ISSN 1822-6515
ECONOMICS & MANAGEMENT: 2009. 14

DIGTAL TIME STAMPING SERVICE FOR SMALL AND MEDIUM ENTERPRISES DEVELOPMENT PROSPECTS IN LITHUANIA

Arturas Mazeika
Mykolas Romeris University and State Tax Inspectorate, Vilnius, Lithuania, arturasm@mruni.lt

Abstract

The need to create measure that would allow improving SME business environment was influenced by rapidly developing economy during the past decade, establishment of new companies and involvement of households in the economy. Social economic development, science and technological advancement processes are more and more indefinite, have more various risks. Understanding of this circumstance allows validating the need to foresee and evaluate on time various threats that may cause negative or incomprehensive unwanted results of SME and government's e-administation, at the same time trying to perform prevention of possible threats, negative and unwanted processes of legal validity evaluation of e-documents. Due to new business and accounting, international cooperation conditions, changes of tax administration, new tax laws (related to the accession of the Republic of Lithuania to European Union) there is substantial increase of legal and tax documents, number of tax administration procedures, requirements for data protection and data quality, also number of legal and natural persons who file returns. In present scientific researches and practical scientific works of evaluation of e-documents' validity, there is lack of adequate evaluation of factors and circumstances, that expresses various dangers. It is possible to state that in scientific researches and actual works e-documents' validity security problems, that are rather serious and of different forms now or will be in the future, are ignored.

Therefore time stamping in many cases is becoming ultimate evidence resolving the status of documents. The paper describes following Time stamping System components - NMI and TSU interface, Time stamping unit (TSU), Archive, User interface, Control system, VPN router. The paper reflects findings from EC funded 6th Framework project BALTICTIME (IST- 027751).

Keywords: e Service, e Document, eGoverment, Small, To; Medium-SIZED, Firms, Time stamping.

Introduction

Present social economic development, scientific and technological advancement has several exceptional features which are influenced by more and more intensive processes of globalisation and formation of new knowledge society type. New knowledge economy, new type of management and administration are common for knowledge-based society and it is spreading in all areas of public sector, without exception of government and municipal government. As well as in today's business, including SME sector and in all other areas of life of contemporary society. Common feature of rise and development of new type management and administration is formation of eGovernment concept, rapid creation of technological and organisational forms of eGovernment, dissemination, implementation and permanent modernization. Formation process of knowledge-based society and knowledge economy, including eGovernment development, importance and role are obvious. This circumstance determines necessity to investigate these processes in detail and integrally, observe and forecast their common trajectory, make focused influence, to administrate and manage. The meaning of observation, forecasting and management of these processes is to understand and evaluate new challenges on time, reasonably define aims and use all opportunities that social economic development, science and technological advancement would be of higher effectiveness level and would enable to reach the most daring and ambitious SME and knowledge society goals.

The need to create measure that would allow improving SME business environment was influenced by rapidly developing economy during the past decade, establishment of new companies and involvement of households in the economy. Social economic development, science and technological advancement processes are more and more indefinite, have more various risks (Melnikas, 2007). Understanding of this circumstance allows validating the need to foresee and evaluate on time various threats that may cause negative or incomprehensive unwanted results of SME and government's e-administation, at the same time trying to perform prevention of possible threats, negative and unwanted processes of legal validity evaluation of e-documents.

Research object. The paper aims to analyze eService created to improve legal environment of small and medium-sized enterprises and enabling to better and more effectively optimize the time of communication with governmental institutions and business partners. In this paper there is also analysis of digital time stamping service and digital time stamping systems components, organization requirements for

ISSN 1822-6515

implementing digital stamp service system. Time stamping helps significantly increase the level of confidence currently required in a public-key infrastructure by making it possible to track timing of signing the documents.

Research methods and resources used. The basis for theoretical part of the paper is scientific researches of Lithuania's time stamping service, while optimization method was helpful tool in research of optimal business activity SME. Main information sources are data bases of Statistical Department under the Government of the Republic of Lithuania, information of Ministry of Finance of the Republic of Lithuania and State Tax Inspectorate.

