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

GROUP REPORT

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.

Copyright Notification

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^{TM} 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^{TM} 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^{TM} Journals & Magazine | IEEE^{TM} Xplore.

[i.19] IEEE^{TM} 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^{TM} 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^{TM} C37.238-2017: "IEEE^{TM} Standard Profile for Use of IEEE^{TM} 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^{TM}: "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^{TM} 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^{TM}/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$^{\text{TM}}$: "Standard for Local and Metropolitan Area Networks -- Timing and Synchronization for Time-Sensitive Applications".

[i.64] IEEE 802.1Q$^{\text{TM}}$: "Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks".

[i.65] IEEE 802.3ae$^{\text{TM}}$: "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$^{\text{TM}}$: "IEEE$^{\text{TM}}$ 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^{TM}	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.

4.2.3 Forensics of network events for O&M

Network forensics is related to the monitoring and the analysis of computer network traffic for example, for the purpose of legal evidence or intrusion detection. Unlike other areas of such forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is majority of time, a pro-active investigation. Timestamped logs will help such investigations to understand the events of O&M, and the call flows. Such investigations in virtual environments face more issues such as data location, Virtual Machine (VM) lifecycle, multitenancy and valid chain-of-custody. The number of parameters to collect and analyse seems to be important. The correlation based on timestamp is one of the techniques that is great help in forensics, but only if the time source and time accuracy is the same throughout of network.

4.2.4 Timestamp for VNF licensing

In traditional network deployments, the Network Functions are implemented in specialized hardware appliances. The Network Function providers typically sell their specific appliances based on an entry fee for the hardware platform and a licensing model for the software. When the demand for functions, capacity, or features increases, the Communication Service Provider upgrades the license or in some cases buy new hardware.

New licensing models are anticipated for the NFV environment to fit with the dynamicity, flexibility, scalability and agility characteristics of the NFV system such as usage-based or capacity-based licensing models. The NFV system needs to support various types of licensing models.

A licensing model defines the usage of license entitlement data with associated metrics that are used to measure the actual utilization of the VNF and verify that the VNF is used within the bounds of the license entitlement rights and limits.

For the subscription licensing model, the VNF license entitlement is only valid for a subscription period (e.g. a month or a year).

Other different licensing models, based on timestamp may exist, that may involve more dynamic usages or enable value-based pricing. The use of a trusted and secure time and timestamping is crucial for the license enforcement functionality that ensures to the involved parties (VNF provider, infrastructure provider (i.e. third party cloud/data center provider), timestamp authority (see [i.42]), and service provider) that the VNF is used within the bounds of the VNF license entitlement agreed between the service provider and the VNF provider.

For the usage-based licensing models, a report of the usage of the VNF, trusted by involved parties, is used to prove the usage of VNF and as input for the charging system. The use of trusted timestamping is needed for this usage-based licensing report.

4.3 Requirements on location of internal events or operations of network

4.3.1 For the O&M

Operations & Maintenance Systems (mostly based on Operations Support Systems) have to configure and provision the network nodes. Such systems have to know the location of such nodes (which data center) in order to dispatch if needed a technician either to repair, to configure or to set up hardware-based systems.

Network statistics collection (Performance Management), alarm monitoring (Fault Management) and logging of various network nodes actions (Event Management) also happens in the O&M center. These stats, alarms and traces form important tools for a network operator to monitor the network health and performance.

Without any location such as those of the hardware, it is difficult to analyse internal events and to decide corrections or operations on a system, even if the operation is made remotely.

4.3.2 For third party such as investigation team, IPR owners, content licensing, etc.

The majority of Intellectual Property Rights or Content Licensing Systems are based on the location where the right or content is used. Furthermore, specific laws on contracts related to franchising, on copy rights and on licensing are different from one country to another. Location information or control of content or software may be required by its owner. Location of a process or of software may be required information for such purposes. In case of breach of property, audit may require such information.

4.3.3 Location for VNF licensing

Some licensing models restrict or prevent the execution of a VNF in a specific NFVI location.

For those licensing models, a use of a trusted location information is crucial for the license enforcement functionality to ensure that the VNF is used within the bounds of the VNF license entitlement agreed between the service provider and the VNF provider.

4.4 Requirements on UE location in mobile or nomadic network

UE location in mobile or nomadic network are needed to route an incoming call or SMS to the UE. This location is more a logical ID managed by the network.

Furthermore, EU telecommunication rules require that operators provide information about caller location to emergency authorities, and route the call to the right PSAP (Public Safety Answering Points).

In the US, the federal regulator (FCC) requires nationwide providers to achieve high accuracy of location =for handset-based technologies, i.e. 50 m for 67 % of calls, 150 m for 95 % of calls, and z-axis (vertical) location accuracy metric of plus or minus 3 m for 80 % of indoor wireless E911 calls for z-axis capable handsets for the majority of US market. Location of a UE can help to providing value added services such as navigation software, social networking services, location-based advertising, and tracking systems.

4.5 Principles

4.5.1 Time definition (UTC /legal time)

The important aspect of frequency spectrum utilization is managed through ITU World Radio communication Conferences (WRCs). Such spectrum utilization needs to be facilitated with the determination and coordination of the international time scale. For the time being, such time scale is defined by International Telecommunications Union Recommendation (Recommendation ITU-R TF.460-6 [i.20]), Standard-frequency and time-signal emissions. It defines Coordinated Universal Time, abbreviated to UTC (see [i.45]). It is within about 1 second of mean solar time at 0° longitude.

Such international time scale is an atomic time scale distributed by various telecommunication systems throughout the world known as Coordinated Universal Time (UTC). UTC is maintained by the International Bureau of Weights and Measures (BIPM) in cooperation with the International Earth reference and Rotation Service (IERS) which forms the basis of a coordinated dissemination of standard frequencies and time signals. It is mostly based on GNSS measurements and in turn based on standards that defines how the country laboratory can measure and contribute to such measurements. Physical realizations of UTC - named UTC(k) - are maintained in such national metrology institutes or observatories contributing with their clock data to the BIPM.

Contributed measurements from such timing centers around the world are used in the determination of UTC, which is adjusted to within 0,9 s of Earth rotation time (UT1) by IERS-determined values of the Earth rotation. The adjustments, made in one second steps known as leap seconds, were implemented the first time in 1972 to permit UT1 to be recovered from broadcast values of UTC for celestial navigation.

This international time scale is used in many Internet and World Wide Web standards and has been distributed among various telecommunications systems throughout the world, usually though the use of the Network Time Protocol (NTP IETF RFC 5905 [i.46]). NTP was designed to synchronize the clocks of computers over the Internet, transmitting time information from the UTC system [i.47]. If only milliseconds precision is needed, devices can obtain the current UTC from a number of official internet UTC servers, however for sub-microsecond precision, devices can obtain the time from satellite signals.

Current telecommunication and navigation systems utilize continuous timing for their data transmissions; consequently, deliberations have been ongoing within the ITU-R on the issue of modifying the definition of UTC to a continuous time scale. (See its definition in [i.22].)

Leap seconds may be an issue in communications networks or in some operating systems. Software developers may have to know about leap seconds to minimize the risk of leap-second triggered system malfunction. Due to this, several proposals have been made to replace UTC with a new system that would eliminate leap seconds but a decision on this topic has been deferred by ITU [i.48].

Standard time is the synchronization of clocks within a geographical area or region to a single time standard, rather than using solar time or a locally chosen meridian (longitude) to establish a local mean time standard. Each country or group of country decides the legal time. One example is the German Time act, EinhZeitG, (see [i.21] on German law on time and the related ITU recommendation on Coordinated Universal Time as the Recommendation ITU-R TF.460-6 [i.20]), in which the German Federal Parliament has passed the act that in official and business communications, date and time, are used according to legal time. The legal time for this country is Central European Time (CET) with a summer time period. Outside this period, it is defined as Coordinated Universal Time plus one hour.

4.5.2 Location definition

A location (see [i.49]) is a particular place or position. Positioning is the ability to accurately and precisely determine location and orientation two-dimensionally (or three-dimensionally when required) referenced to a standard geodetic system (such as World Geodetic System 1984, or WGS84 [i.70]).

The position is based on a real time locating system, made by a set of radio frequency receivers and associated computing equipment used to determine the position of a transmitting device relative to the placement of the aforementioned receivers, that is capable of reporting that position within several minutes of the transmission, used for determining the position of the transmission.

The word geolocation also refers to the latitude and longitude coordinates of a particular location.

These above terms and definitions have been standardized by ISO/IEC 19762 [i.28].

4.6 Multiple VNFCI location

According to ETSI GS NFV 003 [i.29], NFV Infrastructure (NFVI) represents the totality of all hardware and software components which build up the environment in which VNFs are deployed. The NFV Infrastructure can span across several physical locations, i.e. multiple N-PoPs. The network providing connectivity between these locations is regarded to be part of the NFV-Infrastructure.

A Virtualised Network Function Component Instance (VNFCI) is an instance of a VNFC deployed in a specific virtualisation instance. It has a lifecycle dependency with its parent VNF instance. Multiple VNFCIs can be based on different hosts, which do not need to be in the same rack, data center or physical location. These may induce security issues for sensitive functions, such as key location and time synchronization management with migrated images (see ETSI GS NFV-SEC 013 [i.30]).

Network function sensitive sub-functions such as elements of HLR/HSS/AUSF/UDR of a 3GPP networks, need to be secure. Such instances have need to be instantiated in a protected data center with hardware that provide secure enclaves/hardware security modules to reduce the risk of fraud and access to primary main keys. Except for low latency-based services, which require URLCC (Ultra-Reliable and Low Latency Communications), other network functions may be instantiated or migrated to any hardware and data center that is part of the NFVI. Low latency services require instantiation in NFVI close to the user. The use of HMEEs allows the location of the software instances to be attested to a host, which allows the physical location to be attested. Furthermore, some content owners may require that their specific content may be available only to NFV users from a specific country and storage in that country. According to ETSI GR NFV-SEC 011 [i.31], the ADMF (Administrative Function) should be able to request assurance that the LI (Lawful Interception) VMs, containers and any other element involved in the LI service are within the pre-defined location constraints which the NFV MANO layer has been given.

Subsequently, there are some NFV deployments that require location information plus timestamp for each event, and strict control management on the association of VNFCI and NFVI. Each VNFCI may have a separate location based on these requirements. It will be necessary to ensure that sufficient location information (physical location or confirmation that the VNFCI is within the host allocation constraints attested by MANO), is made available (see ETSI GR NFV-SEC 011 [i.31]).

VNF instances may have a single location (location of a specific single VNFCI only), or the union of multiple different locations if the VNF is made of multiple VNFCIs that may have different locations. Such location of each component can be different data center far away from other. A few possible views form on how to solve the key issue on location term of VNF Instance is proposed in clause 5.8.

5 Key Issues

5.1 Key issue 1: Time and distribution of time

Global Navigation Satellite Systems (GNSS) are space time distribution systems that are based on synchronized atomic clocks that transmit their coded position and time to timing receivers. The end nodes extract the time reference using integrated timing receivers. They do not require an additional distribution infrastructure and the signal is usually available to all the end nodes with the same level of accuracy. GNSS are based on the international reference time, Coordinated Universal Time (UTC). This approach is called the distributed PRTC system where the timing receivers act as Primary Reference Time Clocks (PRTCs) (G.8271 see [i.6]). The main advantage of this approach lies in the global availability of the GNSS signal.

The main issue is the need of an antenna with a wide-angle view of the sky, which is not practical for most indoor devices. The needs for lightning protection and antenna cabling are additional issues.

The other main approach of time distribution is to use packet-based network time protocol architecture. In this approach the time reference is distributed to the end node from a centralized PRTC, which could be based on GNSS or not. This approach does not impose the deployment of antennas on each end nodes. Only a centralized entity may be equipped with a GNSS antenna. The main issue for packet-based distribution architectures is that when stringent accuracy is required and depending of the network topology (e.g. several intermediate nodes between the PRTC and the end nodes), a synchronization network planning can be needed to reduce timing errors introduced by noise accumulation and delay asymmetries. In some cases, timing support may be deployed in the intermediate nodes.

Extra security may be added based on MACSEC and IPSEC with IEEE 1588 [i.19] standard for a precision clock synchronization protocol for networked measurement and control systems. The choice of the reference source, of the protocol to transport and the way the time is distributed, may be an issue.

5.2 Key issue 2: Time accuracy

Time accuracy is typically defined as the mean of the time error between the clock under test and a perfect reference clock, over an ensemble of measurements. UTC is the legal basis for time-keeping for most countries in the world, and de-facto time scale. It is maintained by the International Bureau of Weights and Measures (BIPM) in cooperation with the International Earth reference and Rotation Service (IERS). Recommendation ITU-R TF.460-6 [i.20] states that all standard-frequency and time signal emissions should conform as closely as possible to UTC. The accuracy of GNSS receivers depends on several factors such as satellite geometry, atmospheric conditions (e.g. solar storms), signal blockage, indoor usage, multi path conditions (e.g. signal reflecting off walls), and receiver design features. The GPS signal is typically accurate to 10 nanoseconds. Timing accuracy is lost in the interpretation of the signal by the receiver. Therefore, an average GPS receiver typically produces a pulse per second with accuracy of 100 nanoseconds or worse.

Better accuracy is also studied in ITU S15 on profile of IEEE 1588 [i.19] with Coherent PRTC. The coherent network PRTC connects primary reference clocks at the highest core or regional network level. This provides the ability to maintain network-wide enhanced PRTC time accuracy, even during periods of regional or network wide GNSS loss (see Recommendation ITU G.8275/Y.1369 [i.53]).

The accuracy may be lower than those provided by the reference source in the distribution of time.

5.3 Key issue 3: Time Synchronization

Time synchronization for the packet networks is based on:

- The definitions and terminology in Recommendation ITU-T G.8260 [i.4].
- Timing and synchronization aspects in packet networks in Recommendation ITU-T G.8261 [i.5].
- Time and phase synchronization aspects of packet networks in Recommendation ITU-T G.8271 [i.6].
- The clock synchronization is described in Recommendation ITU-Ts G.8262 [i.7], G.8263 [i.8], G.8272 [i.9] and G.8273 [i.10].
- The methods and architecture are described in Recommendation ITU-Ts G.8264 [i.13], G.8265 [i.11] and G.8275 [i.12].
- The profiles are described in Recommendation ITU-Ts G.8265.1 [i.14] and G.8275.1 [i.15].

In an ideal transmission system, the pulses are transmitted in precise intervals and arrive at the receiver with exactly the same time spacing. In real systems, various factors contribute to an imperfect signal that can result in poor frequency or phase synchronization. Frequency synchronization is the alignment of clocks to the same frequency. Similarly, phase synchronization is about aligning two devices to the same phase.

Wireless services have relied on synchronization from the very beginning. GSM/EDGE services depend on frequency synchronization for correct network operation. 3GPP standards mandate 50 parts per billion (ppb) for the frequency stability of a macro BTS at the radio interface. 3G (UMTS/WDCMA-FDD) and 4G (LTE-FDD) applied the same requirements.

Time synchronization has traditionally been required to support billing and alarm functions (maintenance or fault isolation). In this context, synchronization in general needs to be accurate to within hundreds of milliseconds. Another time synchronization application is the monitoring of delays in Internet Protocol (IP) networks. In this case, the requirement is accuracy to within some hundreds of microseconds (the actual requirement depends on the application). Stringent time synchronization requirements (i.e. in the range of a few microseconds) apply to the generation of signals over the air interface of several mobile systems.

Many commercial 5G networks use TDD. TDD radio frames inherently require time and phase alignment between radio base stations, to prevent interferences and related loss of traffic. Time synchronization is also required in FDD networks when different radio coordination features are used.

Furthermore, 3GPP makes it possible to serve several applications such as industrial automation Internet of Thing services, vehicles or drones positioning, and smart grid management, for which time synchronization is fundamental. While many applications benefit from accurate time synchronization, it is important to realize that high time accuracy over large areas can be very costly, especially for virtualised networks, due to poor software measurement quality of the internal clock of the host. For such applications, 3GPP has developed a Time Sensitive Network (TSN) solution with bridges and secured TSN time domain based on IEEE specifications (see specific needed architecture in ETSI TS 123 501 [i.62] and IEEE 802.1Q [i.64]). While such solutions improve the time Synchronization of the clock, they do not entirely solve the virtual software time measurement problem.

Table 5.3-1 provides a summary of phase synchronization requirements for LTE-TDD and LTE-Advanced technologies.

Table 5.3-1: Radio Access Phase Synchronization requirements (see [i.16])

Radio Access Network technology	Phase requirement
LTE TTD	±1,5 µs (< 3 Km cell radius) ±5 µs (> 3 Km cell radius)
LTE MBMS (LTE-FDD and LTE-TDD)	±10 µs
LTE-A CoMP	±0,5 µs to ±1,5 µs
LTE-A Eicic	±1,5 µs to 5 µs
E911 and Locating services	±0,1 µs
Small cells	±3 µs (1 µs to 5 µs) with 100 ppb to 250 ppb

The introduction of RAN virtualisation amplifies the problem of the frequency and phase Synchronization.

