TRACEABLE AND CERTIFIED TIME, FOR DIGITAL SOVEREIGNTY

Summary

Dear readers,

Time has always been ubiquitous in human activities, whether on a philosophical or physical level.

Since the 18th century and the advent of mechanical clocks, clockmakers have contributed to the growth in commercial exchanges, then physicists started to master time measurement with given precision, to make it "reliable".

Although high precision time production is perfectly mastered by the Observatories of Paris and Besançon, the actual technological challenge is to master the security and traceability of the date and time from their source to the final user. This is key to fighting cyberattacks that interfere with the time message.

Indeed, Time holds a central position in our digitized world. Time synchronization is vital for the operation of Data Centers, computers, smart device (IoT) ... and more generally all applications or digital systems, because they involve exchanges of data that must be timestamped accurately. Today, the limitations of the massive deployment of the Cloud, interoperability and IT transactions are all directly connected to the time and its reliability...

The relevant risks such as data loss, transaction errors, transport incidents or even major server failures imply that no transition to the digital world is possible without a complete time information, which shall be certified and accurate.

Now more than ever, controlling Time has become ***a question of sovereignty****. Therefore, the challenge that we are facing... is indeed the cybersecurity of Time!*

Based on this observation and to take up these challenges, in 2013, Maurice Gorgy brought together French laboratories and companies in the Time/Frequency industry on an ambitious project: ***SCPTime®****. This collaborative research project has been approved by the Grand Investments Commission within the scope of the "Investissements d'Avenir" program and signed by the French Prime Minister on June 2nd 2014. The R&D phase is financed by BPIFrance (big collaborative projects) and endorsed by Minalogic.*

This white paper was produced so that everyone can better understand what is at stake related to security and traceability of Time in today's digital economy.
Thus, we will see how the race for precision, once a guarantee of reliability, has gradually given way to the officialization of Time sources and to the resilience in their delivery to users. This is the keystone of the ***SCPTime®*** *company that you will discover in the following pages, genuinely forward-looking.*

Enjoy reading.

Nicolas GORGY

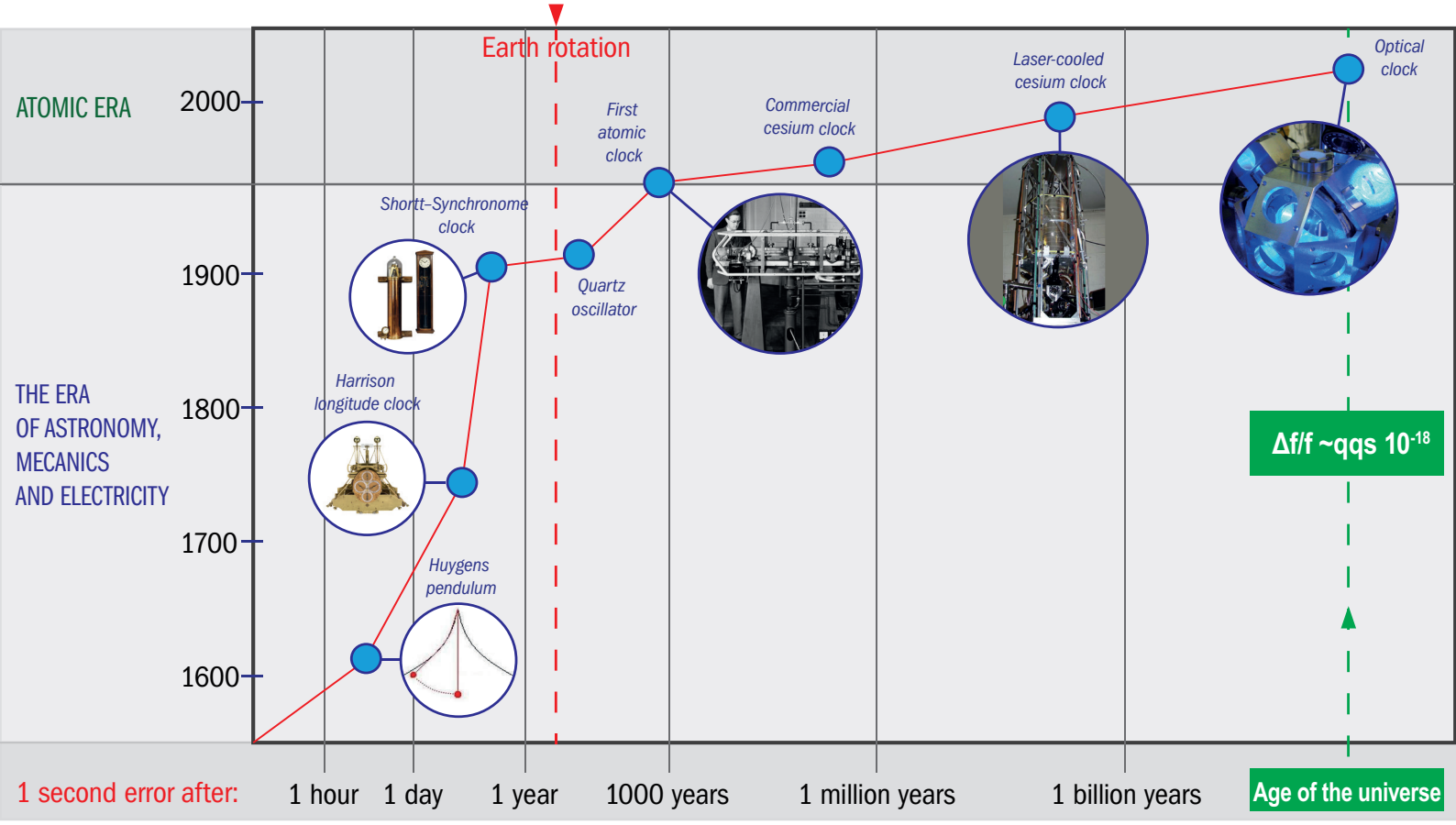
**(Observatory of Paris, CNRS, UPMC, LNE)*

1 - FROM THE RACE FOR PREICISION TOWARDS A NEED OF CERTIFICATION

Over the millennia, man has continuously demonstrated generosity to master Time and exercise its measure, as he tried to do for each of surrounding elements.
From astronomical guides predicting the arrival of seasons for agriculture, to the first hourglasses or other objects capable of counting the elapsed Time, each technology called for a new one as soon as the previous one reached its limit of precision.

METROLOGY AND TIME PRODUCTION: A LONG HISTORY...

This diagram shows the historic development of technologies and accuracy performance.
The accuracy of time dissemination is steadily improved by a factor of 10 every decade.



Source SYRTE SCPTime® partner

As we can see from the previous illustration, it is no longer hourglasses that we are talking about today, but quantum physics! ...

In 1967, the metrological definition of the unit of time was adopted to enter the atomic era. It is even preparing to soon enter the subatomic era (particles)...

Laboratory cesium or atomic fountains using laser cooling techniques of atoms have achieved extreme accuracy. Their relative frequency stability reaches a few Femtoseconds (10^{-15}) at one second, and their accuracy at 10^{-16} or even better...

New technologies in the fields of research, space, energy, Telecommunications and even Digital have gradually required such levels of accuracy.

This race for accuracy has accelerated over the course of major technological discoveries, with the ultimate goal of having the most precise and constant time reference possible, and in other words, the most "reliable" possible according to the criteria established ...

Thus, until less than a decade ago, making Time reliable was to master the reference and to reproduce it while minimizing its drift.

In the digital age, however, with the zettabytes of data consumption, billions of smart devices and the explosion of "All Digital", the challenges of a reliable Time have gone beyond these criteria of precision and consistency.

DEFINITION OF THE SECONDE, THE SI (SYSTÈME INTERNATIONAL) UNIT OF TIME:

"The second, symbol s, is the SI unit of time. It is defined by taking the fixed numerical value of the cesium frequency $\Delta\nu_{Cs}$, the unperturbed ground-state hyperfine transition frequency of the cesium 133 atom, to be 9 192 631 770 when expressed in the unit Hz, which is equal to s^{-1}.

$$1\ Hz = \frac{\Delta\nu_{Cs}}{9\,192\,631\,770} \quad or \quad 1\ s = \frac{9\,192\,631\,770}{\Delta\nu_{Cs}}$$

It follows from this definition that the second equals the duration of 9.192.631.770 periods of radiation corresponding to the transition between the two hyperfine levels of the ground state of the cesium 133 atom."

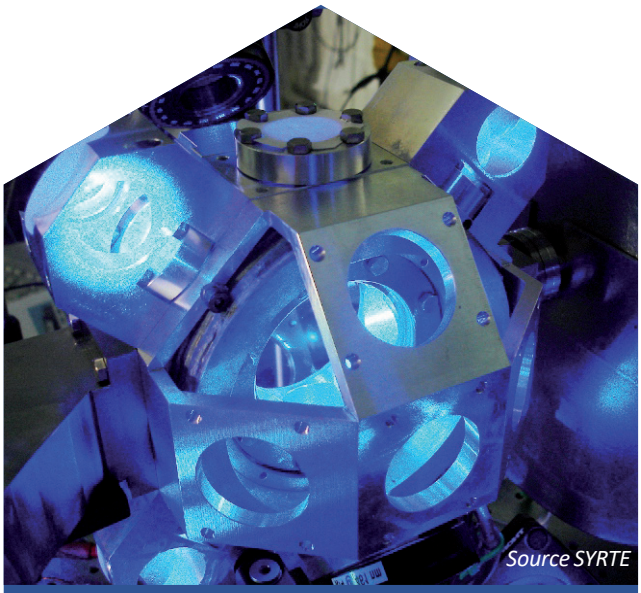
Indeed, as we will see in the following chapters, **Time data - however precise - has lost its reliability because it has become vulnerable.**Time is now subject to cyberattacks, intentional or residual jamming, spoofing, and any form of malicious corruption.

