ETSI GR NFV-SEC 016 V1.1.1 (2023-02)

Network Functions Virtualisation (NFV); Security; Location, locstamp and timestamp; Report on location, timestamping of VNFs

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/NFV-SEC016

Keywords

critical infrastructure, GNSS, location, NFV,
security, time-stamping

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The reliability and the ability to securely measure time and location are important for security. It is a challenge in virtualisation, especially in NFV environment. The present document studies these issues from a security perspective.

1 Scope

The present document is a study on how the location of sensitive VNFs (e.g. VNFs handling data with Data Protection location handling restrictions, network security functions and LI functions) can be attested. The present document considers the use of trusted locstamp and timestamp information derived from Global Navigation Satellite Systems (GNSS), such as Galileo. The present document also considers other physical location binding solutions. The capabilities described also have benefits for other less sensitive virtualised services which may need to verify location of VNFs or data.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IEEE™ ICC 2015 - Workshop on Cloud-Processing in Heterogeneous Mobile Communication Networks (IWCPM)-(2015): "Synchronization Challenges in Packet-based Cloud-RAN Front haul for Mobile Networks".

[i.2] Heavy Reading - White Paper - December 2014: "New Synchronization Requirements for 4G Backhaul & Front haul".

[i.3] 3GPP TR 38.803: "Study on new radio access technology: Radio Frequency (RF) and co-existence aspects".

[i.4] Recommendation ITU-T G.8260: "Definitions and terminology for synchronization in packet networks".

[i.5] Recommendation ITU-T G.8261: "Timing and synchronization aspects in packet networks".

[i.6] Recommendation ITU-T G.8271: "Time and phase synchronization aspects of packet networks".

[i.7] Recommendation ITU-T G.8262: "Timing characteristics of a synchronous Ethernet equipment slave clock".

[i.8] Recommendation ITU-T G.8263: "Timing characteristics of packet-based equipment clocks".

[i.9] Recommendation ITU-T G.8272: "Timing characteristics of primary reference time clocks".

[i.10] Recommendation ITU-T G.8273: "Framework of phase and time clocks".

[i.11] Recommendation ITU-T G.8265: "Architecture and requirements for packet-based frequency delivery".

[i.12] Recommendation ITU-T G.8275: "Architecture and requirements for packet-based time and phase distribution".

[i.13] Recommendation ITU-T G.8264: "Distribution of timing information through packet networks".

[i.14] Recommendation ITU-T G.8265.1: "Precision time protocol telecom profile for frequency synchronization".

[i.15] Recommendation ITU-T G.8275.1: "Precision time protocol telecom profile for phase/time synchronization".

[i.16] ETSI TS 136 133: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management (3GPP TS 36.133)".

[i.17] ETSI TR 136 922: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); TDD Home eNode B (HeNB) Radio Frequency (RF) requirements analysis (3GPP TR 36.922)".

[i.18] IEEE™ Communications Standards Magazine (volume 1, issue 1, March 2017): "Analysis of the Synchronization Requirements of 5G and Corresponding Solutions".

NOTE: Available at Analysis of the Synchronization Requirements of 5g and Corresponding Solutions | IEEE™ Journals & Magazine | IEEE™ Xplore.

[i.19] IEEE™ 1588: "Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[i.20] Recommendation ITU-R TF.460-6: "Standard-frequency and time-signal emissions".

[i.21] German law on time.

[i.22] Coordinated Universal Time (UTC).

[i.23] Downstream Radio Frequency Interface Specification, CM-SP-DRFII14-131120, November 20, 2013, Cable Television Laboratories, Inc.

[i.24] DOCSIS 3.1, Physical Layer Specification, CM-SP-PHYv3.1-I08- 151210, December 10, 2015, Cable Television Laboratories, Inc.

[i.25] DOCSIS 3.0, Physical Layer Specification, CM-SP-PHYv3.0-I12- 150305, March 5, 2015, Cable Television Laboratories, Inc.

[i.26] Data-Over-Cable Service Interface Specifications DCA - MHAv2 Remote DOCSIS Timing Interface CM-SP-R-DTI-I05-170524.

[i.27] ETSI TS 136 104: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Base Station (BS) radio transmission and reception (3GPP TS 36.104)".

[i.28] ISO/IEC 19762:2016: "Information technology -- Automatic identification and data capture (AIDC) techniques -- Harmonized vocabulary".

