Time critical infrastructure

Time requirements in various networks, from IoT to TaaS

States and governments have identified some "critical infrastructure", where critical mean that such infrastructure is so vital that its incapacity or destruction would have a significant impact on individuals, defense or economic security of the country. Based on this definition, critical infrastructure has been subdivided in various groups and key assets;

- Telecommunications
- Electrical power system
- Gas and oil storage
- Transportation
- Banking and finance
- Water supply systems
- Emergency services
- Continuity of government
- Nuclear power plants

Interdependence of each functionality, and dependence of individual group to common function, such as timing, is a main concern. Time dissemination is sometimes name as one the critical infrastructure group.

In parallel vulnerabilities has been identified, as the ability of critical infrastructure to provide continuous operation. Not only the infrastructure need to be reliable, and must be designed as being able "not to fail" and maintain its service any time in view of natural disaster, it has to be criminal-attack resistant. Lessons were learnt from Kobe earthquake, Fukushima accident, World trade center sept.2011 and other cyber attack supported by networks.

More generally, critical infrastructure not only need to be reliable, but it has to be not *vulnerable*. In that sense, GNSS signals, used as time sources (sometimes unique) in a network, is identified as vulnerable, because it is known easy to ***jam or spoof GNNS receivers***.

In fix lines Telecom, the last two three decades have seen drastic evolution of our personal environment. Telecom migrates form the well organized and well-structured PDH/SDH world after the first era of analog, to the more chaotic IP world. Then, all the timing resources embedded in every network operator SDH node vanished, timing signal became no longer available for free and became a commodity that user (or service operator) must take care of. Various network timing and various timing over network were introduced, based on protocols (NTP, and PTP later on), on SDH event timing, or dedicated interfaces over network. Aside the availability, accuracy and traceability (at least common source) became an issue.

Renewable energy dissemination, ***Smart Grid***, are and will be more and more using accurate time references. See the dedicated page "Renewable energy and Smart Grid" on this web site. Following the idea that in the next future (5 Y-15 Y?), network power energy (oil, atom…) role will be to match the need between consumption and power provided by the combination of green renewable energy sources, let's say that 85% will be green energy and 15% will be energy power network provided, compared to the actual situation, exactly the reverse, 85% from earth resources (Oil, Gaz, Uranium,..) and only 15% from renewable. In today's operation, inserting some marginal contribution of green energy in the network is an easy task. Tomorrow, one will have to match the consumption (residential and industry) with a highly fluctuating green resources (solar, wind, sea cycle,…), with a high potential offset between green provision and consumption (sun is working over Saturday and Sunday, wind is working over WE and overnight, while residential consumption is more concentrated on morning / evening and industrial needs concentrated over day…). After some political decision (mainly in Germany, Switzerland, Japan..) to get rid of nuclear energy, there were a lot of activities focusing on green provision, green storage (artificial lakes, bi level reservoirs – uploading when energy is available, down loading when energy is required), wind farms, optimization of wind yield, hydrogen power engine & mobility, etc…

One of the most critical issue , time related, will be to manage the concatenation of diluted consumption, diluted green resources (individual solar roofs, wind farms,..) and network complement (even if it is limited to a 15% contribution). See the "SCCER FURIES" link on this website. The tool will be to have a dynamic measurement of ingoing flow / outgoing flow on quite every street corner, to identify local in/out mismatch, collect all of these local mismatch at network (regional/nation-wide) level, to adjust the global equilibrium by flexibility of static sources (oil, gaz, nuclear). The tool to perform such local mismatch measurement is a PMU, Phase Measurement Unit, which must be able, at local network level and at distribution level, to perform phase and voltage real time measurement. The task is to identify a power variation (indicating a mismatch between provision and consumption) from a phase variation indicating a phase interconnection mismatch. In both cases, the network reaction must be drastically different, one is injecting more or less power, the second is to correct an interconnection. The critical issue is that this information must be locally gained in real time, within a portion of cycle time (ideally one quarter of a cycle), based on time analysis of digital voltage measurement. The digital voltmeter will need to be highly accurate, but the time base used to quantify the evolution (over some ms) of the signal is more than critical. Not only the local time source must be low noise (low time jitter), highly accurate (less than 1 microsecond drift over hours), the local source must be synchronous with all the other time reference used in any and all PMUs, in order to provide a complete, global and accurate energy network behavior, to allow the proper network reaction…. See papers from Pr M Paolone, EPFL Lausane, the time accuracy request of time base in PMU must be in the range of 100ns, network synchronous….. not an easy task, but what a critical issue in energy distribution. It is easy to imagine what could happen if these PMU measurements became wrong by the fault of the local time base or by a lack of network synchronization….