However, this "Time Dimension", without which the "cause cannot be separated from the effect", is more essential than ever in the context of our constantly evolving society. Digital technologies and data exchange are advancing exponentially and need a reliable time reference to ensure normal function.

In daily life on our planet, Time is a sovereign data on which a huge part of our modern, digitized economy relies, **without awareness on our part sometimes**.

In fact, an unreliable or corrupted time signal will cause transport incidents, data loss, transaction errors, service disruptions and damages of all kinds.

Most of the time, these dysfunctions are caused by malicious attacks, inherent to the new digital environment in full expansion, and to which the sources of time synchronization are more and more exposed. However, they can also be the result of electromagnetic disturbances due to solar winds, and many other interferences...



Source SYRTE

2013, THE STRONTIUM OPTICAL CLOCK.

Towards a redefinition of the second

In France, the SYRTE developed two optical lattice clocks with strontium atoms (ultimate limit 10^{-18}). These clocks showed improved accuracy and stability over the atomic fountains. An optical radiation has a frequency 100.000 times higher than that of the cesium 133. This world first is a major step and shall lead to a new international redefinition of the second by 2026.

2 - THE CURRENT STATE OF EXISTING TIME SIGNALS AND THEIR VULNERABILITY

To better understand the challenges of secure time synchronization, let us look at this chapter to identify the main time sources, and understand how the technologies most used to distribute them have become so vulnerable.

TIME SOURCES AND THE NECESSITY TO GET A LEGAL REFERENCE.

Originally driven by political will, sources of Reference Time emerged in the early 20th century with the main objective of harmonizing and facilitating trade.

First national, these Time references became international with the advent of Universal Time (UT) in 1956, then Atomic Time in 1971 and lastly COORDINATED UNIVERSAL TIME (UTC) in 1972.
BIPM *(the International Bureau for Weights and Measures, in Sèvres, France)* is in charge of the calculation of this Internationl Time scale.

UTC has become the only reference time scale used to coordinate time in the world. Today, it always serves as the basis for determining the legal time in many countries.

In France, by Decree 2017-292 of 6 March 2017, legal time is taken from the atomic clocks of Paris observatory, which is responsible for establishing and delivering the local value of UTC (Op), called "Basis of the Legal Time".

Once the official Time sources well-defined, the issue that quickly arose is their transmission and acquisition by **the end user**.

1972, COORDINATED UNIVERSAL TIME (UTC).

Time can now be absolutely the same across the world.
The international committee confirms that this definition refers to a cesium atom at rest at a temperature of 0 Kelvin. The second is divided into 10 billion periods with the cesium atom. Then came the task of binding all laboratories that had such clocks (today through satellite signal exchanges) to jointly check the accuracy of the international time also known as International Atomic Time (TAI). The average time drifts slightly from this absolute standard. Thus, a one-second adjustment is applied if necessary either on June 30 or on December 31 at 23:59:60 UTC, on the decision of the International Earth Rotation and Reference Systems Service (IERS) that replaced BIH in 1987. It is the Coordinated Universal Time (UTC). Since 1970, 36 seconds have been added to the Universal Time (TU). The last adjustment of the "leap second" occurred on December 31st 2016 at 23:59:60 UTC.
Only the UTC(k) timescale by organizations that signed the MRA (Mutual Recognition Arrangement) can take part in the UTC connection, metrologically certifiable and traceable.

TIME SYNCHRONIZATION

As a strictly practical matter, time bases of master clocks, time centers and time servers must be synchronized on one or several external time sources. The synchronization prevents the internal clock from drifting over time and increases its long-term stability. It also allows to recover a normal operation in the event of a clock malfunction or interruption due to maintenance or incidents.

The current transmission modes may use fiber-based computer networks or radio broadcasting technologies (terrestrial or satellite), however, none has, so far, made it possible to guarantee the integrity of the time signal received by the end user.

SINCE 1977 ALLOUIS TRANSMITTER HAS BEEN USED TO BROADCAST TIME SIGNALS

This radio synchronization system is based on the atomic clocks of the LNE-SYRTE (the National Metrology Laboratory) of the Paris Observatory who delivers the French legal time.
Following the shutdown of France Inter longwave transmission scheduled on 31 December 2016, a mission led by the government confirmed that the time dissemination shall be maintained.
It noted that some sensitive applications required the use of multiple time sources, for which the longwave transmission of time signal shall be extended.
In 2019, National Agency of Frequencies (ANFR) was appointed by the government as operator to provide this public time service.
The time signal has been renamed to ALS162.

Some other transmitters around the world that broadcast similar time signals :

- ***in Kyushu, Japan (60 Khz)***
- ***WWVB in Colorado, USA (2.5 MHz)***
- ***BPM in XI'an, China (2.5 MHz JJY)***

France Inter transmitters

National coverage

(Time transmission by radio)

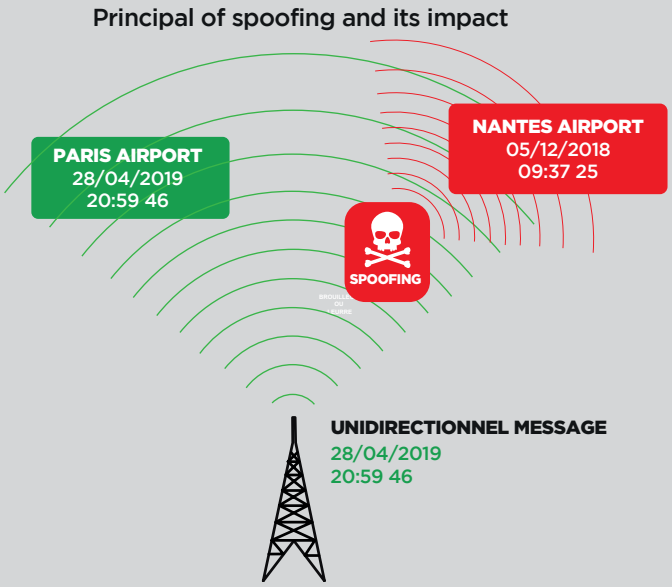
Since the first attempts at early 20th century to broadcast time signals over radio waves with a range of only a few kilometers, the Allouis transmitter in the Cher of 350 meters high and 800 kW of transmission power represents the culmination of this technology.

The main advantage of a transmission by long waves is to provide better reception inside buildings, where other radio signals are hardly picked up, such as those emitted by GNSS (Global Navigation Satellite System) or cell phone networks.

There are similar transmitters in Europe and around the world. Their signals can reach several hundred kilometers range *(2000 km for DCF transmitter in Germany)*.
They have thus been widely used for decades in key industry sectors requiring synchronization reliability, such as electricity production and distribution, air, rail and road transport as well as for the management of public lighting, synchronization of traffic lights or even parking meters...

However, if this technology has allowed for many years to broadcast the UTC reference signal from Paris Observatory and to ensure reliability for users, its unidirectional technology, easy to jam or spoof, no longer allows to guard against a malicious attack.

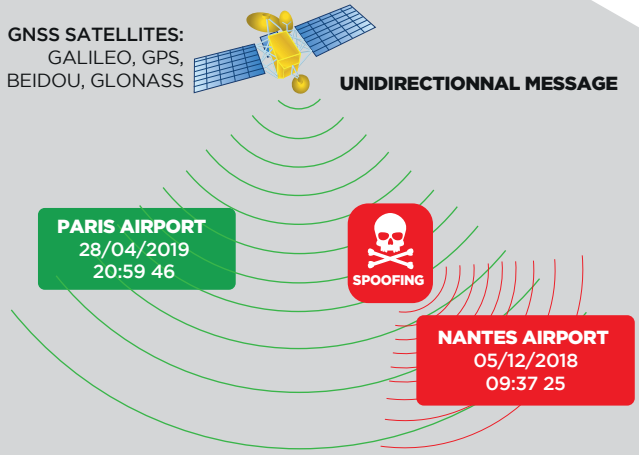
Traditional time broadcasting by radio transmitters: Allouis / DCF / MSF



Allouis (France), DCF (Germany) and MSF (England) radio transmitters broadcast each minute, via radio waves, a one-way time message to synchronize time servers.

The one-way transmission without traceability cannot guarantee the authenticity of the time message. It is highly vulnerable to jamming or more seriously to spoofing by malicious attack before arrival at end user. Such signals can be tampered with as GNSS does.

GNSS transmission via Galileo (Europe), GPS (USA), GLONASS (Russia), BEIDOU (China)



Principal of spoofing and its impact

The satellites of Galileo (Europe), GPS (USA), Glonass (Russia), Beidou (China) transmit a complete, highly accurate time message every 12 minutes to synchronize time servers.

