The 7th Balkan Conference on Operational Research
"BACOR 05"
Constanta, May 2005, Romania

THE ANALYSIS OF THE VALIDATION CERTIFICATE STATUS TIME IN THE PUBLIC KEY COMPLEX INFRASTRUCTURES

ZORAN V. ŽIVKOVIĆ
The Institute of Applied Mathematics and Electronics, Belgrade, Serbia and Montenegro

MILORAD J. STANOJEVIĆ
Faculty of Transport and Traffic Engineering, Belgrade, Serbia and Montenegro

BOŽIDAR RADENKOVIĆ
Faculty of Organizational Science, Belgrade, Serbia and Montenegro

---

Abstract
The modern approach to the electronically transactions security in e-business applications implies synthesized application of the cryptographic systems and mechanisms within the public key infrastructure (PKI). Digital certificate of an e-business subject (user) represents a cryptographic mechanism with the highest security level.
Since every PKI transaction security has been based on the temporary certificate status (valid, revoked), the certificate status must be checked for each transaction. An average time of this demanding operation can be decisive for the PKI acceptability. In this paper the analysis of the factors affecting the validation time and the presented simulation model for its determination has been done. The hierarchical and bridge PKI architectures supporting the B2B application have been analyzed.

Keywords*: Public Key infrastructure, Certificate, Validation, Simulation analysis*

INTRODUCTION

Within the E-commerce business applications on Internet the electronic transactions protection acquires an increasing significance. The key requirements of the E-business authorities are: securing the transactions privacy (confidentiality), checking the authorities` and transactions authenticity, checking the transactions integrity and non-repudiation of transactions exchange. The application of the modern cryptographic algorithms and systems makes it possible to develop such cryptographic mechanisms as enciphering and deciphering, digital signature and digital certificate. With the adequate cryptographic protocols it is possible to bring about the functionality of the mentioned mechanisms required to meet the established security needs.

The process of the secure exchange of electronic transactions is being carried out within the secure architecture based on cryptography (*POI*). In essence, *POI* represents a set of hardware, software, people, policies and procedures required to generate, manage, store, distribute and revoke certificates [1].

Within the procedures of establishing confidence between the E-commerce entities, the status certificate validation represents the highest level of security, while at the same time implies the most demanding operation in terms of time. In case the average time of duration of this operation is relatively long, the E-commerce entities can abandon such *POI* application. Thus, the validation time of the certificate status is a very significant parameter of *POI* application efficiency.

In literature there are suitable solutions for more efficient status cerificate validation in complex *PKI* architectures. The simulation analysis of an adequate hierarchical PKI, on the basis of nested certificates, presented in [2], has shown the approximate increase in validation time speed of certificate path as many as 2,3 to 2,5 times, depending on the applied cryptosystems and hash algorithms. However, the total number of the certificates has been increased as many as 3,85 times. The mathematical model describing the demands speed of status certificate validation, defines the demands speed within various validation methods: based on *CRL* (Certificate Revocation List, segmentzed *CRLs*, more frequent *CRLs* issuance and delta *CRL*. Due to this model it can be proved that the most efficient solution is possible with the delta *CRL* validation [3], [4].

The appraisals of the problem of status certificate validation efficiency given in [2], [3] and [4] did not include the various *PKI* architectures impacts, neither did they comprise the specific features of the applications themselves, though the significance of their impact was pointed out. Consequently, in this paper the more in-depth analysis of the cerificate status time validation has been done. The impacts of the hierarchical and bridge *PKI* architectures with *CRL* and *OCSP+MiniCRL* (Online Certificate Status Protocol, *OCSP*) validation on the average validation time in *B2B* application have been analysed. In the analysis the simulation approach has been used and an adequate model for determining the average validation time of certificate status validation time has been given.

1. THE B2B E-COMMERCE PROTECTION

For the analysis of *PKI* application impact on the certificate status validation time has been shown a *B2B* application of a financial institution rendering financial services to

its clients in the process of *B2B* E-commerce. By means of the Web-server the clients (organisations) can select the transaction type (purchasing/selling), the number of stocks, value of a stock and some other options (figure 1). To protect the transaction privacy, checking of entities` authenticity and transactions themselves, checking of transactions integrity and non-repudiation of transactions exchanges between the transaction entities and the relying party (Web server), in the process of payment, the two *PKI* architectures are being analysed: hierarchical and bridge, and within each of them *CRL* and *OCSP+MiniCRL* certificate status validation is also being analysed. The objective of this analysis is to show the impact of the selected *PKI* architectures and validation methods on the average time of certificate status validation.

