Trusted Time Distribution with Auditing and Verification facilities

Project TSI#2 by ELPROMA Electronics Poland
T. Widomski, J. Kaczmarek, J. Uzycki, K. Borgulski, P. Olbrysz, J. Kowalski, R. Bender

E-mail: info@elpromaelectronics.com Web Site: www.clepsydratime.com

BIOGRAPHY of the Team Leader, on behalf of ELPROMA Electronics Poland Development Team

Tomasz Widomski, M.Sc. in Computer Engineering (Warsaw University of Technology, Poland), postgraduate in Valuation Methods (Warsaw School of Economics, Poland), Elproma CEO (1992-2014), Senior Member of the Board. IT technology visionary and inventor, high-tech startup investor, with over 25 years of experience in international IT.

ELPROMA Electronics Poland - the leading EU manufacture of NTP/PTP time servers. Motorola Inc. partner (2008-2011). CERN White Rabbit co-developer [2][3][4] (2009-2012), member of Atomic Time Scale Group of Laboratories TA(PL). Elproma NTP servers are mostly chosen product for metrology systems [5][30][31].

ABSTRACT

The aim of Elproma Project TSI#2 is to solve the problem that can be summarized in one sentence: “Timeservers know nothing about client side time”. Even most accurate time servers today do not address this problem. Time servers simply transfer responsibility for proper synchronization to the client side.

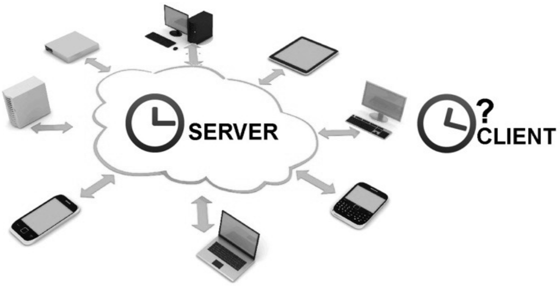

Fig. 1 Time servers are ignorant about the client time

Not being able to control client time synchronization can lead to serious business and legal implications. How can one ascertain at all that an event at a client side has occurred in a valid time? We propose a conceptual and technological framework, together with necessary tools, to define and implement VALID TIME, which we define as a time interval which lower and upper values can be determined depending on a given purpose, market or use case.

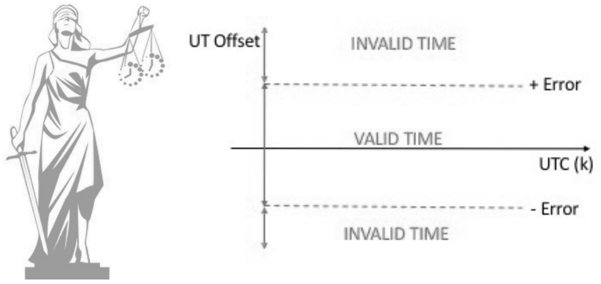

Fig. 2 Valid Time Concept

We also propose a business model where TIME can be commercially offered as an auditable service.

Today time is provided under the same model as electricity or any other utility. Computers can receive time signal from Ethernet sockets at offices or homes, or from wireless networks, including satellite systems. However, if we could distribute time in a way that it can be verified remotely as VALID/INVALID at a client side, we could offer added-value services/systems such as TRUSTED TIME DISTRIBUTION, and remote TIME AUDITING. In today’s world, where safety and security play critical role in B2B (Business to Business), B2C (Business to Consumer), and B2G (Business to Government) applications, markets at both local and global level should be ready to pay for these.

This paper reports results from a Horizon 2020 research project DEMETRA [1][16] undertaken by a consortium composed of 15 organisations from 7 EU member states, co-funded by European Commission under grant agreement no. 640658.

INTRODUCTION

The ability to assess the performance of clock synchronization at the client side calls for introducing a new concept: VALID TIME. We assume a device keeps VALID TIME if the following conditions are satisfied simultaneously:

- client clock is synchronized to trusted ref. of UTC(k) e.g. to NTA (National Time Authority)

- regular remote audits are performed on client clocks to confirm their time incessantly remains in the range defined as:
  UTC(k) +/- max. OffsetError
  Audits should be performed by independent, trusted third party (e.g. operator authorized by NTA*)*
- the above is performed with cryptographic technology offering the following properties:
  integrity, non-repudiation,validity, authentication

Having set the above conditions the TRUSTED TIME DISTRIBUTION system can be defined. Elproma's TSI#2 is a proposal for an implementation of such a system. It includes the necessary tools and components to implement a state level UTC VALID TIME distribution network over the Internet.