To decrease deployment cost of front haul [i.1] and backhaul, of RAN and BBU of Mobile networks, Mobile Network Operators are separating out the baseband and Radio Frequency (RF) components of the base stations, into a split architecture ([i.3]) and in reuse of existing packet-based networks (e.g. Ethernet and SDN) [i.1] and [i.2]).

Virtualised RAN, in which the BBU is built on commercial-off-the-shelf (COTS) hardware, rather than on a RAN vendor's proprietary hardware, requires mobile traffic to be transported without losing synchronization.

Such development induces challenges:

- Ultra-high-bit-rate requirements from the transport of high bandwidth radio streams for multiple antennas.
- Low latency and jitter to meet the demands of joint processing of multiple radio streams.

For example, in case of LTE A, frequency sync requirements are up to 50 ppb and time sync requirements up to 0,5 microseconds (see clause 4.2.2 and ETSI TS 136 133 [i.16] and ETSI TS 136 922 [i.17]). Some research papers mention that ± 130 ns is proposed as the new goal of network limits for 5G (see [i.18]).

The Recommendation ITU G.8272 [i.9] is the first "enhanced" clock specification aimed at meeting the requirements for 5G mobile infrastructure. The document specifies the enhanced PRTC (Primary Reference Time Clock), basically a very high accuracy GNSS timing receiver, capable of delivering time to within 30 ns of UTC.

However, to enable network slicing in the 5G radio access network (RAN), ITU-T is working to improve the profile of IEEE 1588 [i.19] PTP. On its "living list" of key technologies, ITU-T is also studying low layer technology, competing to provide traffic isolation and performance guarantees:

- Slicing Packet Network, using Flex E technology.
- Mobile OTN, using Optical Transport Network (OTN) technology.

Both of these may create dedicated bandwidth channels, enabling latency and throughput guarantees to be provided, as required by 3GPP.

5.4 Key issue 4: Timestamp log and storage

Some industries (e.g. payment services) are imposing timestamp log requirements for security reasons. The Payment Card Industries Data Security Standard specifies twelve requirements for compliance. One of them covers tracking and monitoring all access to cardholder data and network resources, and includes specific stricter requirement on the use of Network Time Protocol (NTP). It requires time synchronization for all logs. All systems need to synchronize their logs timestamps to centralized time servers.

Based on their threat analysis, only central time servers are allowed to receive time from external sources, based on UTC (i.e. using Atomic clocks or GNSS)

If multiple centralized time servers are used, they need to "peer" with each other to keep accurate time.

The storage of such log leads to the provision of integrated log management.

5.5 Key issue 5: Trusted Timestamp/attestation

The main security threats for GNSS based time synchronization are spoofing and jamming. The GNSS signals are very low power signals dominated by white noise. The noise is about a hundred to a few thousand times stronger than the GNSS signals themselves. As a consequence, GNSS signals are susceptible to a lot of unintentional and intentional interferers. Spoofing consists of faking of a false position/time towards a target GNSS receiver, while jamming is an intentional interference targeting the unavailability of the system. Some new GNSS or new LEOs systems (e.g. Commercial Services of Galileo, or Satelles/Iridium) achieve increased security and implement trusted timestamp sources to provide mitigation against spoofing.

Attestation of compiled software packages, (including patches), may be improved in terms of security by information on the place, where and when the signature and hash was processed (see clauses 6.5).

Trusted time may be required by regulation in some communications systems or processes. Trusted timestamp and locstamp for such purpose may be an issue.

5.6 Key issue 6: Location of events

Based national regulations, the process of legal interception usually has to be localized in the jurisdiction of the country where legal interception has been requested. Such laws and regulations may have been made to prohibit any illegal interception of communications other than that specifically authorized for legal interception purposes, or to ensure compliance with foreign authorities to respect mutual legal assistance treaties. Audit by national authorities of any events related interception may be made in order to check if it is the case.

Some Intellectual Property Rights (IPR) may prohibit some content streaming outside certain countries and regions, in order to protect such rights and to let the IPR owner to attribute licences to others parties outside such region. Such streaming process may be based not only on the IP addresses and/or the location of UE but also based on the location of the server or streaming processes. Such audit or control on the location of such events may be made by the IPR owner or its local representative.

The virtualisation of such services may be an issue if the processes do not develop geo fencing system to map virtual processes and physical location inside a geographical country or region border. Cloud providers have already developed the region concept to avoid illegal process outside the region, decided by their customers of such streaming or content distribution providers. The development of cloud gaming, or augmented reality based on edge computing may help them to define a better granularity of the location than determined from regional data centers if needed.

Location of events for multi-tenant use cases are not specifically considered in the present document and may have additional capability requirements beyond those for a single operator deployment.

5.7 Key issue 7: Location of UE

Precise position location (also called positioning or localization) of a UE may use different types of networks, i.e. cellular, indoor (based on WLAN, Bluetooth®, etc.) and satellites infrastructures.

Cellular positioning refers to mechanisms in cellular networks from 2G to 5G for obtaining the position of a subscriber, mainly outdoors.

Indoor positioning focuses on a deployment in buildings, on university campuses, and company premises. Location measurements may utilize ubiquitous computing and is often denoted by alternative terms like *location sensing*.

By their very nature, satellites cover huge geographical areas, and thus satellite positioning can pinpoint the location of a target on a whole continent or even the entire world.

Except for solutions based on GNSS, computed by the UE itself, the UE position is estimated based on knowledge of the geographical coordinates of a network reference such as Bluetooth beacons, radio cells (terrestrial), or WLAN access points.

The case of the satellite based UE location is more complex as the connected cell reference is moving and the satellite may be in either, Low Earth Orbit (LEO) or Medium Earth Orbit (MEO). As LEO and MEO satellites do not synchronize with the Earth's rotation and orbit the earth more rapidly than Geostationary Equatorial Orbit (GEO) satellites (an orbital period of 128 minutes or less for LEO, and an average of between 2 and 8 hours for MEO) multiple satellites are required in order to achieve seamless coverage, and with specific handovers with the UE. GEO is a special case where the satellite always appears stationary above the same point on earth's surface and the UE.

To improve the accuracy, different technologies are based on the measurement of cellular/WLAN/Bluetooth® radio signals in order to calculate the position of the UE, from known geographic information of the radio element, the antenna, from the cell coverage of the GEO, or the indirect computing of LEO/MEO satellite movement. Some measurements are based on the time delay, needed to communicate between the UE and the antenna. The Radio Frequencies (RF) power and used frequency information may be also key in the measurements to improve the accuracy of location of UE.

Increasingly radio elements may be managed and implemented using virtualised solutions. It means a good part of the local processes to manage the connectivity with the UE is based on COTS and software. NFV is key to implementation of the O-RAN or 5G Satellite or WLAN architectures.

In legacy networks, the mapping between geographical coordinates and radio element IDs, which are managed by the network was stable and set up during the initial deployment and configuration of the network. For 5G configurations may be changed easily with NFV. Such location information is used by LEAs to attest for evidence purposes where an LI target was geographically. This is based on information provided by the CSP of its radio sites geographical coordinates, and relies on a high degree of trust in the stability and integrity of the information provided. On top of that, time, RF power and frequencies may be used to improve the accuracy of the location processes. In legacy networks these parameters were not subject to frequent changes whereas they may be much more dynamic in virtualised implementations based on NFV.

5.8 Key issue 8: Multiple VNFCI policy

Due to the possibility of VNFCIs from within a single VNF existing in multiple locations, the question arises of how to define the location of a VNF. A few possible views form on how to solve this problem:

- The VNF can be described by an exhaustive list of locations of all its component instances.
- The VNF can be described solely by the locations of the critical elements (e.g. LI or cryptographic functions).
- The VNF can be described by the location of a singular critical element with functionality for the MANO to attest individual VNFCIs to ensure they lie within the pre-defined constraints (e.g. VNFCI 1 is allowed to be in data center A, but not data center B).

Each method has its advantages and the answer could lie in an amalgamation of the three.

Describing a VNF by an exhaustive list of the location of every VNFCI provides extremely high granularity over how data flows through the VNFI, however the bombardment of information that arises from this method is undesirable for the purposes of NFVI management and monitoring. This could lead to an overload of information, using too much bandwidth and interfering with day-to-day network management.

The second method provides a more high-level view of a VNF's location, allowing for easier management of key infrastructure of the NFVI. One example of this could be for billing purposes of a virtualised mobile network core, the location of a UE usually determines the cost of accessing the network. If the virtual edge device contains VNFs that span across different billing zones (e.g. different countries), that edge device needs to provide location information of the VNFs to accurately locate the UE. This ensures that the connected UE is billed correctly for the locale that the UE is in. What this method does not provide is the ability to trace the exact locations and the path taken by data as it passes through network infrastructure, such information is vital for network forensics and the enforcement of regulatory and lawful requirements.

The third method suggested is the most ideal from a network performance point of view as the amount of additional traffic required is the lowest from the solutions given. Presently there are 2 types of attestation which are possible, boot-time and run-time attestation. Boot-time attestation can provide a one-time location check as the VNFCI boots. Since only one check per VNFCI is needed, the additional traffic through the network can be kept to a minimum. Run-time attestation is a more robust solution as it enables the possibility of real-time location integrity checking while still maintaining a relatively low impact on network performance, however, in practice this is more complicated to implement.

It is key that any solution encompasses the needs of both good network performance and detailed network forensics. To this end, it is recommended that high-level information is available to the NFV MANO and at the application layer (e.g. internally within the VNF and to OSS/BSS), and for network forensics, an exhaustive chronology of component locations can be stored locally for use in post-cybersecurity event forensics or general system fault-finding. This would allow the effective management of network infrastructure whilst catering to the needs of a forensic investigation. One proposed solution is that the location of one central VNFCI is available to the MANO, the remaining VNFCIs of the VNF can then have their logical locations attested, ensuring that they reside within the given constraints.

Location of network infrastructure and multiple VNFCI is further complicated with use of edge computing. VNFD policy such as those induced by 3GPP specifications and GSMA requirements on edge computing may impact location of a VNF, in order to provide low latency and high bandwidth services. Edge computing may vary dynamically based on traffic influence managed by application functions or by UE mobility events, in order to maintain real time quality of services.

In multi-tenant scenarios, further study is needed beyond the present document in order to address location challenges with multiple VNFCI VNFs to support sensitive applications requiring locstamps.

5.9 Key issue 9: Location at Instantiation, Location at Run time

The NIST Definition of Cloud Computing lists five essential characteristics of Cloud Computing. These characteristics are:

- on-demand self-service;
- broadband network access;
- resource pooling;
- rapid elasticity;
- measured service.

Resource pooling means that provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. The customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of geographical abstraction (e.g. country, state, or datacenter). Resources may include storage, processing, memory, network bandwidth and virtual machines.

The ability to virtualize the Physical Machine (PM) gives important benefits in terms of reliability, efficiency, scalability and makes computing available as a utility service. Virtualisation, coupled with migration capability, enables the data centers to consolidate their computing needs and use lesser number of PMs. VM placement and migration techniques are used for load balancing, server consolidation and hotspot mitigation. Thus, VM placement is an important aspect of data center resource management to achieve efficient resource such PMs.

At the end of a migration procedure, the old VM is stopped. Subsequently its resources freed up while a new VM starts up in a location chosen by the VM placement strategy and replicates the service.

The location of a cloud provider's data center has significant impact on the law that applies to the privacy of computation outsourcing. Data centers of cloud providers can be distributed worldwide. It may happen that the client resides in one jurisdiction and the data centers of the cloud, where a task is outsourced, is in another jurisdiction.

Differences in laws between the two locations can affect the privacy-preserving computation procedures of the cloud provider. In the European Union, approaches such as Privacy Level Agreement (PLA) guideline for cloud services [i.57] are needed to ensure that the locations of all data centers where personal data may be processed, stored, mirrored, backed up, and recovered is able to comply with data protection regulations.

Hence, while performing computation on sensitive data, it is important to make sure that the computation procedure does not violate the regulatory acts. Clients may not be able to verify the data handling practices of the cloud provider and thus to be sure that the data are handled in a lawful way. Customers desire a type of geographic descriptor (a *geotag*). One of the natural concerns to address for the cloud is to be able to determine where the customer resources are. In a cloud without boundaries, this is impossible to answer. In a cloud that can be marked with trust and geographic description information, answers to this question can be made trivial-providing new confidence to customers. Given the large and growing number of regulations that stipulate location controls-particularly for privacy-related workloads and government data, this adds a significant breakthrough value. Now, workloads and this kind of data control that fall under the auspices of such regulation are now possibly open to cloud deployments. In the majority of cases, location at run time is required. Due to the former key issue, i.e. "Multiple VNFCI policy", location attested only at the instantiation may not fulfil all requirements related to this clause. However, location at instantiation is probably less costly in terms of computer processing hosted on an NFV system than would be required to support runtime location attestation.

6 Solutions

6.1 Solution 1 for timestamp - time Synchronization and distribution (White Rabbit Network)

6.1.1 General

The White Rabbit (WR) Project is an open-source solution from CERN (see CERN open-source project and its repository [i.50]). This technology provides a versatile solution for control and data acquisition systems, mainly for data centers.

The White Rabbit Network is based on existing IEEE standards while extending these standards in a backward-compatible way. Technically, it is a Bridged Local Area Network with VLANs (IEEE 802.1Q, see [i.64]) that uses Ethernet (IEEE 802.3, see [i.66]) to interconnect switches and nodes, and the Precision Time Protocol (PTP, IEEE 1588 [i.19]) to synchronize them. The main features of the White Rabbit Network are:

- Sub-nanosecond accuracy and picoseconds precision of synchronization.
- Connecting thousands of nodes.
- Typical distances of 10 km between network elements.
- Gigabit rate of data transfer.
- Fully open hardware, firmware and software.

The high accuracy of synchronization in White Rabbit is achieved by extending the Precision Time Protocol of IEEE 1588 [i.19]. White Rabbit seems to become the High Accuracy Delay Request-Response Default PTP Profile, even for long distance up to 100 km on optical fibres.

6.1.2 Architecture description

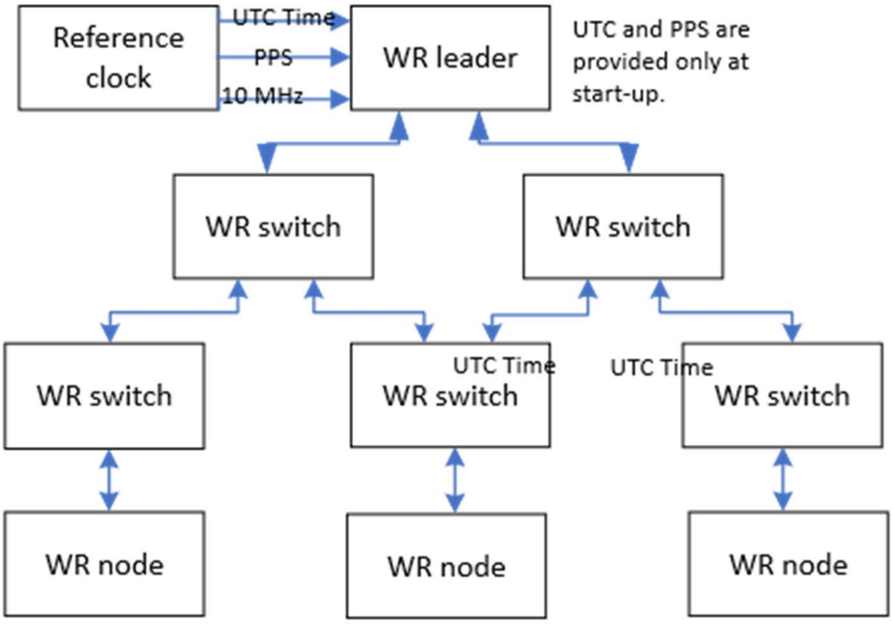

Figure 6.1.2-1: White Rabbit network architecture

Figure 6.1.2-1 shows the layout of a typical WR network that is composed of WR nodes and WR switches, interconnected by fibre links. Data-wise it is a standard Ethernet switched network, i.e. there is no hierarchy: any node can talk to any other node in the network. Regarding time synchronization, there is a hierarchy, that goes from the top, namely from the WR leader, down to other WR switches and consequently nodes. The WR switch, key element of any WR network, is similar to a standard Ethernet switch, but it is also able to precisely distribute the WR leader clock over the network thanks to a technique called precise phase measurement [i.54].