[i.29] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.30] ETSI GS NFV-SEC 013: "Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification".

[i.31] ETSI GR NFV-SEC 011: "Network Functions Virtualisation (NFV); Security; Report on NFV LI Architecture".

[i.32] NISTR 8006: "NIST Cloud Computing Forensic Science Challenges".

[i.33] ESMA Guidelines: "Transaction reporting, order record keeping and clock synchronization under MiFID II".

[i.34] OFCOM's (UK) Metering and Billing directive.

[i.35] Bundesnetzagentur (Germany): "Billing accuracy".

[i.36] IEC/IEEE™ 61850-9-3:2016: "Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation".

[i.37] IEEE™ C37.238-2017: "IEEE™ Standard Profile for Use of IEEE™ 1588 Precision Time Protocol in Power System Applications".

[i.38] Time synchronization in Virtual Machines.

[i.39] An overview of remote interference management - Ericsson®.

[i.40] Telecom Requirements for Time and Frequency Synchronization by Marc Weiss, Ph.D. of the Time and Frequency Division, NIST.

[i.41] Telecommunications Synchronization Overview.

[i.42] Recommendation ITU-R TF.1876-0: "Trusted time source for Time Stamp Authority".

[i.43] IEEE 802.11™: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.44] ISO/IEC 24730: "Information technology, Real time locating systems (RTLS)".

[i.45] Bureau International des Poids et Mesures: "UTC definition".

[i.46] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".

[i.47] How NTP works.

[i.48] ITU and BIPM decision.

[i.49] National Geographic Society definition.

[i.50] CERN project.

NOTE: Repository of the white rabbit project https://ohwr.org/project/white-rabbit/wikis/home.

[i.51] ATIS: "Workshop on Synchronization and Timing Systems".

[i.52] Shannon-Hartley theorem.

[i.53] Recommendation ITU G.8275/Y.1369: "Architecture and requirements for packet-based time and phase distribution".

[i.54] M. Rizzi, M. Lipinski, P. Ferrari, S. Rinaldi, and A. Flammini: "White rabbit clock synchronization: Ultimate limits on close-in phase noise and short-term stability due to FPGA implementation," IEEE™ Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, Sep. 2018.

[i.55] Lee, S. K., Wang, H., & Weatherspoon, H. (2019): "Globally synchronized time via datacenter networks", IEEE™/ACM Transactions on Networking.

[i.56] ITU GSTR-GNSS (2020): "Considerations on the use of GNSS as a primary time reference in telecommunications".

[i.57] CSA Cloud Security Alliance: "Privacy level agreement outline for the sale of cloud services in the European Union".

[i.58] GSMA NG.126: "Cloud Infrastructure Reference Model Version 1.0".

[i.59] U.S. Department of Homeland Security: "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure".

[i.60] ETSI GR NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".

[i.61] ETSI GR NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

[i.62] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".

[i.63] IEEE 802.1AS™: "Standard for Local and Metropolitan Area Networks -- Timing and Synchronization for Time-Sensitive Applications".

[i.64] IEEE 802.1Q™: "Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks".

[i.65] IEEE 802.3ae™: "Standard for Information technology - Local and metropolitan area networks - Part 3: CSMA/CD Access Method and Physical Layer Specifications - Media Access Control (MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation".

[i.66] IEEE 802.3™: "IEEE™ Standard for Ethernet".

[i.67] Ericsson Technology Review, January 13, 2021: "5G synchronization requirements and solutions".

[i.68] Telco Cloud Infra Timing Application - ptp4l, phc2sys and pmc.

[i.69] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU.

[i.70] World Geodetic System of 1984 ((WGS-84) defined by International Civil Aviation Organization.

[i.71] ETSI TS 138 104: "5G; NR; Base Station (BS) radio transmission and reception (3GPP TS 38.104)".

[i.72] ETSI TS 136 101: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio transmission and reception (3GPP TS 36.101)".

[i.73] NISTIR 7904: "Trusted Geolocation in the Cloud: Proof of Concept Implementation".

[i.74] ESMA: "ESMA/2015/1464 Regulatory technical and implementing standards - Annex I, MiFID II / MiFIR".