The corresponding scenario for the analysis presupposes that at each transaction the Web server requests from the financial institution to be digitally signed and presented with the digital certificate of the transaction entity. At the beginning the relying party verifies the certificate digital signature, and, consequently, on the basis of the validation data, obtained from *CA* in the form of *CRL*, or from Validation Authority (*VA*) in the form of the validation response, checks the certificate status (valid/revoked).

In case the certificate is valid, the procedure of paying is continued, otherwise the transaction is cancelled. The relying party performs the validation process of certificate status with an additional server for digital signature verification (figure 1) [5].

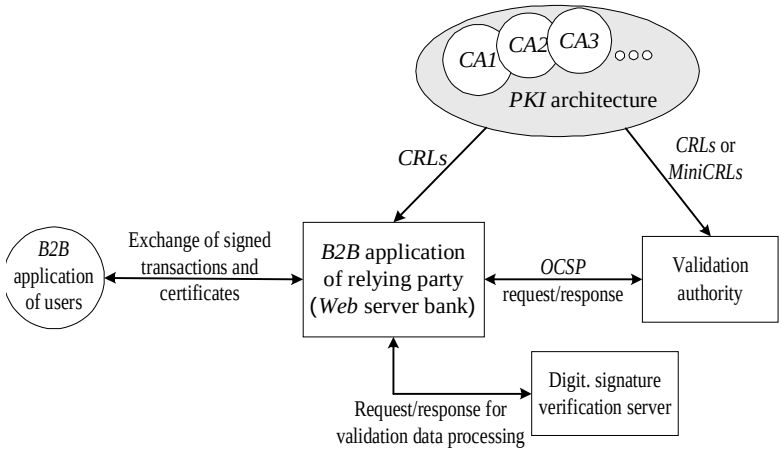

Figure 1 Protected B2B electronic commerce

In the analysis the two *PKI* architectures have been used: hierarchical and bridge architecture. Their topology is proportionate to the potential number of *PK*I users (from 10000 to several hundred thousands) and to the geographical dispersion of the users. The hierarchical architecture comprises the root *CA* and ten subordinate *CA*s (figure 2). The confidence relations of the root and subordinate *CA*s have been one-way defined, starting with the root *CA* and further on to the last one in the hierarchy. The root *CA* issues the certificates to its subordinate *CA*s. All subordinate *CA*s issue the certificate to their users and their subordinate *CA*s. Based on this, a confidence chain to any of the users in the hierarchy always starts from the root *CA*, through the subordinate *CA*s and further on to a

user. To each confidence chain corresponds a certain confidence chain along the certificate paths [5], [10].

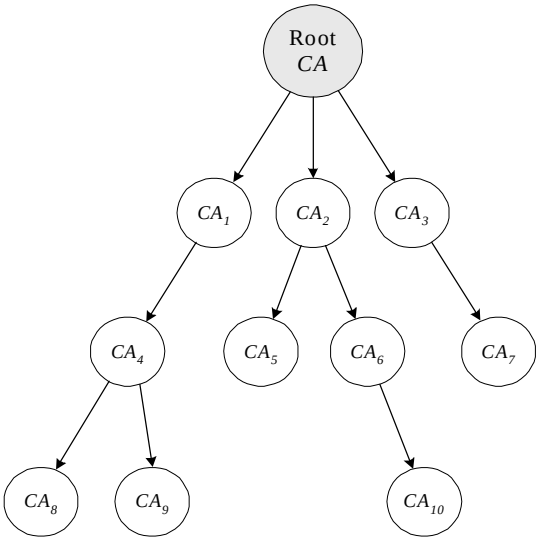

Figure 2 Hierarchical PKI architecture

In the given hierarchy it is possible to set up ten different certificate paths (from the root *CA* to ten different users` *CA* domains). In the *B2B* application, the root *CA* operates in the centre of the financial institution and enables it to (as relying party) receive and carries out financial transactions in order to meet its clients` needs from separate *CA*-domains. The number of the certificates along each of the certificate path (the root *CA*-CA_1-user, root *CA*-CA_2-user, …. , root *CA*-CA_2-CA_6-CA_{10}-user) totals 2,2,2,3,3,3,3,4,4,4, respectively.

