**3GPP TSG-SA3 Meeting #104-e- Ad-hoc *draft\_S3-213411-r1***

**e-meeting, 27 – 30 September 2021** Revision of S3-20xxxx

**Source: Huawei, HiSilicon**

**Title: Address Editor's Note and Clean Up**

**Document for: Approval**

**Agenda Item: 5.5**

# 1 Decision/action requested

***This contribution proposes to do clean up work for TR 33.867.***

# 2 References

# 3 Rationale

The contribution proposes to do clean up work for TR 33.867.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 1 Scope

The scope of present document is to identify and evaluate the requirements and solutions to support user consent for 3GPP services while complying with user privacy considerations.

The details are as follows:

* Review TR 33.849 [3] with regards to the concept of user consent for 3GPP users, and identify what types of data collection and conditions under which the support of the user consent is required; then update them if needed;
* Identify target usage scenarios and trust domains;
* Analyse potential security threats and requirements for conditions under which user sensitive data are collected without user consent, and when user consent indication is not protected;
* Identify potential solutions to address the above security requirements.

NOTE 1: Principles, regulations, and definitions related to privacy, which are recognized differently in each different country or area, are taken into account when deriving the concept of user consent for 3GPP users.

NOTE 2: Even where solutions exist to obtain user consent, collection and exposure of user sensitive data should be minimized and only be allowed where critical to the operation of the related feature.

# 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 23.558: "Architecture for enabling Edge Applications (EA) ".

[3] 3GPP TR 33.849: “Study on subscriber privacy impact in 3GPP”.

[4] 3GPP TS 23.288: “Architecture enhancements for 5G System (5GS) to support network data analytics services”

[5] 3GPP TS 23.501: “System architecture for the 5G System (5GS)”

[6] General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>

# 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].

**Data subject:** As defined in TR 33.849 [3].

**Data controller:** As defined in TR 33.849 [3].

**Data processor:** As defined in TR 33.849 [3].

**Personal data**: As defined in TR 33.849 [3].

## 3.2 Symbols

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

<symbol> <Explanation>

Editor’s Note: Example needs to be deleted

## 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>

Editor’s Note: Example needs to be deleted

# 4 General principles for user consent

## 4.1 Concept of user consent

Editor’s Note: This clause will introduce concept of user consent and why we study user consent in SA3.

4.2 Background information to existing work

Privacy is one aspect for which user consent is needed. Privacy aspect has already been studied in detail in TR 33.849 [3], which provides privacy principles that need to be followed in 3GPP when designing new systems, security architectures and protocols. Parts of TR 33.849 [3] are related to user consent and can be taken into account in this study.

In clause 6.5 of TR 33.849 [3], user consent is introduced as one of the threat mitigation approaches to mitigate the privacy risk, and gives a brief introduction on how explicit user consent can be collected.

In clause 5.3.4 of TR 33.849 [3], conditions which user consent is required for personal information disclosure is defined as: “*Personal data disclosure with the purpose to accomplish a certain application/service needs to be under user's consent, unless the disclosure is performed in the legitimate interest of the data subject, e.g. providing a service.*”

In Annex B of TR 33.849 [3], some regulations related to privacy are introduced.

However, with evolution of 3GPP network, more and more 3GPP services are introduced. Some services can require personal identification information (PII), thus, the identification of target usage case for user consent is necessary.

For different use case, the PII is identified by different identities, e.g., some of them is identified by subscriber ID, i.e., SUPI, and some of them is identified by user IDs. Thus, it is necessary that the source of user consent is identified case by case.

However, as mentioned before, privacy is only one of the drivers for user consent. User consent can also be given or prohibited for non PII.

In summary, different use cases need different solutions for authorization based on user consent. Security issues of how user consent is exchanged among NFs in the network and how they are handled and respected by various features specified by 3GPP will be considered in this study.

# 5A Use Cases

## 5A.1 Use Cases #1: UE Related Analytics of NWDAF

### 5A.1.1 Use Case details

NWDAF can provide UE related analytics services. The NWDAF collects UE related data, e.g. from UE, NFs, 3rd party, and outputs related analytics result, e.g. UE mobility analytics, UE communication analytics, expected UE behavioural parameters related network data analytics and abnormal behaviour related network data analytics as depicted in clause 6.7 in 3GPP TS 23.288 [4].

The NWDAF can process UE related data as the following:

* Collect UE related data to provide UE related analytics for the user, e.g. UE mobility analytics.
* Share analytics result to NF consumers, e.g. internal NF or 3rd AF.

The PLMN NFs or AFs can process UE related data as the following:

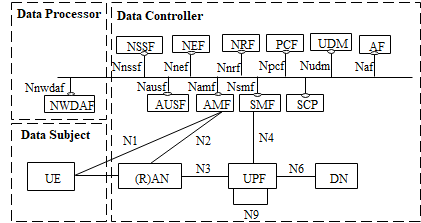
* Collect and store UE related data.
* Share UE related data to NWDAF.

