|  |
| --- |
| 3GPP TR 33.851 V0.1.0 (2020-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security for enhanced support of Industrial Internet of Things (IIoT); (Release 17) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.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.© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Architectural considerations 7

4.1 Rel-16 reference architecture 7

4.2 Rel-17 enhancements for time synchronization 7

5 Key issues 8

5.1 Key issue#1: Security for time synchronization messages 8

5.1.1 Key issue details 8

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key issue #2: Multiple TSN working domains 8

5.2.1 Key issue details 8

5.2.2 Threats 9

5.2.3 Potential security requirements 9

5.3 Key Issue #3: Protection of UE-UE TSC communication 9

5.3.1 Key issue details 9

5.3.2 Security threats 9

5.3.3 Potential security requirements 10

6 Solutions 10

6.A Solution #A: 10

6.A.1 Introduction 10

6.A.2 Solution details 10

6.A.3 Evaluation 10

7 Conclusions 10

Annex <X> (informative): Change history 10

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The present document studies the security impact of time sensitive communication aspects in Industrial IoT based on FS\_IIoT study in TR 23.700-20 [4] and the architecture described in 3GPP TS 23.501 [3].

# 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501 "Security architecture and procedures for 5G System".

[3] 3GPP TS 23.501 "System architecture for the 5G System (5GS)".

[4] 3GPP TR 23.700-20 "Study on enhanced support of Industrial Internet of Things (IIoT) in the 5G System (5GS)".

[5] IEEE 802.1Qcc "IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks -- Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[6] IEEE 1588-2008 "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems".

[7] RFC 7384 "Security Requirements of Time Protocols in Packet Switched Networks".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or abbreviations.

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5G Fifth Generation

5GS Fifth Generation System

ARP Address Resolution Protocol

BMCA Best Master Clock Algorithm

CNC Centralized Network Configuration

CP Control Plane

CUC Centralized User Configuration

DS-TT Device Side Translator

DoS Denial of Service

gPTP generalized Precision Time Protocol

IIoT Industrial Internet of Things

IP Internet Protocol

KI Key Issue

Ln Layer n

MAC Media Access Control

NW-TT Network Side Translator

PTP Precision Time Protocol

TSC Time Sensitive Communication

Rel Release

UE User Equipment

TSN Time Sensitive Networking

TSN AF TSN Application Function

UPF User Plane Function

UP User Plane

# 4 Architectural considerations

##  4.1 Rel-16 reference architecture

The 5G TSC service is described in 3GPP TS 23.501 [3]. It allows the 5G System to be integrated transparently as a bridge in an IEEE TSN network [5], where the 5GS system acts as one or more TSN Bridges of a TSN network with DS-TT and NW-TT introduced in Rel-16 to transparently process and transfer UP TSN messages.

TSN AF is used to configure the 5GS on CP via a CNC. Only the fully centralized model is supported in Rel-16. gPTP is used for time synchronization. In Rel-16, only downlink time synchronization has been addressed, with the GM clock being always on the NW-TT/UPF side.

The security for the TSC service is addressed in 3GPP TS 33.501 [2] Annex L.

## 4.2 Rel-17 enhancements for time synchronization

TR 23.700-20 [4] is studying several enhancements in Rel-17 for the centralized model:

- PTP support, a time-synch protocol based on IP

- Support for uplink time synchronization for gPTP and PTP

- Support for multiple TSN clock domains UE-to-UE communication

- Exposure of TSC capabilities of the 5GS using the NEF framework

# 5 Key issues

## 5.1 Key issue#1: Security for time synchronization messages

### 5.1.1 Key issue details

Time synchronisation is essential for the 5GS providing the TSC service. The time synchronisation mechanisms for the 5GS as IEEE bridge in TSN are shown in the figure of clause 5.27 in 3GPP TS 23.501 [3].

The time synchronisation messages (i.e., PTP or gPTP messages) are used for establishing a common time. They are transmitted in the 5GS user plane between the ingress and egress boundaries involving the DS-TT, the UE, the gNB, the UPF and the NW-TT. The main difference between the UL and DL time synchronisation is that in case of the UL time synchronisation, the messages can be

- either processed and forwarded to a TSN end station or another TSN bridge via NW-TT on network side, or

- processed and forwarded via DS-TTs on the UE side

For delivery of time synchronisation messages, the UPF will forward the UL time synchronisation messages transparently via DS-TT. The DS-TT in the other UE can exactly perform the operations as defined in 3GPP TS 23.501, clause 5.27.1.2.2 [3].

Note, time synchronisation messages are not protected by default in TSN systems. Thus, time synchronisation messages need to be protected in UL and DL, when transferred over a 5GS bridge.