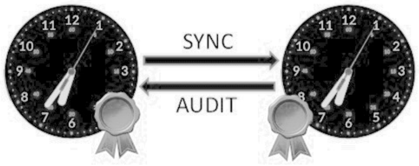

Fig. 3 General Concept of Trusted Time Distribution

STATE OF THE ART AND CRITICALITIES

Applications requiring reliable time synchronization, e.g. such as air traffic control or stock transactions, must have confidence that the system clock is correct within some bound relative to UTC. Computer engineers require a model of system timekeeping where every event that occurs at one computer must be recognized as taking place before the notification about that particular event arrives at another computer, because time is the critical factor in separating cause from effect.

Today synchronization implementations are based on a model that every message contains the time it was sent according to the sender's clock. If that time is later than the receiver's clock indicates, the receiver clock is adjusted to that time. The Ethernet base synchronization protocols determine the time offset of a client clock relative to server clocks. The various network synchronization protocols in use today provide different means to achieve this, but they all follow the same general model. The client sends a request to the Server (Master Clock), and the Server responds with its current time back to Client (Slave Clock). For the best accuracy, the client needs to measure the server-client propagation delay to determine the time offset relative to the server. Since it is not possible to determine the one-way delays (unless the actual time offset is for sure known), protocol measures the total *round-trip* delay and assumes that the propagation times are statistically equal in each direction. In general, this is a useful approximation, however in many cases network asymmetry or traffic overloads can differ significantly, causing unexpected and large errors. Considering state of the art Ethernet synchronization all protocols listed at Network Time Foundation [12] can be taken into account to build trusted time distribution system. This is including implementations of NTP [13], PTP [14], RADclock [15]. However, still none of them can ensure the client clock has been set correctly.

Elproma TSI#2 is lunched using std. Network Time Protocol version 4.2.8. The NTP has been chosen for its free use, source code availability, and error budget data produced by the protocol. This data is very useful for client time AUDIT and network monitoring purpose of TSI#2. While developing service we have had to confront the challenge of measuring and keeping under control the following parameters:

- network asymmetry, traffics, and overloads
- system/network failures
- security and service integrity
- leap second support
- synchronization via Internet better than 10ms

NTP seems to be the best suitable protocol covering needs of TSI#2 development. It covers technology necessary to implement both: time distribution from server to client, and client clock remote audit. For this specific purpose TSI#2 uses Master-Slave structure, where each (Master and Slave) component includes both std. NTP server and NTP client. But in fact also other protocols can be used by TSI#2 too.

For time distribution TSI#2 uses std. NTP synchronization. For client clock AUDIT the opposite direction to NTP operation is involved, providing "pseudo" client-server operations without synchronizing clocks. All communication and integrity of the system is secured with certificates and PKI infrastructure.

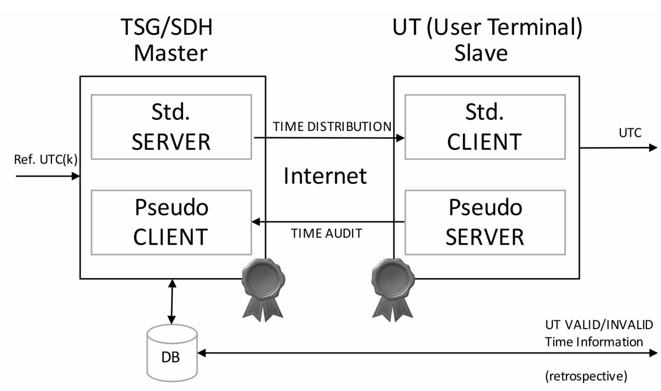

Fig. 4 TSI#2 general scheme

TSI#2 FUNCTIONALITIY

Below we outline the core functionality of TSI#2 service. The service requires input to TSG (Time Signal Generator):

- ref. UTC from NTA (National Time Authority)

The service produces output:

- UTC – available via NTP at UT (User Terminal) level
- VALID/INVALID information available retrospectively from Master TSG side, and related to redistributed UTC at UT level

To produce above outputs TSI#2 requires at least a single pair of TSG/SDH-UT units, where SDH means a System Data Handling, a module responsible for receiving UT and TSG feedback data (e.g. AUDIT logs).

The TSI#2 standard functionality includes:

- TIME DISTRIBUTION – from TSG to UT. providing trusted UTC distribution on UT output.
- TIME AUDITS – to perform periodical remote UT clock inspection. This data is used for validating UT output time (retrospectively).
- UT TIME VALIDATION – based on the performed TIME AUDITS, the system can verify at any past moment if the UT time has been in sync, in line with the VALID TIME definition. Due to potential network failures this information can only be obtained retrospectively (real-time feedbacks cannot be supported). Logs are kept in a separate database (DB) for retrospective time analyses (e.g. examining UTC VALIDITY of each moment of UT operation history).