Due to new business and accounting, international cooperation conditions, changes of tax administration, new tax laws (related to the accession of the Republic of Lithuania to European Union) there is substantial increase of legal and tax documents, number of tax administration procedures, requirements for data protection and data quality, also number of legal and natural persons who file returns. In present scientific researches and practical scientific works of evaluation of e-documents' validity, there is lack of adequate evaluation of factors and circumstances, that expresses various dangers. It is possible to state that in scientific researches and actual works e-documents' validity security problems, that are rather serious and of different forms now or will be in the future, are ignored. Obviously, that problems of such type are considered as especially relevant, so, understanding, analysis and solutions are of great importance. Perception of indicated circumstances determines expediency to discuss more in detail security problems of e-services that are relevant for SME, especially multidimensional validity and security problems that appear in communication processes between SME subjects and government. More detailed discussion of problems, their perception and analysis could form assumptions to solve them more efficiently, as well as to encourage government and SME subjects to modernise administration processes.

In order information systems and provided e-services would meet EU standards and would improve SME business environment, governments, business representatives and scientists are searching for opportunities for business representatives to perform legal procedure via public e-networks, at the same time ensuring reliability of procedures, as well as constant operation, data security, legal validity of e-documents.

The development of eGovernment services facilitate effective services providing for citizens, SME business enterprises or governmental organizations. The effective implementation of eGovernment services requires to process legally secure electronic documents and data files. That will enhance the security of electronic signature showing exactly when a document was signed, establishing an irrefutable sequence of events and also will contribute for development of fully online transactions environment as it requires multi level eSignature system. Much more technically secure and legally safe transactions over public open networks are a significant prerequisite for the further development of fully interactive electronic services. That will facilitate and accelerate the work of state institutions, create conditions for saving time and money, ensure faster, more convenient and efficient servicing.

In the context of development of eServices Digital Time Stamping service can play a significant role. Real importance of time stamping becomes clear when there is a need for a legal use of electronic documents with a long lifetime (Epstein, 2002) During the last years, especially in the context of legal regulation of the use of digital signatures, the organizational and legal aspects of time stamping itself have become the subject of world-wide attention. Time stamping helps significantly increase the level of confidence currently required in a public-key infrastructure by making it possible to track timing of signing the documents. Therefore time stamping in many cases is becoming ultimate evidence resolving the status of documents. The examples for use of time stamps can be validation of electronic signatures, computer logging (evaluation of performance and security issues in systems and networks), online subscriptions (granting revocation of subscriptions), digital notarization services, security policy/logins (additional level of protection), sales orders/receipts, content sealing, etc (Gatautis, Mazeika, Laud & Satkauskas, 2008). The use of electronic services and documents is becoming more and more frequent, presenting a series of advantages, amongst them, safer and faster communication, optimal use of resources and physical space, not to mention that they speed up the process.

Analysis of potential of timestamp usage

In order to guarantee the integrity and the legality of such documents, techniques should be developed to simulate the traditional way of authenticating a document, that is, the electronic document should also be authenticated and signed. Along with the digital signature, the electronic documents begin to have a judicial

ISSN 1822-6515
ECONOMICS & MANAGEMENT: 2009. 14

value before a court of law, and are beginning to be used to solve disputes, in other words, Digital Time-Stamping guarantees the existence and integrity of one document at certain moment and the digital signature guarantees the connection between the document and the person who created it. Particularly in the eGovernment domain, the ability to ascertain the creation times of documents will enable the provision of the following services: a) Electronic signature, public keys certificate authorities; b) Exchanges of documents in governmental and municipal organizations; c) Tax declarations; d) Public procurements; (Gatautis, Mazeika, Laud & Satkauskas, 2008).