The other *PKI* architecture taken into consideration is the bridge architecture. It is obtained when one certificate authority pronounces itself the central (bridge) authority and all others are being cross-certified with it (figure 3). The confidence relations between the bridge *CA* and other *CA*s are two-way relations. The bridge *CA* represents `confidence bridge` between users from individual users` *CA* domains, instead of the `confidence point` in case of the hierarchical architecture. In a given *B2B* application the bridge *CA* operates in the centre of the financial institution as well as the root *CA* in the hierarchical architecture. In each confidence chain between the relying party and any user it is possible to establish ten certificate paths with 2 certificates respectively on each one of them (one cross -certificate between the bridge and end *CA* and one user` s certificate, issued from the appropriate *CA*).

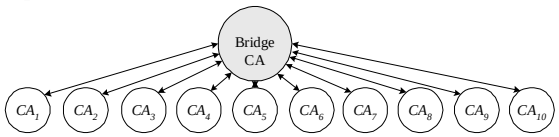

Figure 3 Bridge PKI architecture

2. THE SIMULATION MODEL OF THE CERTIFICATE STATUS VALIDATION TIME

At the moment there are two approaches defining the relying party obtaining the validation data on the certificate status: the revoked certificates lists (*CRL*) and online protocol for the certificate status (*OCSP*), shown on figure 1.

The first approach uses the digitally signed *CRL*s which are periodically issued by *CA*s. The listing size per one revoked certificate in *CRL* is 20-25 Bytes. With the increased number of *PKI* users increases the number of the revoked certificates as well, and accordingly the sizes of individual *CRL*s. The period of time in the course of which *CRL*s are being taken over by CAs and sent to the relying party application (t_{down}) is directly proportionate to the *CRL* size and is in inverted proportion to the transmission speed. After receiving each *CRL*, the relying party performs *CRL* digital signature verification in order to check their integrity (figure 4). For this operation a certain time is required (t_{vercrl}), proportionate to the applied algorithm for digital signature and the key length (approximately 40 ms for *RSA* algorithm with 1024 b - key).

Finally, the validation procedure is completed in such a way that the relying party performs the adequate *CRL* listing with the aim of establishing whether the validated certificate is on the list or not ($t_{listcrl}$) (figure 4). Since each of them originates from the corresponding *CA* domain within the considered hierarchical or bridge architecture, it is necessary to carry out the verification of the certifications chains on the corresponding certificate path. In other words, in a given certificate it is necessary to recognize a certification path it belongs to and the total number of certificates on it, according to the explanation in the chapter 2. The verification time necessary for the chain verification ($t_{listcrl}$) will be proportionate to the certificates number on the certification path, applied algorithm for the digital signature and key length.

Bearing in mind the above mentioned, the total time of certificate status validation time (t_{vss}) can be analytically calculated in the following way:

$$t_{vss} = t_{verls} + t_{down} + t_{vercrl} + t_{listcrl} \quad (1)$$

Due to the fact that the *CRL*s are not issued for each certificate to be validated, but periodically, in accordance with the local policies of the individual *CA*s, the validation status time for the majority of the certificates will be given in the equation:

$$t_{vss} = t_{verls} + t_{listcrl} \quad (2)$$

while for the lesser number of the certificates it will be as it has been shown in the equation 1. In other words, it means that the relying parties subsequent to the take over (receiving) *CRL*s keep and use these *CRL*s up to the moment of their next updating and issuance. This fact implies the presence of still another one among the factors affecting the validation time – *the CRLs issuance policy*.

In the process of creating the *CRL*s issuance policy the care must be taken of the fact that the security risk of eventual misuse of the non-valid certificates is reduced by more often *CRLs* application. Thus, one of the basic criteria can be the number of the revoked certificates per day. In accordance with this, the eventual policy may be applied taking into account as many realisations per day as there is the number of the approximately revoked certificates per day, the realisation implying both the updating and

one *CRL* issuance. Accordingly, it is possible to generalise one of the policies in the form:

$P_n=t_0+ak+bt_p$ (3)

Where is

P_n – *CRL*s issuance policy by a certain *CA* (CA_1, CA_2,…,CA_n).

t_o – the beginning of the first policy realisation,

k – the time interval between the policies,

a – the time interval modifier between some policies,

t – realisation period of a certain policy,

b – the period realisation modifier securing all realisations of a certain policy in a given working time (i.e., 8 hours).

