6). The bridge *PKI* with six CA_s has been analyzed. The users initiate the signed transactions with their own certificates issued by their CA_s, according the Poison's distribution with different arrival frequencies (1/2/3/4/5 requests per second). The number of certificated users is different within individual CA_s, and the number of revoked certificates is 17% in comparison with the total number of users in particular CA_s. In the validation procedure the comparison of initiated user's' certificate with revoked certificates in CRL_s is being made. In the case of identity, the initiated certificate is rejected and the corresponding transaction is regarded as invalid (Fig. 6).

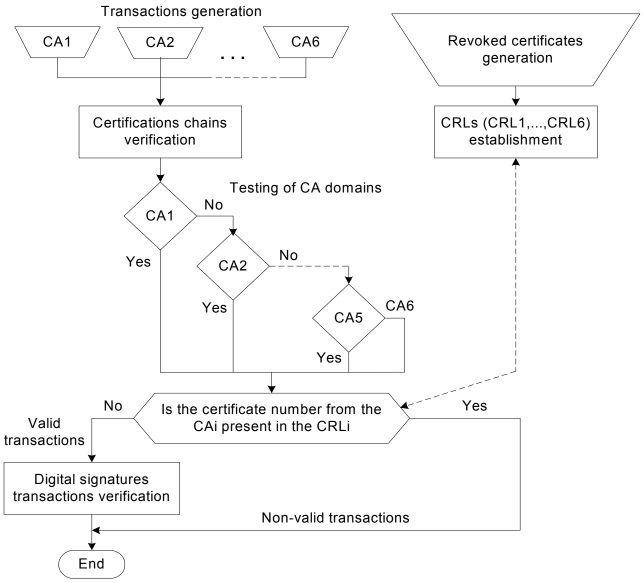
Transactions generation
CA1
CA2
...
CA6
Revoked certificates generation
Certifications chains verification
CRLs (CRL1,...,CRL6) establishment
Testing of CA domains
CA1
No
Yes
CA2
No
Yes
CA5
CA6
Yes
No
Is the certificate number from the CAi present in the CRLi
Yes
Valid transactions
Digital signatures transactions verification
Non-valid transactions
End

Fig. 6. Flow chart of protected *B2B* application

The total number of valid and invalid transactions has been evaluated. In particular, the number of origin and destination transactions according to individual CA_s with regard to the total number of valid transactions has been shown. The performed simulation lasted 24 hours, with 1 ms time unit [13].

On the basis of the obtained results the following conclusions can be drawn:

- in the course of simulation the maximal number of the valid transactions has been registered with the maximal arrival frequency and it is 441755 transactions, minimal number of valid transactions has been registered with the minimal arrival frequency and it is 88621 transactions (Fig. 7);

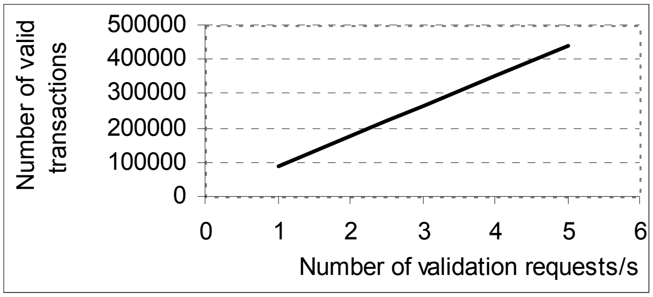

Fig. 7. Total number of valid transactions

- for individual *CA* domains (CA_1, CA_2, …, CA_6) the distribution numbers of valid transactions were: 20%, 12%, 15%, 25%, 10% and 18%, respectively. The largest number of valid transactions was initiated from CA_4, and the least number from CA_5 domain, which has been shown in Fig 8;

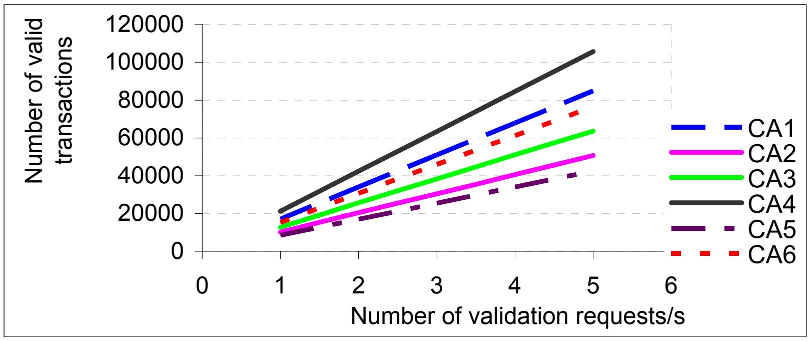

Fig. 8. Total number of origin valid transactions

- for individual *CA* domains (CA_1, CA_2, …, CA_6) the following distribution number of valid transaction were chosen: 12%, 20%, 18%, 10%, 25% and 15%, respectively. The largest number of valid transactions had its destinations in domains CA_5, CA_2... which has been shown in Fig. 9. The ratio of the origin and destination valid transaction numbers according to the separate *CA* domains represents the result of one of the possible solutions for choosing the origin and destination *CA* domains;