Since the UE related data may contain personally identifiable information, thus, processing of those data should consider user consent aspects. The analytics service is provided by PLMN to a specific subscriber. The key point is that the NWDAF in the PLMN only collects network data which is bound to a subscriber ID, i.e. SUPI, and the analysis output is also bound to that SUPI. Even in case that another user borrows the subscriber’s phone, the PLMN cannot output an analysis result bound to that user because the PLMN just knows current collected data is from the subscriber identified by the SUPI. The PLMN does not output any analysis bound to that user who are using the phone, instead, the output is still bound to subscriber because the collected data is identified by the SUPI, not the user’s ID. The only issue is that the analysis may not be precious enough for the subscriber. Since the PLMN does not output any analysis bound to the user who are using the phone, the user’s privacy is not disrupted, so, it is also aligned with regulation. Thus, for this use case, since the service is provided to the specific subscriber, user consent should be collected from subscriber.

### 5A.1.2 Individual Architecture

For this use case, the architecture and framework as specified in TS 23.288 [4], TS 23.501 [5] are regarded as the baseline. The solutions shall build on the 5G System architectural principles as in TS 23.501 [5], including flexibility and modularity for newly introduced functionalities.

Moreover, the individual architecture is shown in figure 5A.1.2-1.



5A.1.2-1 Individual Architecture for data analytics

The UE related data is derived from the UE.

The NFs, for example, AMF, SMF, OAM, AF, etc., collect and store UE related data derived from the UE. Thus, the legal entity of those network entities is data controller. In case that the AF is outside of 3GPP network, the legal entity of the AF is another data controller.

The NWDAF collects UE related data from the NFs, and processes data for UE related analytics to provide UE related analytics services. Thus, the legal entity of the NWDAF is data processor. In case that the NWDAF is NF of data controller, the legal entity of the NWDAF is also data controller.

NOTE: Roaming architecture for NWDAF is not considered in R17.

## 5.2 Use Cases #2: UE Information Exposure for Mobile Edge Computing

### 5.2.1 Use Case details

An edge enabler server (EES) of the edge data network caters to the edge applications running at an edge data network. The EES is configured to expose APIs (e.g. location service, UE identifier (GPSI)) to the edge application server (EAS), and the PLMN NFs are also configured to expose the relevant APIs to the EES.

The EAS collects the UE information via the EES’s APIs to provide specific services, e.g. collect GPSI and related GPS to provide accurate location service, and the EES may collect the UE information via the PLMN NFs’ APIs.

The EAS can process UE information as the following:

* Collect UE information to provide specific services, e.g. collect UE location to provide accurate location service.

The EES can process UE information as following:

* Collect and store UE information.
* Share UE information to EAS.

The NFs in PLMN can process UE information as following:

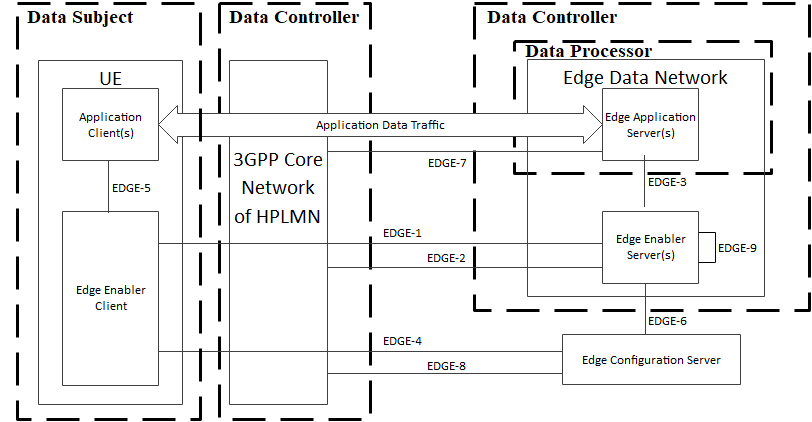
* Collect and store UE information.
* Share UE information to EES.

The MEC service is provided by stakeholder of the EAS (e.g. 3rd party) to a specific subscriber. The key point is that the EAS in the 3rd party can identify the specific user who is using the MEC application. If the EAS requests for the user’s sensitive information from PLMN, e.g. location, GPSI, etc., user consent from the user may be needed because the user’s sensitive information is transferred between different data controllers, i.e. PLMN and 3rd party. Thus, for this use case, since the service is provided to the specific user, user consent should be collected from user.

### 5.2.2 Individual Architecture

For this use case, the architecture and framework as specified in TS 23.558 [2], TS 23.501 [5] are regarded as the baseline. The solutions shall build on the 5G System architectural principles as in TS 23.501 [5], including flexibility and modularity for newly introduced functionalities.