Within the proposed policy (equation 3), each certificate authority defines the local policy P_1, P_2,…,P_{10}, related to the number of realisations per day in accordance with the revoked certificates per day (parameters b and t_p) (figure 4). By using the corresponding parameters t_0, a, k the mutual coordination of local policies is being carried out.

The described *CRL* validation procedure in the hierarchical and bridge *PKI* architecture can be shown in the functionality scheme in figure 4.

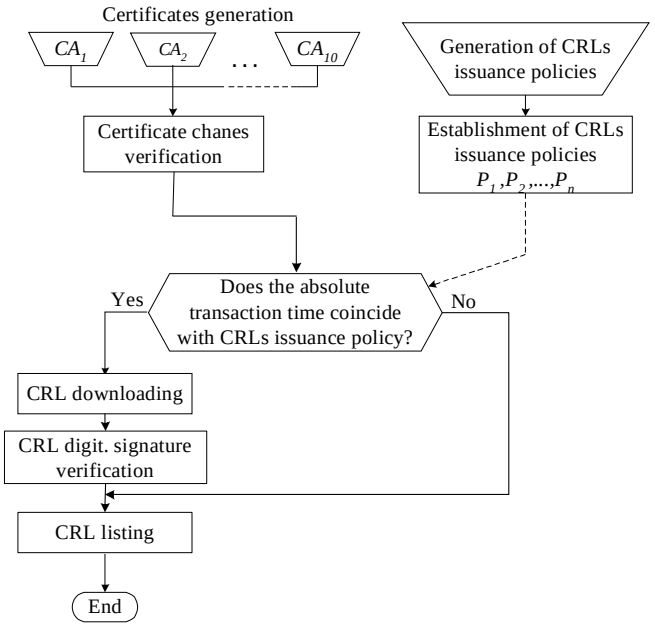

Figure 4 Functionality scheme of CRL validation in a given hierarchical and bridge PKI architecture

In the second approach based on *OCSP*, after certificates chains verification in an identical manner as in the case of *CRL* validation, the relying party submits the request for certificate status to *VA* for each certificate (figure 1). On receiving the request *VA*

makes both the listing previously stored and digitally signed validation responses. The listing time (t_{list}) is several times shorter regarding the *CRL* listing time, due to the fact that the recording size of validation response is 1 byte (compared with 22 bytes per a revoked certificate with *CRL* validation), at the identical listing rate. After identification, *VA* sends to the relying party the appropriate validation response of 2-5 Kbytes (with regard to the variable *CRL* sizes at *CRL* validation (figure 5). The reception time of the validation response (t_{odg}) as well as the request dispatch time (t_{zaht}) have approximately the identical value (about 2 ms) [6], [7]. After the validation response confirmation, the relying party checks its identity and integrity on the basis of digital signature verification (figure 5). This operation takes a certain period of time (t_{vervo}) depending on the applied algorithm for the digital signature and the key length (about 10 ms) [6], [7].

Having in mind the above mentioned, the certificate status total validation time (t_{vss}) can be analytically calculated as follows:

$$t_{vss}=t_{verls}+ t_{zaht}+ t_{list}+ t_{odg}+ t_{vervo} \quad (4)$$

In comparison with the total validation time in case of *CRL* validation (equation 1), the impact of validation data issuance policy can be here ignored. The *VA* secures the validation responses for each request. It is feasible since it generates the validation responses in advance, based on the data it receives from *CA* through *MiniCRL*.

Mini *CRL* are more efficient *CRL* presentation. They contain the compressed data on the revoked certificates (6 bits per a revoked certificate instead of 22 bytes at *CRL*), with the compression level at the ratio 30:1. Accordingly, it is possible to issue *MiniCRL* more frequently so that the *VA* can prepare `fresh` validation responses for each validation request.

The described procedure of the *OCSP* validation with *MiniCRL* (*OCSP+MiniCRL*) in the hierarchical and bridge *PKI* architecture can be represented by the functionality scheme, as in figure 5.