Financial trading for legal and traceability issue of regular bank transaction, and the HF trading (high frequency high speed trading), banking system is now demanding sub-microsecond time accuracy over long distance (such as between NYSE and Chicago, London or Paris). Frequencies of trading increases beyond the several million per second, the need to identify the time of every transaction is becoming critical from the point of view of clarity and a consolidated audit trail.

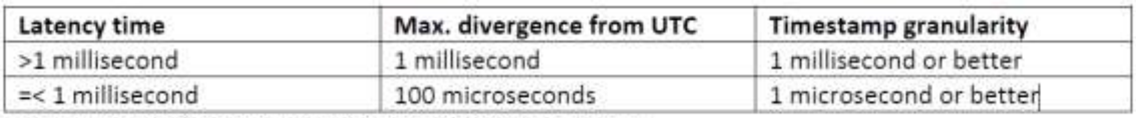
At the microsecond level and below, the realization of a unified 'common clock' accepted by all financial actors, does not exist yet, due to disparities in local time sources, implementations, distributions.

The European Securities and Markets Authority (ESMA) has issued a series of technical standards in support of the MiFID (Markets in Financial Instruments Directive) regulations, under final approval by the European Commission. Despite its vulnerability and its lack of legal traceability to UTC, GNSS is still a proposed time origin…. Physical implementation, mainly in UK, were done over fiber, fully GNSS-free.

RTS 25, part of Regulatory Technical Standards, deals with clock synchronization. Technical regulations are described below:

Article 1 states that business clocks that give the timestamp for any reportable event should be synchronized to **Coordinated Universal Time (UTC)**, using either a link to one of the timing centers maintaining a UTC(*k*) realization of UTC (or the timed signals disseminated by GPS or another satellite system *(which is proven to be easy to jam or to spoof.!!.)*

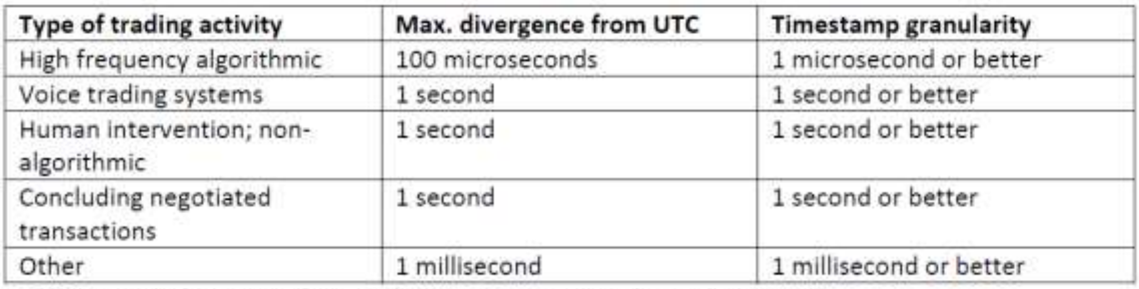
Article 2 describes the level of accuracy (maximum divergence from UTC) that should be achieved by the operators of trading venues, taking into account the gateway to gateway latency of their trading systems.



Latency time	Max. divergence from UTC	Timestamp granularity
>1 millisecond	1 millisecond	1 millisecond or better
=< 1 millisecond	100 microseconds	1 microsecond or better

Table 1: Level of accuracy for operators of trading venues.

Article 3 defines the level of accuracy that apply to members or participants of trading venues, table 2.



Type of trading activity	Max. divergence from UTC	Timestamp granularity
High frequency algorithmic	100 microseconds	1 microsecond or better
Voice trading systems	1 second	1 second or better
Human intervention; non-algorithmic	1 second	1 second or better
Concluding negotiated transactions	1 second	1 second or better
Other	1 millisecond	1 millisecond or better

Table 2: Level of accuracy for members or participants of a trading venue.