Moreover, the individual architecture is shown in figure 5.2.2-1.



5.2.2-1 Individual architecture for data analytics

The UE information is derived from the UE, which may include UE static ID, UE location, etc.

The home PLMN NFs in 3GPP core network store UE information. Thus, the legal entity of those network entities is data controller. In addition, the EES also collects and stores UE information from the 3GPP core network. Thus the legal entity of the EES is also data controller.

The EAS collects UE information from the the EES, and processes the UE information to provide specific services. Thus, the legal entity of the EAS is data processor. The legal entity of the EAS is also data controller.

# 5B Common architecture

Editor’s Note: This clause will capture the common architecture for user consent in 5G system. Common architecture could be derived from different individual architectures for user consent in 5G system.

# 6 Key issues

NOTE: Key issues should align with the background/analysis done in clause 4 and 5 above.

## 6.1 Key Issue #1: User's consent for exposure of information to Edge Applications

### 6.1.0 Use case mapping

As defined in clause 6.6 and 8.6 in TS 23.558 [2], the EES can expose some service capability APIs to the EAS(s). The exposed service capability APIs include EES capabilities and exposed 3GPP Core Network capabilities. Some APIs provided by the EES are related to user's consent such as UE location API specified in clause 8.6.2 in TS 23.558 [2] and UE Identifier API specified in clause 8.6.5 in TS 23.558 [2].

### 6.1.1 Key issue details

The EES exposes UE Identifier API to the EAS in order to provide an identifier uniquely identifying a UE. Further, the EES exposes the UE location API to the EAS in order to support tracking or checking the valid location of the UE. In order to expose such user related private information to the Edge Application servers, consent from the user is needed.

EES capability exposure to the EAS as defined in TS 23.558 [2], mandates the end user's consent for reporting UE's information, particularly for UE Identifier API and UE location API. Also as suggested in TS 23.558 [2], whether and how user's consent is obtained to share the UE identifier with a particular EAS is covered in this key issue.

### 6.1.2 Security threats

Use of user’s information to identify and track the user or user’s behavior without the permission or knowledge of the user, poses huge threat to user’s privacy.

### 6.1.3 Potential security requirements

Architecture for enabling edge applications shall support a mechanism for Edge Application Servers to obtain user's authorization, in order to access to and/or to expose the user's sensitive information (e.g. user's location).

NOTE: When defining any procedures obtaining user's consent, it is needed to clarify “when” user’s consent is obtained, on “what” information it is obtained and provide details on “why” user’s consent is obtained (e.g. for what purposes the user consented information will be used).

## 6.2 Key Issue #2 User consent for UE data collection

### 6.2.1 Key issue details

5GS NFs will collect data about the UE being served. The NFs keep privacy related sensitive data such as profiling information, location information, etc. UE related data may also need to be transferred to another NF to fulfil a service request or, e.g., for analytics purposes. For example, the NWDAF shares the analytics results to the consumer NF which may be an internal NF or a 3rd party and exposes the UE Identifier, UE location in order to support tracking or checking the valid location of the UE.

In order to meet related private information requirements stated above, user consent is needed.

### 6.2.2 Security threats

If the 5G NFs are not aware of the current status of user consent for a specific service, they may share information with other NF’s that are not essential for 5G communication that could lead to a compromise in the users privacy.  For example, sharing location, timings and device ID with a third party service or with a NF from an operator that is neither the home or visited network.

### 6.2.3 Potential security requirements

The 3GPP system shall provide a means for an NF to authenticate a request for information that may compromise a user’s privacy.

The 5GS shall provide a means for an NF to verify the status of user consent for a request for information that may compromise a user’s privacy.

The 5GS shall specify where an NF can find the status of user consent for service that it delivers.

The 5GSshall specify a means that allows a user to change or add consent for a service/for any UE sensitive information collection (e.g. UE location information).

5G NFs shall provide protect potential privacy related information both in transit and in storage.

## NOTE: the key issue covers also user consent not based on privacy regulation.6.3 Key Issue #3: Modification or revocation of user consent

### 6.3.1 Introduction

UDR (via UDM services) holds the user consent for user related data which is provisioned by MNO as a user subscription information. A service provider (external to MNO domain) can use *Nnef\_parameterProvision\_Update* service to update or to revoke the user consent to the UDM/UDR (when applicable).

In some regulatory domains, there exists a "right to be forgotten". In these domains, modification or revocation of user consent may require the data controller to delete the data for which prior user consent was given.

### 6.3.2 Security threats

If user consent modification or revocation is done by an unauthorized party, a service to a consumer can be denied; or service might be granted to the consumer that should not have access to the user data.