The uppermost switch in the hierarchy, also called grand--leader, receives the absolute clock from an NTP source (e.g. the NTP daemon running on a computer), together with the Pulse-Per-Second (PPS) and the 10 MHz from an external reference (e.g. a GPS receiver). At start-up, the WR switch uses the NTP and the PPS to determine the absolute UTC time. Then, it calculates the time using only the 10 MHz signal. After the switch has completed the rebooting routine, i.e. few minutes after powering it on, the NTP service and the PPS are not needed anymore and the grand-leader switch could be potentially disconnected from these sources.

The accuracy of the round-trip time measurement is mostly determined by the accuracy of the 10 MHz source. The grand-leader switch then distributes the time information to further WR nodes via intermediate WR switches.

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].

6.1.3 Function description

The accuracy of the PTP synchronization is implementation-dependent. Such standard is foreseen for sub-nanosecond accuracies. However, typical PTP implementations do not achieve such level of accuracy. WR let achieve sub-nanosecond accuracy by basing its time distribution on PTP and addressing the following issues related to basic PTP's implementation:

- Limited precision and resolution of timestamps.
- Unknown link asymmetry. The asymmetry is not detectable by PTP. Some of the sources of the physical layer asymmetry can be eliminated by proper network configuration in excluding, for example, non-PTP bridges from the network. Others, in particular the inaccuracy caused by physical medium asymmetry or connection length between PHY and timestamping hardware, need to be obtained through a priori-measurement.

- The quality of the PTP syntonization depending on the exchange rate of PTP messages. The higher the quality of the clock that needs to be recovered, the higher the bandwidth needed for PTP-related traffic.

WR addresses these limitations to achieve sub-nanosecond accuracy of synchronization. It uses SyncE (see note 1) to distribute a common notion of frequency in the entire network over the physical medium. Results of precise phase detection measurements are used during normal PTP operation and during the calibration phase. The improved performance of the synchronization is accomplished without increasing PTP message traffic since PTP is only governing the synchronization, while the syntonization is done by SyncE.

WR is an extension to PTP, called WR PTP. It defines its own PTP profile and describes all the WR-specific mechanisms.

The solution enables network-wide sub-nanosecond accuracy of synchronization.

NOTE 1: Synchronous Ethernet (SyncE), a traditional Ethernet plus an embedded synchronization system similar to that already used in Synchronous Digital Hierarchy (SDH)/Synchronous Optical Network (SONET). SyncE has been standardized by the International Telecommunication Union (ITU) in cooperation with IEEE, in Recommendation ITU-T G.8262 [i.7]. It provides mechanisms to transfer frequency over the Ethernet physical layer, which can then be made traceable to an external source such as a network clock. SyncE. Typical PTP implementations use free-running oscillators in each node which causes time drifts between leader and followers. This issue is solved by SyncE that enables network nodes to beat at exactly the same rate.

NOTE 2: 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].

6.1.4 Solution evaluation

The default version of WR allows plug-and-play links up to 10 km with sub-nanosecond accuracy. Because of this, it is being adopted by many time-sensitive centric applications, e.g. financial applications for which stringent clock synchronization is required. Recently, the WR protocol was adopted by Deutsche Börse stock exchange in Frankfurt to synchronize all their network. Several companies in the financial sector also implemented or in process of implementing WR to synchronize their network.

WR allow users to build highly deterministic data center networks with layer 2 prioritization mechanism as defined by IEEE 802.1Q [i.64] for sync traffic. The combination of deterministic latencies and a common notion of time to within sub-nanosecond allows WR to be a suitable technology to solve many problems in distributed real-time controls and data acquisition.

Such distribution uses specific hardware components, to enable software based NFV systems get highly accurate and distributed time information.

6.2 Solution 2 for timestamp - time synchronization and distribution (IEEE 1588)

6.2.1 General

In virtualised systems time synchronization and timestamp generation needs to be based on approaches such as Precision Time Protocol IEEE 1588 [i.19] in order to achieve high accuracy. NTP typically shows around 30x lower accuracy than PTP protocol for 50 % load of Linux based COTS (source ATIS WTSC of 2019). Such protocol may be needed to provide sub-microsecond accuracy and location information in the Ethernet frame with lower cost than traditional methods to attach Global Navigation Satellite System (GNSS) receivers at every station and dedicated media to distribute the signal to every server with 100 ns accuracy.

IEEE 1588 [i.19] implements a management channel between the grand leader and each follower [i.9]. That channel could be used to transfer the location information and time synchronization from the grand leader to the followers.

Following detailed recommendations are made on implementation of time synchronization and timestamp generation in NFV or any virtual environment, based on IEEE 1588 [i.19]:

- A data center is defined as the location where Network Function Virtualisation Infrastructure (NFVI) nodes would be installed.
- The data center provider may have to deploy IEEE 1588 PTP option D (see IEEE 1588 [i.19] to provide timing and synchronization inside the data center.
- A set of redundant PTP grand leader clock references may have to be implemented in every data center in order to provide time and location information to the servers in the data center.
- The PTP grand leader clock references may have to provide a reference time signal that is traceable to a recognized time standard (e.g. Universal Time Coordinated (UTC) in order to provide globally consistent real-time locstamps and timestamps.

NOTE 1: UTC can be retrieved from a UTC time laboratory registered at Bureau International des Poids et Mesures (BIPM) (e.g. a national UTC time lab) or, typically from at least one global navigation satellite system (GNSS).

The PTP grand leaders may have to be equipped with anti-spamming and anti-spoofing mechanisms, such as the usage of different GNSS source, or the authentication of satellite signals.

When a PTP grand leader loses all its input references (e.g. unavailability of GPS^{TM}, Galileo^{TM}, Baidou^{TM}, etc.), it has to maintain a holdover state of at least many days by relying on another external input frequency reference traceable to a Primary Reference Clock (PRC). A resilient optional solution, may be based on redundant and heterogeneous clock sources, with independent failure modes such a CSP/local atomic clock, or national time terrestrial signals based on independent atomic clocks.

Where accurate timing is required (e.g. billing application, gaming applications, security services, etc.) the NFV servers may have to be equipped with NICs that support time distribution using IEEE 1588 [i.19] PTP. Time at the hardware has to be conveyed and to be synchronized to VNF or virtualised components through a NIC. The Follower will be implemented on the NIC card and will maintain the time for different VNFs on the server.

NOTE 2: The support of hardware timestamping will depend upon the application requirements.

The hardware needs to maintain an accurate clock within the NIC for time stamping of external events and also to be read as a time source by VNFs, either directly or through a function abstracted in the hypervisor and with a mechanism for monitoring live system for Generic Event Detection and Timestamping Process with PTP and accuracy measuring.

ITU SG15 have addressed a number of potential security issues with IEEE 1588 [i.19] PTP which occur due to constraints between network domains and COTS servers. It is also more expensive where Ethernet switches have to be PTP aware. The new ITU profile is backward compatible system with nanosecond accuracy.

There are already IEEE amendments on its published version:

- To have more secured options specially on the exchanged PTP TLV (type, length, value) in its annex K of IEEE 1588 [i.19], to develop selection and operation of specific key management technologies like Network Time Security (NTS);
- To add of PTP mapping for transport over Optical Transport Network (OTN);

NOTE 3: 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].

6.2.2 IEEE 1588 related to Mobile Wireless (Cloud RAN)

6.2.2.1 Architecture

Among the telecommunication use cases of NFV is the virtualisation of the 3GPP Evolved Packet Core (EPC) and Radio Access Network (RAN) functions. These 3GPP functions may be disaggregated and recomposed in various combinations as Virtual Machines instances. The Central Offices (COs) are being re-architected as data centers in order to accommodates the IT virtualisation technology. Synchronization is one of the critical real-time functions of Wireless Mobile Networks that share the network infrastructure with the virtualised functions in the CO/Data Center. This real-time function is critical to the coordination of the Wireless Mobile Network infrastructure. The IEEE 1588 [i.19] Precision Time Protocol (PTP) standard has been proposed as the main method for synchronizing the wireless base stations over packet-based networks from the COs/data centers.

Frequency synchronization is used in Mobile Wireless to comply with regulatory requirements but also to manage radio interferences between adjacent cells and among sub-carriers and make easier the handover between cells. The carrier frequency should meet an accuracy of ±50 ppb for wide area base stations, and accuracy of ±100 ppb for Pico base stations (ETSI TS 136 104 [i.27]).

Phase synchronization is required in TDD systems to support phase aligned base stations uplink and downlink transmission since they use the same frequency band. In LTE TDD systems, the base stations are required to be accurate within 3 µs for cells of less than 3 km radius and 10 µsec for cells of more than 10 km radius. (ETSI TS 136 133 [i.16]).

One of the core capabilities that was defined in 3GPP LTE Advanced Release 10 onwards is Carrier Aggregation (CA) in order to achieve peak data rates and improve coverage. CA allows multiple uplink or downlink LTE component carriers in contiguous or non-contiguous frequency bands to be bundled together. In Release 10, the uplink CA deployment is limited to intra-band Carrier Aggregation. Release 11 CA extended it to inter-band Carrier Aggregation where the component carriers are located in different frequency bands.

ETSI TS 138 104 [i.71] specifications require in clause 6.5.3 that "*For intra-band contiguous carrier aggregation, with or without MIMO or TX diversity, the Time Alignment Error (TAE) shall not exceed 130 ns. - For intra-band non-contiguous carrier aggregation, with or without MIMO or TX diversity, TAE shall not exceed 260 ns - For inter-band carrier aggregation, with or without MIMO or TX diversity, TAE shall not exceed 260 ns. - For MIMO or TX diversity transmissions, at each carrier frequency, TAE shall not exceed 65 ns (or 1/4 Tc)*". MIMO is a key antenna technique that was defined to improve spectral efficiency and throughput using spatial multiplexing and pre-coding techniques.

LTE Advanced introduced additional radio coordination features that require phase alignment between radio sub-frames (e.g. inter-cell interface coordination inter-cell interference coordination eICIC, Coordinated Multi-Point CoMP). The phase requirements vary from ±1,5 µsec to ±5 µsec depending on the features and vendors.

eICIC is an interference coordination feature that focuses on small cell deployment specifically. It increases at cell edges the number of users by distributing the traffic load between the small cell layer and the macro capacity. It avoids interference overlap between macro and small cells by time-aligning them. CoMP improves performance at cell edges by mitigating inter-cell interference. It allows in those locations signals to be transmitted from and received at multiple cells.

Table 6.2.2.1-1: LTE and LTE-A requirements set by ETSI TS 136 101 [i.72] and ETSI TS 136 104 [i.27]

Application	Time/phase requirement	Reason to comply	Impact of non-compliance
LTE (FDD)	N/A	Call initiation	Call interference and dropped calls
LTE (TDD)	≠1,5 to ≠5 µs	Time Slot alignment	Packet Loss/collision and Spectral inefficiency
LTE-A eICIC	≠1,5 to ≠5 µs	Interference coordination	Spectral inefficiency and service
LTE-A (TDD or FDD) CoMP/MU-MIMO	≠500 ns	Coordination of signals to/from multiple base stations	Poor signal quality at the edge of cells
LTE-A MBSFN (TDD or FDD)	≠500 ns	Proposer alignment of video signal encoding from multiple e-NBs	Video broadcast interruption

Table 6.2.2.1-2: More stringent requirement set by 3GPP for future networks

Typical applications (For information)	Time error requirements	Specification
Intra-band non-contiguous carrier aggregation with or without MIMO or TX diversity, and inter-band carrier aggregation with or without MIMO or TX diversity	≠260 ns	ETSI TS 136 104 [i.27] V13.1.0 clause 6.5.3.1
Intra-band contiguous carrier aggregation, with or without MIMO or TX diversity	≠260 ns	ETSI TS 136 104 [i.27] V13.1.0 clause 6.5.3.1
MIMO or TX diversity transmissions, at each carrier frequency	≠65 ns	ETSI TS 136 104 [i.27] V13.1.0 clause 6.5.3.1

6.2.2.2 Function description

Centralized/Cloud RAN (CRAN) takes a different architectural approach in RAN (Radio Access Network) design by centralizing and aggregating the baseband processing of the radio nodes.

The 5G CRAN architecture consists of Remote Radio Head (RRH) units co-located with antennas on towers or poles, connected to a centrally controlled and virtualised pool of Baseband Units (BBUs) over a fronthaul network. The baseband processing is shared by several remote radio sites. This architecture enables the implementation of advanced coordination techniques such as CoMP.

5G CRAN implementations are based on COTS based hardware, that usually do not have a local source of Timing & Synchronization (e.g. GPS) although may include PTP Hardware Clock (PHC) which requires timing correction regularly and use a network-based Timing Source e.g. IEEE 1588 [i.19] PTP. In majority of cases, operating systems of COTS have PTP Implementation divided between kernel and user space. The operating system will get time from PTP Hardware Clock (PHC) through NIC that provided layer 2 connectivity with the grand leader clock (the majority of cases is based from time signal of a GNSS and as back up source an atomic clock).

The traditional fronthaul network is implemented with the Common Public Radio Interface (CPRI) over optical fiber links. CPRI is a full duplex synchronous protocol that defines three different logical connections between the Radio Equipment Controller REC and the Radio equipment RE: user plane data, control and management plane, and timing synchronization. CPRI requires tight synchronization accuracy between REC and RE. The clock received at the RE needs to be traceable to the main REC clock with an accuracy of 8.138 ns. In this traditional CPRI deployment, the RRHs are in charge of all radio functions and the BBUs are responsible for all the higher layer functionalities.

In order to meet the bandwidth requirements of LTE-A and the high fiber consumption imposed by CPRI, a packet-based transport network is being introduced to provide statistical multiplexing and a cost-effective technology. To reduce further the bandwidth requirements, several LTE functional splits are being investigated in order to reduce level of centralization. These functional splits present different synchronization requirements.

This use case corresponds to the case where the CO/data center provider owns the Primary Reference Time Clock (PRTC) and the source clock is distributed from Primary Reference Time Clock (PRTC) inside the CO/data center. The PRTC is providing a timing service to the BBU pool inside the CO/data center.

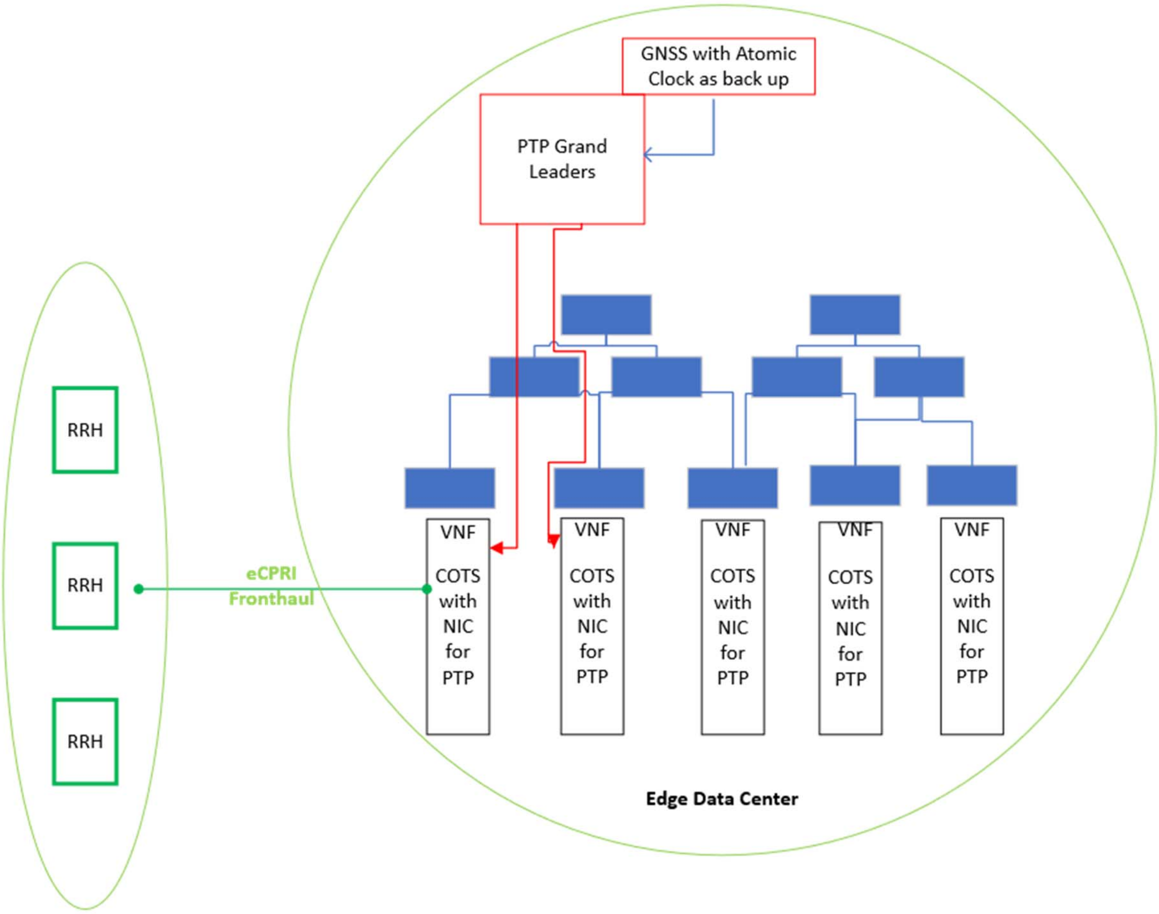

Figure 6.2.2.2-1: C-RAN architecture

In the case of Linux operating system that do support C-RAN/Open RAN, the kernel includes support for PTP clocks provided by network drivers (since hardware PTP relies on physical NIC to provide hardware clock). The actual implementation of the protocol is known as Linuxptp, a PTPv2 or PTPv3 implementation according to the version of IEEE 1588 [i.19] of such standard for Linux. Clock synchronization, described above may use Linuxptp packages that may include ptp4l, phc2sys and pmc programs.