In addition, UT is assembled at DEMETRA[1][16] with TSA (Time Stamp Authority) offering TIME STAMPING based on rfc3161 TSP (Time Stamping Protocol). Any remote user can timestamp its local data files (PDF, DOC, JPG, MP4, etc.). File timestamps are done according to trusted UT (User Terminal) UTC time and can be validated (retrospectively) later, as all synchronization and audit data reminds stored in the DB. This can lead to multiple practical applications, incl. in M2M (Machine to Machine) communication industry or Smart City applications. Confirming events (e.g. pictures, movies, e-tickets) with VALID and TRUSTED time with services such as TSI#2 can have significant market impact.

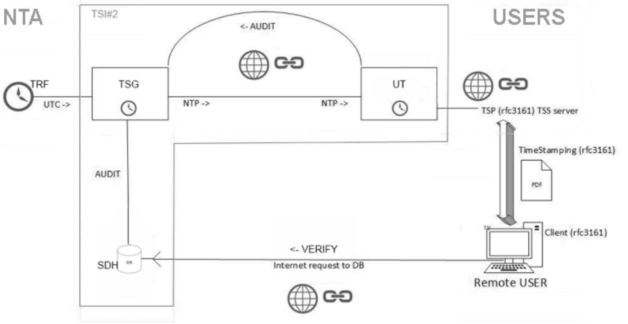

Fig. 5 TSI#2 configuration at DEMETRA[1][16]

More advanced TRUSTED TIME DISTRIBUTION systems would require multiple UT (at least one User Terminal per market branch) connected to single TSG-SDH. Each UT is able to provide UTC output and VALID TIME information. and redistribute it locally via LAN. The unified, common, primary ref. UTC(k) should be provided by NTA.

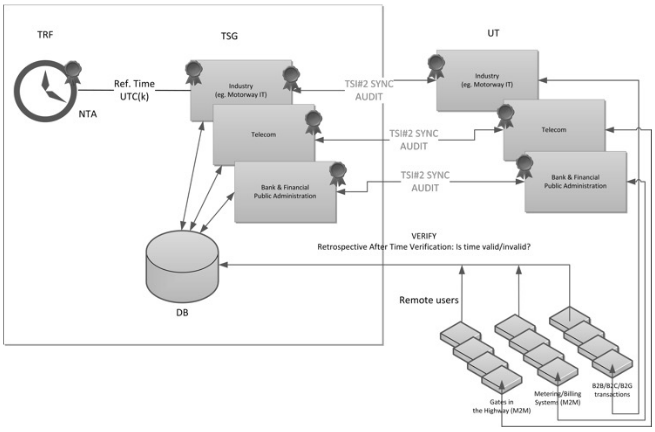

Fig. 6 An advanced configuration of TSI#2 supporting multiple market segments simultaneously: telecom, energy, telecom, finance etc.

TSI#2 AT A GLANCE

The TSI#2 production system can be scaled up depending on the application size, but it should include at least the following set of hardware (HW) components (Fig. 7):

- NTS-7000-TSG-SDH time signal generator (TSG) equipped with system data handler (SDH) and w/ built-in SQL database (DB)
- NTS-7000-UT user terminal (UT) receiving UT time from TSG and providing audits back to SDH level.

where NTS-7000 is a name of a prototype time-server and time-client unit demonstrated under DEMETRA [1][16] in a laboratory for metrology testing. NTS-7000 HW includes Elproma [17] server components (models: NTS-4000, NTS-5000).

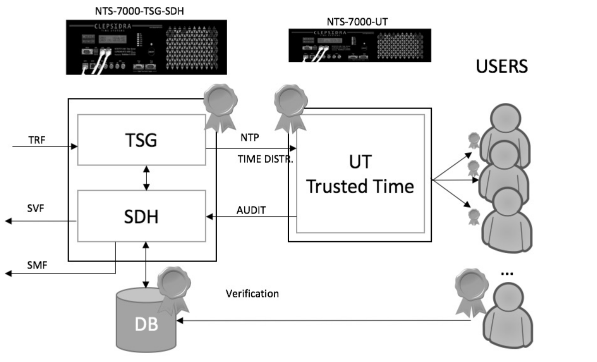

Fig. 7 Minimum configuration of TSI#2 with a single pair of TSG/SDH and UT units

In production environment NTA will provide reference UTC(k) time to TSG (Fig. 7 - TRF input signal) using 1PPS (Pulse Per Second) or 10MHz. In addition, NTP is involved for UTC phase and leap second support.