### 6.3.3 Potential security requirements

5GS shall support to delete the data if the user consent is modified or revoked after prior user consent was given.

5GS shall support to halt gathering and sharing of data as soon as the user consent is modified or revoked after prior user consent was given.

## 6.4 Key Issue #4: KI on relationship between the subscriber and the end-users

### 6.4.1 Key issue details

Based on the discussion over the past meetings, companies had different perspective over the consent provided by the users or the subscriber. As the end-users of the subscription may not be the subscriber, for example, employee may use the subscription of the employer for business proposes. In such scenarios, the user consent can be provided either by the user(s) (employee(s)) or by the subscriber (employer) based on the use cases. For e.g., in the case where PLMN provides service for a subscription, the user consent can be collected from subscriber and for the case where 3rd party provides service for the user, the user consent can be collected from the users (end-users), as subscriber may not be involved or it is irrelevant for the subscriber.

As an outcome of the discussion, it is decided that, the user consent is obtained from the end-user(s) and the consent obtained from the end-users (subscriber and/or users) of the subscription is considered as valid for that subscription.

NOTE: The term end-user defined in TR 21.905 [1].

### 6.4.2 Security Threats

Not applicable.

### 6.4.3 Potential Requirements

Not applicable.

## 6.5 Key issue #5: Unambiguous naming of purposes

### 6.5.0 Use case mapping

In all use cases, user consent is given for specific purposes. Thus this key issue is relevant for all use cases.

### 6.5.1 Key issue details

Data handling (i.e. processing, storage, distribution, usage, etc.) subject to user consent needs to be limited to the purposes for which user consent has been given. It is necessary to unambiguously specify this purpose in order to enforce it. For interoperability, it is necessary to standardize a machine readable format to specify these purposes.

### 6.5.2 Security threats

If the system isn’t aware of the precise limits of user consent given for data handling, there is a possibility that data is handled outside of the given consent. This could result in privacy violation of the user and could also entail a legal risk for the parties involved in processing and in forwarding the data.

### 6.5.3 Potential security requirements

The 3GPP system shall adhere to a publicly specified, machine readable format for specifying processing purposes.

# 7 Potential solutions

## 7.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | |
| 1 | 2 | 3 |  |
| #1: User Consent for Exposure of information to Edge Applications in Real Time | X |  |  |  |
| #2: User Consent for UE Related Analytics of NWDAF |  | X |  |  |
| #3: User Consent for UE Related Analytics of NWDAF |  | X |  |  |
| #4: Check of User Consent for 3GPP Service Exposure | X |  |  |  |
| #5: Privacy preservation of transmitted data |  | X |  |  |
| #6: Revocation for user consent |  |  | X |  |

## 7.1 Solution #1: User Consent for Exposure of information to Edge Applications in Real Time

### 7.1.1 Solution overview

The solution addresses key issue #1 “User Consent for Exposure of information to Edge Applications”.

The solution introduces a new function user consent function (UCF), the UCF can collect and maintain user consent from user in real time. The UCF is operator’s internal AF which can be merged with other internal AF, and can communicate with user.

NOTE: how would the UCF know from what user it collected the user consent form is not addressed in this solution.

NOTE: Whether UCF should communicate with user is not addressed in this solution.

NOTE: How UCF can determine the user is not addressed in this solution if UCF communicates with user.

