|  |  |
| --- | --- |
| 3GPP TR 33.766 V0.7.0 (2025-02) | |
| 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 address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://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 members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Architecture and security assumptions 8

5 Key issues 8

5.1 Key Issue #1: Security aspects of collecting energy related information. 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: Security aspects of exposure of energy related information. 8

5.2.1 Key issue details 8

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

6 Solutions 9

6.0 Mapping of Solutions to Key Issues 9

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

6.1.1 Introduction 9

6.1.2 Solution details 9

6.1.3 Evaluation 10

6.2 Solution #2: Mutual authentication and NEF-AF interface protection for exposing energy related information 10

6.2.1 Introduction 10

6.2.2 Solution details 10

6.2.2.1 Mutual authentication 10

6.2.2.2 Protection of NEF-AF interface 10

6.2.3 Evaluation 10

6.3 Solution #3: AF level Authorization for energy level information notification/retrieval 10

6.3.1 Introduction 10

6.3.2 Solution details 10

6.3.2.1 General 10

6.3.2.2 Subscribe/Unsubscribe procedure of energy related information 11

6.3.3 Evaluation 12

6.4 Solution #4: UE data collection consent. 12

6.4.1 Introduction 12

6.4.2 Solution details 12

6.4.3 System impact 12

6.4.4 Evaluation 12

7 Conclusions 12

7.1 Conclusion for KI#1: Security aspects of collecting energy related information. 12

7.2 Conclusion for KI#2: Security aspects of exposure of energy related information. 12

Annex <X> (informative): Change history 14

# 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".

[5] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[6] 3GPP TS 22.261: "Service requirements for the 5G system".

[7] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[8] 3GPP TS 23.501: "System Architecture for the 5G System".

# 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].

EIF Energy Information Function

<ABBREVIATION> <Expansion>

# 4 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].

# 5 Key issues

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

### 5.1.1 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.

There is, depending on the use case, a need to consider towards compliance to regional legislation for collecting energy related information.

### 5.1.2 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.

### 5.1.3 Potential security requirements

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

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

### 5.2.1 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 [2]. This key issue focus on investigating authorization methods for exposure.

The key issues assumes that the data will be exposed on a monthly or yearly basis, as exemplified in TS 22.261 [6] clause 6.15a.5.2, such linkability attacks using the consumption information as a side channel can be neglected.

### 5.2.2 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.

### 5.2.3 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.

# 6 Solutions

## 6.0 Mapping of Solutions to Key Issues

Table 7.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues | |
| --- | --- | --- |
| KI#1 | KI#2 |
| **Sol#1** | x |  |
| **Sol#2** |  | x |
| **Sol#3** |  | x |
| **Sol#4** | x |  |

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

### 6.1.1 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.".

### 6.1.2 Solution details

According to clause 13.1 of TS 33.501 [3], 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 [3] (thereby protecting data-in-transit hop-by-hop).

The solution can inherit the protection principles from clause 13.1 of TS 33.501 [3] to address the security requirement in KI#1.

### 6.1.3 Evaluation

This solution fulfills the requirement of key issue 1.

The solution implements the protection principles in clause 13.1 of TS 33.501 [3], thereby introducing no new impacts to the 5GS.

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

### 6.2.1 Introduction

This solution for KI#2 proposes mutual authentication and NEF-AF interface protection for EE information exposure.

### 6.2.2 Solution details

#### 6.2.2.1 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 [7], clause 6.1.3a. The identities in the end entity certificates are used for authentication and policy checks.

#### 6.2.2.2 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].

### 6.2.3 Evaluation

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

## 6.3 Solution #3: AF level Authorization for energy level information notification/retrieval

### 6.3.1 Introduction

This pCR introduces a new solution for KI#2 on authorization of AF when AF subscribes/unsubscribes and retrieve energy related information.

### 6.3.2 Solution details

#### 6.3.2.1 General

Based on conclusion for KI#1 clause 8.1 in TR 23.700-66 [2] If an AF is deployed outside the 3GPP operator domain, and is an authorized consumer, the granularities include: per application corresponding to the AF, per UE, and per UE per AF and per PDU session. The procedure for notifying and retrieval of energy related information by the AF is described in section 5.2.2.

#### 6.3.2.2 Subscribe/Unsubscribe procedure of energy related information

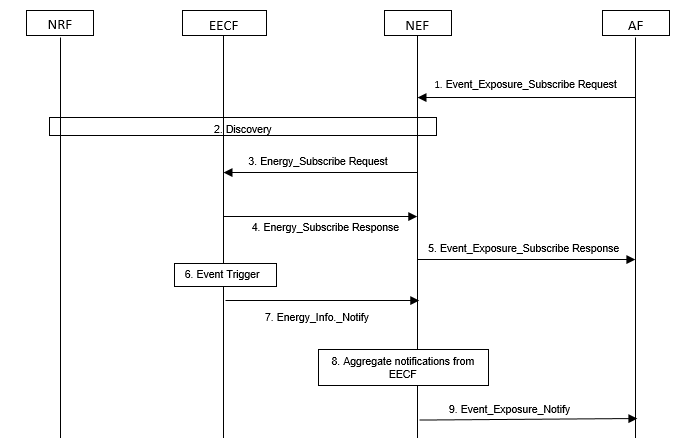


Figure 5.2.2-1: AF level Authorization for energy level information notification/retrieval

The AF authorization is based on clause 13 of TS 33.501 [3]

The token-based authorization mechanism is used. The token is generated for the AF after authorization that includes the level of service access. The token claim may contain the external application ID, UE ID, or AF-Service-Identifier.