The one-way transmission without traceability can not guarantee the authenticity of the time message.
It can be easily jammed or more seriously spoofed by malicious attack before arrival at end user.
Such corrupted signal will affect the functioning of the systems.
Various international studies have showed the increasing dependence to GNSS, in particular major risks for the security of organizations, national sovereignty,
some even undertaking the assessment of huge economic impact of such failure. The risk awareness as well as the high cost of installation and maintenance make this solution progressively less attractive to the users.

Global coverage

(time broadcasting by satellites)

US-owned GPS system was completed in 1995 et public free access is available since 2000. It has paved the way for PNT (Positioning Navigation & Timing) technologies and systems for the broadcast of time signals which will synchronize the users of GPS receiver, using a constellation of satellites orbiting the Earth.

GPS has revolutionized the world with its ability to provide accurate and cost-effective Positioning, Navigation and Timing *(PNT)* service with global coverage.

Just like American GPS, the GLONASS systems for Russia, BEIDOU for China, and Galileo for Europe or IRNSS for India, offer this timing capability on a continental or global scale.

These technologies *(and in particular GPS)* have been well recognized and integrated in a large number of systems since they are capable of providing an accuracy covering almost all uses *(better than 40 nanoseconds in 95% of cases)*, and achieving worldwide coverage that bypasses nations while freed from power constraints of terrestrial transmitters.

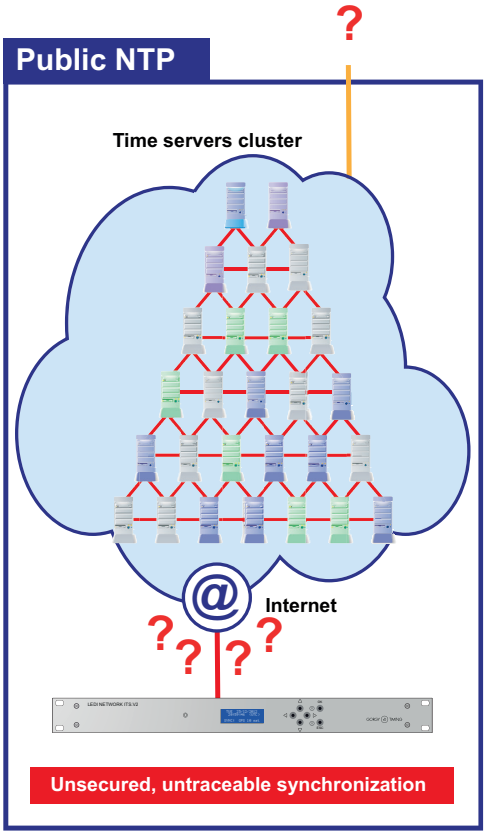
Today, it is commonly considered that more than 90% of timing systems are synchronized on GNSS, *(including a very large majority on GPS)*.
However, these modes of synchronization broadcast a one-way signal to the receivers, just as " terrestrial" radio transmission does, and do not allow for traceability or authentication of information.

GNSS dependency

For these technologies, the source of the time signal comes from atomic clocks aboard the satellites, to which corrective recalibration are applied towards the value of UTC. Indeed, it should be stressed that this is not a legal Time source in itself. GNSS systems use internal reference time scales established from different sets of clocks. These scales are GPS Time (USA), GLONASS Time (Russia), Galileo Time (Europe) and BeiDou Time (China). These System Times are pseudo-timescales and should only be considered as internal technical parameters of GNSS, and not as timescales that may serve as a reference for other human activities. They do not contribute to UTC, even some systems try to get closer to it. **In any case, they cannot claim to deliver the legal time of a country.**

It should also be noted that the military authorities change regularly GNSS parameters without notice, in a deliberate way, either in time of war or just to ensure safety of high-ranking officials when travelling, which causes serious problems of sovereignty and dependency for some countries. Likewise, the reliability of radio signals and in particular those emitted by GNSS can be strongly impacted by meteorological or physical phenomena such as solar winds which frequently disrupt service.
This dependency carries risks that might hinder what we now take for granted. Prolonged disruption of Global Navigation Satellite Systems (GNSS) signals caused by jamming or other cybersecurity threats would result in serious disruption involving the national security of many states and even the global economy.

Two NTP synchronization et broadcasting modes are at risk:

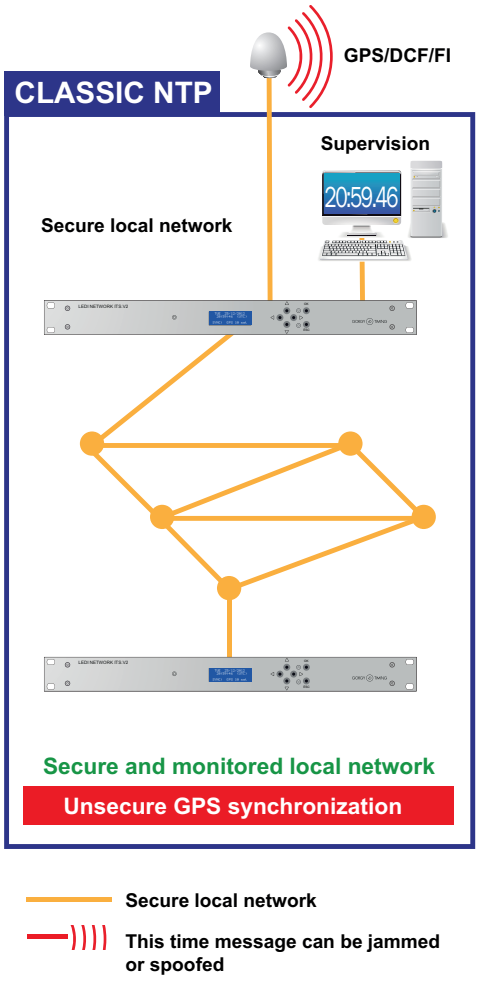


The "public" NTP mode

Using a public NTP server cluster for synchronization is highly risky.

These huge virtual clusters combining several thousands of time servers throughout the world allow users to easily connect on.

However, they do not provide legal proof of the time source, since random time servers that are used to broadcast time are not approved or supported for the most part.



The "classic" NTP mode

In a local network, the NTP can support two modes:
broadcast mode or client/server mode.

In the first mode, the time information is unidirectional and thus uncontrolled.

In the second mode, there is a bidirectional exchange between two systems, therefore traced and secured.

For both modes, the devices refer to Stratum 1 which is generally GPS synchronized.
Therefore, any attack on GPS signal will introduce a cascading error on the whole sync chain until the final client end, due to a corrupted signal source.

3 - THE MAJOR CHALLENGES TO COME

The rapid adoption and widespread proliferation of GPS (and GNSS) has undoubtedly improved our standard of living. At the same time, they have also led to a dangerous dependency and a loss of sovereignty ... because critical sectors or infrastructures such as transport, wired and wireless networks, power grids, data centers and emergency services now largely depend on the synchronization information of GPS, which we have just seen that it is vulnerable.

Cell towers use it to route your phone calls, ATMs and cash registers use it for your transactions, power grids use it to send electricity to your house, and stock exchanges use it to regulate the transactions that enter your equity portfolio or your investment fund ... However, this technology is much more vulnerable to attacks and disturbances, even though most people don't know or want to admit it.

The digitization of our space has accelerated considerably, making an entire section of our economy rely on a sensitive data that has become vulnerable: Time. The past two years have witnessed increasing concerns about threats related to GNSS jamming / spoofing.
We thus see a large increase in the number of time corruption incidents in almost all activities.

The transport and finance sectors, among the most at risk, have suffered many setbacks.

FINANCE :

Much more vulnerable than we would have imagined, the finance sector was the first to address the issue of time synchronization, in particular for the High Frequency Trading *(HFT) (these exchanges are computer-assisted, based on algorithms, and performed down to the range of nanoseconds)*. In fact, the stock exchanges mainly used GPS time signals to manage transactions.

As early as 2013, the famous American FBI investigated the high-frequency trading, rightly suspecting manipulation and market disruption linked to desynchronization. A time lag of a few milliseconds may cause the loss or gain of millions of dollars depending on the volume of shares traded and the stock price trends ...

Many problems were then detected because beyond the HFT, it is the entire sector which requires secure time-stamping of transactions, from ATM operations to payment terminals in stores.
With this, "MIFID II" standards have further framed the time synchronization in this field, with effect as from 2018. But they are still heavily dependent on GPS as source of reference time.

TRANSPORTATION:

In this age of high-speed trains and the unprecedented boom in air traffic, it is easy to understand the need for a secure and traceable reference Time. Positioning, signaling, communication, data processing, ... each of the mechanisms implemented by this industry to deliver its service involves time synchronization, which is essential for the operation of transport, whether land, river, air or sea.

Take the example of air transport. As a user of GNSS systems for the most part, it has been repeatedly affected over the past 5 years by the proliferation of GPS jammers, which cost less than US$20/unit on the Internet (although its use is prohibited!). The aim of these devices is to corrupt the GPS loggers that provide location and movement tracking. However, as we discussed above, the easy accessibility of spoofing devices has now changed things and present a serious cybersecurity threat that hackers are now plunging into.