[i.75] Commission delegated regulation (EU) 2017/574 of 7 June 2016 supplementing Directive 2014/65/EU of the European Parliament and of the Council with regard to regulatory technical standards for the level of accuracy of business clocks.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

2G	Second generation technology standard for cellular networks
3G	Third generation technology standard for broadband cellular networks
3GPP	3G Project Partnership
4G	Fourth-generation technology standard for broadband cellular network technology
5G	Fifth-generation technology standard for broadband cellular networks
ADMF	Administration Function
API	Application Programming Interface
ATIS	Alliance for Telecommunications Industry Solutions
BBU	Baseband Unit
BIPM	Bureau International des Poids et Mesures

BS	Base Station
BTS	Base Transceiver Station
C/A	C/A (GNSS legacy civil signal)
CCAP	Cable Converged Access Platform
CERN	Centre Européen pour la Recherche Nucléaire
CET	Central European Time
CLK	Clock
CMTS	Cable modem termination system
CO	Central Offices
CoMP	Coordinated Multi-Point transmission/reception (3GPP)
COTS	Commercial-Off-The-Shelf
CPRI	Common Public Radio Interface
CPU	Central Processing Unit
CRAN/C-RAN	Centralized/Cloud Radio Access Network
CS	Commercial Service (Galileo)
CSP	Communications Services Provider
dB	Decibel
DHCP	Dynamic Host Configuration Protocol
DHS	Department of Homeland Security
DOCSIS	Data Over Cable Service Interface Specification
DPDK	Data Plane Development Kit
DTI	DOCSIS Timing Interface
DTP	Datacenter Time Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
eICIC	Enhanced Inter Cell Interference Coordination
EPC	Evolved Packet Core
ePTRC	Enhanced Primary Time Reference Clock
EQAM	Enhanced quadrature amplitude modulation
ESMA	European Securities Markets Authority
FCC	Federal Communications Commission
FDD	Frequency Division Multiplex
FIFO	First In First Out
GEO	Geostationary Orbit
GHz	Giga Hertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GS	Group Specification
GSM	Global System for Mobile
GSMA	GSM Association
HAS	High Accuracy Service (Galileo)
HFC	Hybrid fiber-coaxial
HLR	Home Location Register
HMEE	Hardware Mediated Execution Enclave
HSM	Hardware Security Module
HW	Hardware
ID	Identity
IEC	International Electrotechnical Commission
IEEE™	Institute of Electrical and Electronic Engineers
IERS	International Earth Rotation and Reference Systems Service
IP	Internet Protocol
IPR	Intellectual Property Rights
IPSEC	Internet Protocol Security
ISO	International Organization for Standardization
IT	Information Technology
KM	Kilometer
LEA	Law Enforcement Agency
LEMF	Law Enforcement Mediation Function
LEO	Low Earth Orbit
LI	Lawful Interception
LTE	Long Term Evolution
LTE-A	Long Term Evolution - Advanced
MAC	Media Access Control

MACSEC	Media Access Control Security
MANO	Management & Orchestration
MBMS	Multimedia Broadcast Multicast Service
MBSFN	Multimedia Broadcast multicast service Single Frequency Network
M-CMTS	Modular CMTS
MDF	Mediation Function
MEO	Medium Earth Orbit
MHz	Megahertz
MiFID	Markets in Financial Instruments Directive
MIMO	Multiple Input Multiple Output (3GPP)
MPEG	Moving Picture Experts Group
MS	Multiple system (DOCSIS)
N/A	Not Applicable
NB	Node B
NFVI	Network Function Virtualisation Infrastructure
NIC	Network Interface Controler
NIST	National Institute of Standards and Technology
NISTR	NIST Internal Report
NMA	Navigation Message Authentication
NTP	Network Time Protocol
NTS	Network Time Security
O&M	Operations & Maintenance
OFCOM	Office for communications services of UK
O-RAN	Open Radio Access Network
OS-NMA	Open Service - Navigation Message Authentication
OSS	Operations Support System
OTDOA	Observed Time Difference Of Arrival
OTN	Optical Transport Network
PCS	Physical Coding Sublayer
PHC	PTP Hardware Clock
PHY	Physical
PLA	Privacy Level Agreement
PM	Physical Machine
PMA	Physical Medium Attachment
PMD	Physical Medium Dependent
PNT	Positioning, Navigation and Timing
PoP	Point of Presence
ppb	parts per billion
PPS	Pulse-Per-Second
PRS	Public Regulated Service
PRTC	Primary Reference Time Clock
PSAP	Public Safety Answering Point
PTP	Precision Time Protocol
QAM	Quadrature Amplitude Modulation
QoS	Quality of Services
RAN	Radio Access Network
R-DTI	Remote DOCSIS Timing Interface
RE	Radio Equipment
REC	Radio Equipment Controller
RF	Radio Frequency
RFID	Radio Frequency Identification
RoT	Root of Trust
R-PHY	Remote PHY (DOCSIS)
RRH	Remote Radio Heads
RTS	Regulatory technical standard
RX	Receiver
SDH	Synchronous Digital Hierarchy
SDN	Software Defined Network
SLA	Service Level Agreement
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical NETwork

