5GAA [DRAFT] TR E-200008

Technical Report

5G Automotive Association;

WG7;

Misbehaviour Detection

.

***5GAA***

Postal address

5GAA address

5GAA c/o MCI Munich

Neumarkter Str. 21

81673 München – Germany

Internet

http://www.5gaa.org

***Copyright Notification***

No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

Contents

Foreword 4

Introduction 4

1 Scope 5

2 References 5

3 Definitions, symbols and abbreviations 5

3.1 Definitions 5

3.2 Symbols 5

3.3 Abbreviations 6

4 Model and Terms 6

4.1 Misbehavior Model and Concepts 6

4.2 Terms 6

4.3 Attacker Model and Security Objectives 6

5 Related Work 6

5.1 Research 7

5.2 Pilot Deployments 7

5.3 Standards Efforts 7

5.4 Related Areas 7

6 Threat Analysis and Risk Assessment for Day-1 Applications 7

6.1 Identify Day-1 Applications 7

6.2 Identify Attackers 7

6.3 Perform TARA 7

6.4 Define Mitigation and Use-Cases 7

6.5 Derive Requirements 7

7 Application and Domain Specific Mitigation 7

8 Governance and Legal Framework 7

8.1 Governance aspects 7

8.2 Legal framework 7

9 Recommended Strategy 8

9.1 Algorithms 8

9.2 Developer Guidance 8

9.3 Proposed Next Steps 8

10 Conclusions and Recommendations 8

11 Annex <X>: Change history 8

# Foreword

Editor’s Note: the wording of this section has been adapted from the corresponding wording of a working group report. If 5GAA adopts a different wording to account for the existence of the ESP task force, the wording below will be changed accordingly.

This Technical Report has been produced by 5GAA.

The contents of the present document are subject to continuing work within the Task Force (TF) and may change following formal TF approval. Should the TF modify the contents of the present document, it will be re-released by the TF with an identifying change of the consistent numbering that all TF meeting documents and files should follow (according to 5GAA Rules of Procedure):

x-nnzzzz

1. This numbering system has six logical elements:
2. x: a single letter corresponding to the working group or task force:

where x =

T (Use cases and Technical Requirements)

B (Business Models and Go-To-Market Strategies)

A (System Architecture and Solution Development)

S (Standards and Spectrum)

P (Evaluation, Testbed and Pilots)

E (Efficient Security Provisioning task force)

1. nn: two digits to indicate the year. i.e. 16,17,18, etc
2. zzzz: unique number of the document
3. No provision is made for the use of revision numbers. Documents which are a revision of a previous version should indicate the document number of that previous version
4. The file name of documents shall be the document number. For example, document S-160357 will be contained in file S-160357.doc

# Introduction

This document defines terms, summarizes existing misbehaviour detection (MBD) approaches and related work, evaluates requirements for Day-1 V2X deployment and for Day-2 applications, identifies gaps, and proposes next steps on the path to a deployment-ready, robust MBD mechanism for the V2X communications networks.

This paper is organized as follows: A section on concepts, models and terms definitions, followed by an overview of related/existing work; a section dedicated to a Threat and Risk Assessment (TARA) and requirements for Day-1 applications, another on determination of application domain specific mitigation, and finally a conclusion section with recommendations for a strategy and next steps.

# Scope

In the context of this white paper, misbehaviour refers to the wilful or inadvertent transmission of incorrect data within the V2X network, both to a vehicle and the Misbehaviour Authority.

Note that the definition of “misbehaviour” is quite specific and narrow here, i.e., strictly related to incorrect content in V2X packets and misbehaviour reports, in contrast to the general literal meaning of misbehaviour as something outside of the norm, or specification.

Therefore, deliverables in scope are:

* List of published research on plausibility checks and misbehaviour detection algorithms running in on-board units (OBUs), road side units (RSUs) and mobile network operators (MNOs) network elements, based on the content of V2X messages only; highlight gaps that require further research, if any.
* List published research on plausibility and misbehaviour detection algorithms running in the Misbehaviour Authority (MA) based solely on the content of Misbehaviour Reports (MR); highlight gaps that required attention, if any.
* List of TARA or equivalent analysis for Day-1 C-V2X use cases; highlight cases that were not analysed, if any.
* Define a legal framework that defines which private information must be protected by the misbehaviour detection system.
* Define rules and criteria for flagging a device as misbehaving and taking appropriate enforcement actions, such as revocation.
* Define the list of high-level requirements and life-cycle diagram that any misbehaviour detection and reporting system must implement, based on the legal framework and gaps previously identified.