Article 4 specifies the need to demonstrate traceability to UTC by documenting system design, functioning and specifications, and to identify the exact point at which a timestamp is applied. The traceability system should be reviewed at least once a year to ensure compliance with the regulations.

The key points are the target accuracy (sub μs) and the traceability to UTC…
This aspect of UTC traceability should, by itself, eliminate de facto GPS solution, but may keep Galileo in the loop. Security, cyber-resistance, robustness to jamming and spoofing may eliminate all classical GNSS based solutions.
The only options would be HW and SW secure Galileo receivers, multi-frequencies, using reinforced HW such as beam forming antennas or other HW protecting the integrity at receiver level, and secure SW. The actual costs of such solutions are out of scope for commercial applications.

The local UTC(k) labs (physical realization of UTC in every country) offer the opportunity to deliver accuracy and security to worldwide financial markets, providing a means to achieving both a local accurate time feature and a coherently-synchronized solution in intermarket activity, each node being synchronized to UTC.

Timing in banking system, mostly for HF trading, is needing two axes

> time accuracy at both ends, good enough to handle long distance time transfer propagation time
> time traceability to UTC at both ends to achieve global traceability

Combining the accuracy and security requirements, and despite (even because of..) the ease of deployment of PTP solution over existing networks for time synchronization in trading networks, it may appears as a good solution, for accuracy point of view, for replacing lower precision standards such as NTP and IRIG-B, or even replacing high precision solutions requiring dedicated hardware at the host level, such as GPS, by far not as secure as a proper fiber based “out of traffic channel” solution, PTP-WR, operating over dedicated channels or fibers, will become the right standard in HF trading and banking system.

Such a fiber based solution, based on White Rabbit, will provide

- Compliant with MiFID II RTS 25
- ns level Precision timing distribution solution
- No reliance on GPS or internet time
- Eliminates susceptibility to GPS jamming, spoofing,
- Implementation might be done outband “ie away from from traffic load) over fiber optic links, for resilience and security
- Directly traceable and certified to UTC at the point of provision, not the source

Such solution deployed in UK was proven to be capable of achieving approximately 100 nanosecond synchronization to the UK legal time, UTC(NPL), over full trading network.

Implementing secure, GNSS independent, and very accurate time sources, will translate in a strong “legal” obligation over banking system, and “robustness test” will be applied to reveal lack of awareness in financial services sector, to track and eliminate inefficient means of timestamping.

Wireless telephony timing requirement evolved a lot during the last decades. From 2G, FDD (Frequency Division Duplex) to the last TD-SCDMA (the most complex, mixing frequency, time and code duplex technologies), ***Telecom*** 4G and next to come 5G, issues like frequency aggregation at Radio Access Network, exhibit sub microsecond timing requirements (see dedicated paper Timing requirement in Telecom networks).

Main issue is disseminating accuracy to mobile base station to allow high density / high bandwidth traffic, through aggregation on TDD spectrum between BS and mobile, and disseminate a network-synchronous basis between various base station, to provide handover facility (automatic switching from one BS to another while traveling).. There are basically two options : network timing dissemination through network media (fiber and/or network infra) and second on a wireless basis, such as dedicated long wave carrier phase modulation (DCF 77 in Germany, France Inter in France, and similar in US, Japan,…), eLORAN development (deployment on ground of the LF -# 100 kHz- signal of the original signal dedicated to coastal and harbor navigation), and the most common GNSS (GPS, BEIDOU, GLONASS, GALILEO satellite based navigation system). Today’s requirement , down to +/- 130 ns or even +/- 65ns at BS level, exclude classical NTP, PTP protocols, exclude eLoran and DCF-type signals, while security concern impose to reject GNSS-only timing solution (see VOLPE report), leading to the conclusion that the quite unique actual technology providing accuracy and robustness is PTP-White Rabbit.

