|  |
| --- |
| 3GPP TR 33.766 V0.2.0 (2024-05) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on security aspects of energy savings in 5G (Release 19) |
|   |
|  |  |
| 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.© 2024, 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, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview 7

5 Architecture and security assumptions 7

6 Key issues 7

6.1 Key Issue #1: Security aspects of collecting energy related information. 7

6.1.1 Key issue details 7

6.1.2 Security threats 7

6.1.3 Potential security requirements 7

6.2 Key Issue #2: Security aspects of exposure of energy related information. 7

6.2.1 Key issue details 7

6.2.2 Security threats 8

6.2.3 Potential security requirements 8

6.X Key Issue #X: <Key Issue Name> 8

6.X.1 Key issue details 8

6.X.2 Threats 8

6.X.3 Potential security requirements 8

7 Solutions 8

7.0 Mapping of Solutions to Key Issues 8

7.1 Solution #1: Solution reusing existing interfaces and security mechanisms for energy related information collection 9

7.1.1 Introduction 9

7.1.2 Solution details 9

7.1.3 Evaluation 9

7.2. Solution #2: Mutual authentication and NEF-AF interface protection for exposing energy related information 9

7.2.1 Introduction 9

7.2.2 Solution details 9

7.2.2.1 Mutual authentication 9

7.2.2.2 Protection of NEF-AF interface 9

7.2.3 Evaluation 9

7.Y Solution #Y: <Solution Name> 10

7.Y.1 Introduction 10

7.Y.2 Solution details 10

7.Y.3 System impact 10

7.Y.4 Evaluation 10

8 Conclusions 10

Annex <X> (informative): Change history 11

# 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 the security and privacy aspects of energy savings. More especially the document will:

* Identify key issues concerning the privacy and security aspects of collecting energy related information.
* Identify key issues concerning the privacy and security impacts of exposure of energy related information.
* If required, develop solutions addressing the identified key issues.

# 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 23.700-66: "Study on Energy Efficiency and Energy Saving".

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

[4] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

# 3 Definitions of terms, symbols and 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].

<ABBREVIATION> <Expansion>

# 4 Overview

Editor’s Note: This clause includes the overview applicable for the study.

# 5 Architecture and security assumptions

The following architecture and security assumptions are applied to the study:

- Security mechanisms applied for energy saving in this study are based on the architecture assumptions and requirements as described in TR 23.700-66 [2].

# 6 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 6.1 Key Issue #1: Security aspects of collecting energy related information.

### 6.1.1 Key issue details

TR 23.700-66 [2] studies the collection of energy related information for potential exposure.

The integrity and confidentiality of the data collected is of importance to produce correct analytics metrics.

Another aspect of collecting energy related information is the granularity at which it’s collected. Further information on the granularities can be found in TR 23.700-66 [2].

The key issue aims to address the security issues, ensuring integrity and confidentiality of the energy related information collected.

Editor’s Note: Further details are FFS.

### 6.1.2 Security threats

Lack of confidentiality, integrity, and replay protection in collecting energy related information can lead to disclosure of the information and tampering of the information.

Editor’s Note: Further security threats are FFS.

### 6.1.3 Potential security requirements

The data in transit shall support confidentiality, integrity, and replay protection.

Editor’s Note: Further requirements are FFS.

## 6.2 Key Issue #2: Security aspects of exposure of energy related information.

### 6.2.1 Key issue details

The key issue aims to address the security issues related to exposure of energy related information studied in TR 23.700-66 [2].

Authentication and authorization are key aspect of securing exposure of network energy-related data, including consumption, efficiency to external consumers as per KI#1 in TR 23.700-66 [1]. This key issue focus on investigating authorization methods for exposure.

Editor’s note: Privacy aspects of exposure of energy related information is FFS.

Editor’s note: Further details are FFS.

### 6.2.2 Security threats

Potential security threat:

If energy related information is leaked in transit, sensitive information may be disclosed.

Having no authorization or enough level access control can lead to information leakage to authenticated AF’s.

Editor’s note: Further security threats are FFS.

### 6.2.3 Potential security requirements

The exposed energy related information shall be integrity and confidentiality protected.

The producer and consumer of energy related information shall mutually authenticate.

The 5GS should support authorization mechanism for the exposed energy related information.

The 5GS should enable granular level access control to be able to restrict and control the flow of energy related information.

Editor’s note: Further requirements are FFS.

## 6.X Key Issue #X: <Key Issue Name>

### 6.X.1 Key issue details

### 6.X.2 Threats

### 6.X.3 Potential security requirements

# 7 Solutions

## 7.0 Mapping of Solutions to Key Issues

Editor's note: This clause describes the mapping between solutions and key issues.

Table 6.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues |
| --- | --- |
| X |

## 7.1 Solution #1: Solution reusing existing interfaces and security mechanisms for energy related information collection

### 7.1.1 Introduction

The proposed solution addresses the security requirement (confidentiality, integrity, and replay protection for data-in-transit) in key issue #1: "Security aspects of collecting energy related information.".

### 7.1.2 Solution details

According to clause 13.1 of TS 33.501 [1], all network functions shall support TLS and HTTPS with mutual authentication. Network functions can guarantee that data-in-transit is protected by an encrypted connection and is only sent to other authenticated network functions by implementing the protection principles outlined in clause 13.1 of TS 33.501 (thereby protecting data-in-transit hop-by-hop).

The solution can inherit the protection principles from clause 13.1 of TS 33.501 to address the security requirement in KI#1.

### 7.1.3 Evaluation

Editor’s Note: Evaluation is FFS.

## 7.2. Solution #2: Mutual authentication and NEF-AF interface protection for exposing energy related information

### 7.2.1 Introduction

This pCR introduces a new solution for KI#2 for mutual authentication and NEF-AF interface protection for EE information exposure for the study TR 33.766 [2].

### 7.2.2 Solution details

#### 7.2.2.1 Mutual authentication

Clause 12.2 of TS 33.501 [3] highlights the needs for authentication between NEF and an AF that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates is performed between the NEF and AF using TLS.

Certificate based authentication follows the profiles given in 3GPP TS 33.310 [4], clause 6.1.3a. The identities in the end entity certificates is used for authentication and policy checks.

#### 7.2.2.2 Protection of NEF-AF interface

Clause 12.3 of TS 33.501 [3] TLS is used to provide integrity protection, replay protection and confidentiality protection for the interface between the NEF and the AF. The support of TLS is mandatory.

Security profiles for TLS implementation and usage follows the provisions given in clause 6.2 of TS 33.210 [4].

### 7.2.3 Evaluation

The solution resuses Clause 12.2 and Clause 12.3 of TS 33.501 [3] without any change or enhancement.

Editor’s note: Further evaluation are FFS

## 7.Y Solution #Y: <Solution Name>

### 7.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 7.Y.2 Solution details

### 7.Y.3 System impact

### 7.Y.4 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 8 Conclusions

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

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04 | SA3#115 Adhoc-e | S3-241541 |  |  |  | TR Skeleton | 0.0.0 |
| 2024-04 | SA3#115 Adhoc-e | S3-241654 |  |  |  | Included changes from S3-241542, S3-241546, S3-241544, S3-241547 | 0.1.0 |
| 2024-05 | SA3#116 | S3-242606 |  |  |  | Included changes from S3-242576, S3-242577, S3-242578, S3-242579 | 0.2.0 |