### 5.1.2 Security threats

The intrinsic timing aspects that a 5GS Bridge as a TSN Bridge need to support may provide ground for vulnerabilities like:

- Blocking the deterministic transmission with strict latencies boundaries.

- Manipulation of the clock synchronization between NW elements (Master/Slave) and with global time reference (Grand Master).

- Manipulation of Time aware Scheduling and traffic shaping.

- Manipulation to the selection of communication paths and reservation of bandwidth and time slots

### 5.1.3 Potential security requirements

The transfer of time synchronization message shall be integrity and replay protected.

The sender and recipient of time synchronisation messages shall be mutually authenticated.

## 5.2 Key issue #2: Multiple TSN working domains

### 5.2.1 Key issue details

3GPP Rel-16 included support for multiple TSN working domains. DS-TT and NW-TT are required to determine to which working domain an incoming or outgoing communication belongs. This is implemented by a specific *domainNumber* (3GPP TS 23.501 [3], clause 5.27.1.3).

Downlink Time Sync is considered in Rel-16 (TS 23.501 [3], clause 5.27.1.3), such that multiple gPTP messages are sent transparently in the UP to the UE/DS-TT for all cases of Time Domains identified by the IE '*domainNumber*'. This allows any integrity and replay protected TSN bridge to transfer time synchronisation messages to another TSN bridge. This KI is to further study how to protect the 5GS acting as a TSN bridge being accessed by an unauthorized TSN bridge. I.e., a compromised TSN node may send a tampered domainNumber to access other than the intended TSN working domains.

### 5.2.2 Threats

A compromised TSN node (a non-5GS bridge) may send a tampered *domainNumber* to access other domains than the intended TSN working domains (i.e. the 5GS bridge).

TSN domains not verifying the *domainNumber* parameter by any means may be vulnerable to spoofing attacks:

A malicious node may send a tampered *domainNumber* parameter to access other than the intended TSN working domains. This may lead to unauthorized access to the (g)PTP communication within a TSN working domain. This attack may be the initial attack vector for further exploitation, such as rogue master clock attacks and (g)PTP message spoofing.

The impact of this attack may be DoS, accuracy degradation and false times being synchronized.

### 5.2.3 Potential security requirements

TBD

## 5.3 Key Issue #3: Protection of UE-UE TSC communication

### 5.3.1 Key issue details

KI#2 from TR 23.700-20 [4] aims to address UE-UE TSC communication if the network determines that the two UE(s) (including two DS-TT(s) within the same UE) are served by the same UPF. In the candidate solutions, one or more SMFs are used to handle the UE-UE communication. The security protection for the two legs may be determined by the same or different SMFs.

Editor's Note: FFS if security consistency between two legs is needed.

Editor's Note: This KI requires an update of the SID scope.



Figure 5.3.1: UE-UE TSC communication

NOTE: In the above figure, the two UEs can be served by a single NG-AN node or two different NG-AN nodes.

### 5.3.2 Security threats

If the security protection for the one leg or two legs lacks confidentiality, integrity and replay protection, it will be possible for an attacker to eavesdrop, modify data and replay packets. UE-UE TSC communication is vulnerable to several attacks. For example:

- Spoofing: A malicious node may attempt to deceive a receiver by sending fake messages. These spoofed messages may lead the receiver to perform the unexpected actions.

- Replay attack: an attacker eavesdrops on the UE-UE TSC communication, intercepts it, and then fraudulently delays or resends it to misdirect the receiving UE.

- DoS attacks: an attacker may spoof UE through modifying data to prevent (g)PTP communication (DoS).

### 5.3.3 Potential security requirements

TBD

# 6 Solutions

## 6.A Solution #A:

### 6.A.1 Introduction

### 6.A.2 Solution details

### 6.A.3 Evaluation

# 7 Conclusions

TBD

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 21.08.2020 | SA3#100-e | S3-202101 |  |  |  | Skeleton | 0.0.0 |
| 24.08.2020 | SA3#100-e | S3-202102 |  |  |  | Scope of study | 0.1.0 |
| 24.08.2020 | SA3#100-e | S3-202103 |  |  |  | References | 0.1.0 |
| 24.08.2020 | SA3#100-e | S3-201586 |  |  |  | Abbreviations | 0.1.0 |
| 24.08.2020 | SA3#100-e | S3-202105 |  |  |  | Architectural considerations | 0.1.0 |
| 24.08.2020 | SA3#100-e | S3-202106 |  |  |  | Multiple TSN working domains | 0.1.0 |
| 24.08.2020 | SA3#100-e | S3-202118 |  |  |  | New key issue on security for uplink time synchronization | 0.1.0 |
| 24.08.2020 | SA3#100-e | S3-202126 |  |  |  | New Key Issue on protection of UE-UE communication | 0.1.0 |