In France, the airports of Nantes, Lyon and Marseille were victims of this type of incidents on several occasions between 2017 and 2019, leading to the closure for of several hours and serious disruptions in approach procedures of aircrafts in flights, forced to switch to manual mode.

Rail and sea transport are not spared either, even if the incidents are more discreet. However, at the end of 2019, a massive cyberattack, generating the deception of GNSS signals on the entire Shanghai port complex *(whose surface area exceeds 361,000 hectares)*, caused the complete standstill during 24 hours with significant economic impact. This event demonstrated the ability of hackers to generate massive attacks, unable to locate as opposed to the cases until then. Faced with these threats that become more real, impact studies have been launched.

The reports are unequivocal, for example that of ***London Economics*** which predicts for UK, an economic impact of more than £1 billion per day in the event of GNSS malfunction, or the report of the American **CSIS*** *(Center for Strategic and International Studies)*, announcing the urgent need for the States to secure their essential infrastructures *(most of which synchronize their operation with GNSS time signals)*, in the face of increasing attacks designed to disturb these systems ...

MAJOR TRENDS IN THE WORLD:

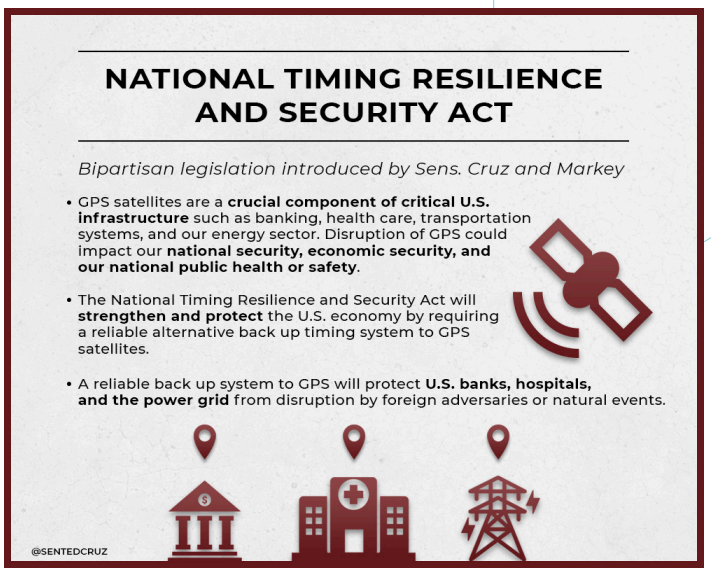
Since 2018, awareness has emerged unevenly across the globe, but is progressing more rapidly as a result of increasing media coverage of the consequences of cyber-attacks.

In UK, for example, a £36 million investment was granted by the Parliament in early 2020 to NPL *(National Physical Laboratory)* for the development of a secure time distribution network to transmit the legal time reference to British citizens, to secure digital economy and essential operators which are vital to the nation.

In Europe, billions of investment has been granted on EGNOS project *(European Geostationary Navigation Overlay Service)*, which attempts to improve the performances and enhance the resilience of Galileo, but still is not providing traceability of time from the source to the end user, or dissemination of legal time.

In the USA, the ***National Resilience and Security Act*** and more recently the presidential decree of February 2020 *("Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services")* show a real awareness of the risks and engage the operators of essential services for the American nation to reduce their vulnerability related to dependency on GPS satellite signals.

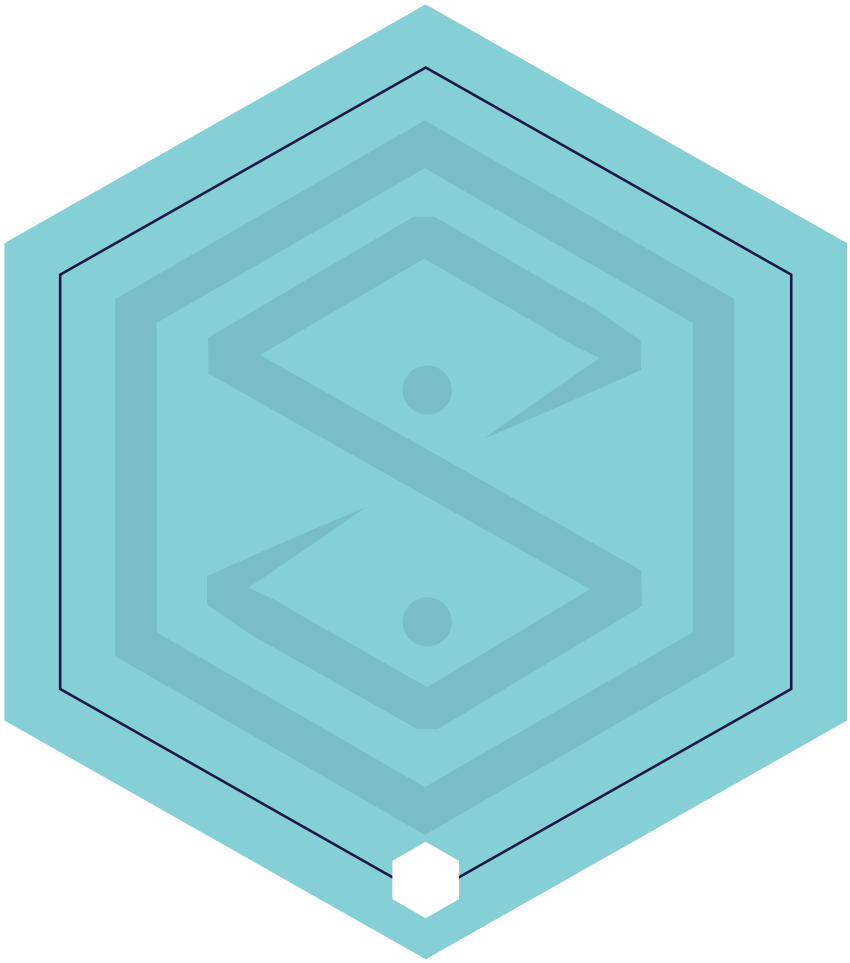
In France, by decree legal Time exists since 2017. The Rules of certification relating to Architectures to deliver an accurate Time with Traceability and Security has been published in January 2020 by French National Metrology and Testing Laboratory *(LNE)*. The CNRS has just requested an impact study about



the malfunctions of GNSS systems. ANSSI organisation *(Information Systems Security National Agency)* is also working on the issue of cybersecurity of Time.

Everywhere in the world and as it has been the case for the financial sector with MIFID II standard, **putting in place regulations is the trend**, in order to impose security standards in the face of economic or societal challenges.

Decree No. 2017-292 of 6 March 2017 regarding French legal time (JORF of 8 Mar. 2017)



4 - THE RESPONSE: SCPTime®

For a nation or a region

The SCPTime® collaborative project was originally intended to make the legal time available and operational to the largest number of users in a country, in a secured and traceable way from its source to the end user. It is in line with the evolution towards a digital society by addressing the challenges of sovereignty and cybersecurity of Time arising from the digital economy.

This ambitious collaborative project supported by Bpifrance (PSPC) for consolidating French Time / Frequency industry, had from the outset an international vocation because it responds to a problem present all over the world. Endorsed by Minalogic Grenoble, the project was approved by the steering committee of "Programme des Investissements d'Avenir" (program for futue investments) and signed by the Prime Minister on 2nd June 2014.

INVESTIR L'AVENIR

TEAM LEADER

GORGY TIMING — LA MARQUE DU TEMPS

SCIENTIFIC LABORATORIES

femto-st SCIENCES & TECHNOLOGIES

LNE-LTFB

OSU THETA

UFC UNIVERSITÉ DE FRANCHE-COMTÉ

LNE — Le progrès, une passion à partager

l'Observatoire de Paris — SYRTE — Systèmes de Référence Temps-Espace

Institut UTINAM

PRIVILEDGED PARTNERS

Business & Decision

Schneider Electric

SNCF

INDUSTRIAL PARTNERS

GORGY TIMING — LA MARQUE DU TEMPS

Syrlinks

tronics microsystems

eolas groupe Business & Decision

TYLEOS CONSULTANTS

µQUANS

SUPPORT PARTNERS

bpifrance — SERVIR L'AVENIR

MINALOGIC

Liberté • Égalité • Fraternité — RÉPUBLIQUE FRANÇAISE — MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

MAIN ACADEMIC, SCIENTIFIC AND INDUSTRIAL PARTNERS:

SYRTE *(Time-Space Reference Systems)* is a department of the Paris Observatory, in charge of the establishment and availability of the French legal time.
The Observatory contributed in particular to the technical studies of Time / Frequency transfer on optical fiber, and the connection of the **SCPTime®** network to the National UTC *(Op)* reference. It also made an active contribution to the development of ATTS (*Certification rules for "Architecture to deliver an accurate time reference with Traceability and Security)*, published by le LNE in 2020. This framework is intended to serve as a certification basis for **SCPTime®.**

FEMTO-ST Institute

The expertise of FEMTO-ST national laboratory mainly covers microcells, optics, Time-frequency metrology and atomic physics.
FEMTO ST and **SCPTime®** are setting a joint laboratory in development and industrialization of innovative metrological equipment resulting from the research activities. **The ANR** *(French National Research Agency)* **is funding this collaborative project for development of SCPTview.**

The Time/ Frequency laboratory of Besançon (LTFB) brings together the resources and competencies of two laboratories of the University of Franche-Comté, UTINAM and FEMTO-ST.
Le LTFB ensures R&D activities through its two laboratories in different fields of Time-Frequency such as:

- Cryogenic oscillators.
- Optical clocks.
- Micro atomic clocks.
- GNSS (GPS, Galileo).
- Time and frequency transfer methods
- Time and frequency transfer in optical fiber.
- Theoretical studies, modelling/ characterization of oscillator stability.