At DEMETRA [1][16] experiment the NTS-7000-TSG-SDH unit is located at INRIM – the NTA. The NTS-7000-UT is located remotely at a user premises, and it is communicating to TSG/SDH over the Internet. The dataflow are protected with cryptographic authentication, and PKI (Public Key Infrastructure) base X509 certificates.

The TSG is a master clock for UT - acting slave (Fig. 4, Fig. 5, Fig 6). NTS-7000 (both: TSG/SDH, and UT) are connected via TCP/IP protocol and use std. NTP for synchronization. We assume the TSG/SDH-UT connection is typically realized via Ethernet/TCP-IP network, and the Internet communication support is strongly recommended for final implementation. The TSG server is distributing cryptographically authenticated NTP messages to synchronize the remote UT. Therefore, TSG reminds exclusively trusted source of UTC time for the remote UT.

The SDH is a part of NTS-7000-TSG-SDH unit as well. However, in large scale systems one should consider SDH to be implemented as separate HW server with a suitable DB archiving policy for long-term archiving of all AUDIT logs.

For UT time auditing the “Reverse NTP” is used (Fig.4). This means that the std. NTP client at UT simultaneously acts “pseudo NTP Server” for TSG/SDH master – the “pseudo NTP client”. All pseudo-NTP operations are performed in “no select’ mode to avoid loops and wrong clock synchronization (server to client).

Independently to remote TSG/SDH audits on UT, the UT also performs self-AUDIT. This is necessary in case of network downtime when UT needs to operate in holdover mode. Nevertheless, both UT audits (“remote” and “self-AUDIT”) bring two groups of error budget. Both can be computed by SDH to provide retrospectively the information on whether UT works according to VALID TIME at any specific past moment. If UT offset error to UTC(k) can be ensured to have remained below 10ms, the UT time is claimed to provide VALID TIME – otherwise it is considered INVALID (Fig. 2).

Lastly, when network communication is down or limited the UT switches to the holdover mode. It can still provide a VALID TIME for a limited period relying on a built-in OSC. As long as UT is not reset or restarted, and the self-AUDIT of UT is in progress, the preliminary VALID time of UT can be claimed for the operation. However, the final validation of UT time can be done only in retrospective at the TSG/SDH master level, once the network connection is reestablished.

One of the most difficult part of our research and development work on TSI#2 have been to come up with an early networking problem detection. Such detection should be able to early recognize any network related problem that might cause synchronization problems at UT. In such a case UT should be quickly separated from the network and temporary switched into autonomous operation in holdover mode using OSC. TSI#2 is using PDV (Packed Delay Variation) low level operations to detect any peak deviation that can be correctly interpreted and used for filtering network related problems. As long as UT remains in the holdover mode the UT self-AUDIT is the only module that can provide preliminary VALID time examination. The early POC (Prove of Concept) PDV level algorithms have shown better than 1ms over-the-Internet synchronization of UT (located in Poland) to remote public NTP servers (located at INRIM in Italy) – see Fig. 8.

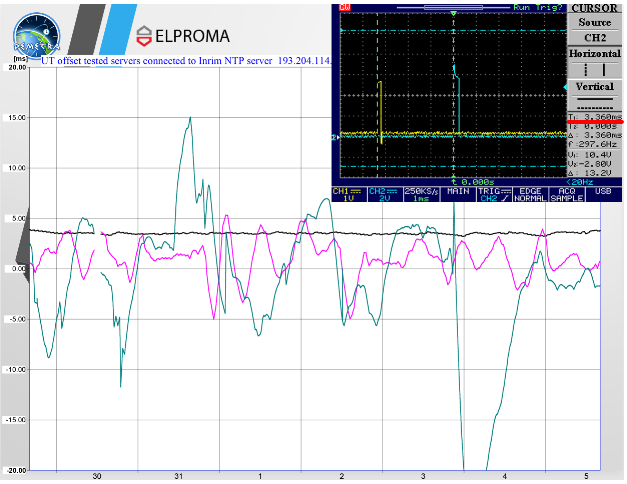

Fig. 8 The UT synchronization (black line) via Internet to public NTP Servers at INRIM. The UT is assembled with PDV level beta algorithms. For comparison, other colors show std. NTP clients synchronized to the same public NTP servers at INRIM. (Note: horizontal axis scale numbers indicates days).