SR-IOV	Single-Root Input/Output Virtualization
SSL	Secure Socket Layer
STL	Satellite Time and Location
SV	Space Vehicle (SV) time
SyncE	Synchronous Ethernet
TAE	Time Alignment Error
TAI	International Atomic Time
TCG	Trusted Computing Group
TDD	Time-division Multiplex
TESLA	Timed Efficient Stream Loss-Tolerant Authentication
TF	Time and Frequency (ITU specifications)
TKG	Telekommunikationsgesetz, German Telecommunications Act
TLV	Time Length Value
TPM	Trusted Platform Module
TS	Technical Specification
TSN	Time Sensitive Network
TTD	True Time Delay
TX	Transmission
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
USNO	U.S. Naval Observatory
UT1	Earth rotation time
UTC	Universal Time Coordinated
vCCAP	Virtual CCAP
VLAN	Virtual Local Aera Network
VM	Virtual Machine
VNF	Virtual network function
VNFC	Virtual Network Component
VNFCI	Virtual Network Function Component Instance
VNFD	Virtual Network Function Descriptor
VNFI	Virtual Network Function Infrastructure
VoIP	Voice over IP
WLAN	Wireless Local Area Network
WR	White Rabbit
WRC	World Radiocommunication Conference
WSTS	Workshop on Synchronization and Timing Systems (ATIS)
WTSC	Wireless Technology and Systems Committee (ATIS)

4 Problem statement: Location and timestamp synchronization in NFV

4.1 Regulatory timestamp requirements

4.1.1 Communications, electronic market regulation, billing, interception, data retention, and critical infrastructures

The NIST Cloud Computing Forensic Science Working Group has stated that accurate time synchronization has always been an issue in network forensics, and is made all the more challenging in a cloud environment as timestamps need to be synchronized across multiple physical machines that are spread across multiple geographical regions, between the cloud infrastructure and remote web clients including numerous end points. Time synchronization has been categorized under the Analysis challenge of cloud forensics (see NISTR 8006 [i.32]) which consists of:

- correlation of forensic artefacts across and within cloud providers;
- reconstruction of events from virtual images or storage;
- integrity of metadata; and

- timeline analysis of log data including synchronization of timestamps.

Time synchronization has been ranked as 5th among the 65 challenges of cloud forensics identified by NIST.

Locating data is another challenging and time-consuming task in a cloud environment. Legal ramifications need to be taken into consideration due to several countries passing laws regarding the geo-location of data. In a cloud environment, data may be dispersed on physical storages across a number of foreign countries and/or moved around according to the VMs topology. In the context of network forensics, it is important to be able to locate the physical or virtual nodes which handle the data even if these resources can be dynamically (re)assigned on demand.

NIST has categorized the location of data under the Data Collection challenge of cloud forensics. The multiple venues and geo-locations challenge, ranked challenge #17 by NIST is due to the impact on chain of custody, finding evidence, and identifying access resources which arise from distributed data collection across a range of sources or geo-location unknowns. The decreased access and data control challenge (#25) results from the cloud customers, lack of control and knowledge of the physical locations of the data. The locating evidence challenge (#27) is related to eDiscovery, which is a critical component in cloud computing and essential for locating data that may be requested in a subpoena.

The time frame and the thoroughness of results are issues due to the lack of knowledge of all locations of data storage. The physical location challenge (#48) is related to (#27), since physical locations of data are unknown (due in part to lack of local storage and access to the hardware), there are difficulties in specifying and responding to subpoenas.

The virtualisation infrastructure provides a flexible environment to host several enterprise applications and telecommunication services. Precise and secure timing services and time-stamping of events are also critical to many of those services (e.g. mobile wireless) and applications (e.g. High Frequency Trading, financial transactions, banking systems, billing, etc.). The virtualisation infrastructure itself requires timing and synchronization for fault management (through logging of events) and Security management (through Identity and Access Management).