La FÉDÉRATION FRANÇAISE DES INDUSTRIES DU TEMPS ET DES MICROTEHNIQUES *(French Chamber of Time and Micro-technologies Industries)* agreed that the Venture Capital Investor of the sector can take stakes in the capital of **SCPTime®** to incorporate this new technology of delivering a secured and traceable time to **the end user**.

LNE *(National Metrology Laboratory)*

Contribution of LNE to SCPTime®

LNE, an organization recognized by ANSSI *(Information Systems Security National Agency)* in the domain of digital security, has established in collaboration with **SCPTime®** the ATTS Rules of certification for an Architecture delivering an accurate Time reference with Traceability and Security.
Today "ATTS" Rules are the first of its kind worldwide to provide certifications regarding solutions of time distribution from the legal time source to end user with accuracy and security.

ATTS certificate, which serves as basis of reference for **SCPTime®**, describes general and technical requirements for ensuring that the time delivered to the user is:

- **Accurate: capable of delivering a time signal with a given uncertainty.**
- **Traced: having assurance that time delivered to the user is connected to original UTC.**
- **Secured and monitored constantly: integration of safety features to protect the system against jamming or spoofing.**

PARTNER CUSTOMERS

SCPTime® has been identified as one of the five major innovative and strategic projects of SNCF Réseau. Time, considered as "hidden interest", is nevertheless a fundamental concept in the transport industry and for its users, especially for:

- Rail production activities, where it helps to ensure the precision of applications and uniform Resource centers at national level.
- Monitoring services, allowing traceability and certifications of timestamp from traps.
- Maintenance and national support, allowing traceability and timestamping of logbook data.
- Users, providing them with accurate and consistent time information on terminals in the station and on new digital interfaces.

UGA Grenoble-Alps University

After presentation of **SCPTime®** concept to IT Systems Management of UGA, it has been agreed to set up an architecture of time distribution to synchronize all networks of the University.

UGA partnered with **GORGY TIMING** to carry out the innovative project of the establishment of a scientific and technical school at La Mure d'Isère, in middle mountain areas. The school is specialized in the secured time distribution field.

CEA Center of Grenoble

Under EASYTECH program, **SCPTime®** and CEA have drawn up a collaborative research project entitled **"Risk Assessment and threat characterization of secured time synchronization STS protocol"**, endorsed by MINALOGIC on 29 May 2019.

The collaboration seeks to benefit from the expertise of CEA in safety requirements as well as identification and prototyping of technical solutions, in order to validate with the upmost rigor STS **"Secure Time Synchronization Protocol"**, a new variant of secured NTP time protocol invented under **SCPTime®** project. STS protocol is used under **SCPTime®** to distribute time **to the end user** in a secure way.

Schneider Electric

Applications of tomorrow become more widely spread geographically. We need to offer systems that can communicate over long distances. **SCPTime®** allows for the secure synchronization of remote production monitoring and management systems and to **provide the proof.**

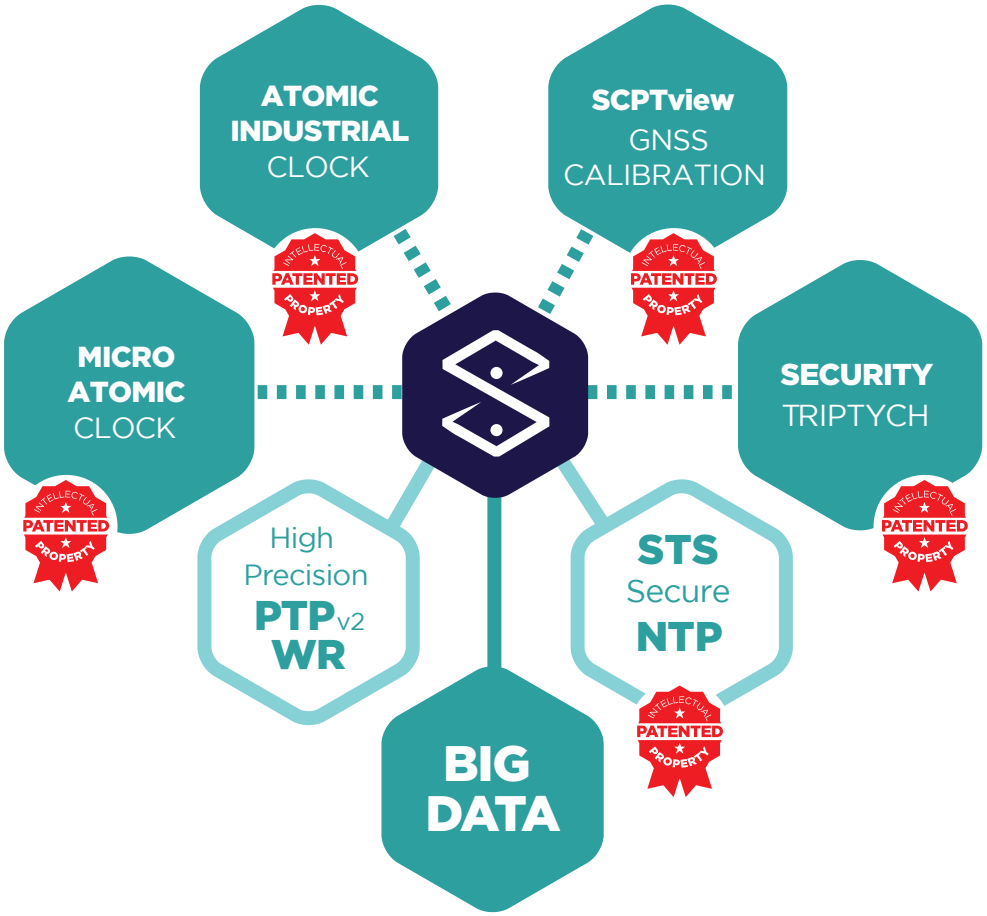
STMicroelectronics
The Nano Plan 2022 project leader, STMicroelectronics, has chosen **SCPTime®** as industrial partner.
This large funding program, which is part of IPCEI *(Important Project of Common European Interest)*, will allow **SCPTime®** to achieve industrial leadership in innovations and in the field of secure Time.

life.augmented

Nano 2022

ADVANCED TECHNOLOGIES

With 5 years of R&D, the SCPTime concept allows the development of patented innovative technologies by bringing together many skills from the French Time / Frequency ecosystem.



SCPTime®: THE FUTURE FOR THE TIME/FREQUENCY SECTOR

Time plays a crucial role in the digital world, both for cybersecurity and regulatory areas. It has become essential to use reliable and legal time sources for authenticating a transaction, qualifying a process, as well as ensuring the operation of synchronization devices of the future.

European and French regulations already applicable to the financial sector will be progressively expanded to other industries. This implies providing proof that synchronization is successfully done to the right reference time *(UTC-based legal time)* with an appropriate accuracy according to user applications. The system shall ensure the traceability and the supply of a certificate.
Under **SCPTime®**, receiving a certified legal time is no longer reserved for the few scientific organizations or laboratories and will be **available to a large number of users**.

SCPTime® is aimed at all sector using IT resources. It can be scaled according to the real user expectations of their use of time, that can range from that of a notary *(certified time to a second accuracy)* to those in high-frequency trading *(certified time to microsecond accuracy)*. The **SCPTime®** offers are tailored to each community of interest, taking into account the increase of legislations and professional practices.

The exponential growth of data sets to be processed, in particular the development of IoT, requires a comprehensive and fine timestamping *(audit trail)*. The use of BIG DATA makes such work possible under **SCPTime®**.

The value proposal of **SCPTime®** goes well beyond the delivery of a reliable and certified time signal ensuring the security of processes. In fact, the capacity of data exploitation offered by the tracing system gives companies the prospects of productivity gains, predictive analytics, and the promise of large-scale optimization of process by synchronization to the unique et legal reference: UTC.

SCPTime® offers a total traceability of time to the end user and the related security to provide an accurate and certified time.

SCPTime® is available in a closed network version within the company: reference time is provided by a calibrated atomic clock.

SCPTime® stands out for simple implementation and competitive advantages as compared with common solutions of synchronization, **thus making available** cost-effective high-tech solution with certification.

CYBER SECURITY IN THE DIGITAL ECONOMY

In the age of digital transformation of the economy, the cybersecurity has risen to become a prominent issue for organizations, governments, and their administrations. Time, which is omnipresent and essential at all levels of the economy, has become the target of cyberattacks like other vital elements of a system.

Many countries have already approved budgets or made official announcements and recommendations to alert the users to this growing threat. SCPTime® is the solution to address this threat.