It is NOT in scope for this whitepaper:

* Physical, network or protocol layers misbehaviour (e.g. incorrect radio frequency, incorrect transmission rate)
* Certain cybersecurity attacks unrelated to message content (e.g. denial of service)
* Research, requirements, design or implementation of a misbehaviour detection system

This paper also considers technical and legal/liability (WG6) aspects. The paper also cooperates with applications (WG2) to understand V2X applications for the risk assessment and mitigation, as well as with WG4 for items that may affect standard organizations.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies.

[1] ETSI TR 103 460: “Intelligent Transport Systems (ITS); Security; Pre-standardization Study on Misbehavior Detection [Release 2]”, Jan 2020.

[2] Rens W. van der Heijden, Stefan Dietzel, Tim Leinmüller, Frank Kargl: "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems", IEEE Communications Surveys & Tutorials 2016 (arXiv:1610.06810v2 [cs.CR] 29 Nov 2018).

[3] Joseph Kamel, Ines Jemaa, Arnaud Kaiser, Loic Cantat, Pascal Urien. Misbehavior Detection in

C-ITS: A comparative approach of local detection mechanisms. Vehicular Networking Conference

(VNC), Dec 2019, Los Angeles, California, United States. hal-02400137

[4] CAMP “Vehicle-to-Vehicle Communications – Misbehavior Detection” ([Link](https://wiki.campllc.org/download/attachments/143491424/V2V-CR%20Final%20Report%20-%20Volume%202%20-%20MBD%20-%20Public%20Disclosure.pdf?version=1&modificationDate=1543300280197&api=v2))

[5] CAMP “Vehicle-to-Vehicle - Field Level Evaluation of Local Misbehavior Detection (LMBD) in a Controlled Environment” ([Link](https://wiki.campllc.org/download/attachments/143491424/V2V_SE_Field%20Level%20Evaluation%20of%20LMBD%20in%20a%20Controlled%20Environment%20-%20Public%20Disclosure.pdf?version=1&modificationDate=1550158974679&api=v2))

[6] “Misbehavior detection in C-ITS - Secure Cooperative Autonomous systems (SCA) project approach” SystemX @ C2C, 12 March 2019 ([Link](https://groupware.car-2-car.org/groupware/login.php?phpgw_forward=/index.php?documentid%3D7886%26menuaction%3Dmydms.uimydms.viewDocument))

[7] Steven So, Jonathan Petit, David Starobinski, “Physical Layer Plausibility Checks for Misbehavior Detection in V2X Networks”, WiSec, May 2019 ([Link](http://people.bu.edu/staro/WiSec2019_RSSI_MisbehaviorDetection_CameraReady.pdf))

[8] IEEE 1609.2.1 “IEEE Wireless Access in Vehicular Environments (WAVE) --Certificate Management Interfaces for End-entities”

[8] ETSI TR 102 638: “Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions V1.1.1”, June 2009

[9] ETSI TR 102 893: “Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA) V1.2.1”, March 2017

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

Many terms used in this document are explained in the WG2 document 5GAA\_A-170188\_V2XDEF\_TR, “5GAA V2X Terms and Definitions”. The following definitions also apply:

Editor’s Note: the line below is an example for formatting purposes. This section should be edited when the rest of the document is complete.

