



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

[ETSI GR NFV-SEC 016 V1.2.1 \(2024-12\)](https://standards.iteh.ai/catalog/standards/etsi/2909274f-76f6-4959-8617-71d3499f373e/etsi-gr-nfv-sec-016-v1-2-1-2024-12)

<https://standards.iteh.ai/catalog/standards/etsi/2909274f-76f6-4959-8617-71d3499f373e/etsi-gr-nfv-sec-016-v1-2-1-2024-12>

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

RGR/NFV-SEC016ed121

Keywordscritical infrastructure, GNSS, ICT, 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 the
[ETSI Search & Browse Standards](#) application.

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 on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed, this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our [Coordinated Vulnerability Disclosure \(CVD\)](#) program.

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

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	9
3.1 Terms.....	9
3.2 Symbols.....	9
3.3 Abbreviations	10
4 Problem statement: Location and timestamp synchronization in NFV	13
4.1 Regulatory timestamp requirements	13
4.1.1 Communications, electronic market regulation, billing, interception, data retention, and critical infrastructures	13
4.1.2 Financial market regulation (timestamp of transaction, especially in high-speed trading).....	14
4.2 CSP timestamp requirements	15
4.2.1 Time/frequency reference source.....	15
4.2.2 Network synchronization, especially mobile radio/5G	15
4.2.3 Forensics of network events for O&M	16
4.2.4 Timestamp for VNF licensing	16
4.3 Requirements on location of internal events or operations of network	17
4.3.1 For the O&M	17
4.3.2 For third party such as investigation team, IPR owners, content licensing, etc.	17
4.3.3 Location for VNF licensing	17
4.4 Requirements on UE location in mobile or nomadic network.....	17
4.5 Principles.....	17
4.5.1 Time definition (UTC /legal time).....	17
4.5.2 Location definition.....	18
4.6 Multiple VNFCI location	18
5 Key Issues	19
5.1 Key issue 1: Time and distribution of time	19
5.2 Key issue 2: Time accuracy.....	20
5.3 Key issue 3: Time Synchronization.....	20
5.4 Key issue 4: Timestamp log and storage	22
5.5 Key issue 5: Trusted Timestamp/attestation.....	22
5.6 Key issue 6: Location of events.....	22
5.7 Key issue 7: Location of UE	22
5.8 Key issue 8: Multiple VNFCI policy.....	23
5.9 Key issue 9: Location at Instantiation, Location at Run time.....	24
6 Solutions.....	25
6.1 Solution 1 for timestamp - time Synchronization and distribution (White Rabbit Network).....	25
6.1.1 General.....	25
6.1.2 Architecture description.....	26
6.1.3 Function description	26
6.1.4 Solution evaluation	27
6.2 Solution 2 for timestamp - time synchronization and distribution (IEEE 1588)	27
6.2.1 General.....	27
6.2.2 IEEE 1588 related to Mobile Wireless (Cloud RAN).....	29
6.2.2.1 Architecture.....	29
6.2.2.2 Function description.....	30

6.2.2.3	Solution evaluation.....	32
6.2.3	IEEE 1588 related to Cable TV	33
6.2.3.1	Architecture.....	33
6.2.3.2	Function description.....	35
6.2.3.3	Solution evaluation.....	36
6.3	Solution 3 for timestamp - time synchronization and distribution (based on trusted GNSS/ LEOs)	36
6.3.1	Architecture description.....	36
6.3.2	Function description	37
6.3.3	Solution evaluation	38
6.4	Solution 4 for timestamp Data centre Time Protocol (DTP).....	39
6.4.0	introduction.....	39
6.4.1	Architecture description.....	39
6.4.2	Function description	40
6.4.3	Solution evaluation	40
6.5	Solution 5 for locstamp - based on binding of trusted hardware's ID with vertical hierarchy location	41
6.5.1	Architecture description.....	41
6.5.2	Function description	42
6.5.3	Solution evaluation	42
6.6	Solution 6 for locstamp - based on indoor positioning such as RFID Tagging	43
6.6.0	introduction.....	43
6.6.1	Architecture description.....	43
6.6.2	Function description	43
6.6.3	Solution evaluation	44
6.7	Solution 7 for locstamp - based on GNSS raw data	44
6.7.1	Architecture description.....	44
6.7.2	Function description	44
6.7.3	Solution evaluation	45
6.8	Solution 8 for locstamp - based on Trusted GNSS Positioning.....	46
6.8.0	Introduction.....	46
6.8.1	Architecture description.....	46
6.8.1.1	Signal authentication.....	46
6.8.1.2	Encryption.....	46
6.8.2	Function description	47
6.8.3	Solution evaluation	47
7	Conclusion.....	48
Annex A: European Securities and Markets Authority: regulatory technical and implementing standards RTS 25 on clock synchronization		54
A.1	Guidelines on clock synchronization	54
A.1.0	General	54
A.1.1	Reportable Events.....	54
A.1.2	Time stamp granularity	54
A.1.3	Compliance with the maximum divergence requirements	54
A.1.4	Application, host and wire timestamps.....	55
A.1.5	Gateway-to-gateway latency	55
Annex B: DHS requirements for critical infrastructure and GNSS		56
B.1	Introduction	56
B.2	Recommendations	56
B.2.0	General	56
B.2.1	Installation and operation recommendations for owners, operators, and installers	56
B.2.2	Development recommendations for manufacturers.....	57
Annex C: Change history		58
History		59

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 IPR online database](#).