It is the only system in the world that provide a 100% guarantee of the continuity and traceability of two-way time signal transmission:

- Certifying the UTC reference time source.
- Certifying the synchronization operations.
- Providing a full traceability of the time signal from legal source (UTC) to the end user over long distances.
- Informing the end user in case of momentary interruption, performance deficiencies or synchronization malfunction.
- Switching to an internal micro atomic clock in case of synchronization loss.
- Providing a certified precision, ranging from the subsecond to a few nanoseconds according to applications.
- Duplicating the cybersecurity concept in each country.
- Proposing a global architecture that is more cost efficient than the multiplication of independent local synchronization systems.

SCPTime® SERVICE ASSETS

With a secured, certified, accurate, and traceable time reference, SCPTime® will add significant value to all the organizations, including:

INCREASED CYBERSECURITY

The number of cyber-attacks is constantly increasing by 25% to 30% every year which costs the global economy several hundred billion dollars. Cybercrime is now a major challenge for all businesses.
Failure of time synchronization related to GPS vulnerability caused serious incidents in 2019 including the closure of the harbour of Shanghai, and the blockage of a few airports over the world,as well. Not to mention the large data loss and corruption of Danish judicial system...
The robustness and traceability of **SCPTime®** system protect users from the risks linked to data corruption and secure the synchronization process as well as the data transmission.
Given the severity of the risks involved, it represents a business-critical added value in the fight against cybercrime and data protection.

IMPROVING FLEXIBILITY

With digitalization of economy and increased trade force, the companies must have the highest level of agility. **SCPTime® allows organizations to reduce technological constraints and to overcome inertia to change**. **SCPTime® ensures a rapid and cost-effective delivery of a Secure, Certified, Precise and Traceable time** signal to fit customer needs, at all required levels of performance, by realizing efficiency, robustness, and responsiveness.

GREATER PRODUCTIVITY

The time dissemination service of **SCPTime®** contributes significantly to business efficiency.
A company having a guaranteed time source that is reliable and uniform within its structure, will ensure an optimal system performance, thereby minimizing the expenditure of time and money on synchronization incidents. The traceability as well as the monitoring make it possible to identify and resolve in real time any incidents concerning the reliability of time signal.

The flexibility and reliability of the time service also reduce the economic costs of company IT investment, management of equipment obsolescence, maintenance, and supervision. The traceability offered by **SCPTime®** service allows companies to optimize preventive maintenance and diagnostic time, contributing directly to their general quality by the stability of the service and the information provided by the traceability system.

MORE ASSURANCE

In a changing and increasingly regulated environment, **legal time is the reference**.
With **SCPTime®**, a company or an individual can integrate into their process, in the same way as a quality certification, a synchronization mode using a certified legal time source. This results in **less issues of non repudiation or corruption of data, and reduced risk of disruption or uncertainty of business**. In terms of attractiveness for prospects and customers of companies, this is a guarantee of cooperation with a reliable supplier, attentive to cybersecurity issues, and which offers them **perfect interoperability thanks to systems synchronized to UTC (world reference)**, as opposed to a time source whose origin and reliability are not guaranteed today...
SCPTime® is the first Time dissemination service providing full supervision and traceability from the legal source to the user, supported by certificates.

TRACEABILITY: GUARANTEE OF SECURITY

In SCPTime®, the traceability is a crucial element of security on several levels:

SCPTIME® TIME ACQUISITION

SCPTime® delivers a complete traceability of time production *(UTC source)*, transmission and distribution. **SCPTime®** is fully compatible with the standards methods to update the system clock. The SCPT agent can be downloaded to facilitate this updating process *(called Acquisition)*.
This Agent is compatible with most of the OSs *(Linux, Windows, Mac...)* and will be available in native mode *(deployment and study in progress)* on proprietary OS *(such as Schneider Electric's Edge Box TM, GORGY TIMING's* **SCPTime®** *regional servers and SNCF's future technical equipment)*.
The embedded agent helps to ensure the tracking of the synchronization, but also extend the certification of the synchronization process run on the device. It includes configurable parameters to fit with the user needs.

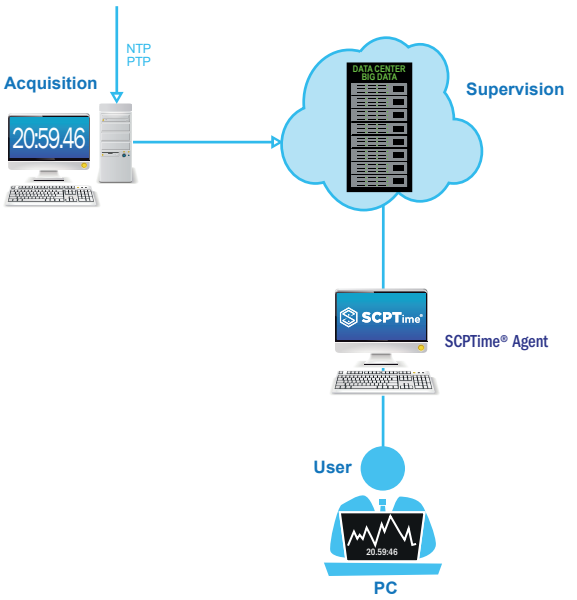
STORAGE OF OPERATIONS

It is based on SCPTrace. SCPTrace is an operation platform that can control all the **SCPTime®** elements, in particular the supervision, storage and certification to companies having subscribed to **SCPTime®** services. The platform also issues licenses to download **SCPTime®** Agent and hosts Customer service.

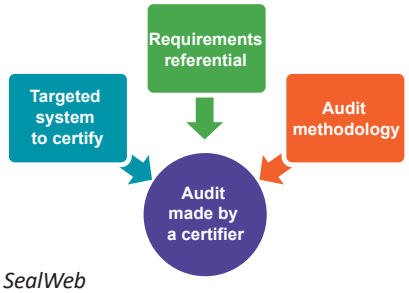
There are 2 levels of operations management. The one is to ensure the safety and the optimization of the flow of Time and the other responsible for the analysis of the operation. This analysis sends the proposed actions to the first system and validates the certification part.

TAILORED SUPERVISION

To carry out the operations, all the synchronization transactions are stored in a BigData-type NOSQL system. SCPT datanalyzers make visible the compliance with good synchronization practices according to professional rules, as well as laws and regulations *(for instance MiFID II)*.
Reporting of various information is provided to each customer in a dashboard with two axes: the business axe, where compliance is highlighted, and the certification axe, where certificates can be published.



CERTIFICATION : A GUARANTEED SERVICE



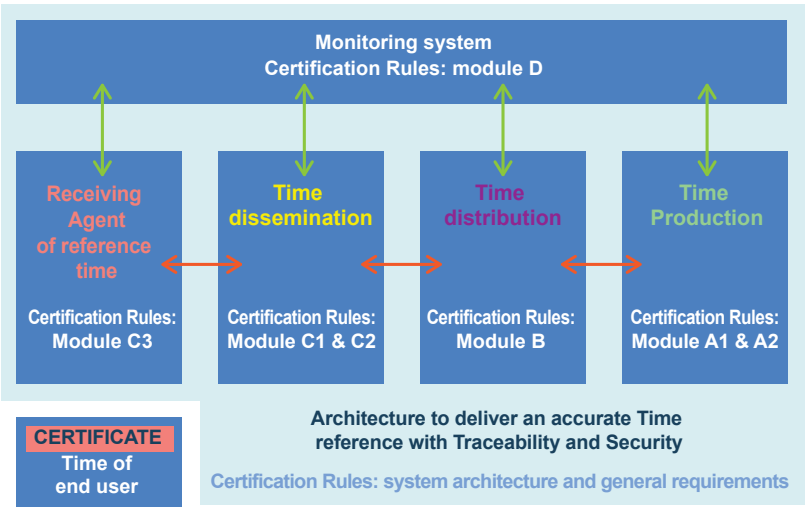
Source SealWeb

The certification consists of a procedure by which a third party, a certifying organization issues a written assurance that a system, process, person or service meets specified requirements of a standard or a reference system.
The SCPTime® service refers to the "ATTS" Rules of certification (Architecture to deliver an accurate Time reference with Traceability and Security), published in January 2020 by French National Metrology and Testing Laboratory. The ATTS reference has been established in collaboration with experts from Time/ Frequency sector, digital networks, information security, and metrologists.

It is the first of its kind, providing certifications regarding solutions of time distribution from the legal time source to end user with accuracy and security.

It ensures that the time delivered to the end user is related to the legal time with a given uncertainty and in a secure manner.