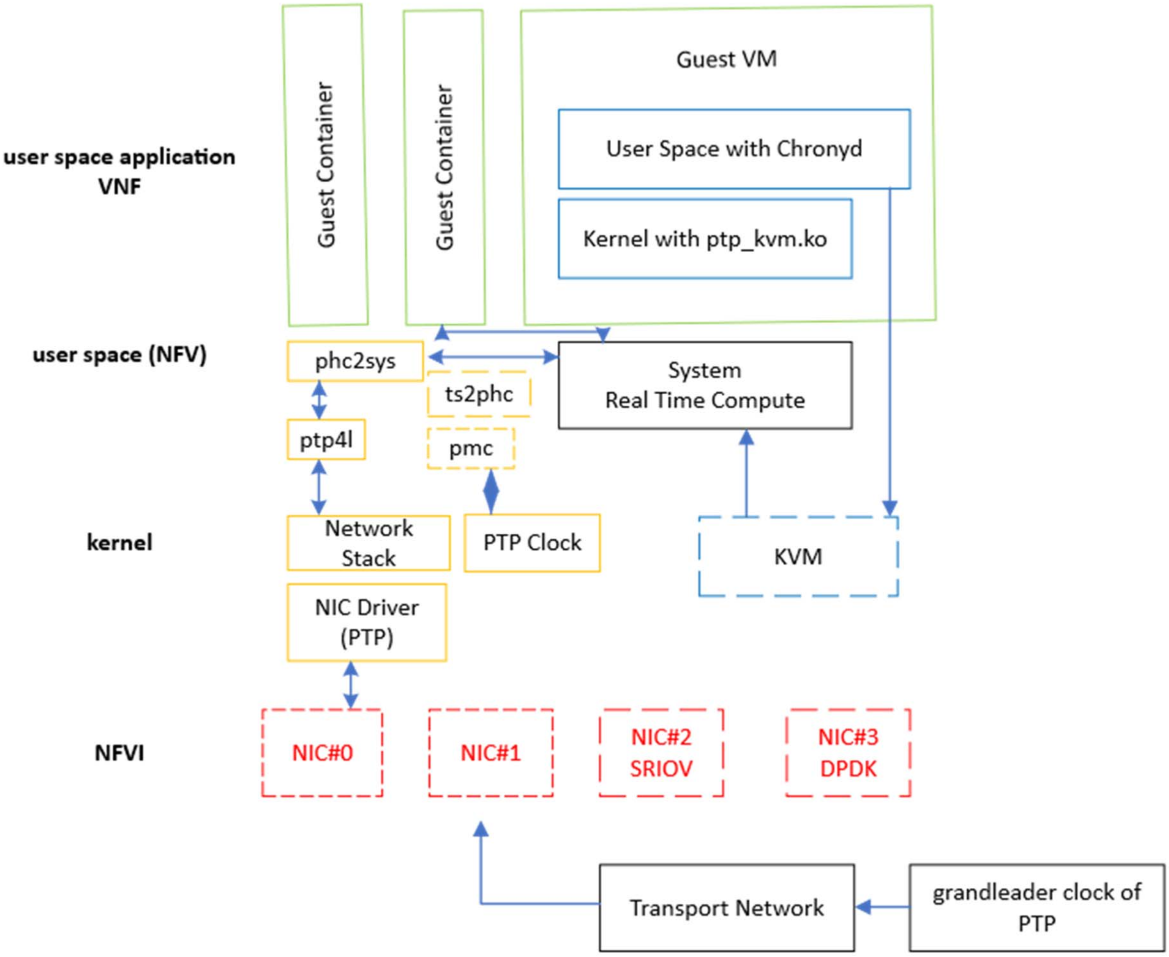

Figure 6.2.2.2-2: Example of end-to-end flow of PTP from the Network Interface Card (NIC) to the application in User Space (Source: Techplayon [i.68])

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].

6.2.2.3 Solution evaluation

C-RAN and Open RAN, offer potential efficiency and operating costs improvements compared to legacy systems. The use of a single centralized primary base station, with baseband processing and control of radio resources enables improved time or frequency synchronization especially in small cell deployments. As more frequencies are transmitted in the same geographical space, coordinated management of overlapping small cells and macro cells becomes essential.

Time is distributed through PTP. Such time source is hardware based but distributed and accessible through virtual NIC in case of NFV VM or container. The local NIC port for PTP can be deployed with SR-IOV, DPDK technologies.

The domain isolation and security of such virtualised systems deserve to be studied carefully if edge computing services of third parties or non-trusted application functions are set up in the same COTS environment, as the attack surface is larger due to multiplicity of the interfaces and components. Separated domains may be recommended to reduce some risks in this multi-tenant NFV case.

6.2.3 IEEE 1588 related to Cable TV

6.2.3.1 Architecture

The DOCSIS architecture is used by Cable operators to deliver voice, IP, linear Broadcast Video, Video on Demand, services to the end customers over the Hybrid Fiber/Coax (HFC) cable network.

The Cable Modem Termination System (CMTS) is defined by the Cable Labs DOCSIS specifications. It forwards (at layer 2 or layer 3) data packets between a Wide Area Network via its network-side interfaces and customer premise equipment via its DOCSIS RF interface ports. The main specifications are:

- Downstream Radio Frequency Interface Specification, CM-SP-DRFII14-131120, November 20, 2013, Cable Television Laboratories, Inc.,[i.23];
- DOCSIS 3.1, Physical Layer Specification, CM-SP-PHYv3.1-I08- 151210, December 10, 2015, Cable Television Laboratories, Inc.,[i.24];
- DOCSIS 3.0, Physical Layer Specification, CM-SP-PHYv3.0-I12- 150305, March 5, 2015, Cable Television Laboratories, Inc.,[i.25].

The CMTS, typically located in the cable operator headend or hub site, provides high speed data services (e.g. internet, VoIP). The CMTS consists of the following logical functions: DOCSIS PHY layer (upstream receiver and downstream transmitter), DOCSIS MAC layer (upstream MAC and scheduler, downstream MAC processing, DOCSIS QoS, security), RF output block, L2 and L3 forwarding blocks, IP processing (DHCP), management (SNMP agent/CLI).

The video Edge QAM, also located in the same network element, is responsible for transporting video on demand and switched digital video services. It receives MPEG streams over IP unicast or multicast packets and generates transport stream on one or more RF outputs for transmission over the HFC cable plant.

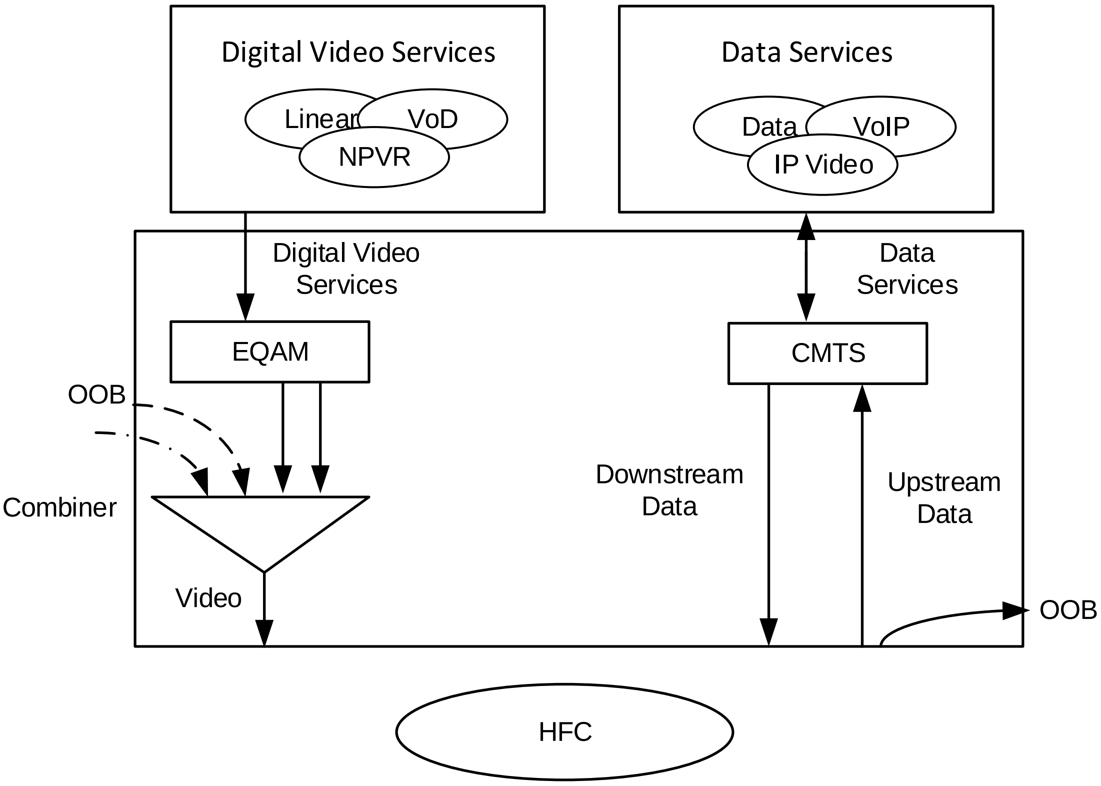

Figure 6.2.3.1-1: CMTS

The Modular CMTS (M-CMTS) architecture was introduced to convert the EQAM into a universal QAM by reusing the EQAM to modulate the bits on to the wire for both downstream DOCSIS data as well as MPEG video. The CMTS downstream PHY layer has therefore been moved to the separate network element device: the EQAM device, also called Physical Downstream component - PHY). The upstream receiver remained at the so-called M-CMTS core component, also referred as DOCSIS MAC component. The M-CMTS core is in charge of the upstream and network-side control plane and data plane processing for the upstream RF interfaces and the network-side interfaces.

The DOCSIS MAC and PHY being in separate devices in the M-CMTS architecture, the DOCSIS Timing Interface (DTI) server has been introduced to keep them tightly synchronized in time and frequency. The DTI protocol, which is a based on a layer 2 ping-pong layer 2, provides an accuracy of less than 5 ns and a frequency stability of less than 1 ns.

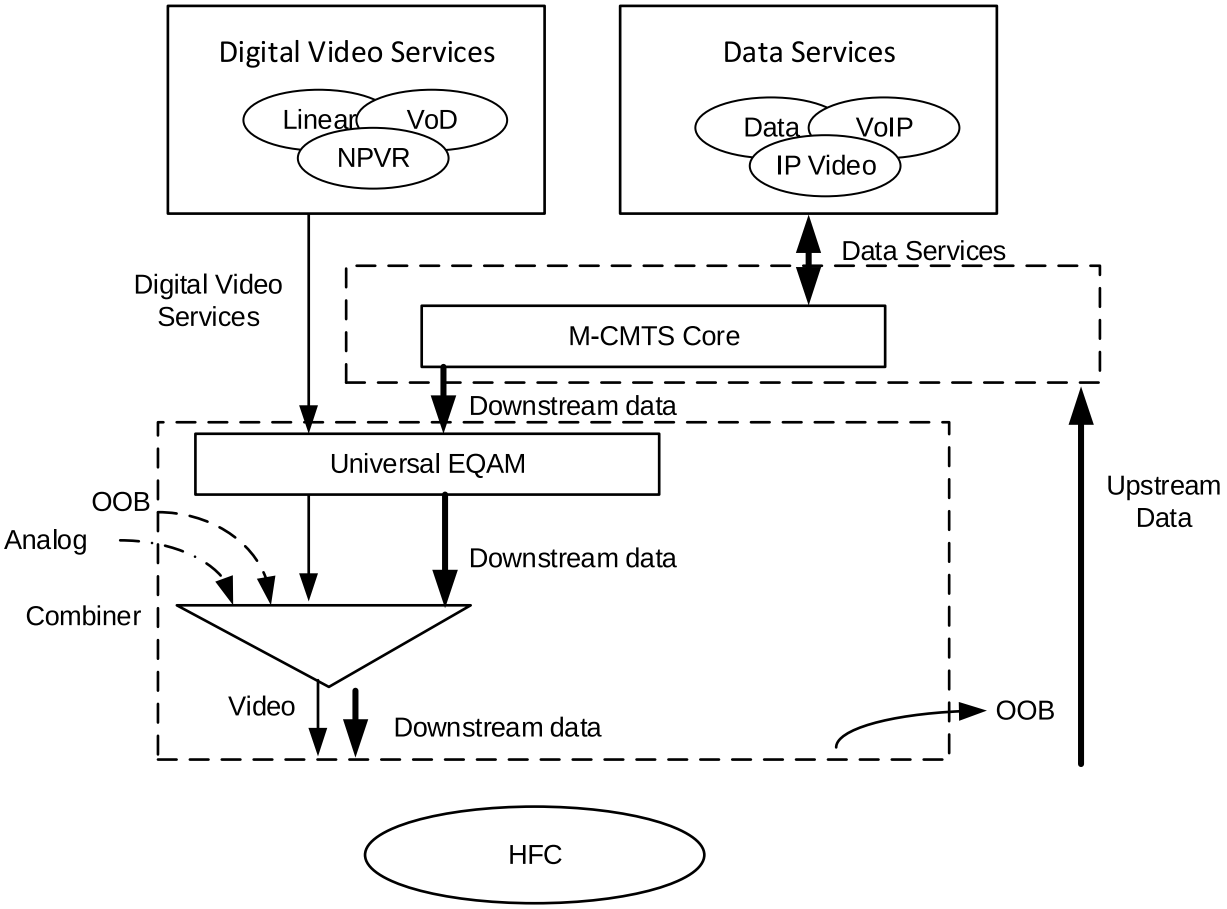

Figure 6.2.3.1-2: Modular CMTS

A recent evolution of the cable architecture, called Cable Converged Access Platform (CCAP), integrates in a single platform the CMTS, Switching, Routing, and QAM functions in such a way that data, video, voice functions are processed over IP before conversion to RF or Optical signals. The CCAP offers video services in the downstream and DOCSIS services in the downstream and upstream directions.

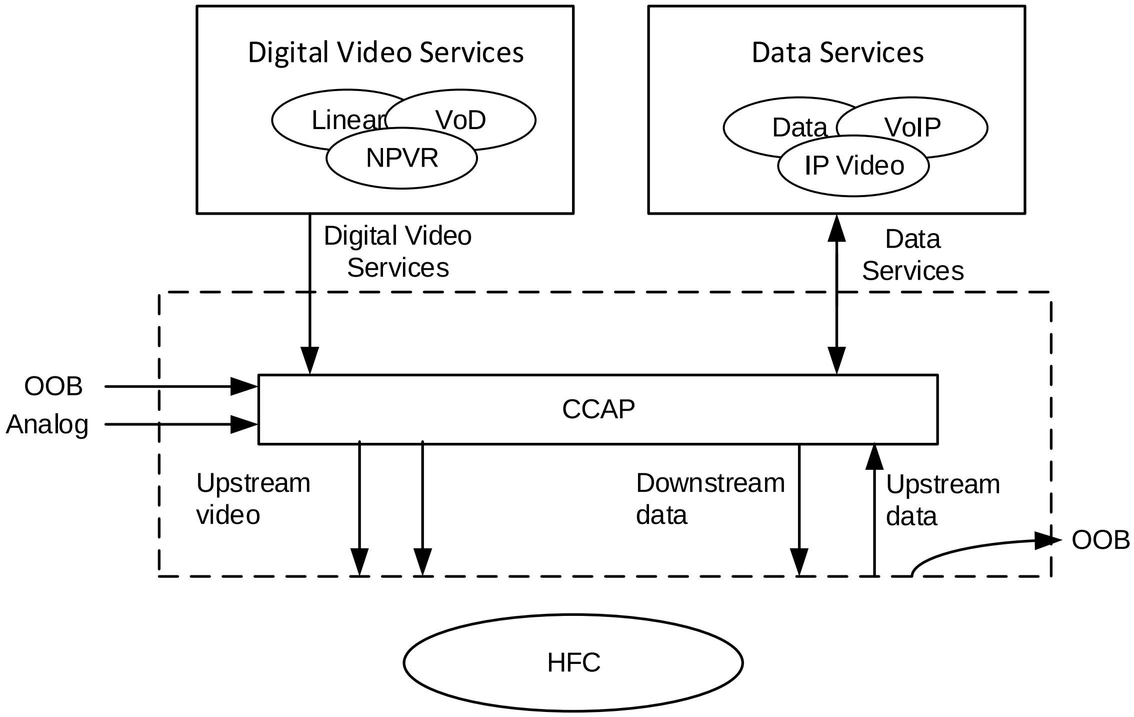

Figure 6.2.3.1-3: Integrated CCAP

6.2.3.2 Function description

The latest evolution of CCAP consists of distributing some functions down in a remote location (e.g. fiber node). There are two popular approaches to a distributed architecture, all conforming to Cable Labs specifications. In the first CCAP distribution architecture, called remote PHY, the CMTS is split between the MAC and the PHY and the latter is moved to a remote node while the DOCSIS MAC stays at the hub site. The second distribution architecture, called remote MAC-PHY, move the entire CCAP to the remote node.