In short, there are three alternative solutions

- **GPS receivers**: accurate to 100ns, known to be vulnerable. high performance ‘flywheel’ oscillator needed to provide short-term stability and holdover (going outside 100ns level)
- **IEEE 1588-2008** (IEEE 1588v2 or PTPv2): accurate to 1000 ns, sensitive to network traffic, cumulative jitter / nb Hops; SyncE requested - fails to address new requirements

- **Assisted Partial Timing Support -APTS (GPS/PTPv2/SyncE)**: autocontrol, removes the full on-path PTP requirement, combine good and bad, GPS receivers vulnerable
- **PTP**-White Rabbit, deterministic PTP, dual way SyncE and DDMTD (Digital Dual Miser Time Difference), allows to reach sub ns level over fiber, and may operate using dedicated channel/wavelength, management channel, or act through an additional wavelength inserted in the channel traffic (in any case, not affected by traffic load)

Railways,Transport network vulnerabilities : vulnerabilities appear to be acts of sabotage, terrorism either directly or indirect (ie through a third party critical group used by transportation, such as energy or timing. Impact would be to stop operation (ie by cutting electrical power feeding), but is might be inserting false informations through the network information network, an attack “man in the middle in information network”, or false timing/localization informations…

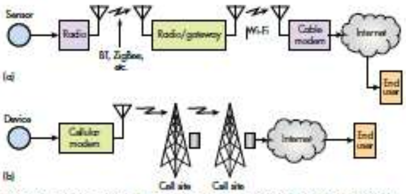
IoT / IoT-Enabled Smart City Framework Smart City technologies are being developed and deployed everywhere. NIST has provided a very interesting report [Time-Aware Applications, Computers, and Communication Systems (TAACCS), Marc Weiss and al., NIST, **Technical Note 1867 Natl. Inst. Stand. Technol. Tech. Note 1867, 25 pages (February 2015) CODEN: NTNOEF],** supporting a global vision of future and impact anticipation to be done.
There is a general agreement to say that there will be billions of intelligent objects connected to Internet, many of them will belong to different “service networks”. This massive collection of sensors, actuators, and/or devices will be connected one to another or to some master control or monitoring point, *via the internet.*

Experts, from NIST or others, are performing recommendations to the 10^9 endpoints to be connected to the internet in the next 5 years or so…

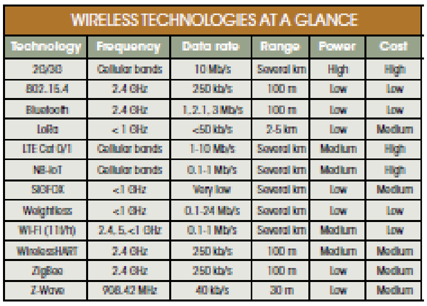
Aside the number of connected objects, one issue will be to handle multiple communications links that may be used to make the connection, as a vast number of connection configuration will be implemented:

Passive / active operation
Data rate of the device:.
Range or distance to the gateway:
The environment: EMI, etc.
Need for encryption or authentication:
Power consumption:
Capacity: Number of connected devices.
Quality of service and reliability.
Network topology: Star, mesh, or other.
Simplex or duplex: One-way vs. two-way communications.
Suitable and available spectrum: Licensed or unlicensed.
Cost: Design, manufacturing, internet access service fees
Internet access: Cellular, DSL, cable, satellite

The wireless connection technologies are expanding carrier, bandwidth, along with the minimum power required. LORA connection is gaining high momentum in IoT connection



The diagram shows typical wireless-connection scenarios for the IoT (a) and M2M (b).



WIRELESS TECHNOLOGIES AT A GLANCE

Technology	Frequency	Data rate	Range	Power	Cost
2G/3G	Cellular bands	10 Mb/s	Several km	High	High
802.15.4	2.4 GHz	250 kb/s	100 m	Low	Low
Bluetooth	2.4 GHz	1, 2.1, 3 Mb/s	100 m	Low	Low
LoRa	< 1 GHz	<50 kb/s	2-5 km	Low	Medium
LTE Cat 0/1	Cellular bands	1-10 Mb/s	Several km	Medium	High
NB-IoT	Cellular bands	0.1-1 Mb/s	Several km	Medium	High
SIGFOX	<1 GHz	Very low	Several km	Low	Medium
Weightless	<1 GHz	0.1-24 Mb/s	Several km	Low	Low
Wi-Fi (11/ah)	2.4, 5, <1 GHz	0.1-1 Mb/s	Several km	Medium	Low
WirelessHART	2.4 GHz	250 kb/s	100 m	Medium	Medium
ZigBee	2.4 GHz	250 kb/s	100 m	Low	Medium
Z-Wave	908.42 MHz	40 kb/s	30 m	Low	Medium