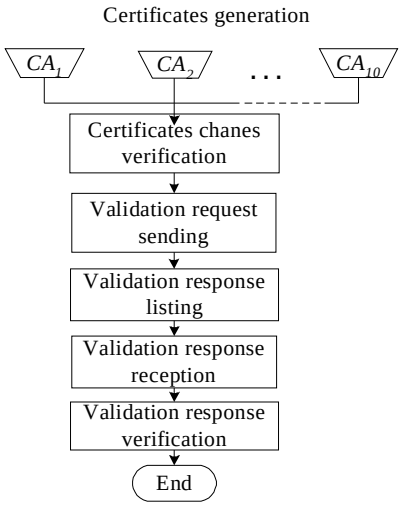

Figure 5 Functionality scheme of the OCSP+MiniCRL validation process in a given hierarchical and bridge PKI architecture

3. THE SIMULATION ANALYSIS OF CERTIFICATE STATUS VALIDATION TIME

The complexity level of the influential factors on the certificate status validation time in the described validation methods, surpasses the capacities of an efficient analytical solution. Thus, the simulation approach has been employed and the simulation models have been developed on the basis of the simulation language *GPSS* [8], [9], [10].

Four models for determination of the average validation time in the hierarchical and bridge *PKI* architecture with CRL and *OCSP+MiniCRL* validation have been developed. Applying analogously presented functionality schemes (figures 4 and 5) the first two procedures (the generation of validation requests and certificate chains verification) have been modelled in the same manner in all models.

The generation of validation requests has been modelled according to Poisson's distribution with the mean time between receptions, defined by the total duration of simulation time (8 hours), the number of *PKI* users (10000, 20000, 40000, 60000, 80000, 100000, 200000, 300000, 400000 and 500000) and the average number of requests per day per user [10]. On the basis of the given values, the mean time between requests receptions was from 288 ms to 6 ms, proportionate to the increasing number of *PKI* users.

The verification process of certificate chains have been modelled in such a manner that for each generated request the corresponding certificate path is recognized, corresponding number of certificates on it (see chapter 2) and the verification time of the given certificate chain (40 ± 5 ms per certificate) [6], [7]. It was achieved by distribution of requests on certain *CA*-domains CA_1, CA_2….CA_{10} at the amount rate of, for instance, 8%, 9%, 7%, 12%, 13%, 11%, 14%, 9%, 8%, 9% , out of the total number of the requests, respectively, and by assigning specific *CA*-domain features to each generated request. Consequently, this process possesses a simple time dependently and can be modelled in the form of a corresponding variable with a uniform time distribution in a given interval. The basic difference when modelling this process between the hierarchical and bridge *PKI* architecture occurs within the certificates chains verification, due to the differences in lengths of the certificates paths and certificates numbers on them (see chapter 2).

The impact of certain *CRL* issuance policies, on the average validation time within the hierarchical and bridge architecture with *CRL* validation have been modelled in such a way that for each generated request the check up is made in order to confirm whether its absolute time coincides with some of the realisations of adopted policies (figure 4). In case of coincidence a longer validation time has been obtained (equation 1), otherwise the validation occurs in a shorter period of time (equation 2). Given the random feature of coincidences and the fact that the validation requests frequency is significantly larger than the frequency of policies realisation, in the model *the interval of coincidences toleration* has been employed with the variable rate amount: 0, 50, 100, 200, 400, 600, 800 and 1000 ms. The impact of each realisation on validation time appears in the selected intervals of coincidences toleration, so that each request from the given interval lengthens the validation time at the rate given by equation 1. In this rate amounts there occur generally ten different times of taking over the *CRLs* (t_{down}) proportionate to the sizes of individual *CRL*s and transmission rate (1,554 Mb/sec) [6], [7]. The relevant data to determine the *CRLs* sizes are as follows: the total number of *PKI* users, the number of

PKI users according to individual *CA*-domains, an average amount of revoked certificates (17%) and the average amount of data per revoked certificate within *CRL* (22 bytes) [6], [7].

With the changes within the coincidence toleration interval (0 ms to 1000 ms) in corresponding models, the increase in the total number of coincidences occurs, proportionate to the increase in the number of *PKI* users, as is shown in figure 6.

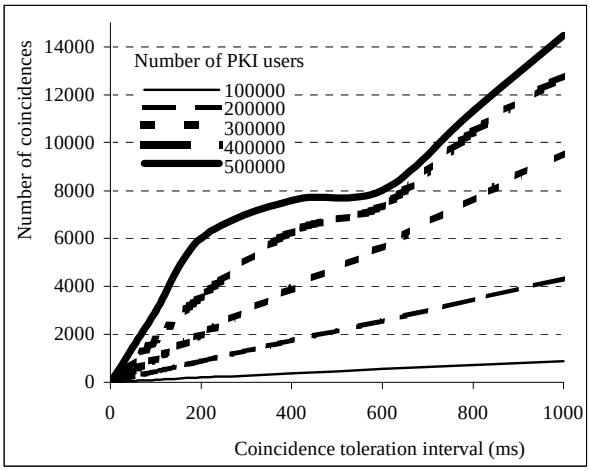

Figure 6 Detection of coincidences within the models for establishing certificate status validation time in the hierarchical and bridge PKI architecture with CRL validation

