Time Stamping Authority

Ing. Jaroslav Pinkava, CSc.

E - SVĚT SE TOČÍ STÁLE RYCHLEJI. STAČÍTE MU?

Time Stamping Authority

The aim of the paper is to give

- the overview of problematic
- and the overview of important references

Time Stamping Authority

Content:

- introductory remarks, terminology
- examples of using of time stamps
- linking schemes
- legislative and standards (EU):

Time-Stamp Protocol (RFC 3161)

Electronic Signature Formats for long term electronic signatures

Policy requirements for time stamping authorities

Time Stamping Authority

- Time-stamp is a digital attestation of the TSA that an identified electronic document, subscribed with a electronic signature, has been presented to TSA at a certain time.
- Time-stamping is a set of techniques enabling one to ascertain whether an electronic document was created or signed at a certain time
- need for a legal use of electronic documents with a long lifetime
- the responsibilities of the owner of the signature, duties and responsibilities of the third party (Time- Stamping Authority, TSA) must be stated as well.
- existence of collision-resistant hash functions enables the verifier given two time-stamped documents to verify which of the two was created earlier.

sem vložte téma prezentace

Time Stamping Authority

Basic terms:

Time stamp should prove:

- freshness (T was created after t1);
- existence (T was created before t2);
- order (T was created before S).

To prove the electronic signature was generated while the signer's certificate was valid, the electronic signature must be verified and the following conditions satisfied:

- the time-stamp has been applied before the end of the validity period of the signer´s certificate,
- the time-stamp has been applied either while the signer´s certificate was not revoked or before the revocation date of the certificate.

Time Stamping Authority

- relying party: recipient of a time-stamp token who relies on that time-stamp token.
- subscriber: entity requiring the services provided by a TSA and which has explicitly or implicitly agreed to its terms and conditions (organization, end-user).
- time-stamp token: data object that binds a representation of a datum to a particular time, thus establishing evidence that the datum existed before that time.
- time-stamping authority: authority which issues time-stamp tokens.
- TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements.
- TSA practice statement: statement of the practices that a TSA employs in issuing time-stamp tokens.
- TSA system: composition of IT products and components organized to support the provision of time-stamping services.
- time-stamp policy: named set of rules that indicates the applicability of a time-stamp token to a particular community and/or class of application with common security requirements.
- time-stamping unit: set of hardware and software which is managed as a unit and has a single time-stamp token signing key active at a time.
- Coordinated Universal Time (UTC): Time scale based on the second as defined in ITU-R Recommendation TF.460-5.

Time Stamping Authority

- **The examples for use of time stamps:**
- ***Electronic signatures:*** **People acknowledge transactions and make contracts by signing documents — in both the paper and digital worlds. Signatures require a time stamp in order to establish when transactions or contracts occurred. A secure time stamp ensures that the time stamp is accurate, has not been altered, and is bound to one specific signature. It also ensures that the electronic signature was applied while the certificate that authorizes the signature was in effect — even if the certificate has long since expired.**
- ***Computer logging*****: Proving when events take place and in what sequence is vital for evaluating performance and security issues in systems and networks. That is equally true when collecting legal evidence against hackers and when upgrading system performance overall. Secure time stamps allow events to be audited long after they took place with assurance that times have not been altered (by a hacker, for example).**
- ***Online subscriptions:*** **The granting and revocation of subscriptions to online services are governed by time. Secure time means that subscriptions are in effect during the period when they are supposed to be and only during that period.**
- ***Digital notarization services:*** **As in the paper world, digital notarization services provide evidence from an unbiased third-party that records were created as claimed. Digital notarization services go a step further — they provide direct evidence those electronic files, inclusive of their respective pages and other digital components, were not altered after they were notarized. It also proves that the notarized file is the only file to which the notarization applies.**

Time Stamping Authority

- <u>The examples for use of time stamps:</u>
- *Security policy/logins:* **A secure time stamp provides an additional level of protection for ensuring that policies with respect to firewalls, logins, and other security procedures are observed and can be audited at any time.**
- *Sales orders/receipts:* **Secure time stamps can prove that any important electronic events — from stock purchases, to funds transfers, to document filings, to invoice payments — are done (or not done) at the time claimed. Compliance: More and more industries – financial securities, manufacturing – have legal requirements that documents and transactions must have certified and auditable time stamps.**
- *Content sealing:* **Any document with a secure time stamp cannot be altered without there being evidence of alteration. A secure certificate's time stamp proves that the document has not been altered after it has been stamped at a specific time.**