Various aspects have to be considered, depending of the “civil responsibility” of specific devices:

- ns timing over a network best effort/guarantee for safety-of-life applications.
- Passive / active sensors, both require time: @ network (P), embedded (A)
- Co-deployment of asynchronous and synchronous protocols. Event synchronization
- Sensors may be part of multiple networks, PAN Personal Area Network (PAN)
  different levels of accuracy or precision,
  the extent of the availability of the technique,
  the amount of power available or needed,
  the verifiability or security of the timing supplied
- real-time data communication which will require TTE : time-triggered Ethernet
- OSI layer vs layer access required for timing (SyncE: layer 1, PTP: layer 2/3,…)
  - Time transfer not considered in the original OSI 7 layers !.
- **Audio/video industry to use standard networks** instead of analog or special-interfaces,
- latency control is essential for many real-time applications like audio/video,
- multicast traffic, (financial and other) : **transit times** must be measured and validated
- Time of flight measurement & correlation of data packets passively or actively monitored
- Correlation of globally synchronized statistics from point-to-point active protocols

In short, there will be multiple factors in IoT networks, covering many different criteria levels, and time will be critical in some applications (est. 1% of global…. Only 10^7 time critical endpoints..!)

- **The IoT will have many devices and applications that require frequency, time or phase synchronization** (operation, successive alarm event datation through different channels)
- **The use of disseminated timing accuracy for root cause analysis**
- Verifying time accuracy and traceability
- Time Sensitive Networking (TSN): suggests extremely low latency (few microseconds or less) by **quiescing** links at the right time, allowing **time-sensitive packets to pass through free of traffic impact**. > the network infrastructure(s) and user(s) must agree on timebase and schedule for every set of time-sensitive paths

In conclusion, IoT deployment will be the source of multiple protocols / multiple configuration of Internet connection, and timing, more or less accurate, will be required at sensor level or at the collecting point level

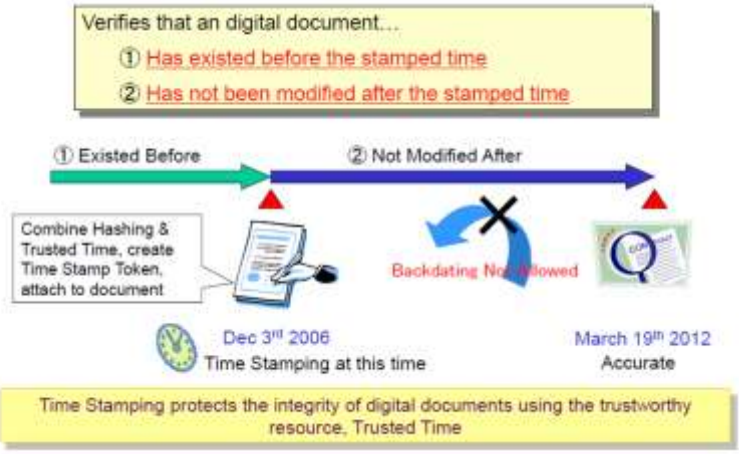
Energy distribution (high voltage network) : fault detection, managed interconnection. Time requirements in High voltage energy distribution serve at least two issues : fault detection, as accurate timing and propagation time of electrical signal might identify very precisely a fault in the network, and accurate timing may avoid phase mismatch issues when interconnecting issues (see the black out that happen some years ago between Germany, Swiss and Italy).