Fig. 9 Testing PDV level algorithms at Elproma Lab

Finally, let us once again highlight that all TSI#2 components and communication remain cryptographically “sealed”. This is the condition that makes the entire infrastructure to be considered tightly integrated and trusted. The proposed infrastructure demonstrates the following properties: Integrity, Non-repudiation, Authentication, Validity.

For the purpose of DEMETRA [1] [16] experiment the UT has been equipped with extra TSA (Time Stamping Authority) server rfc3161. Therefore, any remote users can test and cryptographically timestamp their local file documents according to TRUSTED, and VALID time of UT.

TSI#2 INTERNAL BLOCKS

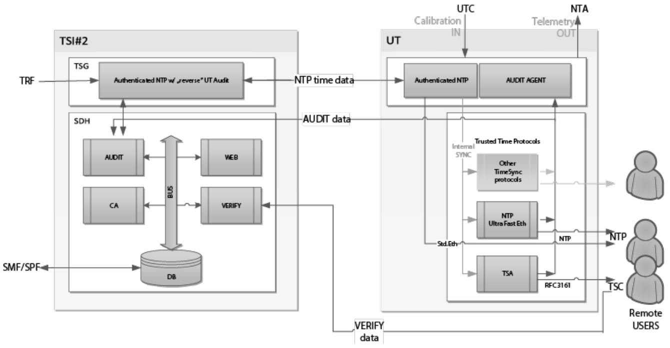

Fig. 10 TSI#2 Internal blocks

TSG – Time Signal Generator includes:

NTP server & pseudo-client with cryptographic authentication. It is responsible mainly for secured time distribution from TSG to UT, but it also supports extra functionality of "Reverse NTP" used for remote monitoring (a part of audit) of UT.

SDH – System Data Handling includes AUDIT, VERIFY, CA and WEB modules that are explained below.

AUDIT server is responsible for collecting audit LOGs from all TSI#2 components. Seemingly, it is operating in the opposite direction to the typical time distribution, but in fact this is a two-way communication server with strong asymmetric key protection. Its main responsibility is to:

- ✓ Regularly receive LOGs from TSG, UT
- ✓ Store all LOG data in DB
- ✓ Generate monitoring signals to external SCADA or other SMF (System Monitoring Facility)
- ✓ Examine data for final UT time validation
- ✓ Provide custom data built-in WEB

VERIFY server is responsible for retrospective time validation requested for the specific past event of UT operational history. An event can be any occurrence in the UT time, which entirely depends on the particular application. VERIFY works on AUDIT data stored in local DB. The final time validation (VALID TIME functionality) of UT confirmation can be provided retrospectively in time only if all AUDITS are received from UT. This is requiring network Links (+) (to be up) at least periodically once per several hours. According to network nature (overloads, asymmetry, broken links etc.) verification cannot be computed in real time. However, the preliminary time "valid/invalid" examination can be done based on UT self-AUDIT located at UT component side.

CA module generates and maintains PKI certificates (PFX/X509) for all TSI#2 components and users. It also includes CRL list of revoke certificates. This component is a part of TSG, but it also can be implemented as a separate IT system with its own backup strategy.

WEB module is providing visual data to remote users who have received access rights to Demetra [1] demonstrator, in particular to the TSI#2 service. It allows for checking the status of all TSI#2 components, downloading utility SW clients (e.g. rfc3161), etc.

UT – User Terminal includes**:**

NTP client and pseudo-server with encrypted authentication. It is responsible for secured time synchronization of UT. Time can be redistributed (NTP server functionality) or passed to other functional blocks like TSA (Time Stamp Authority) rfc3161 server etc.,

TSA server which is a service that allows for rfc3161 time stamping of any data files. TSA timestamps are done according to UT under condition that preliminary self-AUDIT (see below) clam UT time to be VALID,

AUDIT (agent) that supervises AUDIT data at UT side. This is one of most complex subsystems of TSI#2 composed of the following sub-components:

- **Self-AUDIT server** which collects all local statuses and data that lets preliminarily decide (in real-time) whatever UT time is VALID or not. This preliminary information is essential for reliability of TSI#2 service, incl. TSA, as real life networks are not perfect and it is highly likely that customers will experience links(-) down, variable traffics (network overloads), communication asymmetry etc.,

- **AUDIT client** responsible for transferring the Self-AUDIT data to **AUDIT server** located at TSG/SDH master side (see also AUDIT server at SDH),

- **HOLDOVER supervisor** that is a critical functional block. It is tightly linked to **Self-AUDIT server**, and it monitors network performance at PDV (Packed Delay Variation) level (Fig. 8). The holdover supervisor decides whether and for how long holdover mode should be activated at UT. For this reason, holdover supervisor is tightly related also to the NTP service at UT.

