

ŽINIŲ VISUOMENĖ

Digital time stamping for eGovernment

Renaldas Gudauskas

Director of Vilnius University,
UNESCO Centre of Knowledge Economy
and Knowledge Management,
Professor
Phone +3705 236 61 06, www.tzc.vu.lt

Vilniaus universiteto UNESCO Tarptautinio
žinių ekonomikos ir žinių vadybos centro
direktorius, profesorius
Universiteto g. 3, LT-01513 Vilnius,
Tel. +3705 236 61 06
www.tzc.vu.lt

Rimantas Gatautis

Vilnius University,
UNESCO Centre of Knowledge Economy
and Knowledge Management,
Projects coordinator, Assoc. Professor

Vilniaus universiteto UNESCO Tarptautinio
žinių ekonomikos ir žinių vadybos
ekonomikos centro projektų koordinatorius,
docentas
Universiteto g. 3, LT-01513 Vilnius,
El. paštas: rimantas.gatautis@tzc.vu.lt

In new Member States, particularly in target region of Baltic States, eGovernment infrastructure, solutions and services is lagging far behind the EU-15 Member States. EU-15 already reached a level of sophistication that allows at least a two-way interaction between citizens and public authorities (31 per cent of all basic services to citizens entirely available online). Many of the government agencies in the Baltic States already have a presence of electronic public service while the online sophistication of public service delivery in the EU10(n) is mostly one-way interaction (downloadable forms).

The 6th Framework project *BALTICTIME* is targeted to Baltic States region to leverage eGovernment services through development of system providing the layer of Trust in eGovernmental transaction environment for time critical functions or contributes to the validation data for digital signatures.

BALTICTIME will propose qualified time stamping solution (compliant with European signature laws and directives) enables 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 irrefu-

table 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.

The overall objective of the *BALTICTIME* project is 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. In order to meet this goal, the integral, based on open source solutions time.

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.

Main obstacles hampering spread of TSAs must be taken into account, namely:

- **low acceptability by end users** due to low trust on existing TSAs and disputed time stamp accountability
- **fragmentation** of eGovernment services existing in different national environment.

BALTICTIME is designed to enhance the confidence on time stamping service through adopting capacities of Time Standard Authorities of EU metrology system as most autho-

ritative and reliable backbone for Time Stamping Authority. *BALTICTIME* 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. In such a way level of the confidence and accountability of the service eligible for employment in eGovernment services will be created and integral for Europe solution for TSA having strong potential to overcome existing fragmentation will be introduced.

Time stamping systems applicable in legal situations are generally divided into two types: simple and linking schemes.

For implementation of simple scheme a trusted server (called time stamping authority TSA) need to be set up, which function after getting the data item is to attach current time (a secure time stamp) to that item and sign the result electronically. No one except the server itself can alter the time stamp obtained this way or backdate any data item, allowing creation of a false time stamp.

This scheme is used in IETF/PKIX proposed time stamping standard RFC 3161 and in ETSI TS 102 023 v1.2.1 (2003-01) ETSI TS 101 733 v1.5.1 (2003-12) standards. Probably the main drawback of the trusted server approach can be concerns on the reliability of the whole scheme full trust. Current trusted time stamping services cannot be audited because there is no way to determine the time mark included into the time stamp. Also, the TSA has to be trusted on its ability to withstand time scale reordering attacks and/or issuing back-dated time-stamps.

Time stamping based on linking schemes provides relative temporal authentication, where the relative order (between any two ti-

me stamps) of stamp issuing is verified. Several types of linking schemes are proposed and in all of them the time certificate of a later issued stamp is dependent on earlier stamps. Most of the proposed schemes are built upon authentication graphs:

- *Linear linking schemes* (Haber and Stornetta) use a chain as the underlying graph and is based on one-way hash functions that are used to link all time stamps into a log the entries of which comprise cryptographic checksums computed over the whole previous part of the log (impractical, since certificate length increases linear with the number of stamps issued so far);
- *Tree schemes* (Merkle's authentication tree) uses a tree as the underlying graph
 - all the documents time-stamped during period of a second are organised as leaves of a binary tree.