1. To subscribe energy related information if the authorized consumer is AF, the granularities include, per UE, per UE per application, per PDU session with the EECF, the AF sends Event\_Exposure\_Subscribe Request.The message contains the token with token claims as described above. Additionally, the token claims include the type of energy related information i.e., energy consumption information or renewable energy information.

2. The NEF checks whether the AF is authorised for the requested subscription based on the AF token. It needs to check whether the token claims match the AF’s identity and service level access i.e., external application ID, UE ID, or AF-Service-Identifier and type of energy related information. If authorised, the NEF may query the NRF to find the EECF responsible to provide the requested energy related information.

3. The NEF forwards the request to the EECF with subscription based on service level as described in step 2.

4. The EECF acknowledges the execution of request message to the NEF.

5. The NEF based on the confirmation from EECF in step 4, sends a response back to the AF for subscription success.

6–7. The EECF triggers a notification towards the AF and sends the message to the NEF as described in TS 23.502 [5].

8-9. The NEF forwards the message to the AF for single EECF or aggregates reporting information for multiple EECF message as described in TS 23.502 [5].

NOTE: The steps in the scope need to be aligned with the architecture. The EECF is a representation of the EIF.

### 6.3.3 Evaluation

The solution relies on the Event exposure services offered by the NEF while reusing the existing authorization mechanism based on clause 13 of TS 33.501 [3]. The token-based authorization introduces additional token claims necessary to limit the service level access based on AF subscription policies.

NOTE: Applicability and evaluation of the solution depends on the final procedure and architecture.

## 6.4 Solution #4: UE data collection consent.

### 6.4.1 Introduction

This solution addresses KI#1 and aspects in relation of being compliant to regional legislation related to collection of user related information. When a UE registers to the network, it authenticates through a subscription linking to the subscriber to the UE. This implies a relationship between a UE and a subscriber. Regional legislation mandates acceptance from the User prior to collection of user related information.

### 6.4.2 Solution details

The solution proposes to reuse TS 33.501[3] Annex V procedure for user consent aspects for collection of energy related data.

### 6.4.3 System impact

No new system impact

### 6.4.4 Evaluation

The solution reuses mechanisms described in TS 33.501 [3] Annex V and hereby provides the means for complying to regional legislation. No changes to procedures or methods defined in TS 33.501 [3] Annex V is required.

# 7 Conclusions

## 7.1 Conclusion for KI#1: Security aspects of collecting energy related information.

Based on solution 1 and 4, the following conclusion is drawn. The EIF follows the communication principles (SBI) of the SBA architecture without changes, which implies that the protection principles defined in TS 33.501 [3] clause 13.1 can be reused without normative changes required. In case user consent check is required by regional legislation, the EIF will be the enforcement point of “user consent check” for energy related information collection and reuse the principles in TS 33.501 [3] Annex V without the need for normative changes.

NOTE: The EIF, as enforcement point for user consent check, is defined in TS 23.501 [8].

## 7.2 Conclusion for KI#2: Security aspects of exposure of energy related information.

Based on solution 2 and 3, the following conclusion is drawn. The exposure of energy related information to 3’rd party AF’s happens through the NEF, this implies that the following principles are reused without need for normative work. For authentication aspects TS 33.501 [3] clause 12.2 applies, for protection of the interface between the NEF and AF TS 33.501 [3] clause 12.3 applies and for authorisation of the AF TS 33.501 [3] clause 12.4 applies. The corresponding AF authorisation granularities for energy data related exposure can reuse the principles already defined in TS 33.501 [3]. Authorisation with further granularity (e.g., UE, PDU Session and/or QoS flow) may be needed to avoid the risk of unauthorized service access that may violating principles of least privilege that may result in AF gaining access to more data than necessary. By incorporating these granularities, the NEF ensures that external AF access is policed. The definition of token claims and corresponding authorisation granularities is left for implementation. Thus, no normative work is needed.

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 |
| 2024-08 | SA3#117 | S3-243606 |  |  |  | Included changes from S3-243607, S3-243608, S3-243609, S3-243610 | 0.3.0 |
| 2024-10 | SA3#118 | S3‑244302 |  |  |  | Included changes from S3-243963, S3-243964, S3-244215, S3-244404, S3-244405, S3-244406, S3-244503, S3-244504 | 0.4.0 |
| 2024-11 | SA3#119 | S3-245199 |  |  |  | Included changes from S3-245278, S3-245350 | 0.5.0 |
| 2025-01 | SA3#119-e | S3-250221 |  |  |  | Included changes from S3-250171, S3-250172, S3-250173 | 0.6.0 |
| 2025-02 | SA3#120 | S3-250973 |  |  |  | Included changes from S3-251012, S3\_251013 | 0.7.0 |