National regulations from the EU and the USA have also been issued on clock synchronization, location and timestamps:

- The annex on RTS 25 (Regulatory technical standards [i.33]) from the European Securities Market Authority (ESMA) is mainly on clock synchronization and the level of accuracy of business clocks supplementing Directive 2014/65/EU (see [i.69]). This annex does require that any financial transaction needs to be timestamped with a granularity of 100 µs relative to Coordinated Universal Time (UTC).

- The US Financial Industry Regulatory Authority which is providing guidance on quotation, order and transaction reporting facilities requires clock synchronization for audit trail purposes. Financial transactions need to be timestamped with a granularity of 50 ms by traders. Such system has also to be aligned to the U.T.C. of NIST atomic clock source with up to a 50 ms tolerance.

- The SEC Rule 613 requires "Each national securities exchange, national securities association, and member of such exchange or association to synchronize its business clocks which are used for the purposes of recording the date and time of any reportable event. The approved plan requires a granularity of 1 ms and 50 ms synchronization.

- The OFCOM's (UK) Metering and Billing directive was reviewed in 2021 on retail and wholesale for CSP. The Appendix A2 clause 3.3, on measurement capabilities of usage events, mandates that measurements of event duration are to be accurate to ±1 second or ±0,01 % (whichever is less stringent) and the Time of Day given is accurate to ±1 second (see [i.34]).

- The Billing accuracy required by Bundesnetzagentur on end customer billing is based on section 45g of the Telecommunications Act (TKG) of 22 June 2004 (Federal Law Gazette I page 1190, as last amended by Article 1 of the Act of 3 May 2012 (Federal Law Gazette I page 958)) to ensure metering and billing accuracy. It is to give customers confidence that their consumption has been accurately recorded and charged for (see [i.35]).

- There are also regulations related to critical infrastructure such as petroleum industry, power grid, precision agriculture, space applications, surveying & mapping, air traffic control, supply chains, personal navigation, industrial control, emergency services, transit/commuting operations, shipping & maritime applications/financial markets, etc. Such infrastructures may depend on GNSS for "PNT", i.e. positioning, navigation and timing technology and potentially on CSP on the "time/synchronization" of such sector, etc.

- The section 215 of the Federal Power Act of the USA, requires the development of mandatory and enforceable Reliability Standards, which are subject to Federal Energy Regulatory Commission review and approval. This commission mandates precise time synchronization on the electric transmission system with micro-second accuracy. In order to be enforced, two profiles of IEEE 1588 [i.19] Precise Time Protocol (PTP) for power system networks, i.e. IEC 61850-9-3 [i.36] and IEEE C37.238 [i.37] have been developed.

Accurate timekeeping is a key service to many applications that can potentially be migrated to a virtualised infrastructure. However, the virtual machine nature of time-sharing of physical hardware nature makes it a challenge to run time sensitive applications and services (details in [i.38]).

Precise time is key to a variety of applications such as telecommunication systems, energy and utilities, media and entertainment, automotive and financial services. The virtualised infrastructure needs to provide support for time sensitive Network Functions.

Time-stamps are also essential to business transactions for records keeping traceability and for trade synchronization on a global scale. In order to realize a global and consistent database system, a real-time time-stamp can be associated to every data written to it.

The synchronization of nodes within a network typically requires the distribution of time from a central reference source (e.g. UTC) to the individual nodes. IEEE 1588 [i.19] PTP is one of the main standard methods to synchronize devices on a network with microsecond accuracy using hardware timestamping. The protocol synchronizes follower clocks to a PTP leader clock ensuring that events and packet timestamps in all follower clocks are synchronized to the same time base. Moreover, it offers different profiles to tailor PTP to various applications and services with different requirements and performance objectives.

NOTE: Leader and follower terms in the present document maps to master and slave terms respectively for PTP time synchronization as specified in IEEE 802.1AS [i.63] and IEEE 1588 [i.19].