METROLOGY TESTING AT DEMETRA PROJECT

TSI#2 is 1 of 9 new time services developed for the purposes of the DEMETRA [1][16] Project. Each service is expected to be tested at both the SHORT-LOOP campaign at INRIM laboratory, and the END-TO-END campaign at the end-user premises.

In case of TSI#2, the SHORT-LOOP campaign will demonstrate service performance when operating at LAN and Internet. Under the END-TO-END campaign we will perform production environment tests over the Internet only.

The DEMETRA Demonstrator [1][16] is based on a reference time facility (TRF), relying on EGNSS and UTC(k) time laboratories, a data storage system, and a validation facility which measures the quality of the disseminated time independently from TSI. This common infrastructure provides the support to all TSI time services that distribute time through different channels and by means of different technologies.

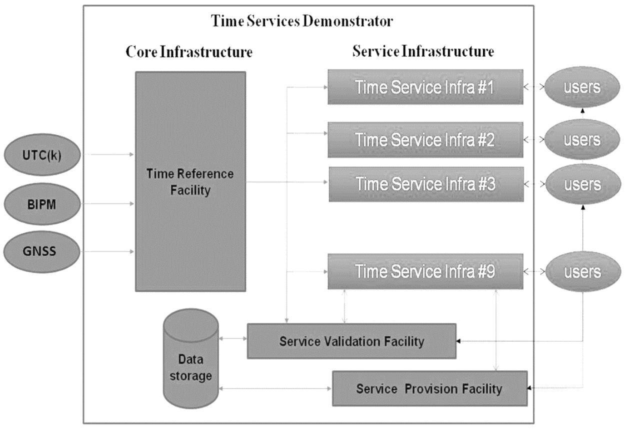

Fig. 11 DEMETRA infrastructure

BUSINESS OPPORTUNITIES

Time is the critical factor in separating cause from effect and the global market is continuously decreasing time intervals for e-business transactions. Therefore, properties such as: integrity, non-repudiation, authentication, and validity become more and more important, similarly to the accuracy of time. A very good example supporting our case is the ESMA MIFID II and MIFIR regulation [18].[1]

In case of safety-critical applications in areas such as Air Traffic Control or Smart City and Security Monitoring, the lack of accurate synchronization becomes a big issue. Dimming or spoofing GPS emerges as a problem of tomorrow. Thereby, market opportunities for advanced time synchronization services is growing and maturing.

Applications using cryptography and secure e-document exchange typically require accurate (NTA) official time UTC to work seamlessly. Some public services even require highly accurate timekeeping by the law. Billing and services and similar applications must know the time accurately. Virtual machines (VM) and virtually networked computing systems requires time synchronization even in areas beyond safety-critical systems, for example to ensure cohesion in common shared memory or IoT/Cloud based shared file systems. At a first glance it may seem very distant and still not very much relevant, but noteworthy, not so long time ago Google Inc. put considerable money on Spanner Google's Global-Distributed Database development [19] that use "Truetime" synchronization, and which aim is exactly to power Google's database at IoT infrastructure.

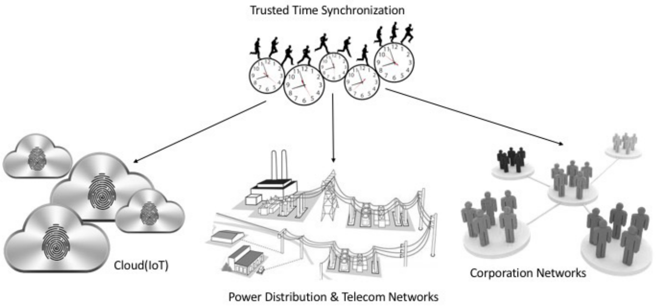
Trusted Time Synchronization
Cloud(IoT)
Power Distribution & Telecom Networks
Corporation Networks

Fig. 12 Trusted Time Distribution Market Share

Even sorting e-mails, or databases can also be difficult if time stamps are incorrect. Assuming lag aspects of using e-documents the trusted time and valid time seems to be important, in particular in public administration.

In addition, tracking security breaches, network usage, or problems affecting a large number of components can be nearly impossible if the time stamps in LOGs are inaccurate or according to wrong time ref. For telecom services, synchronizing can seriously compromise communication and the voice service can stumble. Wrong synchronization provides the throughput of data connections to be reduced and the network connections in the Internet can be totally lost. In case of mobile communication, handover between cells could fail and the quality of user experience be compromised.