**example term:** example definition.

**Target of Evaluation:** the product or system that is the subject of the evaluation

## 3.2 Symbols

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

Symbol format (EW)

<symbol> <Explanation>

## 3.3 Abbreviations

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

APN Access Point Name

ASAP As soon as possible

BSA Basic Set of Applications

CA Certificate Authority

CRL Certificate Revocation List

C-V2X Cellular Vehicle-to-Everything

ECA Enrolment Certificate Authority

ETSI European Telecommunications Standards Institute

GAA Generic Authentication Architecture

GBA Generic Bootstrapping Architecture

IMSI International Mobile Subscriber Identity

IP Internet Protocol

ITS Intelligent Transport Services

PKI Public Key Infrastructure

RSU Roadside Unit

SCMS Subscriber Credential Management System

SIM Subscriber Identity Module

TVRA Threat, Vulnerability and Risk Assessment

TARA Threat Assessment and Remediation Analysis

ToE Target of Evaluation

UE User Equipment

USIM Universal Subscriber Identity Module

V2I Vehicle-to-Infrastructure

V2N Vehicle-to-Network

V2P Vehicle-to-Pedestrian

V2V Vehicle-to-Vehicle

V2X Vehicle-to-Everything

# 4 Model and Terms

This section describes the MBD model and terms.

## 4.1 Misbehaviour Model and Concepts

Information in V2X packets is being used by receiving vehicles to make safety critical decisions. It is therefore imperative that such information is correct and trustworthy, representing the true physical reality. Cryptographic techniques such as digital certificates and signatures are commonly used to ensure a receiver can verify that a transmitter has valid security credential and the received packets are indeed sent by the claimed transmitter without being tampered with. However, that is not enough to guarantee that the information in V2X packets is indeed correct and trustworthy. For example, digital certificates may be stolen and used by malicious attackers to impersonate the original certificate owner and launch attacks. Or the SW or FW of a legitimate V2X node may be compromised by attackers such that the payload of the V2X packets maybe maliciously modified to suit the attackers’ needs before being transmitted.



**Table 1**. Examples of possible misbehaviors, some are in scope and others are out of scope of the specific Misbehavior Detection addressed in this white paper.

For these reasons, the correctness of V2X messages cannot be guaranteed simply by verifying the digital certificate and signature. In the context of this white paper, misbehaviour refers to the wilful or inadvertent transmission of incorrect data within the V2X network. Note that the definition of “misbehaviour” is quite specific and narrow here, i.e., strictly related to incorrect content in V2X packets, in contrast to the general literal meaning of misbehaviour as something outside of the norm, or specification. For example, **Table 1** lists a number of behaviours that are outside of the governing specifications for a V2X node, but many of them have nothing to do with the content of the packets and hence are not considered in scope for the context of this white paper.

Note that incorrect information in V2X packets could be caused by a number of circumstances, including but not limited to the malicious attacks discussed earlier. Faulty on-board components, or temporary malfunction of a sensor such as GPS not working when inside a tunnel, or cameras failing to detect objects in poorly lit condition, could result in misbehaving packets as well. Whatever the cause or motivation, the net effect is the same – the information sent out in a V2X packet is substantially different from the physical reality that it is beyond the nominal margin of error considered acceptable by the industry.

To address such concern, the general approach is to first detect such misbehaviour locally by receivers of such misbehaving packets. This process is called Local MBD (LMBD). Some of these misbehaviours may also be reported to a central authority in the Public Key Infrastructure (PKI) called Misbehaviour Authority (MA). MA may investigate and corroborate such reports and the process is called Global MBD (GMBD). If deemed necessary, the certificates used by the misbehaving node (and all the future certificates that would have been used by it) may be identified and revoked to permanently remove the negative influence of such node from the network.

Misbehaviour detection and report maybe done by any V2X node receiving a suspicious packet, such as an OBU in a vehicle or an RSU.

V2X messages contain the full V2X networking stack, from layer 1 (Wireless PHY) to layer 7 (Specific V2X Applications). Many of such messages are periodic in nature while others are event-triggered. Misbehaviour could mean incorrect information in any layer in the stack, but the primary concern would be the semantic content in the application payload of the packets. Therefore, misbehaviour detection could be done in each of these layers, or at least could leverage all the information available at these layers. For example, RF properties in the PHY layer may provide important clues that are harder to be tampered with than applications payload and so could be used to assist misbehaviour detection at the higher layer. On the other hand, misbehaviour at the application layer may be very specific to each application. For example, a traffic light management system using V2X may exhibit its own misbehaviour that is entirely different than a platooning application.

Many V2X applications may be built on top of common V2X messages. For example, periodic broadcast of Basic Safety Messages (BSM) or Cooperative Awareness Messages (CAM) enable a broad set of safety applications such as Left-Turn Assist, Lane Change Warning, Emergency Brake Warning, etc. Therefore, misbehaviour detection for BSM/CAM may be considered a common service, such as at Facility Layer in ETSI architecture, offered to benefit a broad set of applications.