4.1.2 Financial market regulation (timestamp of transaction, especially in high-speed trading)

As indicated above, there are stricter regulation on timestamp in the financial markets. The European regulation MiFID II (The Markets in Financial Instruments Directive II) enforced from 2018 has raised the requirement for some deemed high frequency to the level at least of microsecond, enforced by the regulator (European Securities and Market Authority) and its Regulatory technical standards called RTS 25. In the past. MiFID requirement of 1 millisecond granularity was adequate for most case. RTS 25 are mostly guidelines on time synchronization, timestamp granularity, trade reporting, transaction reporting, record keeping, and kill switches.

4.2 CSP timestamp requirements

4.2.1 Time/frequency reference source

CSPs are using centralized time servers, a network appliance that receives the precise time from a hardware reference clock, to provide time synchronization to client devices. Reference clocks are hardware clocks which for example, could be atomic clock, Global Navigation Satellite Systems (GNSS), and/or national time and frequency radio broadcasts.

4.2.2 Network synchronization, especially mobile radio/5G

There are two core areas for the requirement of timestamp synchronization:

- Requirements for services or applications such as real time communication service or cryptographic system (e.g. certificate validation of SSL or replay attack mitigation).

- Requirements for infrastructure, especially with New Radio (5G). In many cases, such systems will rely on Time Division Duplex (TDD) for dividing radio resources between uplink and downlink, that may create interferences between radio emitters, or remote interferences due to tropospheric ducting [i.39]. Fronthaul and backhaul based on optical links may also require stricter time synchronization.

There are three kinds of synchronization:

- Frequency synchronization, aligns clocks with respect to frequency (e.g. Frequency Division Duplex (FDD) applications, especially for radio mobile network). In frequency synchronized systems, the significant instants occur at the same rate for all synchronized nodes.

- Phase synchronization, aligns clocks with respect to phase (e.g. Time Division Duplex (TDD) applications). In systems synchronized based on the phase, the timing signals occur at the same instant.

- Time synchronization, aligns clocks with respect to time (e.g. Finance service industries). Time synchronization refers to the distribution of an absolute time reference to a set of real-time clocks. The synchronized nodes share a common epoch and time-scale.

Past networks required data transport to be performed at the same frequency with the same bandwidth offered to all nodes, independent of traffic. They were governed through clocks of varying quality, with the measure of quality for these called the clock stratum level (see [i.40] and [i.41]).

CSP networks have evolved to have an asynchronous, or packet, core, with access technologies such as wireless cell networks at the edge. Packet data networks generally do not require accurate synchronization (millisecond). However, synchronization is required for the services or applications, and particularly in radio edge of network at least due to interference mitigation requirements. As services or radio access do require various types of synchronization, the underlying network requires special transport systems to deliver that or requires synchronous clock sources.

3GPP next generation mobile networks, i.e. 5G, are faced with providing step-changes as they will cater for high-bandwidth high-definition streaming and conferencing, machine to machine, interconnectivity and data collection for the Internet of Things, including ultra-low latency applications such as driverless/connected cars. The higher wireless user data-rates are up to 20 Gbps that may be based on shorter radio transmission distance. The information transported between Base Band Units (B.B.U.s) and Remote Radio Heads (RRHs) is generally in the form of sampled radio signals, that require excellent signal to noise ratio and lower interferences with other radio sources, based on Shannon-Hartley theorem (see [i.52]).

Already, for Long Term Evolution-Advanced (LTE-A) signals which may have bandwidths up to 100 MHz, a single uncompressed sampled radio waveform requires a link bit-rate of over 5 Gb/s (assuming 16-bit samples).

Higher accuracy, especially in case of Internet of Things or connected cars will be required in 5G. 3GPP 5G requirements result in drastic improvements on time management compared to 4G:

Table 4.2.2-1: 5G requirements (source: Workshop on Synchronization and Timing Systems (WSTS) of ATIS [i.51], 26/03/2019)

	Enhanced Primary Reference Time Clock (ePTRC, defined in Recommendation ITU-T G.8272 [i.9])	Transmission Network	Base Station
4 G	250 ns	1 000 ns (including holdover, 30 ns per hop, > 20 hops	250 ns
5 G	50 ns (and new positioning services: 3 ns, see [i.67])	Tracing 100 ns, 5 ns per hop, > 20 hops	50 ns or 3 ns In case of new positioning services, based on OTDOA (Observed Time Difference of Arrival) about ±1 ns (local)

As NFV is based on software, time accuracy may be an issue. Virtual machines may lose time due to hypervisor scheduling or other competition for hardware access between multiple processes. Furthermore, the number of processes will vary dynamically.