Due to new business, accounting and international cooperation conditions, changes in tax administration, new legislation (related to Lithuania's accession to EU as well), there is increase in numbers of tax documents and tax procedures and requirements for data quality (Daugirda, 2007). Because of the enlisted reasons the quantity of the issued/received documents is changing in all areas of business sectors. According to the principles of document submission/exchange, their features and content valid documents can be divided into such subgroups: business-to-business − B2B, business-to-government − B2G, government-to-business − G2B, government-to-government − G2G. B2B group comprises documents circulating between business subjects, i.e. various contracts, documents confirming sales/purchases, transactions and other. B2G group comprises various obligatory documents for business defined by laws, i.e. returns, notes, payment documents. This document group in respect to its validity is very relevant for SME and subjects of government institutions as especially for this document's group there are many legal discussions in order to determine and make legal evaluation of the fact of document submission/reception and its content. G2G group comprises documents related to certificates issued by the governmental institutions, registrations in various data bases, explanatory notes, extracts, decisions, etc. Notarial documents also are included in this group. Governmental institutions use internal and external documents, such as orders, decisions, official notes, etc. It is difficult to define one specific group of the documents as each of them has its validity importance, though according to the legal disputes and their quantity dynamics the most relevant are groups of B2G and G2B groups.

In order to define potential of the usage of timestamp as measure providing higher validity degree for the (traditional and electronic) documents, for the analysis of the dynamics of received/issued B2G and G2B documents a few institutions were chosen such as The State Social Insurance Fund Board under the Ministry of Social Security and Labor (hereinafter – SSIFB), State Tax Inspectorate (hereinafter – STI) and notaries, that provide public services for SME subjects and natural persons. Such decision was influenced by the factor that SME subjects according to legal requirements (form and deadlines) submit and receive the largest quantity of documents from the mentioned institutions.

Table 1. Dynamics of documents of the group B2G provided to STI by SME

Year	Number of return types	Submitted returns			Ratio	
		Total	Via electronic means	Total	E-returns	Paper forms
2004	33	1314785	102.272	1.212.513	7,78	92,22
2005	37	3038619	1.050.559	1.988.060	34,57	65,43
2006	42	3426866	1.786.361	1.640.505	52,13	47,87
2007	50	3961275	2.618.605	1.342.670	66,11	33,89
2008	54	4454464	3.279.646	1.174.818	73,63	26,37

Baffing on STI date

Analysis of process of SME business activities declaration is provided in the Table 1 and confirms increasing document flows between business and government representative STI. In 2006 the number of documents provided via electronic means and paper forms became equal, later it increased till 73,63 percent in 2008.

By providing services for the businesses STI according to legislation has to answer 50 percent of documents, received by electronic means. This fact increases total amount of e-documents in 2008 (including B2G 3279646 documents and G2B 1639823 documents) up to 4919469 documents. Analysis of SSIFB documents is provided in the Table 2 also and shows increasing flows of document of groups B2G and G2B.

ISSN 1822-6515
ECONOMICS & MANAGEMENT: 2009. 14

Table 2. Dynamics of business to B2G and G2B documents in SSIFB for SME

	2006	2007	2008
SSIFB received documents (B2G)	586882	1696953	1786864
SSIFB issued documents (G2B)	596854	1460894	1474260
SSIFB internal documents (G2G)	136214	229931	314298
Legal acts (G2B).	151569	1186783	1604183
Total amount per year	1471519	4574561	5179605

Baffing on STI date

Various deals between small and medium businesses are confirmed by notaries. That is various acquisitions of assets, issuing commissions, vouchers and other legal important documents. Their dynamics is provided in Table 3.