## 4.2 Terms

* Directly related to MBD: Plausibility check, local misbehaviour detection, global misbehaviour detection, MBD report,
* Supporting MBD: Checks in applications, checks in network stack, checks in computing platform, checks in RA and PCA, checks in OU/RSU computing platform
* Definition: What constitutes misbehaviour

## 4.3 Attacker Model and Security Objectives

Generally speaking, two kinds of attackers are of concerns in the context of MBD for V2X networks. The first kind of attackers are internal attackers, i.e., malicious or faulty V2X nodes with necessary hardware, software and valid V2X credentials that allow them to inject bogus information into the V2X network at will to other unsuspecting nodes. If other nodes accept such bogus information without question, it may negatively affect the safety and efficiency of the overall traffic in the attackers’ single or multi-hop communication range. The other kind of attackers are external attackers who can manipulate the environment to cause sensor malfunction or misreading. Both of these active attackers are capable of causing incorrect information in V2X packets.

To illustrate more concretely how these two kinds of attackers can mount attacks to cause undesirable misbehaviour, i.e., incorrect information in V2X packets, categorization of most serious active attacks is described in more details below. This is not meant to be an exhaustive list of attacks. A few attacks that are commonly discussed in networking security literature but are not in scope of this discussion are also called out to further distinguish the specific threats concerned by MBD.

* Masquerade Attacks: An attacker may obtain valid security credentials such as digital certificates by some means (e.g., from illegal marketplace that sells stolen security credentials) and then use them with a HW/SW/FW platform that is under their control and capable of V2X communications with other legitimate V2X nodes. Because the platform is fully under attacker’s control, it can generate whatever V2X packets to suit their needs and so the entire V2X packets can be full of bogus information. The platform itself usually would have wireless communication capability to transmit and receive standard V2X packets. But the platform may not be a vehicle or RSU at all. Such platform may be physically stationary or mobile, for example, even if it impersonates a vehicle by using a vehicle’s digital certificates.
  + Sybil Attacks: Sybil attacks are launched by an attacker to emulate multiple or even a large number of devices by concurrently using many certificates which are valid for a given time period. This attack may be launched to create a fleet of ghost vehicles, or to subvert a reputation system of a [network service](https://en.wikipedia.org/wiki/Network_service) by exerting a disproportionately large influence.
* Data Manipulation Attacks: Instead of setting up a full platform with HW/SW/FW as in the case of Masquerade Attack, an attacker can also just attempt to compromise some part of a victim’s platform by exploiting some vulnerabilities such that it can manipulate some part of the content of the V2X packet. This kind of attacks can be launched via numerous kinds of entry points because the entire attack surface of a vehicle or RSU can be exploited for that purpose, and so can be further broken into several notable sub-categories as discussed below.
  + Internal Sensor Spoofing Attacks: A message is manipulated by changing the actual internal sensor readings. For example, this can be done via malware injected into certain part of the SW/FW stack so that some fields in the V2X packets are manipulated.
  + External Sensor Spoofing Attacks: This sub-category of attacks creates interference with input from sensors that report external circumstances, e.g., GPS spoofing attack has been demonstrated from a car following a victim vehicle, and this would result in bogus GPS locations in the V2X packets sent by the victim.
  + Replay Attacks: An attacker may record packets from a legitimate node and repeat it sometime later. If it simply repeats the packet without any modification, it may be too easy to identify because V2X packets would have timestamps that would give it away quickly. But the attacker may be able to manipulate some of it such as the timestamp and make it harder to detect. Such attacks could be considered as a special case of Data Manipulation Attacks.
  + Wormhole/tunnel attacks: A message from one geographic location is transmitted at a different geographic location by an attacker. This is easy to detect for messages such as BSM/CAM beacons with absolute location data, but maybe less obvious for other application messages that do not bear such location fields.

The common nature of these Data Manipulation Attacks is that the attacker may be able to manipulate some part of the payload but not others (for example, GPS spoofing affects all the fields related to or derived from GPS, but not others).