The remote PHY architecture allows separating the hardware-bound physical layer and RF components from the virtualised software functionality. A pool of servers centralized in a data center can be used to serve distributed Remote PHY nodes providing elasticity, efficiencies and improved network flexibility.

The Remote DOCSIS Timing Interface (R-DTI) has been defined as the timing protocol for the timing/frequency synchronization between CCAP core and node in R-PHY architecture. R-DTI is based on IEEE 1588 [i.19] protocol with a specific profile for DOCSIS R-PHY. The PTP grand leader is typically deployed in the CCAP location while the follower is in the R-PHY devices.

The R-PHY calls for the following timing and frequency requirements:

- Phase alignment ≤ 1 ms;
- Frequency accuracy ≤ ±5 ppm;
- Frequency drift ≤ 10 ppb/s;
- Phase jitter < 500 ns peak-to-peak.

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

The usage of Linux based COTS may require as in C-RAN case specific user space application and kernel with PTP NIC driver in order to manage the end-to-end flow of PTP, to distribute accurate time through the network and vCCAP services.

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].

6.2.3.3 Solution evaluation

Virtualisation of CCAP, specially based on NFV, brings advantages to cable and MS operators especially in enabling extra services such as those associated with edge mobile computing platforms, as it may provide a common platform for independent scaling of control and data plane functions.

With modular components supporting Wi-Fi wireless access gateway, LTE, 5G and other functions, such NFV based solution, enables dynamic use of COTS resources across multiple virtualised applications. Time is distributed through PTP. Such time sources are based on hardware, but distributed and accessible through virtual NIC in case of NFV VM or container. In cases where a high level of accuracy is required, the source may be GNSS with Atomic clock as a secondary source.

However, security especially of network management and time/phase synchronization may require studies in the implementation, especially to get sufficient time accuracy and strict isolation between different domains, especially those with interfaces to third parties, or non-trusted hosted application functions. Multi-tenant NFV systems with sensitive application functions based on vCCAP further increases attack surface.

6.3 Solution 3 for timestamp - time synchronization and distribution (based on trusted GNSS/ LEOs)

6.3.1 Architecture description

GNSS satellites include three or four atomic clocks that are monitored and controlled so that they are highly synchronized and traceable to national and international standards (i.e. UTC).

For time synchronization, the GNSS signal is received, processed by a local leader clock, time server or primary reference, and passed on to downstream devices, systems or networks so that their local clocks are also synchronized to UTC. Typical accuracies range from better than 1 microsecond to a few milliseconds depending on the synchronization protocol.

It is the process of synchronization to GNSS that can provide atomic clock accuracy without the need for a local atomic clock. Still, local atomic clocks are sometimes desired as a long-term back-up solution in the event of a GNSS signal loss such as a weather-related outage, signal interference or other scenarios such jamming or spoofing.

In any event, GNSS clock synchronization eliminates the need for manual clock setting (an error-prone process) to establish traceability to national and international standards. This allows various events to be correlated even if they are time-stamped by different clocks. The benefits are numerous and include legally traceable/validated timestamps, regulatory compliance, secure networking, and operational efficiency.

Most time resources are delivered through a GNSS satellite constellation which is generally in Medium Earth Orbit (MEO), such as GPS (United States), Galileo (European Union), GLONASS (Russia), and BeiDou (China).

GNSS system uses various timescale and parameters for processing time [i.56]. Figure 6.3.1-1 shows timescale and parameters in GPS system and how the time information is processed in the GPS signal. This is applicable to GNSS system as most GNSS system has similar mechanism for time processing.

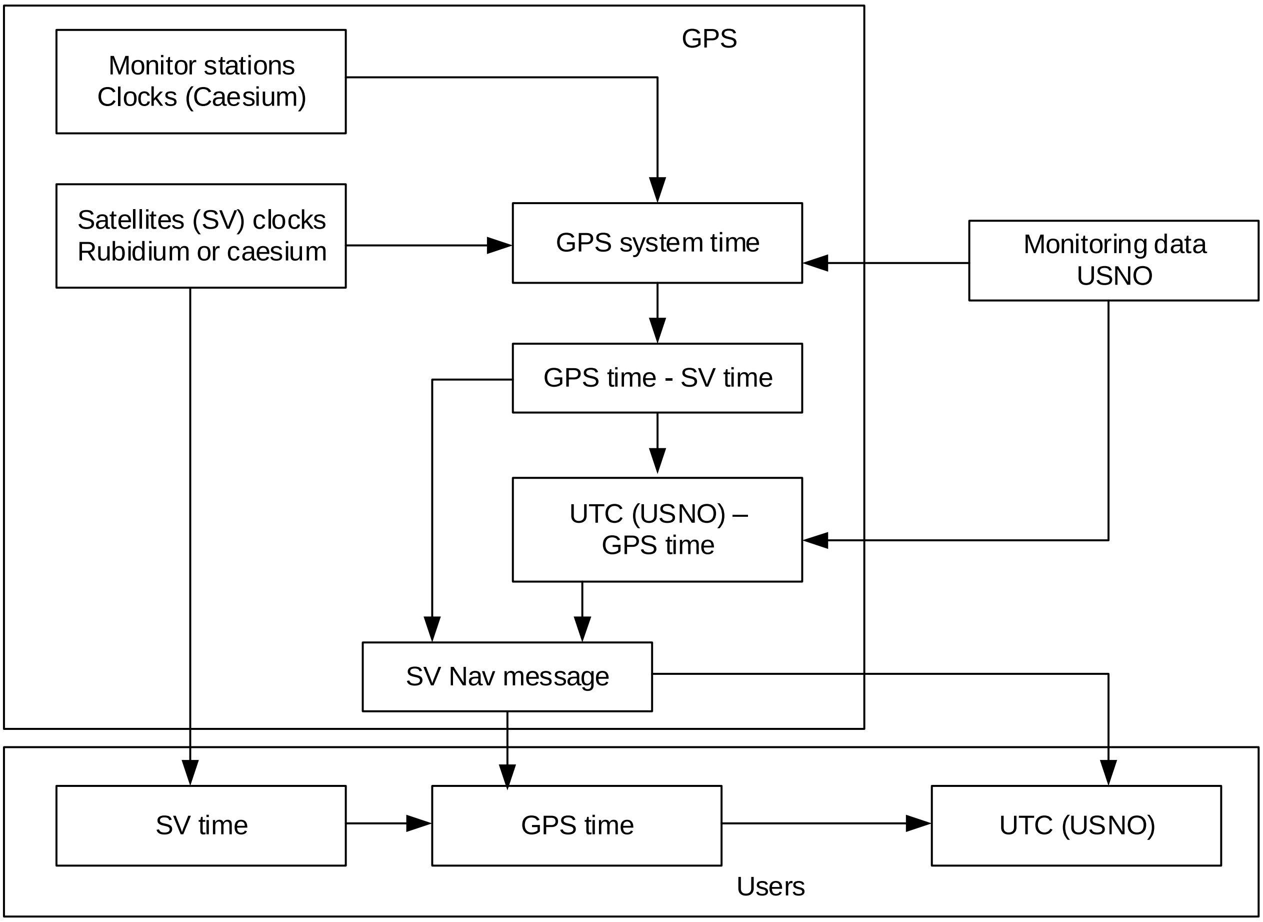

Figure 6.3.1-1: Timescales and parameters in GPS system

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].

6.3.2 Function description

As an example of GNSS, the GPS system uses its own timescale, named "GPS system timescale", abbreviated as "GPS time". This GPS time is established by the control segment and is used as the primary time reference for all GPS operations. The GPS time is referenced to a UTC zero time-point maintained by the U.S. Naval Observatory (USNO).

USNO has an ensemble of atomic clocks, which are used to derive a timescale called UTC (USNO). The clocks in the ensemble contribute to International Atomic Time (TAI) and Coordinated Universal Time (UTC). UTC (USNO) and UTC (NIST) are kept in very close agreement, typically to within 20 nanoseconds, and both can be considered official sources for time in the United States.

GPS time is linked by measurement to UTC (USNO). GPS time and UTC (USNO) were aligned at the beginning of the GPS timescale epoch, which was at 00:00 UTC Sunday, 6 January, 1980.

Each satellite maintains its internal timescale, named Space Vehicle (SV) time which receives the updated models of the differences SV time versus GPS time, and GPS time versus UTC (USNO) from the ground monitoring station as ground segment by uplink channel.

This modelling information is present as various parameters in GPS navigation messages embedded in each emitted GPS electromagnetic signal towards the Earth.

It is possible for a GPS receiver to process all these parameters from all received satellite signals to rebuild a local realization of GPS or UTC (USNO) timescale and produce a physical timing signal on a PPS output port.

All GNSS receivers obtain GNSS time or UTC timescale by receiving space signals into a GNSS receiver. However, GNSS signals may encounter some errors before it is received and processed by the receiver. These errors on GPS/GNSS signal transmission needs to be corrected in order to obtain high-precision satellite clock time. GNSS signals are encountering different errors as they enter Earth's atmosphere and processed by the receiver. These errors may be broadly classified into three categories:

- satellite-related errors;
- signal propagation-related errors;
- receiver-related errors.

According to statistical calculations, the accuracy of one-way timing can be as much as 20 ns after correcting for such errors.

GNSS are susceptible to vulnerabilities and threats. Unforeseen outages or intentional attacks can have a devastating impact on the operations of critical infrastructure assets that rely on a steady stream of precise timing or location information. Measures that can be taken to enhance resiliency can be found in the DHS (US Department of Homeland Security) report entitled "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure" presented in annex B of the present document.

Galileo provides for civilian usages, more resilient and secured signals with its Galileo High Accuracy Service (HAS). Galileo Commercial Service (CS) signal's encryption functionalities, with the data received containing authentication and high accuracy information previously generated outside the Galileo system. This is an essential feature to ensuring Galileo's high accuracy and authentication services.

Alternative systems that are capable of backing up and augmenting GNSS are for example Low Earth Orbit (LEO).

The private company Iridium, which operates a fleet of approximately 60 LEO satellites for global communication, also provides a commercial timing and location service called STL (Satellite Time and Location). STL is based on a proprietary non-standards-based solution designed by Satelles. Due to the fact that Iridium's LEO satellites are 25 times closer to the receiver than traditional GNSS satellites, the STL signals are 1 000 times (30 dB) stronger than today's civil GNSS L1 signals. The encryption of the STL signals can be considered as an additional benefit, as it makes the system spoofing resistant. STL utilizes modern cryptographic techniques to deliver a secure, trusted time and location capability that is effectively impervious to manipulation.

STL leverages Iridium's satellite infrastructure to broadcast signals specifically designed to enable precision time and frequency measurements. These measurements can be used by a receiver for a variety of purposes, including:

- computing position fixes directly;
- independent of GNSS;
- transferring sub-microsecond timing to a user or device;
- aiding GNSS acquisition;
- augmenting GNSS measurements when not enough GNSS satellites are in view.

STL signal bursts are received by a receiver about once every second. Precise time can be calculated by processing a single burst, typically in under two seconds.

6.3.3 Solution evaluation

Backup capabilities solutions such as STL and Galileo "HAS" are an essential safeguard for telecommunications networks, electrical power grids, transportation systems, and other types of infrastructure that rely on accurate time to operate, even if GNSS is unavailable or degraded. STL and Galileo "HAS" deliver alternative time synchronization source to basic GNSS, at the levels of stability, reliability, and trust required by critical infrastructure applications. The views of Satelles and Galileo "HAS" are mainly aligned with the findings of the Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS) that the DHS issued.

In settings where both basic GNSS and STL time and location fixes are possible, STL and Galileo "HAS" complement basic GNSS with additional PNT information.

Any NFV based applications, which require highly accurate time, may use such time source, based on NIC to specific hardware. As each COTS may need such hardware, the cost of such solution may be important.

In case of resiliency requirements, such GNSS/STL source may be backed up by an atomic clock as a secondary source, but it will add extra cost.

Specific kernel and or user space applications will be needed to enable access to accurate and secured time sources through virtual NIC.

To avoid that each computing node may have a specific NIC to get access to the source of time, time distribution and synchronization using PTP or White Rabbit, may be studied as complementary solution to reduce such cost. GNSS/STL secured wire-based distribution from its antennas to each COTS, may complement such solution to reduce the cost.

6.4 Solution 4 for timestamp Datacenter Time Protocol (DTP)

6.4.0 introduction

A data center, needs to keep accurate track of time across a large number of servers and network components. Precise time synchronization has become a critical due to stringent requirements of time critical applications such as real-time big data analytics, high-performance computing, and financial trading. Clock synchronization protocols in data center networks such as NTP and PTP are fundamentally limited by the characteristics of packet-switched networks. In particular, network jitter, packet buffering and scheduling in switches, and network stack overheads add non-deterministic variances to the round-trip time, which need to be accurately measured to synchronize clocks precisely. The Datacenter Time Protocol (DTP) is a clock synchronization protocol that does not use packets at all, but is able to achieve nanosecond precision [i.55]. In essence, the DTP uses the physical layer of network devices to implement a decentralized clock synchronization protocol. By doing so, the DTP eliminates most non-deterministic elements in clock synchronization protocols and has virtually zero protocol overhead since it does not add load at layer-2 or higher at all.

6.4.1 Architecture description

DTP exploits the fact that two peers are already synchronized in the PHY in order to transmit and receive bitstreams reliably and robustly. In particular, the receive path (RX) of a peer physical layer recovers the clock (CLK) from the physical medium signal generated by the transmit path (TX) of the sending peer's PHY standard as shown in Figure 6.4.1-1. As a result, although there are two physical clocks in two network devices, they are virtually in the same circuit.

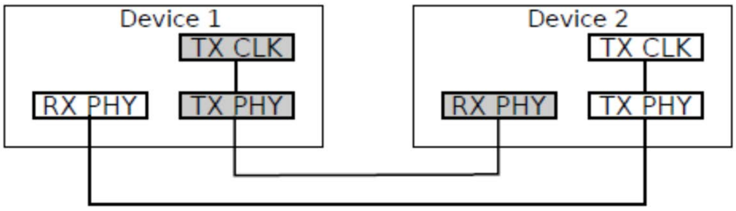

Figure 6.4.1-1: Peer synchronization at PHY level for DTP-enabled device (Source [i.55])

The DTP proposes a sublayer at the 10GbE PHY specifically to IEEE 802.3ae [i.65] 10 Gigabit/S Ethernet. The following figure shows DTP proposal for adding the sublayer to 10GbE PHY layer.

According to the IEEE 802.3ae [i.65], the physical layer (PHY) of 10 GbE consists of three sublayers (Figure 6.4.1-1): The Physical Coding Sublayer (PCS), the Physical Medium Attachment (PMA), and the Physical Medium Dependent (PMD).

The PMD is responsible for transmitting the outgoing symbol stream over the physical medium and receiving the incoming symbol stream from the medium. The PMA is responsible for clock recovery and (de-)serializing the bitstream. The PCS performs 64b/66b encoding/decoding.