Table 3. Dynamics of documents SME confirmed by notaries

Year	Number of notaries	Number of deals	Average number of deals per notary per year
2005	227	150097	661
2006	250	176189	705
2007	261	182852	700
2008	271	143265	529

Baffing on STI date

Numbers of deals confirmed by notaries testify the beginning of economic slowdown in 2008. Though in 2008 number of notaries reached 271, number of deals decreased from 182852 to 143265. Still analysing this pessimistic fact we can state that timestamp service that provides for (traditional and electronic) documents higher validity degree is important and there is basis for discussion as the problem of the state level. There is need for governmental decisions of development of timestamp service related to publicity of and accessibility of this service. There are several alternative solutions, though they still have drawbacks and undoubtedly that creation of effective digital timestamp service is based on open source principals would improve environment of SME and would encourage development of e-Government.

Components of the Time stamping

System Introduction of the systems for identity management (eID, etc.) providing accountability and security for two-way interaction and higher online sophistication level services is one of the key factors for successful eGovernment public services acceptance. Time Stamping Authority (TSA) being integral part of the system is to large extent responsible for the confidence and accountability of these services. EC funded BALTICTIME project aims to develop the legal and accountable digital time stamping (DTS) system providing the layer of Trust in eGovernmental transaction environment and to demonstrate DTS system performance for time critical functions or validation data for digital signatures. The main part of DTS is Time Stamping Authority (TSA). The functions of TSA are determined by the standard RFC 3161 (Adams, Cain, Pinkas & Zuccherato, 2001): “The TSA's role is to time-stamp a datum to establish evidence indicating that a datum existed before a particular time. This can then be used, for example, to verify that a digital signature was applied to a message before the corresponding certificate was revoked.” The implementation and deployment of the BALTICTIME time stamping authority will enable the long-term validation (beyond the expiration of various signing keys) of digital signatures by allowing anyone to compare the times of creating the signature and the expiration of the signing key.

The structure and the hardware configuration of a Trusted TSA system are presented in Figure 1. To cope with a large number of time stamping requests, we see the TSA to be deployed in a distributed manner, with one of the sites acting as a main system (TSA main site), keeping its time standards synchronized and its archive linked with the outside world (directly connected to the National Metrology Institute), while the other sites (TSA remote sites) synchronized and linked with the main site. A distributed system can also provide better availability which is important in time stamping applications where some party is always interested in obtaining the timestamp as soon as possible.

ISSN 1822-6515
ECONOMICS & MANAGEMENT: 2009. 14

Table 4. The main site of a TSA is composed of the following hardware components

No.	Name	Purposes
P1/M	NMI and TSU interface	1. Time source for Time Stamps generation by TSU. 2. Warrant traceability of Remote timing system (P1/R) to the UTC(k) time scale. 3. Synchronize the TSA main site hardware components.
P2/M	Time stamping unit (TSU)	Time stamps generation
P3/M	Archive	Storage of issued time stamps
P4/M	User interface	Webservice maintenance for small users
P5/M	Control system	Operation control of the TSA main site hardware components
P6/M	VPN router	Main and remote TSA sites secure communications

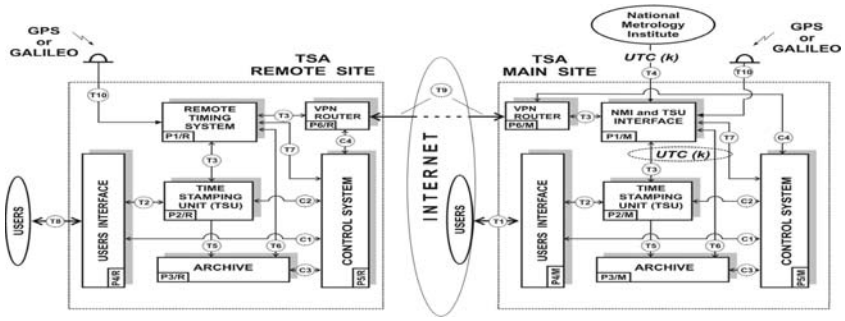

Figure 1. The remote site of a TSA is composed of the following hardware components