Time Stamping Authority

Linking schemes

- time stamps from the same round are not automatically ordered. It is useful (in some obstacles) to have an relative ordering for these time stamps.
- cryptographic way to achieve a relative order for the documents is to create dependencies between the *time certificates* attached to the documents.
- Concrete procedure that specifies which time stamps are directly dependent on which time stamps is called a *linking scheme*.

  For any i, $n_i<n_i+1$, then $T_n=H(T_{n1},T_{n2},\ldots, T_{nm})$.

Linear linking scheme is time stamp T_i for document (hash of document) D_i computed as $T_i = H(D_i,T_{i-1})$.

Binary linking schemes. The idea is to link the time stamps not only to the element directly preceding it but also to some other element (further in the past).

Time Stamping Authority

- EU Legislative
- Final report of the EESSI Expert Team ([19], July 1999) identified strategic objectives in Electronic Signature Standardization. In the document are given general requirements for electronic signatures, described different types of electronic signatures (general, enhanced, qualified).
- Directive on a Community framework for Electronic Signatures
- there are some differences in the legislative in various Member States in this area.
- Czech Legislative
- The Czech Law on electronic signatures has no mention on time stamping problematic at this time.

- This will be changed in the near future:

  - EU Directive, new version (July 2003 – start of process)

  - Czech Republic – <u>qualified time stamps</u>, legislative conditions are in preparation

Time Stamping Authority

Time-Stamp Protocol (RFC 3161)

This protocol defined TSA as Trusted Third party that creates time-stamp tokens in order to indicate that a datum existed at a particular point in time. TSA is required:

- to use a trustworthy source of time;
- to include a trustworthy time value for each time-stamp token;
- to include a unique integer for each newly generated time-stamp token;
- to produce a time-stamp token upon receiving a valid request from the requester, when it is possible;
- to include within each time-stamp token an identifier to uniquely indicate the security policy under which the token was created;

Time Stamping Authority

Time-Stamp Protocol (RFC 3161)

- to only time-stamp a hash representation of the datum, i.e., a data imprint associated with a one-way collision resistant hash-function uniquely identified by an OID;
- to examine the OID of the one-way collision resistant hash-function and to verify that the hash value length is consistent with the hash algorithm;
- not to examine the imprint being time-stamped in any way (other than to check its length, as specified in the previous bullet);
- not to include any identification of the requesting entity in the time-stamp tokens;
- to sign each time-stamp token using a key generated exclusively for this purpose and have this property of the key indicated on the corresponding certificate;
- to include additional information in the time-stamp token, if asked by the requester using the extensions field, only for the extensions that are supported by the TSA. If this is not possible, the TSA SHALL respond with an error message.

Time Stamping Authority

Electronic Signature Formats for long term electronic signatures.

(RFC.3126 and in technically equivalent ETSI Standard TS 101 733)

- **electronic signature may exist in many forms including:**

- **the Electronic Signature (ES), which includes the digital signature and other basic information provided by the signer;**
- **the ES with Time-Stamp (ES-T), which adds a time-stamp to the Electronic Signature, to take initial steps towards providing long term validity**
- **the ES with Complete validation data (ES-C), which adds to the ES-T references to the complete set of data supporting the validity of the electronic signature (i.e., revocation status information).**

- **There exist also an ES format with extended validation data (ES-X) with additional requirements**
- **format ES-A is considered for archival depositary of electronic signatures**

Time Stamping Authority

Policy requirements for time stamping authorities

(draft-ietf-pkix-pr-tsa-0i.t xt)

Requirements for a baseline time-stamp policy for TSAs issuing time-stamp tokens, supported by public key certificates, with an accuracy of one second or better.

