|  |
| --- |
| 3GPP TR 33.882 V0.2.0 (2022-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on personal IoT networks security aspects(Release 18) |
|   |
|  | 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.© 2022, 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

1 Scope 6

2 References 6

3 Definitions of terms and abbreviations 6

3.1 Terms 6

3.2 Abbreviations 7

4 Assumptions 7

5 Key issues 7

5.1 Key Issue #1: Authentication and authorization for PINE 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Authorization of PIN capabilities 7

5.2.1 Key issue details 7

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

6 Proposed solutions 8

6.1 Mapping of solutions to key issues 8

6.A Solution #A: <Title> 8

6.A.1 Introduction 8

6.A.2 Solution details 8

6.A.3 Evaluation 8

7 Conclusions 9

Annex A (informative): Change history 9

# 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.

# 1 Scope

The present document studies how 5G security architecture and procedures can be enhanced to support Personal IoT Network. The aim of this document is to study the security aspects of Personal IoT Networks for any potential enhancements in alignment with the outcome of SA2 study in TR 23.700-88 [2]. The study will look at the following aspects, performing gap analysis where necessary:

1) Study potential security enhancements for authentications required to secure Personal IoT Networks.

2) Study the security protection and access control for communications required to secure Personal IoT Networks.

3) Study the security enhancements for privacy required to secure Personal IoT Networks.

4) Other security aspects for any potential enhancements in alignment with the outcome of SA2 study in TR 23.700-88 [2].

# 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 TR 23.700-88: "Study on Personal IoT Networks"

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

# 3 Definitions of terms and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1], 3GPP TR 23.700-88 [2], 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].

For the purposes of the present document, the following terms and definitions given in TR 23.700-88 [2] apply:

**Personal IoT Network:** A configured and managed group of PIN Element that are able to communicate each other directly or via PIN Elements with Gateway Capability (PEGC), communicate with 5G network via at least one PEGC, and managed by at least one PIN Element with Management Capability (PEMC).

**PIN Element:** A UE or non-3GPP device that can communicate within a PIN (via PIN direct connection, via PEGC, or via PEGC and 5GC), or outside the PIN via a PEGC and 5GC.

**PIN Element with Gateway Capability:** A PIN Element with the ability to provide connectivity to and from the 5G network for other PIN Elements, or to provide relay for the communication between PIN Elements.

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1], 3GPP TR 23.700-88 [2], 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].

PIN Personal IoT Networks

PINE PIN Element

PEGC PIN Elements with Gateway Capability

AF Application Function

API Application Programming Interface

NEF Network Exposure Function

QoS Quality of Service

URSP UE Route Selection Policy

# 4 Assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

# 5 Key issues

## 5.1 Key Issue #1: Authentication and authorization for PINE

### 5.1.1 Key issue details

A key aspect of the planned support of the 5G system for PIN is the ability of a UE (referred to as PEGC) to act as a gateway for PIN elements (PINEs), which are not acting as 5G UEs, to connect to 5GC.

According to TR 23.700-88 [2], a PINE without 3GPP capability cannot directly connect to the 5GC, but through the PEGC. Whether the PINE without 3GPP capability needs to be known by the 5GC and how to identify the PINE needs to be studied, e.g., for controlling access of the PINE to connecting 5G data networks, differentiating the PINE for policy provisioning, authorizing the PINE for traffic relay, etc.

### 5.1.2 Security threats

5GS supports the policy and QoS differentiation for the traffic between a PINE and 5GS. The network resource may be misused by the malicious, unauthenticated, and unauthorized PINE.

### 5.1.3 Potential security requirements

The PINE in a Personal IoT network should be authenticated.

The PINE in a Personal IoT network should be authorized.

Editor’s note: Further requirements might be added if found.

## 5.2 Key Issue #2: Authorization of PIN capabilities

### 5.2.1 Key issue details

Some aspects of a PIN network might be configurable by an Application Function through the 5G NEF, for instance (depending on details defined in the SA3 study on PIN [2]) QoS of a PIN Element or URSP rules related to a PIN Element.

From a security point of view the scope of access granted to an AF needs to be restricted to the level of certain PEGSs or PINs and needs to be subject to permissions and consent granted by resource owners.

So far TS 33.501 [3] defines authorization of exposure capabilities on a rather general level in Clause 12. That is, authorization is based on operator policies using the identity of the AF (clause 12.2 in TS 33.501 [3]) as well as the OAuth authorization mechanism (Clause 12.4 in TS 33.501 [3]). No details about handling of permissions or providing consent to a specific application function are defined.

In case of PIN the requirements for API security might be especially demanding, since on the one hand a PIN network might consist of several UEs and on the other hand a single UE might contribute to several PINs.

Therefore, aspects related to ownership and possible operation models of PINs shall be included in the analysis of the Key issue.

### 5.2.2 Security threats

An application function associated with one PIN might use the NEF API to manipulate another PIN.

An application function associated with a PIN might use the NEF API to manipulate resources not assigned to the PIN.

### 5.2.3 Potential security requirements

The 5GS shall be able to restrict resource request from an Application Function associated with a PIN to the resources associated with the PIN.

Application functions associated with a PIN shall be able to use APIs for accessing resource only with authorization from the resource owner.

# 6 Proposed solutions

## 6.1 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.A Solution #A: <Title>

### 6.A.1 Introduction

### 6.A.2 Solution details

### 6.A.3 Evaluation

# 7 Conclusions

Editor's Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107-e-Ad Hoc | S3-221502 |  |  |  | Skeleton | 0.0.0 |
| 2022-06 | SA3#107-e-Ad Hoc | S3-221504 |  |  |  | Scope of TR 33.882 | 0.1.0 |
| 2022-06 | SA3#107-e-Ad Hoc | S3-221676 |  |  |  | KI on Authentication and authorization for PINE | 0.1.0 |
| 2022-08 | SA3#108-e | S3-221892 |  |  |  | Add terms and abbreviations | 0.2.0 |
| 2022-08 | SA3#108-e | S3-222343 |  |  |  | New Ki related to authorization of exposed PIN capabilities | 0.2.0 |
| 2022-08 | SA3#108-e | S3-222374 |  |  |  | Add threat and requirement to PINE authentication | 0.2.0 |