Here again there are two main questions : availability of timing signals and integrity of the timing signal, and common time-reference between distant nodes . Availability and integrity mean that we probably need to have in place alternative and independent timing routes from a secure time origin, such as UTC(country) which is the legal time representation in the country, or, at least, implement a local clock stable enough to be able to reject any spoofing attempt and detect jamming (that’s the easiest part) and go in holdover to guarantee time integrity,

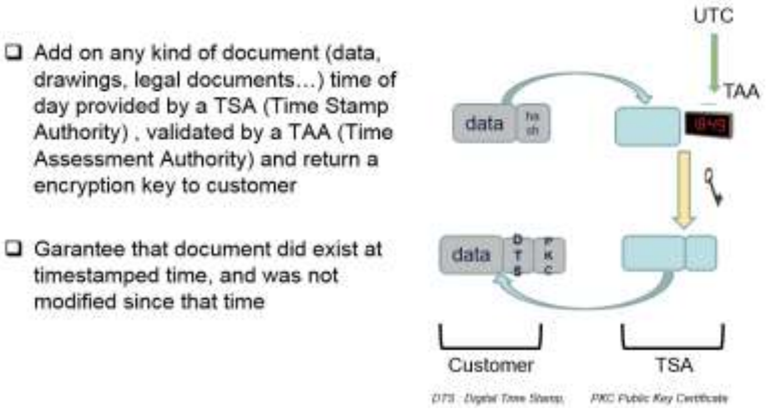
Cryptography is inherently highly demanding of time synchronization. Moreover, accurate timing is by itself a powerful tool, if we add a time mechanism to an encryption algorithm, or operate a time-specific encryption (TSE) or time release encryption (TRE), time encryption at sending level and receiving level will allow to detect any intrusion such as "man in the middle", or using a time instant key (TIK), the receiver will be able to decrypt the message only with the right TIK. Specifying in what time interval a ciphertext can be decrypted will be useful feature. Time accuracy at both end, and time delay of propagation from A to B, are defining high accuracy timing requirements. If a signal need some ms to travel over some 1000's ok km, it is just some µs is both ends are distant by less than some kms. Then time accuracy will fall in the range of sub µs.
There are huge development in this area, looking for time-lock crypto, avoiding the general mistake of using third party time reference, despite the potential vulnerability. Replacement of vulnerable third party might involve time based tools, such as "no unlocking after a certain elapsed time", or similar algorithms. There are lest three variants of protocols providing time-released encryption, forcing the receiver to solve some time consuming problem before being able to decrypt, use of third party trusted entity providing a piece of information needed to decrypt, algorithms (factorization, quadratic,..) to implement TRE. An encryption concept, such as "sending message to the future", under the public key / private key sharing protocol, is also an option using accurate time to the encryption process. One can also name the "time lock puzzle" encryption process. Applications of time encryption are numerous, one can cite sealed-bid auctions (define date of opening, and guarantee prior date inviolability), stock trades, and HF trading (on top of intrinsic time accuracy and traceability requirements, confidential data collection during secret trial, electronic voting, etc)…See dedicated papers about encryption, a complete subject by itself.

In short, sub µs-accurate and secure time is , there again, highly requested.

Time stamping, is a developing feature. More and more, we are all planning to save the earth and use less and less paper. A paper- less transaction, between individuals and administration / government, legal contracts, patents deposit, legal acts, .. are now exchanged via Internet, and need to be "signed and certified". Time is a critical tool in encryption and data certification. A typical example of such process, aiming to define the time at origin and status at origin, to guaranty that such document was not modified since it has been created, is described on the graph below:

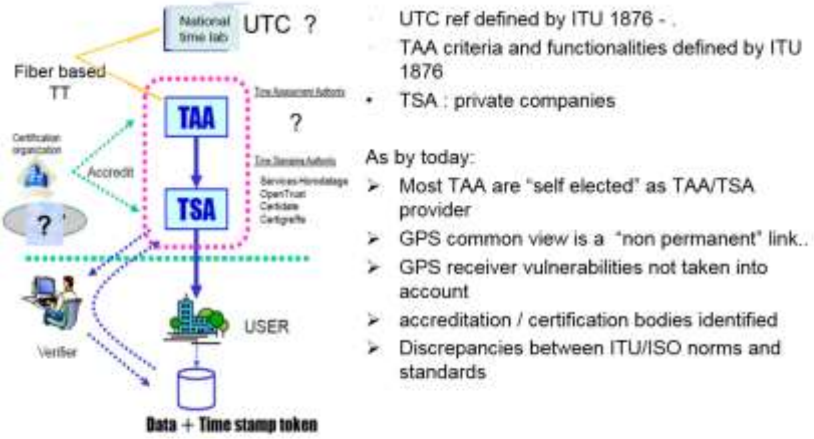

Verifies that an digital document…
① Has existed before the stamped time
② Has not been modified after the stamped time
① Existed Before
② Not Modified After
Combine Hashing & Trusted Time, create Time Stamp Token, attach to document
Backdating Not Allowed
Dec 3rd 2006
Time Stamping at this time
March 19th 2012
Accurate
Time Stamping protects the integrity of digital documents using the trustworthy resource, Trusted Time