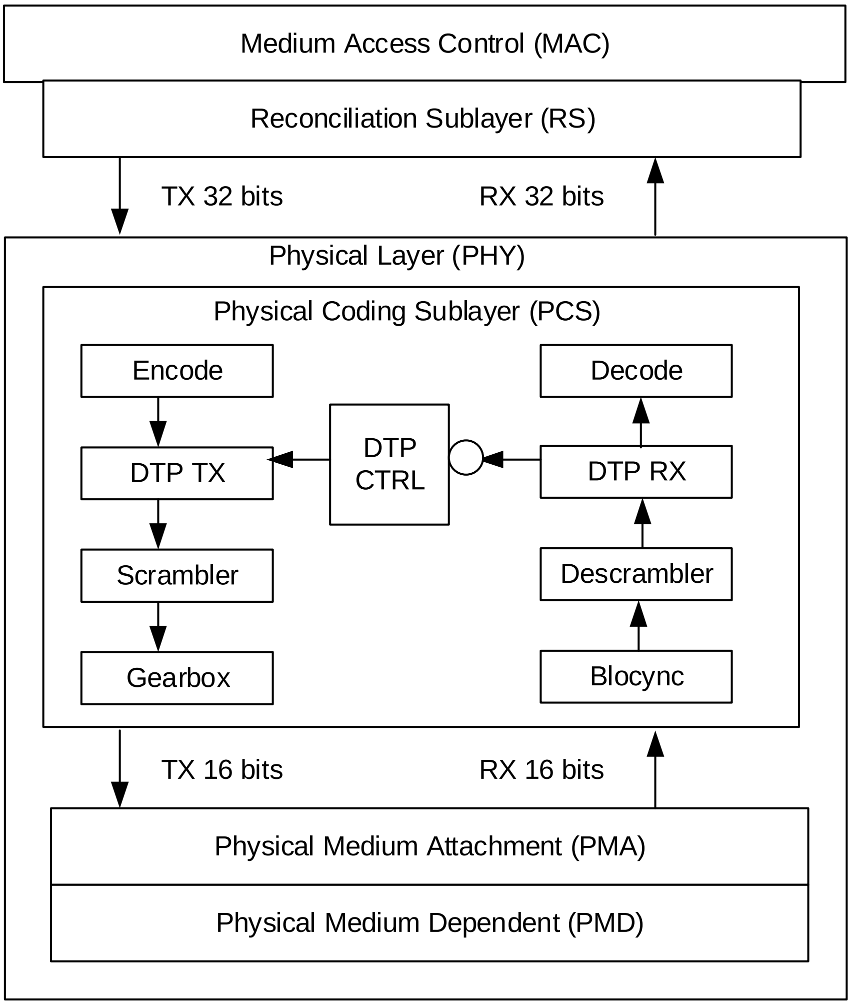
Medium Access Control (MAC)
Reconciliation Sublayer (RS)
TX 32 bits
RX 32 bits
Physical Layer (PHY)
Physical Coding Sublayer (PCS)
Encode
Decode
DTP TX
DTP CTRL
DTP RX
Scrambler
Descrambler
Gearbox
Blocync
TX 16 bits
RX 16 bits
Physical Medium Attachment (PMA)
Physical Medium Dependent (PMD)

Figure 6.4.1-1: Proposed DTP sublayer in IEEE 802.3ae [i.65] 10 Gbit/s Ethernet Standard (Source [i.55])

6.4.2 Function description

The control logic of DTP in a network port includes an algorithm and a local counter. The DTP-enabled PHY as depicted in the figure below is exactly the same as PCS layer except that it has DTP Control, DTP TX, and DTP RX sublayers. Specifically, TX DTP inserts a protocol message on the transmit path for which DTP RX receives the message on receive path and forwards to DTP control through a synchronization FIFO represented by a circle in the figure. The processing of DTP message happens as such that the upper layer is oblivious of these operations. Lastly, when an Ethernet frame is processed in the PCS sublayer it is left untouched by the DTP sublayer. DTP can also work with external protocol such as PTP, in that a PTP server will periodically broadcast DTP counter and UTC time to other servers.

6.4.3 Solution evaluation

While DTP for extremely high precision synchronization capabilities across the network is an interesting proposal, it has not been implemented in the 10GbE PHY yet. It may be used for any NFV process that are required in the same data center with two accurate clocks as source of time. It does also require replacing network devices, which can be done incrementally and with very small amount of hardware resource consumption.

Any NFV based applications, which require highly accurate time may use DTP in the same data center. As DTP needs specific hardware time distribution system, specific kernel and or user space application will be needed to enable access of the distributed and accurate time source through virtual NIC at VM or Container level. Each computing node may need access to such a source of time. In case of high level of accuracy requirement, the source may be GNSS with Atomic clock as a secondary source. Atomic clock may increase resiliency but at cost.

However, security especially of network and DTP management may require studies in the implementation, especially to achieve strict isolation between different domains, especially those with interfaces to third parties, or non-trusted hosted application functions.

6.5 Solution 5 for locstamp - based on binding of trusted hardware's ID with vertical hierarchy location

6.5.1 Architecture description

For this solution there are two kinds of trusted hardware module:

- The Trusted Platform Module (TPM), is defined by Trusted Computing Group (TCG). TPM is on the computer's motherboard. It is a hardware cryptographic module that can securely store sensitive data and perform various cryptographic operations. Authentication (a process to prove the identity attribute of an entity, i.e. the TPM acting as the integrity reporting entity) and attestation (a process that enables the software integrity state to be reported and verified in order to determine its trustworthiness) are necessary steps to ensure trusted computing. A TPM can authenticate itself using the credentials stored in the shielded memory and provide integrity measurements reports to prove platform software is trustworthy (see ETSI GR NFV-SEC 009 [i.61]).

- The Hardware Security Module (HSM), mostly defined by Global Platform. HSM is an external device added to a system. HW security modules (HSM) provide physical and logical protection for data and in particular for cryptographic material, such as keys. In addition, they offer highly secured cryptographic services, with physical and logical protection. HSMs are fully contained solutions for scalable cryptographic processing, key generation, and centralized key storage. As purpose-built appliances, they automatically include the hardware and firmware (i.e. software) necessary for these functions in an integrated package. They may be optimized for a specific or general purpose (e.g. performance, environment, portability, and interface) (see ETSI GR NFV-SEC 009 [i.61]).

In addition to secured processes, TPM/HSM allow reporting on certain measurable platform behaviours. TPM/HSM accomplish this by identifying and measuring both hardware and software components of the platform they are deployed in. TPM/HSM include mechanisms that allow for establishing of cross-layer-bindings. Within the NFVI layer hardware-based Security Modules (SMs), e.g. TPM's and HSM's, are typically used to form hardware-based Roots of Trust (RoTs).

Trusted Computing Group (TCG) defines attestation as follows: "The process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. Both forms of attestation require reliable evidence of the attesting entity".

The evidence and proofs of the platform values are vital in at least two dimensions of attestation (local and remote). Local attestations occurs within the system. Remote attestation allows changes to a host to be detected externally to the host by authorized parties.

ETSI GR NFV-SEC 018 [i.60] identifies and studies such Remote Attestation architectures applicable to NFV systems, based on TPM/HSM. SEC 018 includes the definition of attestation scope, stakeholders, interfaces and protocols required to support them. Additionally, it identifies and discusses functional and non-functional capabilities to be supported in an NFV system and provides a set of recommendations to increase the security of NFV.

Attestation proposed by ETSI GR NFV-SEC 018 [i.60] may improve the security of timestamp generation and the above layer during runtime processes.

As specified in GSMA NG.126 [i.58], cloud infrastructure operators need to ensure that remote attestation methods are used to remotely verify the trust status of a given cloud infrastructure platform. The basic concept is based on boot integrity measurements leveraging TPM/HSM built into the underlying hardware. Remote attestation can be provided as a service, and may be used by either the platform owner or a consumer/customer to verify that the platform has booted in a trusted manner. The practical implementation of the remote attestation provides 'Trust' visibility of the cloud infrastructure and enables compliance in cloud data centers by establishing the root of trust and builds the chain of trust across hardware, operating system, hypervisor, VM, and container. It includes asset tagging for location and boundary control. Asset is any computing device while tag is one or more attributes associated to the asset such as identity, location, etc. The platform trust and asset tag attestation information are used by Orchestrators and/or Policy Compliance management to ensure workloads are launched on trusted and location/boundary compliant platforms. They provide the needed visibility and auditability of infrastructure in both public and private cloud environments.

As mentioned above, if one of the measurements included a geographic location identifier (geo-tag), policies could then limit applications to specified countries, states, or regions. This is especially important because a growing number of privacy laws and other governmental regulations stipulate controls and protections that vary depending on location or restrict data to certain geographical boundaries.

NIST collaborated with Intel, and others to build a model that expanded on the trusted pools concept to implement location descriptor-based controls on top of trust-based controls to manage and measure compliance for workloads and data in the cloud. The resulting recommendation from this proof-of-concept model, NIST IR 7904 [i.73] Trusted Geolocation in the Cloud: Proof of Concept Implementation, was published as an internal report in December 2015. Determining the physical location of an object, such as a cloud computing server, is known as geolocation. It can be a logical description of geographic information, such as country or city, or it can be GPS-based latitude and longitude information. Geolocation can be accomplished in many ways, with varying degrees of accuracy, but traditional geolocation methods are not secure and they are presently enforced through management and operational controls not easily automated and scaled; therefore, traditional geolocation methods cannot be trusted to meet cloud security needs. NIST IR 7904 [i.73] describes geolocation as follows: "Geolocation enables identification of a cloud server's approximate location by adding that information to the server's root of trust. The hardware root of trust is seeded by the organization with the host's unique identifier and platform metadata stored in tamperproof hardware. This information is accessed using secure protocols to assert the integrity of the platform and confirm the location of the host".

Geo-tagging constitutes the process of defining, creating, and provisioning a set of geolocation objects to a computing device securely, i.e. locstamp. An interesting and very relevant application of the locstamp is the enforcement of boundary control based on lockstamps; the concept is called geo-fencing. Geo-fencing is about defining geographical or virtual boundaries using a variety of GPS, RFID, Cellular technologies, but also geolocation attributes based on TPM/HSM ID mapping to geographic coordinates of where is the related TPM/HSM. Geo-fencing is also about ensuring that the boundaries are not violated; but if they are violated, that appropriate remediation is enforced. Applications supporting geo-fencing allow an administrator to set rules and apply triggers so that when a device, or workload, or data attempts to cross a boundary so defined by the administrator, the action is blocked and appropriate alerts are sent out for further investigation.

6.5.2 Function description

Based on root of trust and geo-tagging concepts, described above, NFV based applications may easily generate trusted timestamp and locstamp, through kernel instructions requiring each host's unique identifier stored in a HMEE (such hardware ID may be stored or derived from parent CPU). Such identifiers are mapped by the applications with geographic coordinates where such physical components are located.

6.5.3 Solution evaluation

Geo-tagging can be enabled to definitively provide increased visibility to the physical geolocation of the server, which may enable many controls that require HMEE-based roots of trust to assert the location of workloads and data. These attributes and the associated controls are dependent on the boot integrity assertion of the platform; hence, they become a great adjacency to trusted compute pools and boot integrity. It may provide locstamps information related to some NFV processes, if needed.

This HMEE based solution is economical but induce a strict management of the mapping hardware ID and geographic coordinates mapping. Such an association does not offer a guarantee that the node/HMEE has not been moved from its location to another location and does not provide the kind of guarantee which is needed for sensitive application function deployed on NFV. An inertial measurement unit and internal small battery with detector of electric level change, are mounted with the computing node may increase the level of security and in producing alarms that the COTS are going to be moved or disconnected.

6.6 Solution 6 for locstamp - based on indoor positioning such as RFID Tagging

6.6.0 introduction

ISO/IEC has defined many standards related to RFID (Radio Frequency Identification), but some other RFID Standards are managed by Electronics Product Code Global Incorporated.

Such technologies let use wireless communication between a tag or object and interrogating device (or reader) to automatically track and identify such objects. The tag transmission range is limited to several meters from the reader. Based on ISO standards, there are different classes of active, semi passive or passive radio systems:

- Class 0: Basic read-only passive tag using backscatter where the tag was programmed at the time its chip was made.
- Class 1: Basic read-only passive tag using backscatter with one-time non-volatile programme capability.
- Class 2: Passive backscatter tag with up to 65k of read-write memory.
- Class 3: Semi-passive tag with up to 65 k read-write memory and a battery incorporated to provide increased range.
- Class 4: Active tag using a battery to enable extra functionality within the tag and also to provide power for the transmitter.
- Class 5: An active tag that provides additional circuitry to communicate with other class 5 tags.

The passive classes of radio system let only a short range of communication (less than 3 m), low volume of transmitted data (less than 128 octets) but offer no maintenance and a low cost of production.

The term beacon has been used in the RFID industry, as an active RFID to emit periodically or on demand, a message, that will identify this object and indirectly its position. For example, ISO/IEC 24730 [i.44] defines a real time locating system:

- Part 1: Application Programming Interface (API);
- Part 2: 2.4 GHz;
- Part 3: 433 MHz;
- Part 4: Global Locating Systems.

However, in the IEEE 802.11 [i.43] WLAN IEEE standards family, there is a management frame that the IEEE 802.11 [i.43] WLAN access point (or the beacon sender) transmits to provide time synchronization and specific parameters in order to facilitate stations locating and identifying a Base Station Subsystem. It provides another real time locating system, based in most cases, on layer 2 multicasts. It is a more costly system, but provides more accurate position. Furthermore, IEEE WLAN RFID tags can readily communicate directly with standard WLAN infrastructure without any special hardware or firmware modifications and can co-exist alongside WLAN clients such as laptops and so on. Such beacon may be based on system on chips that includes crypto accelerator and real-time clock, that may help to design a trustable system.

6.6.1 Architecture description

Through identification of the different surrounding beacons within data center rooms, a COTS server equipped with IEEE 802.11 [i.43] WLAN, or ISO/IEC 24730 [i.44] system may be able to attest the location in which a VNF is being run.

6.6.2 Function description

Such radio information may be processed to locate where the NFV process is executed or just the raw radio information of each beacon/tag observed by the IEEE or ISO system.

Such information (raw encrypted beacon identifier data or signed location or the RF fingerprinting) may be added to different messages that NFV is processing to be communicated to a party, such as an LI system MDF may transmit this information to an LEMF). This would allow the LEMF verify in which data center the interception related to a target usage has been performed, in addition to the Network Function Identifier and type provided in hardware based legacy systems.

Obviously this requires that the receiving party of such location data is aware of the different beacons that are in the different data centers in order to be able to resolve the beacon information provided to a physical location.

6.6.3 Solution evaluation

Such system has probably lower cost than any locstamps system described in the present document. The drawback is related to the possibility to jam such system, as IEEE 802.11 [i.43] WLAN IEEE has lower protection against it, or to duplicate the different beacon emitted data in another data center.

The higher the number of beacons, the better the accuracy of the position. However, a trade-off is required between the desires to acquire frequently updated information from tags possessing the shortest transmission intervals versus overall polling efficiency for the general tag population. It consumes time and resource if the location system of each COTS is spending the bulk of its time constantly polling beacons, which could impact performance in an environment with many beacons present.

Such system may be used also to track the COTS or NFVI itself if beacon or tag is installed in it. A "chokepoint" triggers, located at the entrance of the server room or of the data center, can initiate behavioural changes in tags that can immediately alert the common location system that the tagged asset is outside of the chokepoint. If such move is legitimate, it may be used to update automatically the CSP inventory databases. If it is not the case, location system at the chokepoint can also trigger alerts through external applications using email or SNMP traps.

6.7 Solution 7 for locstamp - based on GNSS raw data

6.7.1 Architecture description

As indicated in clause 5.6, location of events may need a trusted locstamp. A third party may attest later the location of such event in the log or after the delivery of flow data provided from a specific network function such as lawful interception. The party that is getting the flow data, may obtain one or more signed location messages from the one or more of the computing nodes.

The COTS servers of an NFV domain may be configured to obtain through a specific NIC, a secured GNSS raw signal data, obtained from one or more GNSS receivers. The HMEE is configured to produce a locstamp derived from the raw GNSS data and from its own hardware ID (see solution 5, such hardware ID may be stored or derived from parent CPU). Such computing node may generate a signed location message comprising the locstamp and the hardware ID. The secure location message may be included in all data flows or limited to specific flow of data associated with sensitive application functions of a hosted VM or container. It is signed with the certificate of the HMEE. This VM or container may get the signed location message through a virtual NIC and specific feature in the kernel that manage the specific NIC described above.

Such feature would allow another VNF or another entity external to the VNF to access such locstamp through an API.

6.7.2 Function description

The sensitive application, mentioned in the clause 6.7.1, may produce specific and enriched flows of data and transmit them to a third party or element, which may decrypt and analyse the GNSS RF raw signal data (RF signal are sampled). A signed description of the resources of the computing node and a state of the computing node may be transmitted to such third party if needed.