### 7.1.2 Solution details

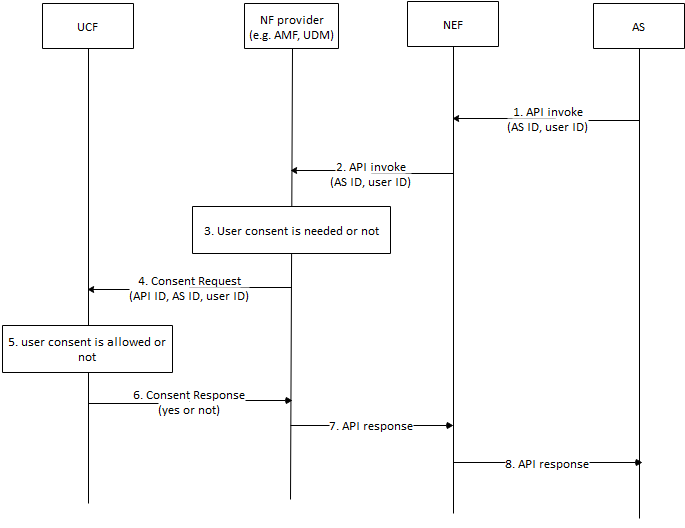


Figure 7.1.2.1 Authorization based on User Consent

1. AS sends API invocation to NEF, requesting for user’s sensitive information, e.g. location. The invocation includes AS ID and user ID. The user ID is associated to specific user.
2. The NEF sends the API invocation with the AS ID and the user ID to NF provider to retrieve the information.
3. The NF provider checks whether authorization of user consent is needed or not based on the invocated API according to local policy, e.g. regulation, if the invocation requests the user’s sensitive data, the NF provider may check whether user is allowed based on local policy. Otherwise, if the invocation requests non-user information or policy is not needed, the NF provider may not check the consent.
4. If check of consent is needed, the NF provider sends Consent Request message with the API ID, the AS ID and the user ID to the UCF.
5. The UCF checks whether consent is allowed. The UCF may push application request to the user for consent via application layer, the UCF may also push SMS to the user assocated with the MISDN. The request shows that user consent is needed for sharing your sensitive information to 3rd party. If consent is received or rejected, the UCF replies result to the NF provider. The UCF may store the consent for future use.
6. The UCF sends Consent Response to the NF provider with the result.
7. If the result shows that consent is allowed, the NF provider response to the API invocation, otherwise, the invocation is cancelled.

NOTE: How AS’s purpose for data processing is determined is not addressed in this solution.

NOTE: How to track where data has been communicated to in case of a requirement for later deletion is not addressed in this solution.

### 7.1.3 Solution evaluation

The solution is incomplete.

## 7.2 Solution #2: User Consent for UE Related Analytics of NWDAF

### 7.2.1 Solution overview

The solution addresses key issue #2.

The solution gives an overview for user consent on services provided by NWDAF.

### 7.2.2 Solution details

#### 7.2.2.1 NF Authorization based on User Consent

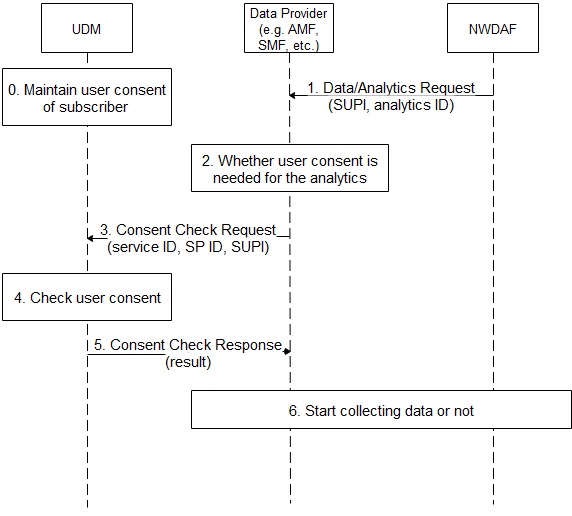


Figure 7.2.2.1-1 NF Authorization based on User Consent for NWDAF

1. The UDM maintains user consent for the subscriber.
2. The NWDAF sends Data/Analytics Request to Data Provider, the request includes SUPI and analytics ID.
3. If the request is for specific analytics, e.g. may collect UE’s information for UE related analytics, the Data provider checks whether user consent is needed for the analytics according to local policy, e.g. regulation.
4. The Data Provider sends Consent Check Request message to the UDM. The message includes the service ID, the Service Provider ID and the SUPI. The service ID is associated with the analytics ID.
5. The UDM checks user consent according to the maintained user consent.
6. The UDM sends Consent Check Response message to the Data Provider. The message includes the result, i.e. permission granted or denied.
7. The Data Provider starts to collect the requested data based on the result.

NOTE: If step 2 is done in another place like in NWDAF or UDM, the details are not addressed in this solution.

NOTE: When UDM itself is data provider, the details are not addressed in this solution.

#### 7.2.2.2 User Consent Format

The UDM maintains the following parameters for user consent for services provided by NWDAF:

* UE ID: refers to a subscriber, can be SUPI.
* Service Provider ID: refers to a service provider who provides data analytics service for the UE, can be PLMN ID.
* Service ID: refers to a data analytics service, can be analytics ID.

Those parameters are combined to indicate that a specific subscriber has user consent to consume specific network analytics service provided by the specific service provider.

#### 7.2.2.3 Obtain of User Consent

The subscriber may give its consent to operator when the subscriber signs service contract with the operator.

### 7.2.3 Solution evaluation

The solution is incomplete.

## 7.3 Solution #3: User Consent for UE Related Analytics of NWDAF

### 7.3.1 Solution overview

The solution addresses key issue #2.

The solution gives an overview for user consent on services provided by NWDAF.