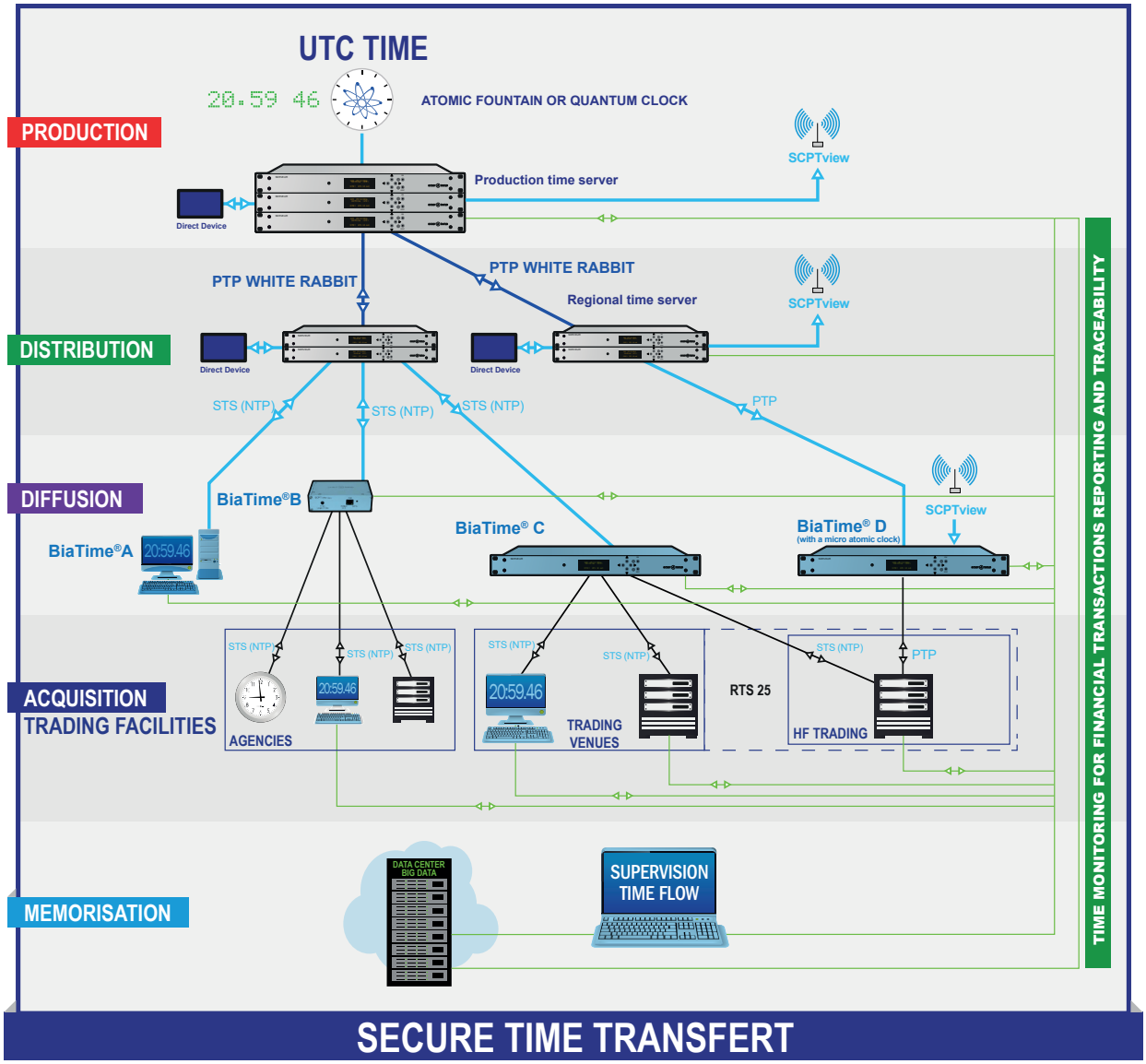
The constraints will be largely reduced for end users, as **SCPTime®** facilitates obtaining the certificates by managing the complexity imposed in accordance with provisions of cybersecurity *(see recommendation of ANSSI)*.
As a result, the users that meet the requirements of **SCPTime®** deployment benefit from various certificates which identify the target precision (accuracy classes), synchronization frequency (compliance level), qualitative rate of clock updates *(Success rate)* and use of SCPT Agent *(Extend)*.
This European certification is a proactive tool for legal protection such as "anti-claim management" or "Nachtragmanagement".



A certified architecture allows to deliver a qualified time with a given accuracy to its origin, and where appropriate, the correct use by connected device (the notion of acquisition). We refer to an architecture to deliver a time reference certified to be accurate, traceable, and secure.

SCPTime ® ARCHITECTURE

In SCPTime® technology, robustness is attained by the architecture, of which the general principles are shown schematically below:



Each component of **SCPTime®** architecture is monitored for a complete traceability of events and of the time signal from its UTC legal source **to the end user**. The architecture meets the requirements of the ATTS certification rules published by LNE in January 2020.

SCPTime® SERVICE

Our world is changing. The technologies are progressing exponentially. Fast-moving business that takes priority over the traditional economy is making companies switch to the digital transformation. They have to enhance their flexibility, and focus on management of short-term technology investments.

In the new multisectoral world where interoperability, flexibility and data security are key words.
Time has become an issue of **sovereignty** and a fundamental element of cybersecurity.

As described in previous chapters, the fact that most one-way communication technologies used by time sources are now obsolete and vulnerable has brought new challenges to businesses.

Four major themes have been identified on the time synchronization in organizations:

CYBERSECURITY:

It is a set of safety tools and process to ensure protection of the digital environment. Time occupies a central and fundamental position at the heart of a cyber-environment.

SCPTime® architecture offers full traceability from original legal time signal to the end user, and for the first time, provide a sound basis for diagnosis and encryption process.

LEGALITY:

The growing global trade on the internet has resulted in fundamental needs of integrity, authentication, non-repudiation, or validity of data. Major trends are to set the regulations to ensure a global and coordinated operation. In this regard, only a universal and legal reference will enable to achieve these objectives.
SCPTime® delivers a legal time *(UTC reference time)*, currently in the process of LNE certification *(LNE: National Metrology Laboratory of France)*.

ACCURACY:

In terms of time signal, individual needs for accuracy and service guarantee shall be satisfied to meet the requirement in every field, from Transport, Finance, Telecom, Energy to major Government Agencies.

SCPTime® offers a range of services tailored to each business line, delivering time signal to an accuracy from subsecond to microsecond, thus fully covering the needs of the market.

TECHNOLOGICAL ADAPTABILITY:

The fast pace of developments in technologies is requiring organizations to match their infrastructure to their needs to remain competitive.
After 4 years of research and development, **SCPTime®** Architecture and dissemination system of legal time provide businesses with flexibility, consistent and **competitive** service level on the cutting edge of new technologies.

SOME EXAMPLES OF PREVAILING NEEDS BY BUSINESS FIELD

	Legality	Security	Accuracy	Technology
Industry	●●●	●●●	●●	●●●●
Transport	●●●	●●●●	●●●	●●●●
Banking	●●●●	●●●●	●●●●	●●●
Energy	●●	●●●●	●●●●	●●●
Army	●●●●	●●●●	●●●●	●●●●
Administration	●●●●	●●●●	●	●●
Emergency relief	●●●●	●●●	●	●●
Insurance	●●●●	●●●	●	●
Notary public	●●●●	●●●	●	●
Justice	●●●●	●●●	●	●
Surveillance	●●●●	●●●	●●	●●
School	●●	●●	●	●
Hospitals	●●●●	●●●	●●	●●●●
individuals	●●●	●●●	●	●

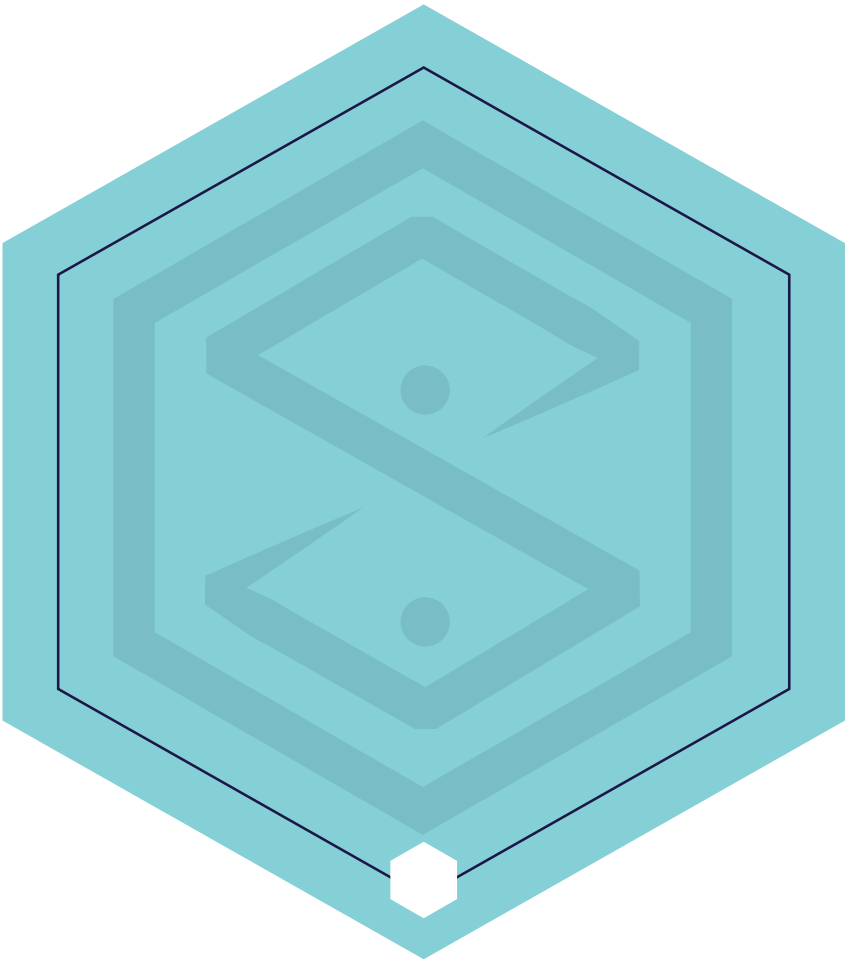
SCPTime® SUBSCRIPTIONS

SCPTime® services are scaled to meet the needs of various users.
The SCPTime® architecture allows to provide the end user with a flexible and highly competitive solution compared to traditional solutions.