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™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

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

Foreword

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

Modal verbs terminology

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

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

Introduction

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

1 Scope

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

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

- [i.1] [IEEE™ ICC 2015](#) - Workshop on Cloud-Processing in Heterogeneous Mobile Communication Networks (IWCPM)-(2015): "Synchronization challenges in packet-based Cloud-RAN fronthaul for mobile networks".
- [i.2] [Heavy Reading - White Paper \(December 2014\)](#): "New Synchronization Requirements for 4G Backhaul & Fronthaul".
- [i.3] 3GPP TR 38.803: "Study on new radio access technology: Radio Frequency (RF) and co-existence aspects".
- [i.4] Recommendation ITU-T G.8260: "Definitions and terminology for synchronization in packet networks".
- [i.5] Recommendation ITU-T G.8261: "Timing and synchronization aspects in packet networks".
- [i.6] Recommendation ITU-T G.8271: "Time and phase synchronization aspects of packet networks".
- [i.7] Recommendation ITU-T G.8262: "Timing characteristics of a synchronous Ethernet equipment slave clock".
- [i.8] Recommendation ITU-T G.8263: "Timing characteristics of packet-based equipment clocks".
- [i.9] Recommendation ITU-T G.8272: "Timing characteristics of primary reference time clocks".
- [i.10] Recommendation ITU-T G.8273: "Framework of phase and time clocks".
- [i.11] Recommendation ITU-T G.8265: "Architecture and requirements for packet-based frequency delivery".
- [i.12] Recommendation ITU-T G.8275: "Architecture and requirements for packet-based time and phase distribution".
- [i.13] Recommendation ITU-T G.8264: "Distribution of timing information through packet networks".

- [i.14] Recommendation ITU-T G.8265.1: "Precision time protocol telecom profile for frequency synchronization".
- [i.15] Recommendation ITU-T G.8275.1: "Precision time protocol telecom profile for phase/time synchronization".
- [i.16] ETSI TS 136 133: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management (3GPP TS 36.133)".
- [i.17] ETSI TR 136 922: "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); TDD Home eNode B (HeNB) Radio Frequency (RF) requirements analysis (3GPP TR 36.922)".
- [i.18] IEEE™ Communications Standards Magazine (volume 1, issue 1, March 2017): "Analysis of the Synchronization Requirements of 5G and Corresponding Solutions".
- NOTE: Available at Analysis of the Synchronization Requirements of 5g and Corresponding Solutions | IEEE™ Journals & Magazine | IEEE™ Xplore.
- [i.19] IEEE™ 1588: "Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".
- [i.20] Recommendation ITU-R TF.460-6: "Standard-frequency and time-signal emissions".
- [i.21] [German law on time.](#)
- [i.22] ITU: "[Final Acts WRC-12](#)", World Radiocommunication Conference (Geneva, 2012).
- [i.23] Downstream Radio Frequency Interface Specification, CM-SP-DRFII4-131120, 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 - MHA v2 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] [NISTIR 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 (UK): "[Metering and Billing directive](#)".
- [i.35] Bundesnetzagentur (Germany): "[Billing accuracy](#)".
- [i.36] IEC/IEEE™ 61850-9-3:2016: "Communication networks and systems for power utility automation - Part 9-3: Precision time protocol profile for power utility automation".