Figure 6 shows that the number of coincidences significantly rises within architectures of more than 100000 users, wherein the *CRLs* issuance policies with more than one realisation during the simulation period are employed, proportionate to the number of revoked certificates per day. The non-linearity of increase in number of coincidences, demonstrated with the most numerous *PKI* architectures (400000 and 500000), shows the random character of coincidences. The total number of the generated requests coinciding in time with the realisations of the given policies is quite negligible with regard to the number of requests without coincidences. This shows that the applied policies do not affect to great extent the average validation time. However, if some `more complex` policies were employed (with a greater number of realisations per day), this impact would be especially evident with *PKI* of greater number of users. In particular models, for realisation of certain policies the following parameters values have been used (table 1).

Total number of users *(N)*	Initial realisation of the first policy t_o (hour)	Time shift between policies k (min)	Realisation period of one policy t_p (hour)	Coincidence toleration interval (ms)
up to 300000	3	3	1	1000
400000	2	3	1	1000
500000	1	3	1	1000

Table 1 The relevant parameters of CRLs issuance policies

The given parameters values in the table 1 represent one of the choices, wherein the care has been taken of the possibility of realisation of all ten policies in the course of the 8-hour simulation time.

The verification process of *CRL* digital signature, according to the scheme in figure 4, has a simple time dependency. Based on the data from literature [6], [7], it has been established that its time interval is 40 ± 5 ms for each signed *CRL*. It is modelled in the form of a corresponding variable with the uniform time distribution in a given interval.

The *CRL* listing process, according to the scheme in figure 4, has more complex dependency. For its modelling it is necessary to initially recognize the *CA*-domain it originates from. It is the basis on which the calculation of listing time is made (t_{list}) proportionate to the each *CRL* size and the selected listing rate (e.g. 1 Mbytes/sec). The relevant data for calculating values of certain *CRLs* have already been presented.

Similar to the process of *CRL*s listing, the process of listing validation responses is also modelled within *OCSP+MiniCRL* validation, according to the scheme in figure 5. The essential deference arises from the fact that the amount of data for one validation response on the validation responses list is 1 byte [6], [7].

The presented simulation models contain a great number of random variables. The random values generation can be obtained by using modificators in the form of intervals, i.e. widening (the uniform distribution). However, when using the *GPSS* simulation language, the problem of transparent sample taking occurs which has been taken care of. Bearing in mind this fact, in the given models the presented weakness has been overcome by using the different flows of random numbers generator with all types of access values. Thus, the changes occurring in one part of the model do not affect the performance of other parts of the model, since the randomness sources are statistically independent [9].

With the aim of testing the effects of the random variables variability the experimenting with the models according to the tests plan has also been carried out. According to the experiment plan five independent models realisations have been planned. In each realisation special care was taken of the statistical independence by using different, independent flows of random numbers for each of random variables. The obtained experiment results present the mean values of all five realisations which gives more accurate simulation results shown on the diagram in figure 6 and 7.

By comparative analysis of the results, shown on the diagram in figure 7 (*HCRL, HMINI, BCRL, BMINI* curves) it is noted that the bridge architecture yields the shorter average validation time (BCRL, BMINI curves). For lesser number of *PKI* users (up to 60000) *CRL* validation yields shorter average validation time (*BCRL* curve). For a larger number of *PKI* users the *OCSP+MiniCRL* validation yields significant shorter average validation time, which retains almost constant amount within a wide scope of *PKI* users (*BMINI* curve).