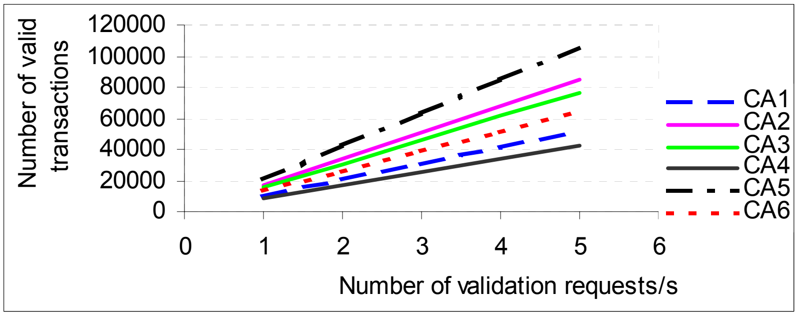

Fig. 9. Total number of destination valid transactions

- the largest number of invalid transactions due to the revoked certificates has been registered with the maximal arrival frequency and it is 7869 transactions, while smallest the number of invalid transactions was registered with the minimal arrival frequency - 1858 transactions (Fig. 10);

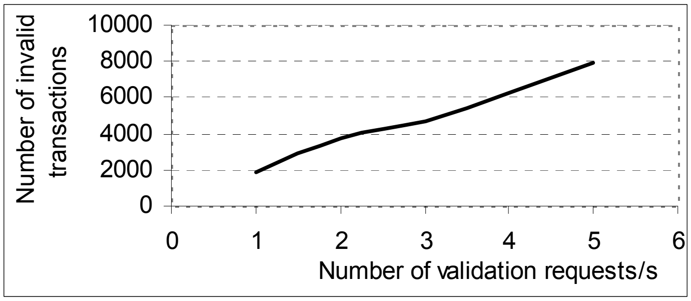

Fig. 10. Total number of invalid transactions

- the obtained results show the validation efficiency and detection performance of the invalid transactions based on the digital signature and the certificate.

In this simulation model care has also been taken of the statistical independence as in the previous ones.

6. Discussion

The presented simulation results of complex PKI architectures, refer to specific architectures with specific topologies. A hierarchical PKI consists of four levels (0,1,2,3). Root CA operates on level 0, while 3, 4 and 3 subordinate CAs operate on levels 1, 2 and 3, respectively (Fig. 2). A bridge trust model contains a bridge CA and ten peer-to-peer CAs operating on the same level (Fig. 3).

Based on the chosen selection criteria for an efficient PKI architecture, in a given B2B application, and obtained simulation results, we can draw the following conclusions.

- increasing the number of levels in a hierarchical PKI, certification paths become longer and thus the number of certificates in them increases. In this case, it is expected that the total number of validated certificates will be distributed among a larger number of classes (Fig. 4). The distribution of validated certificates within individual classes will be carried out according to the number of CAs at individual levels and the number of PKI users within individual CAs. Increasing the CA number of higher levels as well as the respective PKI numbers, is expected to result in an increase of the number of validated certificates at higher frequency classes and vice versa.
- in a bridge PKI architecture, an architecture expansion, due to new CAs, occurs at the same level. As a result, the certification path length and the corresponding certificate number, remain constant. This will ensure that the distribution of the validated certificate numbers will remain within the defined classes (Fig. 5), regardless of the increase of the CA and PKI user numbers.

The developed simulation models are not sensitive to the input data, but the obtained results will depend on them. The developed models can generate, in a simple manner, results for various certificate number distributions in individual CA domains, different percentages of nonvalid certificates in individual CA domains, as well as for various levels of validation requests. Furthermore, the models are flexible relative to various numbers of hierarchical levels and numbers of CAs at individual levels.

Simulation experiments have shown that the same results are obtained for various PKI architectures, numbers of CAs and hierarchical depths. This indicates that the bridge architecture is more efficient than the hierarchical one, according to the selection criterion.

In addition, the experiments have shown that the various levels of validation requests and various user distributions among individual CA domains, always result in corresponding linearity trends. In this paper the PKI architecture analysis has been carried out with regard to one possible criterion. Research in this area could be extended by considering some other efficiency criteria in complex PKI architectures.

7. Conclusion

Further development of business Internet based applications is jeopardized by increased security risks, threats and attacks. Efficient security policy measures are needed to minimize these risks.