No.	Name	Purposes
P1/R	Remote timing system	1. Time source for Time Stamps generation by TSU. 2. Warrant traceability of remote timing system (P1/R) to the UTC(k) time scale. 3. Synchronize the TSA remote site hardware components. **Note:** Remote timing system is a part of NMI and TSU interface.
P2/R	Time stamping unit (TSU)	Generation of timestamps
P3/R	Archive	Storage of issued time stamps
P4/R	User interface	Time stamping service maintenance for big users
P5/R	Control system	Operation control of the TSA main site hardware components
P6/R	VPN router	Main and remote TSA sites secure communications

To allow the extraction of linking chains between timestamps issued by different sites (unless their times of issuance are very close together), the archives have to be synchronized with each other. Synchronization of archives really means that there are links between linking items in different archives. To create linking chains from already existing timestamps in archive A_1 to future timestamps in archive A_2, the archive A_1 sends its currently last linking item L' to the archive A_2. The archive A_2 takes its last linking item L_n and computes $L_{n+1} = h(L_n, L')$. It also stores L'. A linking chain from an old timestamp in A_1 to a new timestamp in A_2 will pass through L' and L_{n+1}.

The procedure just described creates "one-way" synchronization between A_1 and A_2. To get the synchronization also in the other direction, we repeat the procedure with the roles of A_1 and A_2 swapped. The frequency of executing this procedure gives the granularity of synchronization – if links between different archives are generated every t seconds then we are guaranteed the existence of a linking chain between the timestamps from those two archives if their issuance times differ by at least t seconds. To find this linking chain, the archive units must record which linking items have been used for synchronization.

If two timestamps are issued by two different TSUs almost simultaneously (less than t seconds apart) then there might exist no linking chain from one stamp to the other. In this case we cannot use linking items to show that one timestamp was issued before the other one. But we can still convince ourselves that both those timestamps have been issued later than some earlier timestamp, and before some later timestamp, thereby verifying their validity. The applications that check timestamps should gracefully handle such situations where two obviously valid timestamps with no linking chain between them have been presented. Such timestamps should be treated as simultaneous and if necessary, other criteria used to order them. Also,

ISSN 1822-6515

if the signature keys of the TSUs are still valid then the applications can extract the absolute times from the timestamps and compare them.

In a simple hash-and-sign time stamping the TSA receives the digest of a document, appends the current time to it and signs the resulting data structure. When the signing key expires, the timestamp loses its validity — we cannot verify whether the signature on the timestamp was created before or after the expiration. Linking-based time stamping allows the determination of the issuing order of two timestamps (but not the precise time of their issuing) even after the key used to sign the timestamps has expired. Moreover, linking-based time stamping does not allow even a malicious TSA to back-date documents (a hash-and-sign TSA can easily do that by including a wrong time in a timestamp).

Let $T_1, T_2, T_3,...$ be the issued timestamps. Let $X_i = h(T_i)$ be the digest of the timestamp T_i, where h is a one-way hash function, i.e. given some bit-string y it is very hard to find such x that $h(x)=y$. In linking-based time stamping, the time stamping server additionally constructs and stores the *linking items* $L_i = h(X_i, L_{i-1})$. In essence, the linking item L_i contains X_i and L_{i-1}, hence it cannot have been created earlier than them. By transitivity, L_n contains all X_m and L_m where $m<n$. The proof (called the *linking chain*) that L_n is later than L_m can also be presented — it consists of all X_i where $m<i\leq n$. With the help of those X_i, L_n can be recomputed from L_m (Buldas, Laud, Lipmaa & Villemson, 1998).

Similarly, we can present a proof that L_n is later than X_m for $m\leq n$. We use the existence of such proofs to show that one timestamp is earlier than the other one by letting each timestamp T_n contain the linking item $L_{n'}$ where n' is smaller, but not much smaller than n (we can make n' equal to $n-1$). In this way we can show that T_m, where $m\leq n'$, is earlier than T_n by showing that $L_{n'}$ is later than X_m. (Buldas, A. Laur, S. 2007). Indeed, then T_n will contain $L_{n'}$ that will in effect contain X_m that is the digest of T_m.