### 7.3.2 Solution details

#### 7.3.2.1 NF Authorization based on User Consent

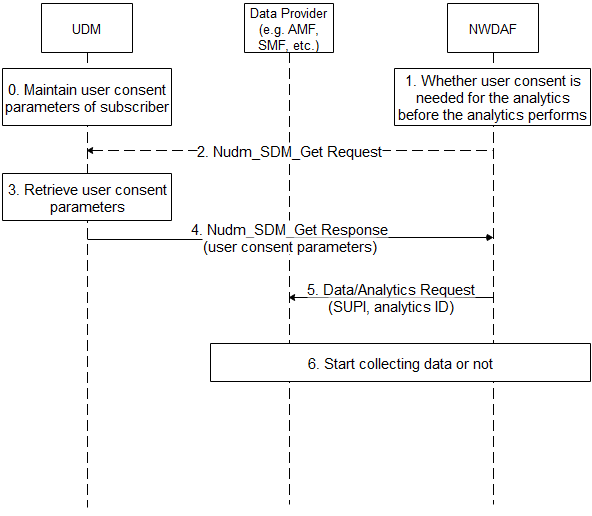


Figure 7.3.2.1-1 NF Authorization based on User Consent for NWDAF

1. The UDM maintains user consent for the subscriber.
2. If the NWDAF receives request for specific analytics from Data Consumer, e.g. it may collect UE’s information for UE related analytics, the NWDAF checks whether user consent is needed for the analytics according to local policy, e.g. regulation.
3. If there is no user consent paramters in the NWDAF’s UE context, the NWDAF sends Nudm\_SDM\_Get Request message to the UDM. The input “Subscription data type(s)” shall be set to “user consent subscription data”, the input “Key for each Subscription data type(s)” shall be set to “SUPI”, the input “Data Sub Key(s)” shall be set to “data processor ID” and/or “purpose of data process”.
4. The UDM retrieves user consent parameters.
5. The UDM sends Nudm\_SDM\_Get Response message to the Data Provider. The message includes the user consent parameters. The NWDAF stores the user consent parameters in the NWDAF’s UE context.
6. Based on the user consent parameters, the NWDAF sends Data/Analytics Request to Data Provider, the request includes the SUPI and the analytics ID.
7. The Data Provider starts to collect the requested data based on the result.

#### 7.3.2.2 User Consent Format

The UDM maintains the following user consent parameters for services provided by NWDAF:

* UE ID: refers to a subscriber, can be SUPI.
* Data Processor ID: refers to a service provider who provides data analytics service for the UE, can be PLMN ID.
* Purpose of Data Processing: refers to a data analytics service, can be service operation name (e.g. Nnwdaf\_AnalyticsSubscription\_Subscribe), with specific analytics ID input.
* User Consent Result: whether there is consent for data processor to process the data according to purpose of data processing.

Editor’s Note: whether purpose of data processing is sufficient is ffs.

Those parameters are combined to indicate that a specific subscriber has user consent to consume specific network analytics service provided by the specific service provider.

#### 7.3.2.3 Obtain of User Consent

The subscriber may give its consent to operator when the subscriber signs service contract with the operator.

The subscriber may change or add consent to operator when the subscriber changes its subscription with the operator.

### 7.3.3 Solution evaluation

TBA

## 7.4 Solution #4: Check of User Consent for 3GPP Service Exposure

### 7.4.1 Solution overview

The solution addresses key issue #1 “User Consent for Exposure of information to Edge Applications”.

### 7.4.2 Solution details

#### 7.4.2.1 Check of user consent on NEF/CAPIF

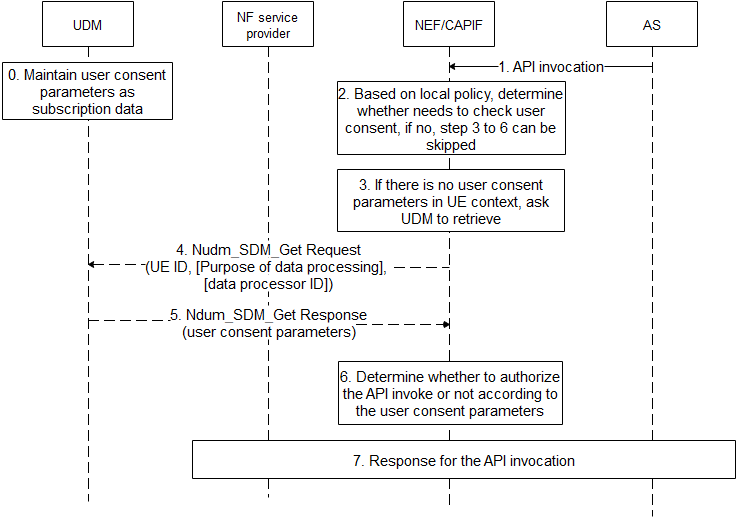


Figure 7.4.2.1-1 Check of User Consent on NEF/CAPIF

1. UDM maintains user consent parameters as subscription data as depicted in 7.4.2.2.
2. AS sends API invocation to NEF/CAPIF, requesting for processing user’s data, e.g. if the invocated service is “Nnef\_Location\_LocationUpdateNotify” with inputs with AF ID, and GPSI, it means that the AF asks NEF/CAPIF to retrieve location of UE identified by the GPSI.
3. The NEF/CAPIF determines whether the invocated service needs to check user consent based on operator’s local policy, e.g. whether regulation is required, whether the invocated service is to process user’s personal information, etc.. If there is no need to check user consent, step 3-6 can be skipped.