Given policy requirements are primarily aimed at time-stamping services used in support of qualified electronic signatures

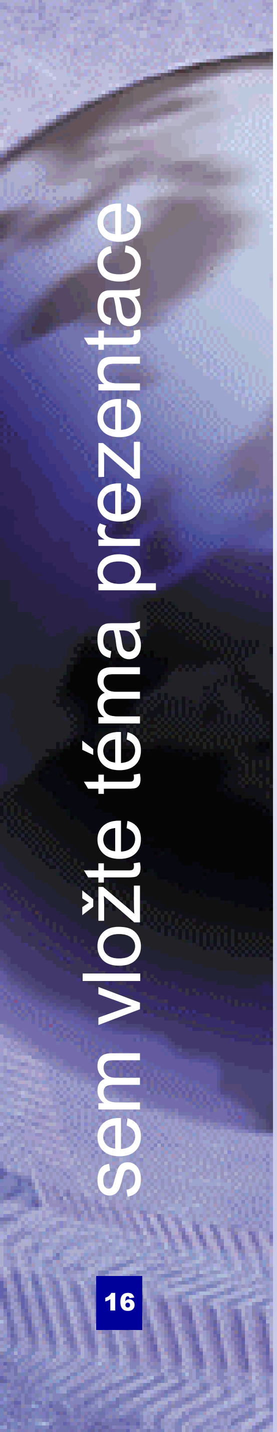
In document are given many conditions for practical functioning

Time Stamping Authority

Time Stamping Authority

Time-stamp policy and TSA practice statement

- The time-stamp policy states "what is to be adhered to," while a TSA practice statement states "how it is adhered to", i.e., the processes it will use in creating time-stamps and maintaining the accuracy of its clock.
- The relationship between the time-stamp policy and TSA practice statement is similar in nature to the relationship of other business policies which state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.
- A time-stamp policy is a less specific document than a TSA practice statement. A TSA practice statement is a more detailed description of the terms and conditions as well as business and operational practices of a TSA in issuing and otherwise managing time-stamping services.
- The TSA practice statement of a TSA enforces the rules established by a time-stamp policy. A TSA practice statement defines how a specific TSA meets the technical, organizational and procedural requirements identified in a time-stamp policy.
- A time-stamp policy is defined independently of the specific details of the specific operating environment of a TSA, whereas a TSA practice statement is tailored to the organizational structure, operating procedures, facilities, and computing environment of a TSA. A time-stamp policy may be defined by the user of times-stamp services, whereas the TSA practice statement is always defined by the provider.



Time Stamping Authority

The TSA shall (in TSA Practice Statement) ensure that it demonstrates the reliability necessary for providing time-stamping services.

- a) The TSA shall have a risk assessment carried out in order to evaluate business assets and threats to those assets in order to determine the necessary security controls and operational procedures.
- b) The TSA shall have a statement of the practices and procedures used to address all the requirements identified in this time-stamp policy.(This policy makes no requirement as to the structure of the TSA practice statement).
- c) The TSA's practice statement shall identify the obligations of all external organizations supporting the TSA services including the applicable policies and practices.
- d) The TSA shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the time-stamp policy (The TSA is not generally required to make all the details of its practices public).
- e) The TSA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services as specified in section 7.1.2.
- f) The TSA shall have a high level management body with final authority for approving the TSA practice statement.
- g) The senior management of the TSA shall ensure that the practices are properly implemented.
- h) The TSA shall define a review process for the practices including responsibilities for maintaining the TSA practice statement.
- i) The TSA shall give due notice of changes it intends to make in its practice statement and shall, following approval as in (f) above, make the revised TSA practice statement immediately available as required under (d) above.

Time Stamping Authority

Other requirements:

- The TSA shall implement specifieds controls
- The TSA shall (in TSA Disclosure Statement) disclose to all subscribers and potential relying parties the terms and conditions regarding use of its time-stamping services.
- document defined requirements on key management life cycle
- Administrative and management procedures, personnel
- Protection of informations and assets
- Trustworthy systém
- Reliability of organization
- compliance with legal requirements, etc.

Time Stamping Authority

Conclusions:

In article was given some overview on problematic connected with the notion Time Stamping Authority.

At this day there are TSA used rather rarely.

But as the necessary (in many important applications – for example electronic commerce, government sector, health services and others) component of electronic signatures is time-stamping forthcoming technique and important tool.

Thank You For Your Attention