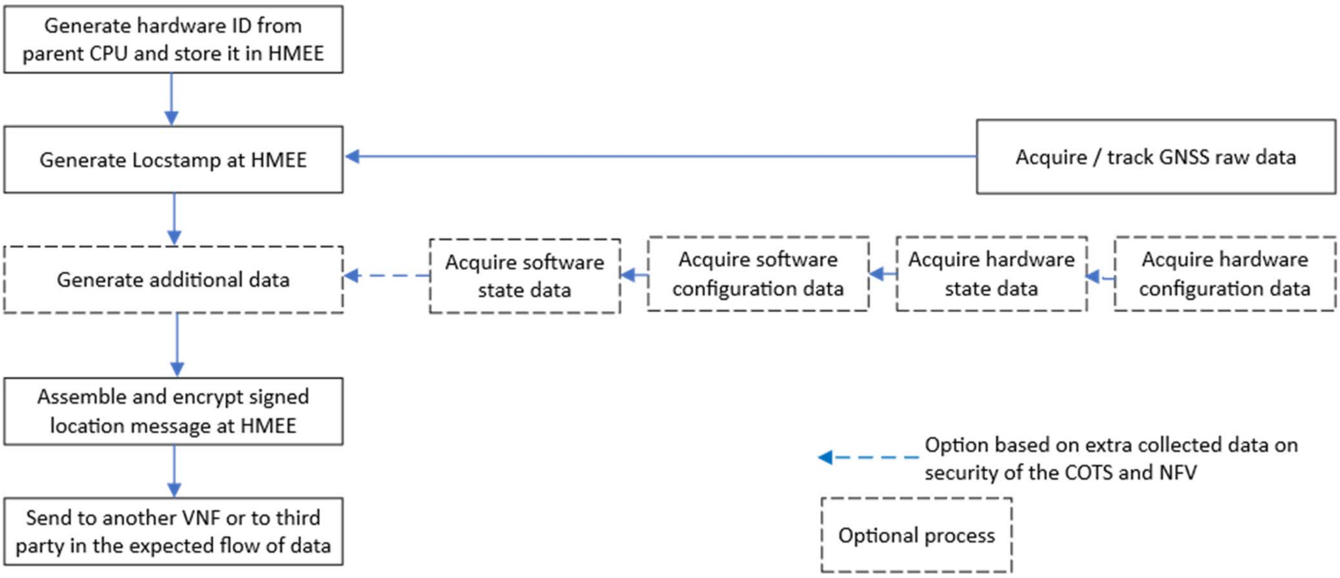
Generate hardware ID from parent CPU and store it in HMEE
Generate Locstamp at HMEE
Acquire / track GNSS raw data
Generate additional data
Acquire software state data
Acquire software configuration data
Acquire hardware state data
Acquire hardware configuration data
Assemble and encrypt signed location message at HMEE
Send to another VNF or to third party in the expected flow of data
Option based on extra collected data on security of the COTS and NFV
Optional process

Figure 6.7.2-1: Call flow on GNSS RF raw data

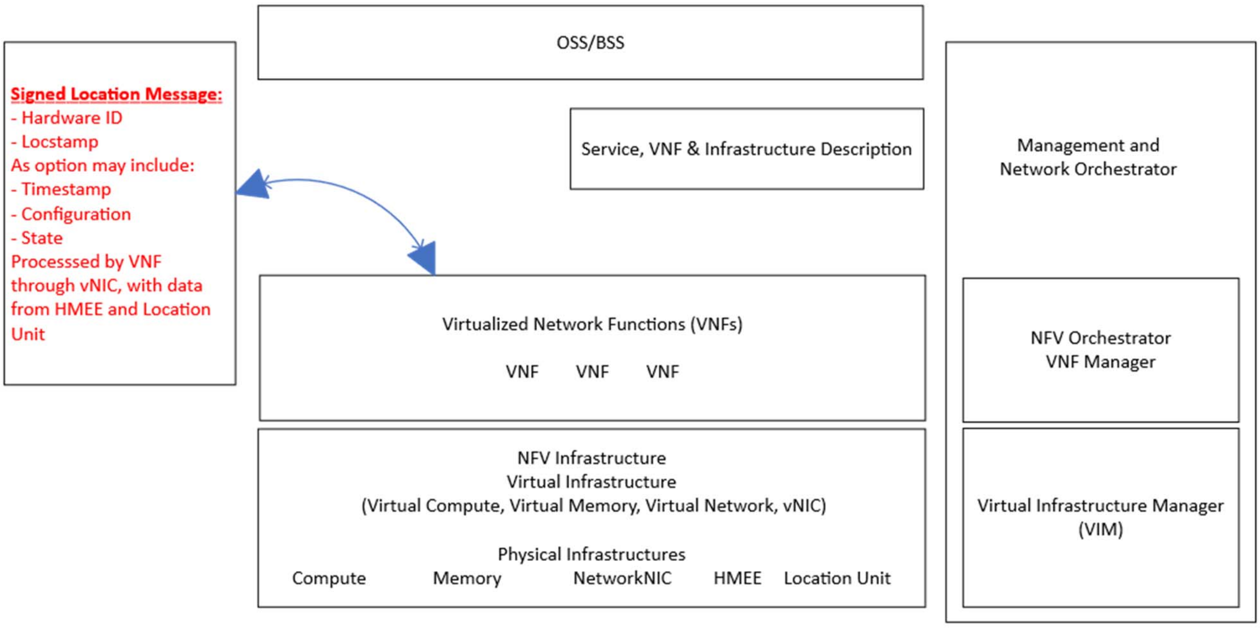
OSS/BSS
Signed Location Message:
- Hardware ID
- Locstamp
As option may include:
- Timestamp
- Configuration
- State
Processsed by VNF through vNIC, with data from HMEE and Location Unit
Service, VNF & Infrastructure Description
Management and Network Orchestrator
Virtualized Network Functions (VNFs)
VNF
VNF
VNF
NFV Orchestrator
VNF Manager
NFV Infrastructure
Virtual Infrastructure
(Virtual Compute, Virtual Memory, Virtual Network, vNIC)
Physical Infrastructures
Compute
Memory
NetworkNIC
HMEE
Location Unit
Virtual Infrastructure Manager (VIM)

Figure 6.7.2-2: Generation of signed location message based on locstamp from GNSS RF raw data (high level feature)

6.7.3 Solution evaluation

Through the use of this solution, OSS/BSS or authorized third parties are able to obtain trusted signed location information (with hardware ID and GNSS raw signal data), in support of audit or other VNF location control policies.

It is possible to reduce cost if one or more GNSS receiver and each HMEE shares the same trust zone. Security may be increased if the GNSS receivers are configured to detect GNSS signal spoofing or jamming. Another security feature can be added such as an inertial measurement unit and internal small battery with detector of electric level change to produce an alarm if the COTS equipment is moved or disconnected.

To improve the run time security, the third party or OSS/BSS may compare the hardware ID and the locstamp in the one or more signed location messages with ID data and location data of said computing nodes in a registry of trusted computing nodes and may determinate a current trust score of each node.

6.8 Solution 8 for locstamp - based on Trusted GNSS Positioning

6.8.0 Introduction

There are a number of security issues with tracking systems which utilize existing GNSS. Mitigating these issues is important to enable the development of critical applications:

- Signal authentication: There should be a method to authenticate the GNSS signal.
- Framework or standardized methodology to verify the integrity of a device and assess its security.
- Standardized telematics protocols that provide communications security.
- Significant privacy issues, such that it is difficult to obtain the location and preserve privacy at the same time.

All open civil GNSS signals are transmitted in the clear, conforming to interface specifications that are fully available in the public domain. Receivers will accept any input that conforms to the specifications and treat it as if it came from a GNSS satellite. Combined with the extremely low power levels of GNSS signals this makes it almost trivially simple to spoof or jam a legitimate GNSS source.

6.8.1 Architecture description

6.8.1.1 Signal authentication

In GNSS, authentication can be defined as the capability of a GNSS receiver to verify the authenticity of the GNSS information and of the entity transmitting it, to ensure that it comes from a trusted source. Authentication is an intrinsic GNSS capability remaining internal to the GNSS receiver.

Different authentication techniques may be considered, including Navigation Message Authentication (NMA). NMA has the advantage of having a low system impact as it requires only upgrades of the GNSS satellite's navigation data generation subsystem along with low-cost implementation on the receiver side.

Up until now, the main operational GNSS systems which have considered including authentication capabilities are GPS and Galileo.

In the case of GPS, a Chips-Message Robust Authentication (Chimera) approach, which is a hybrid NMA and spreading code authentication technique has been proposed for use within the new GPS L1C signal. The NMA portion of this scheme is based on a well-established standard, the asymmetric Elliptic Curve Digital Signature Algorithm (ECDSA) P-224, which simplifies the integration of the scheme into existing GNSS receivers.

In the case of Galileo OS-NMA (Open Service - Navigation Message Authentication) this feature consists of digitally signing the Open Service Navigation message in the E1 band, making use of forty reserved bits in the Galileo E1B data message and the Timed Efficient Stream Loss-Tolerant Authentication (TESLA) protocol, thus keeping the rest of the navigation message unencrypted.

6.8.1.2 Encryption

The idea behind encryption is to make GNSS signals unreadable to non-allowed users. The encryption codes and algorithms used are secret and without them it is impossible to spoof. Moreover, receivers compatible with this solution need to include the classified algorithms, have the relevant key repository and be certified for such use.

The encryption can be symmetric (sender and receiver both hold the same secret information) or asymmetric (different information held by the two parties).

Current examples of encrypted GNSS signals are GPS P(Y) code for military use, Galileo PRS (Public Regulated Service) or commercial Galileo HAS (High Accuracy Service).

6.8.2 Function description

The COTS of an NFV domain is configured to execute one or more of authentications, encryption or decryption function based on an HMEE and to get through a specific NIC, position trusted GNSS signal data, obtained from one or more GNSS receivers localized next to this computing node. The HMEE is configured to produce a locstamp derived from the raw GNSS data and from its own hardware ID (see solution 5 with hardware ID stored in the HMEE).

Such computing node may generate a signed location message comprising the locstamp and the hardware ID, that may be include in all data flows or only specific flows of data associated with sensitive application functions of a hosted VM or container. This VM or container may get the signed location message through a virtual NIC and specific feature in the kernel that manage the specific NIC described above.

The sensitive application may produce specific enriched flow of data and transmit them to a third party or element, which may decrypt and analyse the GNSS raw signal data. A signed description of the resources of the computing node and a state of the computing node may be transmitted to such third party if needed.

To improve the run time security, this third party or destination element may compare the hardware ID and the locstamp in the one or more signed location messages with ID data and location data of said computing nodes in a registry of trusted computing nodes and may determinate a trust score of each node.

To reduce the processing cost, the location message comprising the locstamp and the hardware ID may be only signed (integrity protection only) rather than secured using both integrity and confidentiality protection.

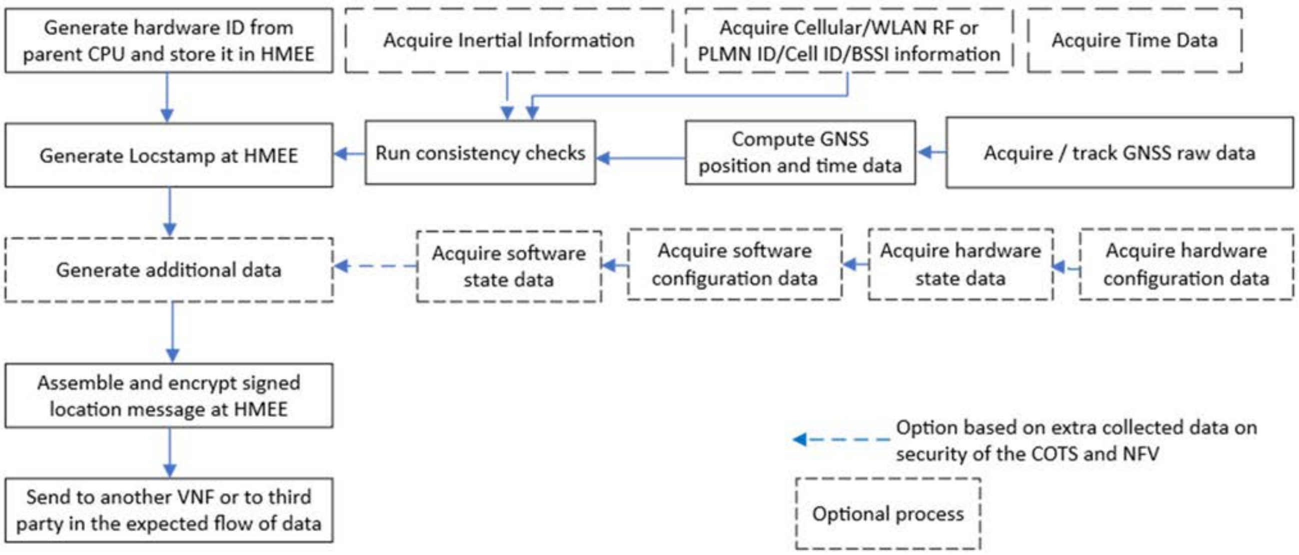
Generate hardware ID from parent CPU and store it in HMEE
Acquire Inertial Information
Acquire Cellular/WLAN RF or PLMN ID/Cell ID/BSSI information
Acquire Time Data
Generate Locstamp at HMEE
Run consistency checks
Compute GNSS position and time data
Acquire / track GNSS raw data
Generate additional data
Acquire software state data
Acquire software configuration data
Acquire hardware state data
Acquire hardware configuration data
Assemble and encrypt signed location message at HMEE
Send to another VNF or to third party in the expected flow of data
Option based on extra collected data on security of the COTS and NFV
Optional process

Figure 6.8.2-1: Call flow to get and process trusted GNSS data

6.8.3 Solution evaluation

A CSP operator of a NFV based service can give its clients an SLA that their applications will be executed on certified computing nodes, transmitting trusted location information to them during any run time system, based on COTS equipped with hardware trusted GNSS receiver and HMEE.

Trusted COTS servers are provided to which specific virtual machines or containers for applications with country-bound and/or mission-critical security constraints, can be directed.

Using this approach, the scope of applications which can be executed in a cloud architecture is enlarged without impacting the protection of personal data, intellectual property or specific critical 3GPP services.

Further study of multi-tenant deployments may be required to identity additional isolation and reporting requirements.

7 Conclusion

The present document introduces nine keys' issues related to time and to location, and eight solutions. The below table compares the issues covered by the different solutions.

Key issues vs solutions	Solution 1 Time and distribution of time, with White Rabbit system	Solution 2 Timestamp and time synchronization and distribution with IEEE 1588 [i.19]	Solution 3 Timestamp and time synchronization and distribution with trusted GNSS/ LEOs	solution 4 Timestamp and time distribution based on Datacenter Time Protocol (DTP)	Solution 5 Locstamp based on binding of trusted hardware's ID with geographical location	Solution 6 Locstamp based on indoor positioning such as RFID Tagging	Solution 7 Locstamp based on GNSS raw data	Solution 8 Locstamp based on Trusted GNSS Positioning
Key issue 1 Time and distribution of time	Solution 1 provide higher accuracy than solution 2. Security studies may be needed in isolation of such solution.	PTP of IEEE 1588 bring accuracy in time and low cost in time synchronization, but security studies may be needed in isolation of such solution.	The distribution of trusted GNSS/LEOs may be costly due to adaptation to each COTS that may host sensitive applications requiring trusted timestamps. Specific Kernel to manage dedicated NIC and virtual NIC port at VM or Container are needed.	DTP brings low-cost accuracy and low latency in time distribution and to generate timestamps. Solution 3 will complement such system if accuracy and trusted time source are needed. Security studies are recommended in isolation of such system and integrity of time information.	Not covered	Not covered	Not covered	Not covered

Key issues vs solutions	Solution 1 Time and distribution of time, with White Rabbit system	Solution 2 Timestamp and time synchronization and distribution with IEEE 1588 [i.19]	Solution 3 Timestamp and time synchronization and distribution with trusted GNSS/ LEOs	solution 4 Timestamp and time distribution based on Datacenter Time Protocol (DTP)	Solution 5 Locstamp based on binding of trusted hardware's ID with geographical location	Solution 6 Locstamp based on indoor positioning such as RFID Tagging	Solution 7 Locstamp based on GNSS raw data	Solution 8 Locstamp based on Trusted GNSS Positioning
Key issue 2 **Time accuracy**	If the source of time such GNSS/Atomic clock is accurate, solution 1 addresses the key issue.	The time accuracy by such solution is far better than the NTP based system with NFV. Security may be studied on isolation especially in multi-tenant environment even with multi domain.	One of the highest level of time accuracy is proposed by such solution, which may be complemented by solution 1 to reduce cost.	Such distribution and synchronization is high with this solution but only in the same data center. Security may have to be studied in case of multi-tenant NFV based system to isolate carefully the sensitive application function that may need trusted timestamp.	Not covered	Not covered	Not covered	Not covered
Key issue 3 **Time synchronization**	Addresses key issue.	Addresses key issue.	Time synchronization may be costly if such solution is the only system to provide time to each application function of NFV, as each COTS have a NIC that provide such information. It may be completed with solution 1 or 2.	Such solution is interesting but only if the NFV system is hosted in only one data center.	Not covered	Not covered	Not covered	Not covered