Editor’s note: how does the NEF know the purpose from API invocation is ffs.

1. If there is no related user consent parameters in UE context, the NEF/CAIPF invokes Nudm\_SDM\_Get Request service to retrieve related user consent parameters. Otherwise, step 4-5 can be skipped.

Editor’s note: how to ensure user consent parameters are current / not outdated is ffs.

1. The NEF/CAPIF sends Nudm\_SDM\_Get Request message to the UDM, the message shall include UE ID, and may include purpose of data processing, data processor ID. The UE ID can be SUPI which is resolved with the GPSI by NEF/CAPIF using existing mechanism. The purpose of data processing is format combined with service operation name and some of specific inputs which are derived from the API invocation, The data processor ID can be AF ID or more generic which is resolved from the AF ID in the API invocation.

Editor’s note: how does the NEF know the purpose from API invocation is ffs.

1. The UDM returns requested user consent parameters, which includes user consent result.
2. The NEF/CAPIF determines whether to authorize the API invocation or not according to the user consent parameters. If the user consent result of the purpose of data process is not allowed, the NEF/CAPIF rejects the AF’s request with specific cause. If the user consent result of the purpose of data process is allowed, the NEF/CAPIF accepts the AF’s request. If there is no explicit user consent results, the NEF/CAPIF can decide to reject or accept the AF’s request based on operator’s local policy.
3. The NEF/CAIPF response for the API invocation based on determination in step 6.

#### 7.4.2.2 User Consent Parameter

The UDM maintains the following user consent parameters:

* UE ID: can be SUPI.
* Data Processor ID: refers to a data processor who process data for the UE, can be AF ID, or more generic, e.g. “3rd party” or “all”.
* Purpose of data processing: combined with service operation name and some of specific inputs, e.g. Nnef\_AnalyticsExposure\_Subscriber with Analytic ID set to “UE communication analytics”, which means to allow AF to ask for UE’s communication analytics information.

Editor’s Note: Further information elements to uniquely define a purpose are FFS.

* User Consent Result: whether there is consent for data processor to process the data according to purpose of data processing.

### 7.4.3 Solution evaluation

TBA.

## 7.5 Solution #5: Privacy preservation of transmitted data

### 7.5.1 Introduction

This solution addresses key issue #2.

During the transfer of data/metadata/analytics-output from one NWDAF to another NWDAF, it should be ensured that any information that can reveal the identity of the user or compromise in another way the privacy of the user is protected.

Therefore, appropriate measures should be taken by the sender NWDAF to protect any information that can hamper privacy and maybe reveal the identity of the user. Some of the examples are positioning information, user profile information, etc. This information should be processed/filtered by a NWDAF before sending the data to another NWDAF.

Thus, the privacy-sensitive information has to be protected (in accordance with the regulatory requirements and the operator's policies) before being transferred to any other NWDAF.

### 7.5.2 Solution details

To protect the sensitive and private information of the user, a privacy framework is introducedBy this, different privacy rules can be applied by different operators/vendors based upon specific policies and requirements, e.g. by local policy.

The privacy rules can be stored in the home network in

* UDM/UDR if privacy is configured per subscriber, or
* NRF if privacy is generic for all the subscribers of one or several NFs.

User privacy policies and rules can be retrieved from UDM. NRF can also push this information to NFs.

Service requests related to User data need to be indicated, e.g. by an IE 'DataPurposeID'. The NF Service Consumer (i.e. requester NWDAF1 NF) needs to send this 'DataPurposeID' along with the request to the NF Service Producer (e.g. NWDAF2). Based on this IE, the NWDAF2 will process privacy related data accordingly to the specific policy or requirement valid in this operator network, before sending a service response to the requester NWDAF1.