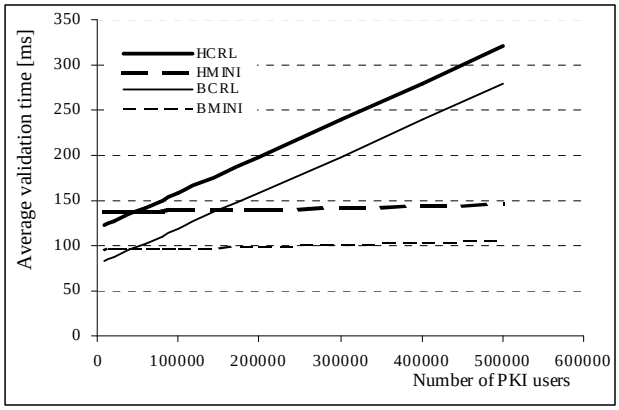

Figure 7 Certificate status validation time in the hierarchical and bridge PKI architecture with CRL and OCSP+MiniCRL validation

In the hierarchical *PKI* architecture (*HCRL, HMINI* curves) there is a similar regularity, but here the validation times are longer than at the bridge *PKI* architecture.
The linear flows of validation average time in all analysed cases show absence of impact of *CRL* issuance policies, in accordance with the earlier given explanation, even at the maximal coincidence toleration interval whereby the shown results (1000 ms) were obtained. The linear increase in validation time with the *CRL* validation (*HCRL, BCRL* curves) confirms the negative impact of *CRLs* sizes on the certificate status validation time.

CONCLUSION

The digital certificate validity presents the highest level of security when exchanging the electronic transactions between the E-commerce entities on Internet. Within the more complex *PKI* users` communities, the time needed to check the certificate validity can be of the highest importance when a suitable *PKI* application is to be accepted. In the paper the impact of some key factors on certificate status validation time have been analysed: *PKI* architecture (hierarchical and bridge), the certificates validation type (*CRL* and *OCSP+MiniCRL*), *CRL* issuance policy, the number of *PKI* users and the PKI type of application (*B2B*). Because of the complexity of the stated factors the simulation approach has been used. The four simulation models for calculating the average validation time in the hierarchical and bridge *PKI* architecture with *CRL* and *OCSP+MiniCRL* validation were presented. The comparative analysis of obtained results have also been done which shows significant advantage of the bridge *PKI* architecture with the *OCSP+MiniCRL* validation in case of a larger number of *PKI* users.

When analysing the impact of *CRL* type of validation on certificate status validation time, an potential mathematical model of *CRLs* issuance policy has been presented, which has also been applied in corresponding simulation models. Subsequently, it has been established (for given mathematical models parameters) that *CRLs* issuance policy does not have impact on certificate status validation time, bearing in mind the fact that the number of time coincidences between requests for certificate

status validation and realisations of given policies, is significantly lesser than the number of non-coincidences. In both the hierarchical and bridge *PKI* architecture, the *CRL* type of validation presented a negative impact on the validation time in terms of the increase in the average certificate status validation time, proportionate to the increased number of *PKI* users.

BIBLIOGRAPHY

[1] S. Kiran, P. Larean, S. Lloyd, *PKI Basics – A Technical Perspective*, PKI Forum, Novembar 2002;

[2] A. Levi, M. Ufuk Caglayan, *An Efficient, Dynamic and Trust Preserving Public Key Infrastructure*, Bogazici University, Department of Computer Engineering, 2000;

[3] D.A. Cooper, *A Model of Certificate Revocation*, In the Proceedings of the Fifteenth Annual Computer Security Applications Conference, pages 256-264, Dec. 1999;

[4] D.A. Cooper, *A More Efficient Use of Delta-CRLs*, In the Proceedings of the 2000 IEEE Symposium on Security and Privacy, pages 190-202, May 2000;

[5] Z. Živković, M. Stanojević, *Simulaciona analiza procesa elektronske trgovine baziranog na složenoj infrastrukturi javnog ključa*, ETRAN 2004, Zbornik radova, Republika Srbija, Juni 2004;

[6] *Vulnerability Analysis of Certificate Validation Systems*, CoreStreet, Ltd. One Alewife Center, Suite 200 Cambridge, MA 02140, 2004;

[7] *Certificate Validation Choices*, CoreStreet, Ltd. One Alewife Center, Suite 200 Cambridge, MA 02140, 2004;

[8] T. J. Schriber, *An Introduction to Simulation Using GPSS/H*, John Wiley &Sons, New York, 1991;

[9] B. Radenković, M. Stanojević, A. Marković, *Računarska simulacija*, Univerzitet u Beogradu, FON, Saobraćajni fakultet, Beograd, 1999;

[10] Z. Živković, M. Stanojević, B. Radenković, *Simulacioni model funkcionisanja zaštite u elektronskom poslovanju*, XXXI simpozijum o operacionim istraživanjima, SYMOPIS, Zbornik radova, str. 45-50, Fruška Gora, Republika Srbija, 2004.