[1] MiFID is the Markets in Financial Instruments Directive (2004/39/EC). It has been applicable across the European Union since November 2007. It is a cornerstone of the EU's regulation of financial markets seeking to improve the competitiveness of EU financial markets by creating a single market for investment services and activities and to ensure a high degree of harmonized protection for investors in financial instruments

CONCLUSIONS

1. Network synchronization protocols like NTP or PTP, currently do not provide feedback on the status of synchronization at the client side. Servers and Master Clocks are simply transferring responsibility of synchronization to clients. Elproma proposes a TSI#2 solution where Servers and Master Clocks (TSG level operations) provide reference UTC time and automatically perform audits to validate the client clock synchronization.
2. Being able to audit the client time allows us to introduce the concept of VALID TIME. Under TSI#2 the UT (User Terminal) is claimed to provide VALID TIME if in the course of a remote audit performed by the Server, the measured client time remains in the range defined as: *UTC(k) +/- max. OffsetError*.
   The TSI#2 provides the necessary infrastructure and tools, consisting of both SW and HW components, to claim the client time as VALID or INVALID.
3. TRUSTED TIME DISTRIBUTION is a wider concept that takes into account the security properties such as: integrity, non-repudiation, validity, authentication. Although some of the existing synchronization protocols already support cryptographic authentication only they still do not provide remote monitoring (periodical audits) on client clock synchronization, so they are not fully resistant to manipulation. TSI#2 use std. NTP authentication, but it also involves other than NTP authentication methods to protect all: synchronization, audits, communication and even HW/SW component configuration. These methods overcome the recently discovered problems like NTP 'Heartbleed' vulnerability (CVE-2014-0160) related to OpenSSL used by NTP [29].
4. If we could distribute time in a way that it can be verified remotely as VALID/INVALID at a client side, we could offer added-value services/systems such as TRUSTED TIME DISTRIBUTION, and remote TIME AUDITING. In today's world, where safety and security play critical role in B2B, B2C, B2G applications, markets at both local and global level should be ready to pay for these services. Trusted, valid time might be considered a utility, similar to electricity, and be provided under a new business model where hardware is provided for free and the customer is charged for the trusted time provision service.
5. A new market is opened for added-value time services. TSI#2 can support audits and time distribution systems required by ESMA MIFID II and MIFIR [18] for financial sector. TSI#2 uses NTP, but it can also base on other more accurate protocols like PTP/WR[2]. TSI#2 infrastructure model remains open and can be freely adjusted or extended.
6. Client clock synchronization and auditing over the Internet can be improved using early network connection problem detection. To avoid synchronization random peaks related to network traffic, overloads, asymmetry etc., we perform the PDV (Packed Delay Variation) level analyses and enable a temporary holdover mode at the client (UT) side.

REFERENCES

[1] P. Tavella and DEMETRA consortium, "The Horizon 2020 DEMETRA project: DEMonstrator of EGNSS services based on Time Reference Architecture", Metrology for Aerospace (MetroAeroSpace), 2015 IEEE Benevento 2015, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7180634

[2] G.Daniluk (ELPROMA), T.Wlostowdki (CERN) "White Rabbit" The sub-nanosecond synchronization for embedded systems Precise Time and Time Interval Systems and Applications (PTTI), Long Beach, CA, USA, 14-17 November 2011 http://www.clepsydratime.com/file_upl/PDF/Seminaria/Elproma%20CERN%20%28White_Rabbit%29.pdf

[3] A.E. Wallin, T. Fordell, J. Myyry, P. Koponen, M. Merimaa, "Time Transfer in a Wide Area White Rabbit Network", 28th European Frequency and Time Forum, 23-26 June 2014, Neuchâtel, Switzerland.

[4] M. Lipinski, "White Rabbit: a PTP application for robust sub-nanosecond synchronization", IEEE ISPCS, 35-30, 2011.

[5] P. Defraigne, F. Roosbeek, A.Somerhousen "Sertting Up a NTP Server at Royall Observatory of Belgium", PTTI 2004

[6] W. Aerts, G. Cerretto E. Cantoni and J.-M. Sleewaegen, "Calibration of Galileo signals for time metrology", IEEE transactions on UFFC, 12/2014 61(12):1967-75.

[7] P. Defraigne et al, "Advances on the use of Galileo signals in time metrology: calibrated time transfer and estimation of UTC and GGTO using a combined commercial GPS-Galileo receiver", in Proc. of the Precise Time and Time Interval Systems and Applications (PTTI), Bellevue, WA, USA, 3-5 December, 2013.