* Denial of Service (DoS) Attacks: DoS can be launched by a node to exhaust a network resource so that the system stops responding or functioning properly. A naïve but easy to detect example would be for a node to generate and transmit fully formed messages at very high rate to potentially congest the channel and overload the network. This is done at the application layer and is relatively easy to detect. DoS can also be launched at the physical layer such as jamming attack. Because DoS in general does not manifest itself as incorrect data in V2X packets, it is not considered in scope of this white paper.

It is concerning if an attacker launches such attack in one locale and targets one or two victims, but if any of these attacks are launched at scale across a larger geographic area against many victims, the impact would be devastating. So misbehaving entities in the V2X network must be considered a dangerous threat and it is the responsibility of misbehaviour detection to detect, report and mitigate this threat as much as possible. While the ultimate mitigation would be to identify and revoke the truly misbehaving entities by the MA, the impact of such misbehaving V2X packets should also be mitigated locally by each V2X receiver.

On the other hand, it is important to recognize that most MBD algorithms are not 100% bullet proof, so non-zero false positive and false negative are to be expected. False positives cause a non-misbehaving node to be falsely accused of misbehaviour and hence negatively impacted in the system, from its messages being dropped to its certificates being revoked wrongfully. False negatives are real misbehaviours being missed and hence malfunctioned sensors or worse yet malicious attacks being undetected. Often MBD algorithms can be tuned to balance the overall impact of false positives and false negatives when careful considerations are given to the consequences in each case.

In addition, MBD itself also introduces new attack surface into V2X system and expose new attack vectors such as the following:

* **Slander Attacks**: False misbehaviour reports are purposefully created about non-misbehaving devices and reported to the MA to discredit the victims which may lead to the victims’ certificates being wrongfully revoked. This could also be done by combining with Sybil attacks to appear as multiple coordinated reporters.
* **Denial of Service Attacks against the MA**: An attacker can overload MA by just sending bogus MB reports that would force the MA to analyse each report and waste communication and computing resource. This is especially impactful if combined with Sybil attacks to scale up the load against MA.
* **Evasion Attacks**: Once a specific MBD algorithm is known to be used, an attacker may also exploit the specifics of the algorithm to evade the detection, for example, to keep the offset of the misinformation from the ground truth under certain threshold so to avoid detection, or purposefully inject noise to cause a Machine Learning (ML) algorithm to fail for ML-based MBD system.

While the above attacks are not the primary concern of MBD itself, they may introduce new kinds of vulnerability into the entire V2X network. Therefore, it is important and necessary to design MBD and reporting with robust protection against these new attacks. For example, accountability on the reporters may help mitigate against Slander Attacks and DoS against the MA. However, this must be balanced with the privacy concerns such that reporters’ privacy is not significantly compromised compared with non-reporters and so that reporters are not being penalized inadvertently.

In summary, the following security objectives should be achieved by incorporating misbehaviour detection into every V2X receiver (vehicle or RSU):

* Detect misbehaviour in all V2X packets and filter out these packets to reduce the potentially negative impact locally and in real time
* Report non-transient misbehaviour to MA to assist in revoking of misbehaviour entities from the network permanently
* Ensure the addition of MB detection and reporting does not introduce significant new security and privacy risks to the V2X system

# 5 Related Works

This section summarizes published research on V2X misbehaviour detection.

This section also highlights gaps in the current research for misbehaviour scenarios that are in scope of this document.

## 5.1 Current Research

### 5.1.1 Detection approaches

#### 5.1.1.1 False beacon information detection

1. Physical layer detection
2. Data-centric detection
3. Machine-learning based detection
4. Neighbour list exchange
5. Additional information exchange
6. Path history detection mechanisms
7. RSU pseudonym linkability

#### 5.1.1.2 False warning detection

1. Data-centric detection
2. Voting-based detection

#### 5.1.1.3 Node trust evaluation

1. Reputation-based methods
2. Cooperative trust establishment
3. Data-centric trust evaluation
4. Local pseudonym linking

### 5.1.2 Reporting approaches

#### 5.1.2.1 Unicast MR to the misbehaviour authority

#### 5.1.2.2 Broadcast MR to neighbours: pros, cons and alternatives

## 5.2 Gaps in Current Research

# 6 Threat Analysis and Risk Assessment for Day-1 Applications

This section lists existing threat analysis for Day-1 applications as defined by ETSI and identifies gaps in the analysis (e.g. use cases that were not analysed).