As hash-and-sign time stamping is unable to provide long-term integrity of timestamps, linking-based time stamping will be implemented in BALTICTIME. Still, signing the timestamps is useful for including certain metadata with the timestamps, in particular the issuing time of the timestamp. Such signatures by themselves have a rather short validity period, but the links between the timestamps allow us to also convince ourselves in the validity of old timestamps, including their metadata. One of the effects of the linking is that each timestamp in some sense contains all preceding time stamps, hence the signature on a timestamp is also a signature on all previous timestamps.

If the linking-based time stamping is implemented as described above, then the verification of a linking chain between linking items L_m and L_n is of complexity $O(n-m)$ which is definitely too much. Fortunately, if we let each linking item directly depend not only on the immediately preceding linking item, but also on a well-chosen earlier linking item, then the verification complexity can be reduced to completely acceptable $O(\log n)$.

Conclusions

Present global crisis provides an opportunity for governments to coordinate urgent structural reforms, encouraging entrepreneurship, needed for long term development and stimulating economic recovery. Timestamp service as public service could be a mean – assistance for small and medium-sized enterprises. It is a mean allowing to optimise modern administration, providing higher validity degree for e-documents ensuring accessibility and stable presence. EU directive 2006/112/EC encourages usage of electronic documents in the business environment due to their unique possibility, quickly to authorise and execute constant monitoring of business processes, ensuring safer business space. That enables to save many management costs in business and administrative expenditures in governmental institutions, promotes concept of eGovernment. The question of timestamp services that ensure higher validity degree of e-document must be considered immediately as it is a mean encouraging SME and improving business environment. Government institutions that are responsible for SME must choose the type of service provision: a) timestamp service provider is a private commercial institution and service provision is paid (partially paid) by the state; b) timestamp service provider is a state institution and service provision is paid (partially paid) by the state. Deeper analysis requires green or balanced managerial principle that allows saving natural resources because due to increased usage of paper, green areas of the plane are being destroyed and usage of energetic resources for recycling of the paper increases unwanted greenhouse effect.

ISSN 1822-6515

References

1. Adams, C. Cain, P. Pinkas, D. and Zuccherato, R. “Internet X. 509 Public Key Infrastructure Time-Stamp Protocol (TSP)”, IETF RFC 3161, August 2001.
2. Ahto Buldas, Peeter Laud, Helger Lipmaa and Jan Villemson.1998. Time-Stamping with binary linking schemes. In Advances in Cryptology − CRYPTO'98, LNCS 1462, 486−501. Springer−Verlag, 1998.
3. Ahto Buldas, Sven Laur. Knowledge-binding commitments with applications in time-stamping. In The International Conference on Theory and Practice of Public-Key Cryptography (PKC 2007). Beijin, China, April 16−20, 2007. LNCS 4450, p. 150−165, 2007.
4. COUNCIL DIRECTIVE 2006/112/EC of 28 November 2006 on the common system of value added tax Official Journal of the European Union 347/1.
5. Daugirda Dainius. (2007). System of electronic declaration in Lithuania: Efective administration. The theoretical and practical journal Public administration, 2007/3 (15), p. 9−13. ISSN 1648−4541.
6. Epstein, Julian. “Cleaning Up a Mess on the Web: A Comparison of Federal and State Digital Signature Laws.” 5 New York University Journal of Legislation and Public Policy 491 (2001−2002).
7. Melnikas B. (2007). Globalization, Knowledge based society and e-Goverance: Security problems. The theoretical and practical journal Public administration, 2007/3 (15), p. 53−64. ISSN 1648−4541.
8. Rimantas Gatautis, Arturas Mazeika, Peeter Laud and Rytis Satkauskas (2008). Enhancing e-Government Services through Digital Time Stamping: Time Stamping System Specifications Volume 5, number 24, Communications of the IBIMA, 2008 p. 204−210, ISSN: 1943−7765.