Features	Criteria	BiaTime®A subscription	BiaTime®B subscription	BiaTime®C subscription	BiaTime®D subscription
Synchronization	NTP^{STS} on internet	✔	✔	–	–
	NTP^{STS} on direct link	–	–	✔	–
	PTP/SyncE/WR	–	–	–	✔
Security	Alerts	✔	✔	✔	✔
	Data authenticity	✔	✔	✔	✔
	Hold-over	–	✔	✔	✔
	Arbitration	–	–	✔	✔
	Triad	–	–	✔	✔
Certification	Legal Time source	✔	✔	✔	✔
	Guarantee of availability	✔	✔	✔	✔
	BiaTime®B Box	–	✔	–	–
	BiaTime®C Server	–	–	✔	–
	BiaTime®D Grand Master	–	–	–	✔
Accuracy	Second or better	✔	✔	✔	✔
	0,1 second or better	–	✔	✔	✔
	milliseconde or better	–	–	✔	✔
	microseconde or better*	–	–	–	✔

** Accuracy increased to 50 nanoseconds as an option*

Type	Synchronization	Security	Certification	Accuracy
BiaTime®A subscription	NTP^{STS} on internet	Alert + data authenticity	Legal Time source + guaranteed service availability	Second or better
BiaTime®B subscription	NTP^{STS} on internet	Alert + data authenticity + Hold-over	Legal Time source + BiaTime®B Box included + guaranteed service availability	0,1 second or better
BiaTime®C subscription	NTP^{STS} on direct link	Alerte + data authenticity + Hold-over + Arbitration	Legal Time source + BiaTime®C server included + guaranteed service availability	Millisecond or better
BiaTime®D subscription	PTP/SyncE/WR	Alerte + data authenticity + Hold-over + Triad	Legal Time source + BiaTime®D Grandmaster included + guaranteed service availability	Microsecond or better*



TIME TECHNOLOGIES INTERNATIONAL SCHOOL

5 - A SCHOOL TO BE READY FOR FUTURE: "**TTIS** " Time Technologies International School

BUILD FOR THE FUTURE

Today, the recruitment of qualified staff or enhancement of researchers and engineers' skills have all become matters of concern for secured time distribution market and digital world.

In this context, on the initiative of Maurice GORGY *(President of GORGY TIMING)* and Konstantin PROTASSOV *(Vice President of UGA)*, **SCPTime®** partnered with **Université Grenoble Alpes** to carry out the innovative project of creating a scientific and technical school at La Mure d'Isère focusing on secured time distribution subjects.

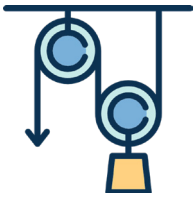
SCPTime®

UGA Université Grenoble Alpes

MODERN LEARNING

Time Technologies International School offers an educational programme responding to the needs of international professionals. The short duration training sessions (of 1 to 2 weeks) are given in English or French and learner-friendly, using the latest digital tools and modern communication.

Combining practical and theoretical lessons, the training will be professional and will allow the acquisition of in-depth skills. A university certification will be granted to trainees.



Atomic fountain
Quantum physics

Frequency
Syntonization

Time
Synchronization

Cybersecurity
related to Time

Smart City
IoT (Internet of Things)

COMMITTED PARTNERS

Since its creation, the French Institutions and industrial actors that relate to secured time transmission themes have shown their commitment to the project and validated the benefit of the scientific school initiative in middle mountain area.

The local actors are strongly involved in this wealth and innovation-creating project through investment.

- **Town of La Mure**
  Provides logistics arrangements: optical fiber with support of the department, improvements to roads. It is also part of the smart city project. La Mure is an essential partner in terms of support for TTIS school.

- **Community of Communes of Matheysine & Matheysine Development**
  The CCM will play a major role in the scientific school project. As the future owner of the former station building, it will provide pre-financing and project management for the interior renovation of the building. It will ultimately be responsible of the management of building occupancy including hosting a third party like learning lab.

- **Department of Isère**
  Currently in charge of the former railway station building, the Department of Isère will be responsible of exterior renovation of the building. The Department contributes also to the financing of future work in the building.

- **Auvergne-Rhône-Alpes Region**
  AURA Region is a financial partner concerning all work related to the building. It will also lend support for the educational starting up of the training.

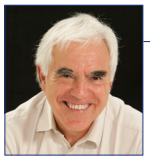
- **The DIRECCTE and the Prefecture of Isère**
  In the frame of the scientific school project, DIRECCTE and the Isère Prefecture manage the relationship with the government. As the former station is a state-owned building, it is essential to ensure good communication with the government. The DIRECCTE and the Isère Prefecture carried out the transfer of the building from the Department to the Community of Communes.

- **One River One Territory Agency of EDF Hydro Alpes**
  One River One Territory, the EDF agency in Vizille, supports businesses, employment, innovation and economic vitality in the valleys of South Isère where EDF Hydro Alpes operates hydroelectric facilities. As such, it supports regional initiatives aimed at strengthening their economic attractiveness, for example by contributing to the emergence or the structuring of new job creating sectors. That is why EDF One River One Territory is involved as a partner in the project of scientific school TTIS in La Mure.

TIME TECHNOLOGIES INTERNATIONAL SCHOOL

A RENOWNED SCIENTIFIC COUNCIL

The school will be led by a scientific council composed of prominent international figures from secured time transmission field.



Gérard BERRY
Member of the French Academy of Sciences, Academy of Technologies, and Academia Europaea. Professor Emeritus at the College of France, CNRS (National Centre of Scientific Research) Gold Medal 2014.

Maguelonne CHAMBON
R&D Director of National Metrology Laboratory, Paris.

Philippe ELBAZ-VINCENT
Director of Cybersecurity Institute (UGA)
Membre of the Scientific Coordination Committee of Carnot Institute LSI.

Éric GAUSSIER
Professor at Université Grenoble Alpes,
Director of the LIG Computer Science Laboratory in Grenoble,
Director of the Multidisciplinary Institute in Artificial Intelligence.

Florent KIRCHNER
Strategic director of the SPARTA cybersecurity competence network, Cybersecurity Program Director of LIST Institute, CEA Saclay.

Yann LECOQ
Director of FIRST-TF Labex,
LNE-SYRTE, Paris Observatory.

Pierre LEMONDE
Director of Research at CNRS, Néel Institute in Grenoble, former Science & Technology Counselor at French Embassy in China.

Enrico RUBIOLA
Professor at Université de Franche-Comté,
Chairman of European Frequency and Time Seminar (EFTS), Besançon.

Christophe SALOMON
Membre of Sciences Academy,
Director of Research at CNRS,
Normale Supérieure de Paris.

Christine VERDIER
Professor at Université Grenoble Alpes,
Manager of the department Computer Science, Mathematics and Applied Mathematics of UFR.

Shougang ZHANG
Director of National Time Service Center (NTSC), Xi'An, China.

UGA Université Grenoble Alpes

UNIVERSITÉ DE FRANCHE-COMTÉ

France Horlogerie
INDUSTRIES DU TEMPS ET DES MICROTECHNIQUES

l'Observatoire de Paris SYRTE
Systèmes de Référence Temps-Espace

FIRST TF
Facilities for Innovation, Research, Services and Training in Time & Frequency

A PRIVILEGED LEARNING ENVIRONMENT

The station of Petit Train La Mure d'Isère

The training will be held at La Mure in Isère about 40km from Grenoble, place of establishment of **SCPTime®**, in the middle mountain areas.

The gathering of professionals and learners from different backgrounds in a relatively isolated place will allow exchange dynamics, therefore encouraging the sharing of experiences in secure distribution of Time.

The restored building of former station of Petit Train of La Mure, where the school will be located, is a place of historical and symbolic significance over time.

The petit train of la Mure

The Himalayan footbridges of lake Monteynard

L'Obiou

*"The innovative scientific school **TTIS***
intends to remain faithful to the spirit of innovation
*and research from which **SCPTime®** arose.*

It will deliver the first training sessions
in October 2020 in the magnificent historic halls
of the Matheysin Museum in La Mure, in the middle mountains.

Genuinely forward-looking,
TTIS aims to satisfy a dual ambition to train its
students in the latest techniques for
Securing time synchronization,and prepare them
for the challenges raised by the mastery of
*a **Secure, Certified, Precise and Traceable Time***
required by the digital transformation ."

SCPTime®

Quartier Beauregard - 38350 La Mure d'Isère (Grenoble France).

Phone: +33 476 30 48 20 Fax: +33 476 30 85 33

e.mail: scptime@scptime.fr- www.scptime.com

La FRENCH FAB

SAS au capital de 10000 € - 834 844 698 R.C.S. Grenoble - SIRET 834 844 698 00011 - NAF 6110Z - N° TVA FR23834844698