[8] P. Defraigne, W. Aerts, E. Pottiaux, Monitoring of UTC(k)'s using PPP and IGS real-time products, accepted in GPS solutions,19 (1), p. 165–172, 2015. doi : 10.1007/s10291-014-0377-5.

[9] P.Waller, F.Gonzalez, S.Binda, I.Sesia, I.Hidalgo, G.Tobias, P.Tavella, "The In-orbit Performances of GIOVE Clocks", IEEE Transaction on Ultrasonics, Ferroelectrics, and Frequency Control, Volume 57, issue 3, March 2010, pp. 738-745.

[10] L. Galleani, P. Tavella, "Detection and identification of atomic clock anomalies", Metrologia, Vol. 45 Issue: 6, Pages: S127-S133, December 2008.

[11] I. Sesia, L. Galleani, P. Tavella, "Application of the Dynamic Allan Variance for the Characterization of Space Clock Behavior", IEEE Transactions on Aerospace and Electronic Systems, Volume 47, issue 2, April 2011, pp. 884-895.

[12] Network Time Foundation
http://www.networktimefoundation.org/

[13] Network Time Protocol (NTP) site http://www.ntp.org

[14] Precision Time Protocol sites:
PTPd https://github.com/ptpd/ptpd
Linux PTP Project http://linuxptp.sourceforge.net/

[15] SyncLab RADclock
http://www.synclab.org/radclock/

[16] P.Tavella I. Sesia, G. Cerretto, G. Signorile, D. Calonico, R. Costa, C. Clivati, E. Cantoni, C. De Stefano, M. Frittelli, V. Formichella A. Abadessa, A. Cernigliaro, F. Fiasca, A.Perucca, S. Mantero,

T. Widomski, J. Kaczmarek, J. Uzycki, K. Borgulski, P. Olbrysz, J. Kowalski, P. Cerabolini, L. Rotiroti, E. Biserni, E. Zarroli, V. Leone M.T. Veiga, T. Suárez, J.Diaz, P. Defraigne, N. Ozdemir, Q. Blaire
M. Gandara, V. Hamoniaux E. Varriale, Q. Morante
V. Dhiri, E. Giulianini , M.Mangiantini A.E. Wallin
L. Galleani D. Hindley
European Project DEMETRA: Demonstrating Time Dissemination Services, PTTI 2016

[17] Elproma (CLEPSYDRA) Time Server site: http://www.clepsydratime.com

[18] European Securities and Markets Authority (ESMA), MiFID II regulations https://www.esma.europa.eu/policy-rules/mifid-ii-and-mifir

[19] Spanner: Googles's Globally-Distributed Database http://static.googleusercontent.com/media/research.google.com/en//archive/spanner-osdi2012.pdf

[20] D. Mills Computer Network Time Synchronization: The Network Time Protocol on Earth and in Space, Second Edition 2nd Edition (CRC Press)

[21] Jean-Loup Ferrant, Mike Gilson, Sebastien Jobert, Michael Mayer, Laurent Montini, Michel Ouellette, Silvana Rodrigues, Stefano Ruffini *Synchronous Ethernet and IEEE 1588 in Telecoms: Next Generation Synchronization Networks (Willey)*

[22] Peter Rybarczyk Expert Network Time Protocol (APress)

[23] David Deeths, Glenn Brunette Using NTP to Control and Synchronize System Clocks (SUM Press)

[24] Mills, D.L. Public key cryptography for the Network Time Protocol. Electrical Engineering Report 00–5-1, University of Delaware, May 2000. 23 pp.

[25] Mills, D.L. Clock discipline algorithms for the Network Time Protocol Version 4. Electrical Engineering Report 97–3-3, University of Delaware, March 1997, 35 pp.

[26] Mills, D.L., and P.-H. Kamp. The nanokernel. Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting (Reston, VA, November 2000).

[27] Mills, D.L., J. Levine, R. Schmidt and D. Plonka. Coping with overload on the Network Time Protocol public servers. Proc. Precision Time and Time Interval (PTTI) Applications and Planning Meeting (Washington, DC, December 2004), 5–16.

[28] Mills, D.L. Improved algorithms for synchronizing computer network clocks. IEEE/ ACM Trans. on Networks 3, 3 (June 1995), 245–254.Mills, D.L. Precision synchronization of computer network clocks. ACM Computer Communication Review 24, 2 (April 1994). 28–43.

[29] OpenSSL vulnerability (CVE-2014-0160) https://www.us-cert.gov/ncas/alerts/TA14-098A

[30] SIQ reference http://www.clepsydratime.com/Awards/SIQ-SI

[31] VSL reference http://www.clepsydratime.com/Awards/VSL-NL