Each vertex of the tree is labelled with a cryptographic hash of the labels of the child vertices of said vertex. Authentication consists of re-computing the root of the tree when the sibling vertices of the path to the root vertex are given. That scheme was practical enough to launch commercial time stamping service by Surety Technologies. In their scheme, root hash values are computed at every second and are then composed by using linear linkage. The same scheme with minor modifications was used in the Belgium TIMESEC project. The main improvement of such scheme is that the number of hash steps during verification is reduced from N to $\log(N)$. However, the server interaction during each verification event and secure storage of the root hash values are needed.

- *Accumulator schemes* (the only known viable alternative to the graph based schemes) further reduce the storage re-

quirements, by introducing a trapdoor into the scheme. Unfortunately such schemes directly violate the objective of increasing trust in stamping services as to date, there is no known efficient construction of trapdoorless accumulators.

- The linear linking scheme was employed for off-line verification trying to eliminate servers' availability issues. The main idea of that scheme, presented by Pinto and Freitas, is that time stamps comprise a part of the linkage chain that represents a time-interval, so that if two such intervals intersect, one is able to verify the order of these time stamps off-line. However, for off-line verification both the size of time stamps and the number of verification steps needed are impractical. First practical linkage based scheme with off-line verification was proposed by Buldas et al. In their scheme, each time stamp has logarithmic size and every two stamps can be efficiently compared off-line, after some additional (extension) procedure. Their research was related to the work of Estonian State Chancellery on the Estonian Digital Signature Act, and to a research project CUCULUS funded by Estonian Informatics Centre.

Efforts to consolidate existing and emerging solutions for evidence-creating systems were made in OpenEvidence (An OPEN source technology for data certification Value-added services (IST-2001-35174)) project, completed in 2003. Existing complementary technologies for time stamping, archiving, signature validation and certification were integrated and enhanced with interoperable Open Source solutions. The developed software and the test bed services were targeted to promo-

tion of trusted third party services supporting dematerialisation of documents.

For *BALTICTIME* project, as suggested in ETSI standard, trusted party scheme is selected as a backbone for whole time stamping service infrastructure. Although, following **novel solutions are proposed to eliminate assumption of full trust:**

I. To develop the interface between National Time Standard Authorities and Time Stamping Authorities, which will enable:

- Generation of auditable time stamps through time scale synchronisation and transfer to time stamping server ensuring of traceable time value included in to the time stamp;
- Correct and accurate time acquisition from NTSA, (the prime providers of Coordinated Universal Time UTC), which can be considered as internal source of common TSA)
- Easy transfer and cost effective implementation of time stamping service in any country or region having National Time Standard Authority.

II. To employ results generated in “OpenEvidence” for eDocuments archiving system and to develop archiving system integral with time scale generator, which will enable following functions:

- Formal interaction with trusted time scale;
- Complete evidence of electronic record conservation;
- Electronic record integrity protection over any period of time;
- Digital signatures validity preservation over any period of time;
- Proof of electronic record authenticity and unchangeableness over complete archiving period;

- Complete audit trail of electronic record conservation.

III. To introduce the security system based on interoperable certificate data base enabling:

- Online authorisation of subscribers through interoperable certificate data base;
- Role-based TSA security (ensuring no super-users existence) for TSA protection and compliance with stringent privacy legislation and industry guidelines.

Real importance of time stamping becomes clear when there is a need for a legal use of electronic documents with a long lifetime. 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.

The *BALTICTIME* consortium consolidates research efforts from enlarged Europe for metrology and standardisation, time stamping systems, security and archive software development and eServices provision. Consortium members' expertise is indispensable for the development of secure and accountable time

stamping system and service as envisaged in this project. Achievement of these goals without such a pan-European co-operation and best practice transfer would imply a considerably longer time-to-application, time-to-acceptance, and a risk too high to take for one organisation. For these reasons, joint research efforts across Europe are necessary to achieve a critical mass in terms of specific knowledge required, as well as to boost RTD. Participants from Lithuania, Latvia, Estonia, Poland, UK and Italy are involved to carry out *BALTICTIME* project. This transnational approach will create confidence in the area of eGovernmental services all over Europe, thus enhancing exploitation of research results, integration in services and acceptability. Partnering at European level ensures that research results and solutions are applicable across Europe and meets European rather than national standards and interoperable solutions enabling to make one of the steps for overcoming the fragmentation of eGovernment services in EU-25.