Key issues vs solutions	Solution 1 Time and distribution of time, with White Rabbit system	Solution 2 Timestamp and time synchronization and distribution with IEEE 1588 [i.19]	Solution 3 Timestamp and time synchronization and distribution with trusted GNSS/ LEOs	solution 4 Timestamp and time distribution based on Datacenter Time Protocol (DTP)	Solution 5 Locstamp based on binding of trusted hardware's ID with geographical location	Solution 6 Locstamp based on indoor positioning such as RFID Tagging	Solution 7 Locstamp based on GNSS raw data	Solution 8 Locstamp based on Trusted GNSS Positioning
Key issue 4 Timestamp log and storage	Addresses key issue, except that of consistent timestamp based from the same time source.	Addresses key issue, except that of consistent timestamp based from the same time source.	Addresses key issue, especially as such time source are trusted. To reduce cost. It may be complemented by solution 1 or 2 but with a risk on the trustiness of the time value processed by each NFV computing node.	Addresses key issue.	Not covered	Not covered	Not covered	Not covered
Key issue 5 Trusted Timestamp/attestation	Solution 1 fit partially the security and trusted timestamp sources against spoofing (see note).	Solution 2 fit partially the security and trusted timestamp sources against spoofing (see note).	Solution 3 does cover trusted timestamp /attestation. It may be completed by solution 1 or 2 but with a risk on the trustiness of the time value processed by each NFV computing node.	Solution 5 fit partially the security and trusted timestamp sources against spoofing (see note).	Not covered	Not covered	Not covered	Not covered

Key issues vs solutions	**Solution 1 Time and distribution of time, with White Rabbit system**	**Solution 2 Timestamp and time synchronization and distribution with IEEE 1588 [i.19]**	**Solution 3 Timestamp and time synchronization and distribution with trusted GNSS/ LEOs**	**solution 4 Timestamp and time distribution based on Datacenter Time Protocol (DTP)**	**Solution 5 Locstamp based on binding of trusted hardware's ID with geographical location**	**Solution 6 Locstamp based on indoor positioning such as RFID Tagging**	**Solution 7 Locstamp based on GNSS raw data**	**Solution 8 Locstamp based on Trusted GNSS Positioning**
Key issue 6 Location of events	Not covered	Not covered	Not covered	Not covered	Solution 5 does cover such needs but with the risk that COTS moved from another place may induce misinterpretation on the location of such NFV event, if the mapping is not up dated. The cost of such system has to be considered as dedicated NIC and hardware may be needed for each COTS.	Solution 6 does cover such key issue. The risk of change of location of the COTS that host the sensitive function is lower by alarm made by "check point" (see clause 6.6)	Solution 7 does cover partially such key issue, unless VM or Container host a communication application function that may transmit location of such event to the third party that may decrypt and check the encrypted value of raw data from GNSS. The cost of such system may be reduced by secured distribution to each NIC that host any sensitive application function that need such location.	Solution 7 does cover such key issue. The cost of such system may be reduced by secured distribution to each NIC that host any sensitive application function that need such location. Studies on the security of such distribution of trusted location through different NFV domains and multitenant. Isolation may be key point of such studies.

Key issues vs solutions	Solution 1 Time and distribution of time, with White Rabbit system	Solution 2 Timestamp and time synchronization and distribution with IEEE 1588 [i.19]	Solution 3 Timestamp and time synchronization and distribution with trusted GNSS/ LEOs	solution 4 Timestamp and time distribution based on Datacenter Time Protocol (DTP)	Solution 5 Locstamp based on binding of trusted hardware's ID with geographical location	Solution 6 Locstamp based on indoor positioning such as RFID Tagging	Solution 7 Locstamp based on GNSS raw data	Solution 8 Locstamp based on Trusted GNSS Positioning
Key issue 7 **Location of UE**	Not covered	Not covered	Not covered	Not covered	It is covered only with C RAN/ O RAN or vCCAP or Edge Computing cases but with low accuracy location.	It is covered only with C RAN/ O RAN or vCCAP or Edge Computing cases but with low accuracy location.	Not covered	Solution 8 do not cover such case in majority of case, unless it is a specific UE such as Public Safety. Such UE can decrypt and process the trusted data from some GNSS (Galileo) and STL system.
Key issue 8 **Multiple VNFCI policy**	Not covered	Not covered	Not covered	Not covered	Partially covered	Partially covered	Partially covered	Partially covered
Key issue 9 **Location at instantiation, location at run time**	Not covered	Not covered	Not covered	Not covered	Solution 5 may answer to such issue.	Solution 6 may answer to such issue.	Solution 7 may partially answer to such issue, as it depends on a third party.	Solution 8 may answer to such issue.
NOTE: Trusted timestamps may require a trusted time source such as encrypted GNSS signal with extra resiliency based extra local source such as Atomic Clock to reduce risks of spoofing and jam attacks.								

While none of the solutions fully address the challenges associated with "Multiple VNFCI" policy (see clause 5.8) they can be mitigated by additional policy control (e.g. affinity policy) in order to enforce location constraint or logical location.

The management of Locstamp and Timestamp are covered by two different complementary solutions for any NFV system in a sensitive application. Each solution may require a specific virtual NIC. They may need not only virtual NIC needed for VM or container, which need to generate trusted locstamp and timestamp for such sensitive application, but also a specific driver in the kernel that will interfere with physical dedicated NIC.

The impact of the different solutions varies according to the required levels of security and accuracy.

Further studies on isolation and security of the different solutions described in this present document, may be required in case of multi-tenant edge computing and untrusted application function, which are hosted on the same COTS.

Annex A: European Securities and Markets Authority: regulatory technical and implementing standards RTS 25 on clock synchronization

A.1 Guidelines on clock synchronization

A.1.0 General

The European Securities and Markets Authorities has defined technical specifications and implementation rules related to clock synchronisation (see [i.33]).

Article 50 of MiFID II and the related regulatory technical standards apply to Trading Venues and their members and participants and requires them to comply with accuracy requirements regarding the maximum divergence of their business clocks from UTC and to timestamp reportable events to a specific granularity.

A.1.1 Reportable Events

Article 50 of MiFID II refers to the obligation of Trading Venues and their members/participants to synchronize the business clocks they use to record the date and time of any "reportable event". ESMA considers it relevant to provide examples of "reportable events" for the purposes of Article 50.

A.1.2 Time stamp granularity

Article 50 of MiFID II applies to a broad range of reportable events (section 7.1). Commission Delegated Regulation (EU) 2017/574 [i.75] specifies two types of accuracy requirements: the maximum divergence from UTC and the timestamp granularity.

A.1.3 Compliance with the maximum divergence requirements

Commission Delegated Regulation (EU) 2017/574 specifies two types of accuracy requirements: the maximum divergence from UTC and the timestamp granularity. This section of the guidelines only concerns the former requirement. Article 4 of Commission Delegated Regulation (EU) 2017/574 states that 'Operators of Trading Venues and their members or participants should establish a system of traceability to UTC'. This includes ensuring that their systems operate within the granularity and a maximum tolerated divergence from UTC as per Commission Delegated Regulation (EU) 2017/574.

Furthermore, operators of Trading Venues and their members or participants should evidence that the crucial system components used meet the accuracy standard levels on granularity and maximum divergence of UTC as guaranteed and specified by the manufacturer of such system components (component specifications should meet the required accuracy levels) and that these system components are installed in compliance with the manufacturer's installation guidelines.

Relevant and proportionate testing of the system should be required along with relevant and proportional monitoring thereof to ensure that the divergence from UTC remains within tolerance. The relevance and proportionality will depend on the applicable maximum divergence from UTC. As per Article 1 of Commission Delegated Regulation (EU) 2017/574, systems that provide direct traceability to the UTC time issued and maintained by a timing center listed in the BIPM Annual Report on Time Activities are considered as acceptable to record reportable events. The use of the time source of the U.S. Global Positioning System (GPS) or any other global navigation satellite system such as the Russian GLONASS or European Galileo satellite system when it becomes operational is also acceptable to record reportable events provided that any offset from UTC is accounted for and removed from the timestamp. GPS time is different to UTC. However, the GPS time message also includes an offset from UTC (the leap seconds) and this offset should be combined with the GPS timestamp to provide a timestamp compliant with the maximum divergence requirements in Commission Delegated Regulation (EU) 2017/574. Users of such systems should be aware of the relevant risks associated with their use such as solar flares, interference, jamming or multipath reflections and that the receiver is correctly locked to the signal. Therefore, appropriate steps should be taken to ensure that these risks are minimized. In particular, the Recommendation ITU-R TF.1876-0 [i.42] on trusted time source should be considered by entities planning to use GPS receivers that will be subject to the more stringent accuracy requirements.

For the purposes of Article 4 of Commission Delegated Regulation (EU) 2017/574, for users of a satellite system, the accuracy required under the RTS should apply to any point within the domain system boundary where time is measured. However, the first point at which the system design, functioning and specifications should be considered is on the receiver used (e.g. the model of the GPS receiver and the designed accuracy of the GPS receiver) to obtain the timestamp message from the satellite (and any associated antenna). This should not include the GPS satellite system and the satellites traceability to UTC.

When a leap second is to be added or subtracted from UTC as announced periodically by the International Earth Rotation and Reference Systems Service (IERS) this should be handled in accordance with the Recommendation ITU-R TF.460-6 [i.20]. This recommendation states that a positive leap second begins at 23:59:60 and ends at 00:00:00 and a negative leap second is represented by the time moving from 23:59:58 to 00:00:00.

Timestamps can be maintained in local time so long as when data is provided to competent authority the timestamp is converted to UTC (Zulu time). Some timestamp messages may consist of a timestamp and a divergence from UTC applicable for that timestamp. Again, on timestamps provided to a competent authority the divergence should be applied to the timestamp so that only one timestamp is provided to the competent authority.

A.1.4 Application, host and wire timestamps

Application and host timestamps are generated within the software application whereas wire timestamps are generated by separate hardware whilst also taking a copy of the network packets containing the relevant information. ESMA considers that any of these timestamps will be acceptable for members or participants to use. Trading Venues should note that given the requirements to record events at the matching engine will likely require the use of application timestamps.

A.1.5 Gateway-to-gateway latency

Trading Venues may list multiple gateway-to-gateway latency times for different percentiles. For the purposes of clock synchronization, ESMA considers that Trading Venues should use the gateway-to-gateway latency time at the 99th percentile.

Trading Venues have obligations to monitor in real-time the gateway-to-gateway latency under Article 13(c) (ESMA/2015/1464)51 [i.74]. If the gateway-to-gateway latency improves from greater than 1 millisecond to less than or equal to one millisecond then their requirements under Article 50 for the granularity and maximum divergence change. This type of scenario is most likely to occur following a change to a new matching engine or technology enhancements to a venue's existing infrastructure and therefore the timestamp requirements should be considered when such work is planned.

Annex B: DHS requirements for critical infrastructure and GNSS

B.1 Introduction

- US Department of Homeland Security (DHS) published recommendations (see [i.59]) for improving the operations and development of GNSS equipment used by Critical Infrastructure. The objective is to improve the security and resilience of PNT (positioning, navigation, and timing) equipment across the spectrum of equipment development, deployment, and use. Specifically, recommendations consider Installation and operation strategies that can be implemented for current equipment.

- Strategies that can result in more resilient new and/or improved products based on existing technology and knowledge.

B.2 Recommendations

B.2.0 General

These installation and operation strategies and development opportunities described can significantly enhance the ability of GNSS receivers and associated equipment to defend against a range of interference, jamming, and spoofing attacks.

Two categories of recommendations are considered:

- installation and operation strategies for owners, operators;

- installers on one side and development strategies for manufacturers on the other side.

B.2.1 Installation and operation recommendations for owners, operators, and installers

The following 11 recommendations can improve the resilience of equipment receiving and processing GNSS signals. The recommendations can be employed immediately on current equipment:

1) Obscure antennas. Install antennas where they are not visible from publicly accessible locations or obscure their exact locations by introducing impediments to hide the antennas.

2) Provide decoy antennas. Leave or install a clearly visible antenna as a decoy placed it in a location that is readily observed from publicly accessible spaces, and far from the actual antenna.

3) Carefully select antenna locations. Choose a location where the antenna has an adequate view of the sky.

4) Employ blocking antennas. Blocking antennas not only help protect a receiver from interference and jamming, but can also attenuate spoofing signals.

5) Introduce redundancy. If it is feasible and affordable, install two or three antennas at widely diverse locations (e.g. near different ends of a building).

6) Calibrate. Determine the delay characteristics of antenna and antenna electronics, making sure the bulk delay is small enough to be compensated in a timing receiver.

7) Avoid using low elevation signals. By using lower elevation signals, system performance may be degraded due to Atmospheric errors and signal multipath.

8) Use position hold for stationary timing receivers. In this position hold mode, they need to receive signals from as few as one satellite in order to provide timing measurements.

9) Employ high-quality holdover devices. Timing receivers should be backed up by an independent timing source, such as a Rubidium or Cesium clock.

10) Add a sensor/blocker. Sensors can detect characteristics of interference, jamming, and spoofing signals, provide local indication of an attack or anomalous condition, communicate alerts to a remote monitoring site, and collect and report data to be analysed for forensic purposes.

11) Practice good cyber hygiene. Since both the GNSS receiver and any associated processors are computers, and often networked computers, good cyber hygiene, like that used for any other mission critical computer, is essential. Firewalls, virus protection, and other defences should be installed and maintained.

B.2.2 Development recommendations for manufacturers

Manufacturers should develop and produce future GNSS receivers, along with their integration into different types of equipment, to provide enhanced competence, including robustness and security. The following 11 recommendations can be used by equipment designers and manufacturers for such enhancements:

1) Extend data spoofing whitelists to sensors. Existing data spoofing whitelists implemented in government reference software should also be implemented in sensors.

2) Plan for growth. Receiver and processor hardware and software should be architected and designed for adaptability and growth.

3) Implement software assurance. Sound software assurance practices should be followed.

4) Return to known good state. Software should be written so that the processing returns to a known good state either manually by an external command or automatically if the processing is determined to be in an unacceptable state.

5) Address all components. The development strategies 1, 2, 3 and 4 would be employed in both the GPS receiver and any associated processor.

6) Enable secure remote access and management. When onsite access and management are not possible or sufficient, it should be possible to securely connect the receiver or associated processor to a network for management and information extraction.

7) Enhance anti-jam capabilities. The GPS receiver should be specified and developed to provide good anti-jam capabilities so that it can operate through high received levels of interference and jamming.

8) Enhance anti-measurement spoof processing. The GPS receiver should be specified and developed to provide good anti-measurement spoofing-recognizing, rejecting, and reporting spoofing signals that cause the receiver to produce erroneous time of arrival measurements or frequency of arrival measurements.

9) Implement anti-data spoofing. Receiver software should be modified to implement anti-data spoofing using whitelists that describe valid message contents.

10) Use more GPS signal types. L2C, L5 and L1C are modernized civil GPS signals which are more robust than the L1 C/A legacy signal and should be leveraged for increased resistance to interference, jamming, and spoofing.

11) Instrument receivers capture data. To support both debugging and forensic analysis, receivers should capture data when they detect anomalous situations.

Annex C:
Change History

Date	Version	Information about changes
May 2017	0.0.1	Inclusion of ToC based on agreed T Doc NFVSEC(17)000038r1 Version 0.0.1 prepared by the rapporteur
December 2017	0.0.2	Inclusion of NFVSEC(17)000157 on Issues on Time Accuracy and distribution/Trusted timestamp with an agreed minor modification, NFVSEC(17)000125r2 on Time synchronization requirements on timestamp based on some regulations /solutions, NFVSEC(17)000079r1 on Time definition (UTC/legal time), NFVSEC(17)000077r4 on Time synchronization issue, requirement and one solution, Version 0.0.2 prepared by the rapporteur
December 2019	0.0.3	NFVSEC(19)0000116r1 Updates on 3GPP requirements related to time, time synchronization for 5G, and changes in standards from IEEE 1588 and associated ITU profile
February 2020	0.0.4	NFVSEC(20)000011- 4 Requirements, Assumptions and Principles
September 2020	0.0.5	NFVSEC(20)000081r1 - SEC016 License Management use case
Mai 2021	0.0.6	NFVSEC(21)000037 BT review NFVSEC(21)000032r1 Solution for locstamp based on indoor positioning such as RFID Tagging
September 2021	0.0.7	NFVSEC(21)000066r3 Multiple changes in adding extra clauses such new solutions, for timestamp such as Datacenter Time Protocol, locstamps such as locstamps based on binding of HMEE with location, based on trusted GNSS, Annexes A and B
May 2022	0.0.8	NFVSEC(22)000042
July 2022	0.0.8a	Editorial review by NFV Chair in NFVSEC(22)000063

History

Document history		
V1.1.1	February 2023	Publication