Following the ITU 1876 and ISO 1814 recommendations, we have to define the time origin (legal time: UTC(country), the TSA, Time Stamping Authority who will encrypt your document with reference to the legal time at encryption, and the TAA, Time Assessment Authority, who will be providing certificates to TSA and perform control on the timing chain status:



- ❑ Add on any kind of document (data, drawings, legal documents…) time of day provided by a TSA (Time Stamp Authority) , validated by a TAA (Time Assessment Authority) and return a encryption key to customer
- ❑ Garantee that document did exist at timestamped time, and was not modified since that time

The roles of various organization and the scope of various norms are described below:



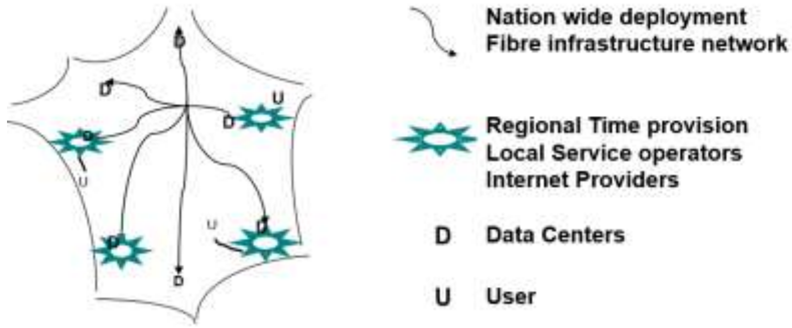
- UTC ref defined by ITU 1876 - .
- TAA criteria and functionalities defined by ITU 1876
- • TSA : private companies

As by today:

- ➢ Most TAA are "self elected" as TAA/TSA provider
- ➢ GPS common view is a "non permanent" link..
- ➢ GPS receiver vulnerabilities not taken into account
- ➢ accreditation / certification bodies identified
- ➢ Discrepancies between ITU/ISO norms and standards

There are still some work to do to improve and secure the global concept. In fact the key issue is that we cannot rely on GNSS-only time dissemination, as we have seen in many occasion on this web-site that GNSS signals are easy to spoof or to jam. Even if the original proposed standards were using GNSS as prime sources, the evolution is to move towards a more secure time reference, such as fiber-based WR protocols.

Time as a Service : all the examples given so far address many aspect of our daily activities. The global conclusion is that a traceable trusted time, at some level of accuracy, will be required everywhere, and primarily in local data center. Then we can imagine a time network, getting time from UTC(k), the legal time in the country, and disseminating this time all over the country, using nationwide fiber network. The first dissemination access will be data center located in every main city. Globally, this may service huge number of customer, and this service may represent a significant value for customers, subscribing services performed or collocated in disseminated time-aware data centers. This is the concept of "Time as a Service". The hidden idea is that, on the contrary of most of vendors claiming TaaS capability, but delivering either GPS signals (!) or NTP time coming from Anywhere (!), an unknown sources even over static IP addresses, the network I am describing is the following:



- ➢ Getting time from and only from the national UTC(k)
- ➢ This time is disseminated through, for example, a PTP White Rabbit network, operating over fiber independent of traffic network, either management fibers, alien wavelength or dark fiber,
- ➢ redundancy over and independent forth and back loop for high availability
- ➢ adequate calibration and supervision process SCADA, providing and managing sync-path

In conclusion, our personal surrounding will be more and more connected, and a lot of applications (Telecom, Smart Grid, railways, Time stamping, IoT networks, …) will be , with different level of accuracy and availability, time critical. Timing protocols, over fiber or wireless connection, using as less as possible specific HW, will be required