The main impact of *BALTICTIME* project is targeted to Baltic States region to leverage eGovernment services through development of system providing the layer of Trust in eGovernmental transaction environment for time critical functions or contributes to the validation data for digital signatures.

The introduction of Digital Time Stamping service will:

- **Increase online sophistication of public service delivery.** *BALTICTIME* will foster the higher level of online services by enhancing the security of online subscription: *BALTICTIME* developed time stamping service will grant and revoke the subscriptions to online services (subscriptions are in effect during the period when they are supposed to be and only during that period);

- **The implementation of EU electronic signature directive in Baltic States,** which states:

New services and product related to or using electronic signatures should not be limited to the issuance and management of certificates, but should also encompass any other service using, or ancillary to, electronic signatures, such as registration services, time stamping services, directory services...

BALTICTIME proposed qualified time stamping solution (compliant with European signature laws and directives) enables 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 of people and business companies. eGovernment provides a major contribution to increasing economic competitiveness at local, regional, national or Community level by streamlining bureaucratic procedures and increasing public sector efficiency, it plays a significant role in raising productivity levels in the economy as a whole. For European economies, characterised by ageing populations, increasing budget constraints and liabilities and in some cases high levels of unemployment, boosting competitiveness is a more pressing imperative than ever before. The public sector is challenged

to play a key role in modernising Europe's economy and society, so that Europe becomes more competitive and dynamic, with sustainable growth and capable of creating more and better jobs while providing for greater social cohesion.

The pilot *BALICTIME* system has great potential to overcome existing fragmentation

of eGovernment services as is being designed with maximum simplicity and platform independence, based on open source solutions for easy transfer and implementation in various application owners and eGovernment infrastructures in different countries, assuring integrity of the data management.

REFERENCES

Work Programme for the Specific Programme for RTD: "Integrating and Strengthening the European Research Area" Priority thematic area of research "Information Society Technologies". 2004.

Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions. Challenges for the European Information Society beyond 2005: Starting point for a new EU strategy. 2004.

IETF PKIX Working Group established Nov. 1995 with the intent of developing Internet standards needed to support an X.509-based Public Key Infrastructure.

Digital Time stamping and the Evaluation of Security Primitives (TIMESEC). funded by the Federal Office for Scientific, Technical and Cultural Affairs. Start-up in 1996.

PINTO, F.; FREITAS, V. (1999). Digital Time stamping to Support Non Repudiation in Electronic Communications.

BULDAS, A.; Laud, P.; LIPMAA, H.; WILLEMSON, J. (1998). Time stamping with Binary Linking Schemes. In: Hugo Krawczyk, editor. *Advances in Cryptology – CRYPTO '98*, volume 1462 of Lecture Notes in Computer Science. Springer-Verlag, p. 486–501.

SKAITMENINĖ LAIKO ŽYMA E. VYRIAUSYBEI

Renaldas Gudauskas. Rimantas Gatautis

Santrauka

Elektroninės vyriausybės paslaugų plėtros kontekste yra svarbu ne tik identifikuoti paslaugą teikiančią asmenį ar organizaciją, bet ir momentą, kai paslauga buvo suteikta. Skaitmeninė laiko žyma yra vienas iš sprendimų siekiant tiksliai nustatyti paslaugos suteikimo laiką. Vienareikšmio

ir visuotinai priimtino šios problemos sprendimo nėra. Rinkoje egzistuoja keletas alternatyvių sprendimų, tačiau jie vis dar turi trūkumų. Neabejotina, jog efektyvios skaitmeninės laiko žymos paslaugos sukūrimas paskatintų elektroninės vyriausybės paslaugų plėtrą.

Įteikta 2006 m. balandžio 19 d.