Cryptographic security measures yield an efficient solution for this problem. Encryption, decryption, digital signature and digital certificate represent secure cryptographic mechanisms for application in basic security services and they are presented in this paper. Their functionality comes to the fore within *PKI* technology. However, by introducing *PKI* the complexity of communication models with regard to the traditional ones is also increased. With an increased number of certification authorities and the number of *PKI* users within complex PKI_S, it is necessary to analyze efficiency of possible trust models and status certificates validation. Such analyses provide a solution to the problem of cryptographic interoperability and functionality of *PKI*.

We have shown a computer simulation application of the functional analysis and selection of an efficient trust model, within a *B2B* application. Two simulation models have been developed: for hierarchical and bridge *PKI* analysis. The obtained results may serve as a valid measure when selecting efficient *PKI* architectures for the security support in *B2B* applications. The simulation model has also been developed for the protected *B2B* electronic commerce, on the basis of which it is possible to analyze more efficiently operation of *PKI* architectures. In developing the simulation models care has been taken of the transparent sample-taking problem, as well as of the statistical independence in the simulation process.

8. References

1. Radenković, B., Stanojević, M., Marković, A.: Computer Simulation. Faculty of Organizational Sciences, Faculty of Transport and Traffic Engineering, Belgrade. (1999) (In Serbian)
2. Stinson, D.: Cryptography Theory and Practice, Second Edition. Chapman and Hall/CRC, A CRC Press Company. (2002)
3. Weise, J.: Public Key Infrastructure Overview. Sun Microsystems, Inc., California U.S.A. (August 2001)
4. Klepzig, K.: Modeling and Simulation of Public Key Infrastructure Applications. SANS Institute. (2003)
5. Kiran, S., Larean, P., Lloyd, S.: PKI Basics – A Technical Perspective. *PK*I Forum Note. (November 2002)
6. Schriber, T.: An Introduction to Simulation Using GPSS/H. John Wiley&Sons, New York. (1991)
7. Austin, T.: PKI. John Wiley&Sons, Inc, New York. (2001)

8. Polk, W., Hastings, N.: Bridge Certification Authorities: Connecting *B2B* Public Key Infrastructures. White paper, US National Institute of Standards and Technology. (2001)
9. Polk, W., Hastings, N.: Public Key Infrastructures that Satisfy Security Goals. US National Institute of Standards and Technology, Department of Commerce. (2003)
10. Živković, Z., Unkašević, T.: Security of Web Commerce. XLVII Conference for Electronics, Telecommunications, Computers, Automation, and Nuclear Engineering, ETRAN 2003, Proceedings, Herceg Novi, Serbia and Montenegro. (June 2003) (In Serbian)
11. Živković, Z., Stanojević, M.: The Simulation Analysis of e-Business Activities Based on the PKI. INFO M, Vol 3, No 10, Beograd. (2004) (In Serbian)
12. Živković, Z., Stanojević, M.: Selection of Efficient Trust Model in Complex *PKI*. The 10th Symposium on computer sciences and information technologies, YU Info 2004, Proceedings (CD), YU Info Association, Kopaonik, Serbia and Montenegro. (March 2004) (In Serbian)
13. Živković, Z., Stanojević, M.: The Simulation Analysis of e-Commerce Processes based on Complex *PKI*. XLVIII Conference for Electronics, Telecommunications, Computers, Automation, and Nuclear Engineering, ETRAN 2004, Proceedings, Čačak, Serbia and Montenegro. (June 2004) (In Serbian)
14. Živković, Z., Stanojević, M., Radenković, B.: The Simulation Model of Protection Operating in Electronic Business. XXXI Symposium on Operations Research, SYMOPIS, Proceedings, pp. 45-50, Fruška Gora, Serbia and Montenegro. (2004) (In Serbian)

Zoran V. Živković, received the B.Sc. degree in 1977 from Technical Military Academy of Zagreb and M.Sc. degree in 2005 from the University of Belgrade, Faculty of Transport and Traffic Engineering, Department of the Telecommunication Traffic. He is Assistant General Director of Institute for Applied Mathematics and Electronic of Belgrade. Also, he works as researcher in field of electronic transactions protection in electronic business on Internet. He is author of over 10 scientific and expert papers.

Milorad J. Stanojević received the B.Sc. degree in 1973 from the University of Niš, Serbia and Montenegro, and the M.Sc. and Ph.D degrees in 1981 and 1991, repectively, from University of Belgrade, Serbia and Montenegro. Since 1976, he has been with the Faculty of Transport and Traffic Engineering, University of Belgrade, where he is currently Associate Professor of traffic and transport cybernetics and computer simulation. He published a number of scientific papers and a book Computer Simulation (Belgrade, Serbia and Montenegro:University Press, 1999). His research interests include estimation, prediction, control, and simulation methods in traffic engineering