- [i.37] IEEE C37.238™-2017: "IEEE™ Standard Profile for Use of IEEE™ 1588 Precision Time Protocol in Power System Applications".
- [i.38] Meinberg: "[Time synchronization in Virtual Machines](#)".
- [i.39] Ericsson®: "[An overview of remote interference management](#)".
- [i.40] Marc Weiss, Ph.D. of the Time and Frequency Division, NIST: "[Telecom Requirements for Time and Frequency Synchronization](#)".
- [i.41] Reeve: "[Telecommunications Synchronization Overview](#)".
- [i.42] Recommendation ITU-R TF.1876-0: "Trusted time source for Time Stamp Authority".
- [i.43] IEEE 802.11™: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
- [i.44] ISO/IEC 24730: "Information technology, Real time locating systems (RTLS)".
- [i.45] International Bureau of Weights and Measures (BIPM): "[UTC definition](#)".
- [i.46] IETF RFC 5905: "Network Time Protocol Version 4: Protocol and Algorithms Specification".
- [i.47] EECIS: "[How NTP works](#)".
- [i.48] ITU-R Sector: "[ITU-R FAQ on Universal Time Scale \(UTC\) - Leap Second](#)".
- [i.49] Void.
- [i.50] CERN: "[The White Rabbit Project](#)".
- NOTE: [Repository of the White Rabbit Project](#).
- [i.51] ATIS: "[Workshop on Synchronization and Timing Systems](#)".
- [i.52] "[Shannon-Hartley-theorem](#)" from Wikipedia®.
- [i.53] Recommendation ITU G.8275/Y.1369: "Architecture and requirements for packet-based time and phase distribution".
- [i.54] M. Rizzi, M. Lipinski, P. Ferrari, S. Rinaldi, and A. Flammini: "White rabbit clock synchronization: Ultimate limits on close-in phase noise and short-term stability due to FPGA implementation," IEEE™ Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, September 2018.
- [i.55] Lee, S. K., Wang, H., & Weatherspoon, H. (2019): "[Globally Synchronized Time via Datacenter Networks](#)", IEEE™/ACM Transactions on Networking.
- [i.56] ITU GSTR-GNSS (2020): "Considerations on the use of GNSS as a primary time reference in telecommunications".
- [i.57] CSA Cloud Security Alliance: "Privacy level agreement outline for the sale of cloud services in the European Union".
- [i.58] GSMA NG.126: "Cloud Infrastructure Reference Model Version 1.0".
- [i.59] U.S. Department of Homeland Security: "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure".
- [i.60] ETSI GR NFV-SEC 018: "Network Functions Virtualisation (NFV); Security; Report on NFV Remote Attestation Architecture".
- [i.61] ETSI GR NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".
- [i.62] ETSI TS 123 501: "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".

- [i.63] IEEE 802.1AS™: "Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications".
- [i.64] IEEE 802.1Q™: "Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks".
- [i.65] IEEE 802.3ae™: "Standard for Information technology - Local and metropolitan area networks - Part 3: CSMA/CD Access Method and Physical Layer Specifications - Media Access Control (MAC) Parameters, Physical Layer, and Management Parameters for 10 Gb/s Operation".
- [i.66] IEEE 802.3™: "IEEE™ Standard for Ethernet".
- [i.67] Ericsson Technology Review, January 13, 2021: "[5G synchronization requirements and solutions](#)".
- [i.68] "[Telco Cloud Infra Timing Application - ptp4l, phc2sys and pnc](#)".
- [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] International Civil Aviation Organization, Doc 9674 AN/946: "[World Geodetic System - 1984 \(WGS-84\)](#)".
- [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.
- [i.76] [SEC Rule 613](#): "Securities and Exchange Commission".
- [i.77] Federal Energy Regulatory Commission: "[Federal Power Act](#)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

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

dB	Decibel
GHz	Gigahertz
km	Kilometer
MHz	Megahertz
ppb	parts per billion

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 - International Bureau of Weights and Measures
BTS	Base Transceiver Station
C/A	C/A (GNSS legacy civil signal)
CA	Carrier Aggregation
CCAP	Cable Converged Access Platform
CERN	Centre Européen pour la Recherche Nucléaire (European Organization for Nuclear Research)
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
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	Data centre 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
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GS	Group Specification
GSM	Global System for Mobile
GSMA	GSM Association
HAS	High Accuracy Service (Galileo)
HFC	Hybrid Fiber-Coaxial
HLR	Home Location Register
HMEE	Hardware Mediated Execution Enclave
HSM	Hardware Security Module
HW	HardWare
ID	IDentity
IEC	International Electrotechnical Commission
IEEE™	Institute of Electrical and Electronic Engineers
IERS	International Earth Rotation and Reference Systems Service

IP	Internet Protocol
IPR	Intellectual Property Rights
IPSEC	Internet Protocol SECurity
ISO	International Organization for Standardization
IT	Information Technology
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 and 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
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 Controller
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
PPS	Pulse-Per-Second
PRC	Primary Reference Clock
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 Virtualisation
SSL	Secure Socket Layer
STL	Satellite Time and Location
SV	Space Vehicle time
SyncE	Synchronous Ethernet
TAE	Time Alignment Error
TAI	International Atomic Time
TCG	Trusted Computing Group
TDD	Time Division Duplex
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
URLLC	Ultra-Reliable and Low Latency Communications
USNO	U.S. Naval Observatory
UT1	Earth rotation time
UTC	Universal Time Coordinated
vCCAP	Virtual CCAP
VLAN	Virtual Local Area 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 NISTIR 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 μ s 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 UTC of NIST atomic clock source with up to a 50 ms tolerance.

- The SEC Rule 613 [i.76] requires "Each national securities exchange, national securities association, and member of such exchange or association to synchronize its business clocks that 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 $\pm 0,01$ % (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 [i.77] 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) [i.69] 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.