The threat analysis can be TARA or equivalent.

## 6.1 Identify Day-1 Applications

* Start with ETSI definition
* Work with WG2.for additional use cases not covered by ETSI, if any

ETSI TR 102 638 defines day-1 use cases, also called Basic Set of Applications (BSA). The table below summarizes applications classified as BSA:

|  |  |  |
| --- | --- | --- |
| **Applications Class** | **Application** | **Use case** |
| Active road safety | Driving assistance -  Co-operative awareness | Emergency vehicle warning |
| Slow vehicle indication |
| Intersection collision warning |
| Motorcycle approaching indication |
| Driving assistance - Road Hazard Warning | Emergency electronic brake lights |
| Wrong way driving warning |
| Stationary vehicle - accident |
| Stationary vehicle - vehicle problem |
| Traffic condition warning |
| Signal violation warning |
| Roadwork warning |
| Collision risk warning |
| Decentralized floating car data - Hazardous location |
| Decentralized floating car data - Precipitations |
| Decentralized floating car data - Road adhesion |
| Decentralized floating car data - Visibility |
| Decentralized floating car data - Wind |
| Cooperative traffic efficiency | Speed management | Regulatory / contextual speed limits notification |
| Traffic light optimal speed advisory |
| Co-operative navigation | Traffic information and recommended itinerary |
| Enhanced route guidance and navigation |
| Limited access warning and detour notification |
| In-vehicle signage |
| Co-operative local services | Location based services | Point of Interest notification |
| Automatic access control and parking management |
| ITS local electronic commerce |
| Media downloading |
| Global internet services | Communities services | Insurance and financial services |
| Fleet management |
| Loading zone management |
| ITS station life cycle  management | Vehicle software / data provisioning and update |
| Vehicle and RSU data calibration. |

## 6.2 Identify Attackers

## 6.3 Identify threats and risk analysis

Work with WG2.

ETSI TR 102 893 describes the Threat, Vulnerability and Risk Analysis (TVRA) used by ETSI

It defines 5 security objectives for ITS:

* Confidentiality
* Integrity
* Availability
* Accountability
* Authenticity

It also identifies 2 potential Targets of Evaluation (ToE):

1. A single vehicle
2. A single roadside unit

For each ToE and security goal, ETSI TR 102 893 identifies one or more threat groups and assigns a score for the risk and impact of each threat. The table below summarizes the scores identified in the document for vehicle

<<Insert summary table>>

And the next table does the same for roadside units:

<<Insert summary table>>

ETSI TR 102 893 does recognize the actions of both malicious agents as a threat; however, it does not include the threats to the Misbehavior Authority as a Target of Evaluation.

## 6.4 Recommendations

## Recommend use case prioritization and highlight the use cases not covered.

# 7 Application and Domain Specific Mitigation

Include experts from other domains to add more checks and strategies, and collect feedback.

Especially consider standard checks in OBU/RSU system, network stack, V2X stack, etc., as input to MBD.

Cross-work item with WG2.

# 8 Governance and Legal Framework

## 8.1 Governance aspects

## 8.2 Legal framework

# 9 Recommended Strategy

## 9.1 Algorithms

Recommend algorithms needed for plausibility checks, local, and global MBD. Highlight gaps where more research is needed.

## 9.2 Developer Guidance

Guidance for V2X systems, communication, and application developers to support MBD

## 9.3 Proposed Next Steps

Call to action. Liaise with ETSI.

# 10 Conclusions and Recommendations

Editor’s Note: This section will summarise any conclusions and recommendations, but it may not be needed.

# 11 Annex <X>: Change history

This is the last annex for TRs which details the change history using the following table.

This table can be used for recording progress during the WG drafting process till WG approval of this TR.

Date: use format YYYY-MM

Subject/Comment:

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Meeting** | **TDoc** | **Subject/Comment** |
| 2020-02-05 | F2F#13 | E-200008 | Initial version |
| 2020-05-12 | Online #14 | E-200008-revised | Updates to align with WI description, including adding a section on governance. |