

Trusted Timestamping RFC3161 can act Public Notary in future

When Notary Public receives a document they scan it to see if it is complete. It is also notarial responsibility to check the date of the document. As long as document is dated on the same or earlier day it is ok to notarize. However, if the document is dated on a future date the person presenting document needs to wait until that date or later. It is because, there must be a notarial certificate attached with a official valid date to the notarized document. Widespread access to open-source public libraries such as OpenSSL provides new ways of using public key infrastructure (PKI) in industry, which is enabled by digital signatures and data authentication. This functionality, in connection with Time Servers, creates a new group of services of so-called Trusted Time-Stamping of events in industry, which permanently associates events, alarms, and B2B transactions with the time and date of their real occurrence.

The importance of time

Time is ubiquitous in industry and its synchronization is required for the correct operation of most devices, particularly those controlled by computers. Despite its importance, this issue does not belong to the main hot topics of popular discussion, even though the effects of errors in synchronization each year cause billions in losses in the power distribution and telecom industry. This issue is also a future key for business in industrial automation, as well as the financial sector, state authorities and public administration.

Weighting the value of time

The U.S. Securities and Exchange Commission announced 2016, that Barclays Capital Inc. and Credit Suisse Securities (USA) LLC have agreed to settle separate federal securities laws while operating alternative trading system known as dark pool. Both Barclays and Credit Suisse were charged with dark pool violations. Firms collectively will pay more than US\$150 million¹ to settle cases. But reviewing sec.gov history there are much more similar cases, estimating for past decade the total penalty across financial market a volume of billion US dollars.

Equally very heavy losses are caused by phase-synchronization errors in power distribution networks, especially in the final stages, when the voltage drops.

Synchronization in Telecom² is

essential. It maintains the appropriate transmission bandwidth in wireless and fiber-optic connectivity. It stabilizes the radio frequencies of mobile base stations (BTS) allowing efficient radio spectrum usage. But exactly the same challenges remind valid considering laser beam inside fiber or quantum photonics communication in general.

Poor synchronization means worse audibility, more frequent disconnecting, voice echoes, signal reflections, crosstalk interferences - and thus lower sales revenues for the telecom service providers. Weak synchronization also seriously slows down data transmission in Internet fiber-optic connections, giving rise to frequent complaints, finally providing to financial losses too.

Computers in our immediate vicinity also require more-less accurate date and time. When handling events and carrying out their functions, they record information about the workflow of connected systems in special LOG files, which can be used as annexes or be a part of very official audit reports. By means of these LOG records, we can determine the exact time and location of an error, alarm or emergency. There are new growing markets like eg. Smart City - where trusted time will play important role.

Any place where consequences may have a financial impact or concern the safety of people, or when automation performs functions under the penalty of law, reliable time stamping is no less important than correct synchronization, because it provides additional unprecedented properties, such as:

- └ **non-repudiation** of the events eg. described in the LOG file;
- └ **authentication of TSA**, the Time stamping Server Authority;
- └ **originality and integrity** of all stamped information. It protects against violation, tampering, data corruption etc.

Trusted RFC3161 time stamping can be performed on any data type, in the form of a file in any format or length.

Cloud/IoT technology, which is increasingly popular today in industry called M2M/telemetry (machine to machine communication), more and more often uses cryptographic time-stamping for signifying data transfer between machines. Why? Because, if more autonomous computer operations are daily life, there is less human attention placed into details of computing operation.

Also a global distribution of food, water, agriculture goods, chemicals, and medicines can stay deadly biohazard if missing continuous trusted environmental monitoring of temperature or the max. period of validity.

Dealing with reliable time is not limited to industrial applications. It can also be used for individual or households purposes, e.g. when using Acrobat Reader. Information and multimedia (photos) contained in a PDF document can further simplify complex, today still very expensive procedures of patent protection. Cryptographic stamping can help preserve author rights and intellectual property protection.

September 2016, Tomasz Widomski

¹ <https://www.sec.gov/news/pressrelease/2016-16.html>

The mission of the U.S. Securities and Exchange Commission is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.

² J.Ferrant S.Jobert, L.Montini, S.Rodrigues, M.Gilson, M.Mayer, M.Ouellette,

S.Ruffini Synchronous Ethernet and IEEE 1588 in Telecoms - Weley 2013