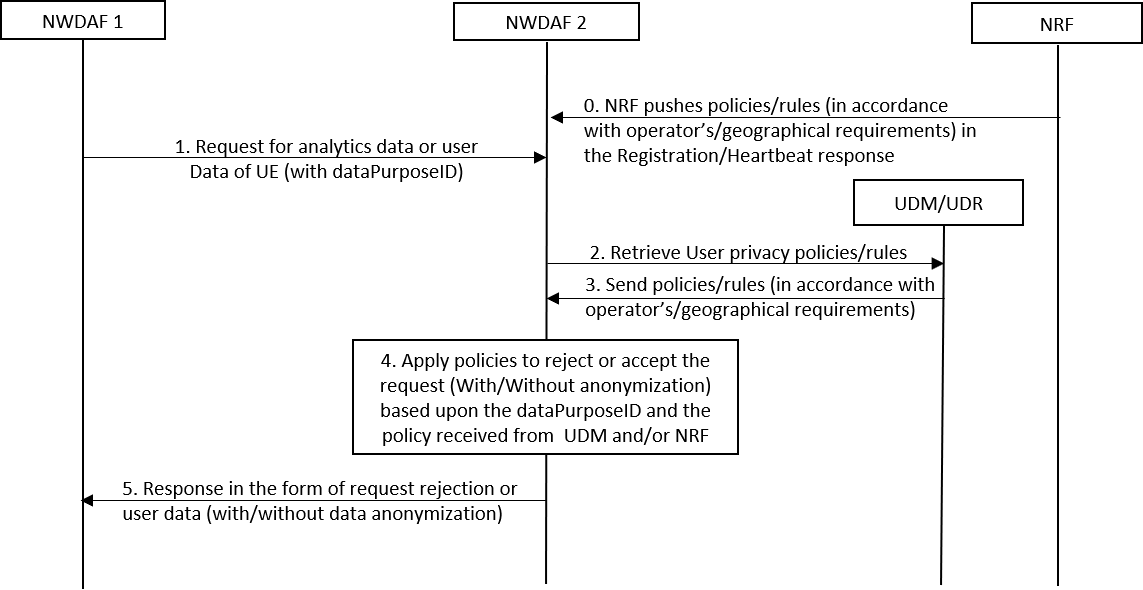


Figure 7.5.2-1: Generic Procedure to preserve user privacy based upon the predefined policies

Step 0: If an operator configures the privacy rules in the NRF (generic for all subscribers), then the NRF can push the policy/rules to NF in the response of registration/heartbeat. A heartbeat message is sent by NFs every some seconds (i.e. 10-20 seconds). Therefore whenever the privacy rule is changed in the NRF, the NRF can push updated rules to the NFs.

Step 1: NWDAF1 sends a user data request to NWDAF 2 (Sending NWDAF Instance) with an additional IE DataPurposeID indicating the purpose.

NOTE: DataPurposeID specifies the purpose of the user data request corresponding to an analytics ID. For instance, the DataPurposeID can be 'Advertisement' corresponding to the user data request of analytics ID 'location'.

Step 2: NWDAF2 sends a request to retrieve the user privacy policies for a specific subscriber from the UDM/UDR. Or it can use the locally configured policies based upon the operator's or geographical requirements.

Step 3: UDM/UDR sends the privacy policies configured for the subscriber either by the operator or by the user or based upon the privacy local policy for a specific geographical region.

Step 4: NWDAF2, after receiving the policies, applies them to the requested user data for the DataPurposeID. For instance, because of the privacy policy it can either reject the request completely or it sends the data without or with anonymization. The latter preserves the sensitive information of the user. Policies received in Step 0 are also applied along with policy received in Step 3.

Step 5: NWDAF2 sends the processed data to NWDAF1 as a response to the initial request.

### 7.5.3 Evaluation

TBD

## 7.6 Solution #6: Revocation for user consent

### 7.6.1 Solution overview

The solution addresses key issue 3.

The solution gives an overview for revoking user consent due to some regulatory requirements.

### 7.6.2 Solution details

Figure 7.6.2-1 illustrates the general procedure for user consent revocation.

The overall assumption is that user consent is part of subscription of the UE stored in UDM. If there is revocation or modification requirement on user consent, UDM shall initiate the subsequent procedures in the network. There are several means for a UE to trigger the user consent revocation, for example, out-of-band way, i.e. the user can revoke a contract.



Figure 7.6.2-1 user consent revocation procedure

The pre-condition is that, a data consumer or an intermediate NF (e.g. including NWDAF/NEF) shall subscribe to the user consent revocation as a service at UDM, reusing the subscription notification procedure, e.g. Nudm\_SDM\_notification service. To be detailed, the inputs shall be set as: “Subscription data type(s)” is set to “user consent subscription data”, the “Key for each Subscription data type(s)” is set to “SUPI”.

Another precondition is that any NF acquiring user consent from the UDM shall register to this revocation service.

Step1: UDM updates subscription information which aims to revoke the user consent due to the request from user. User can request to withdraw its specific user consent corresponding the user data, e.g. location, identity through the demand on network. How does the user require the revocation is not captured in this solution.

Editor’s Note: How does the UDM decide whether a data consumer is allowed to subscribe to the service is ffs

Editor's note: how to achieve the necessary granularity of subscription to receive only relevant consent revocation information (i.e. related to that data, and for what purpose) is FFS.

Step2a: UDM shall send out the Nudm\_SDM\_Notify message which shall include UE ID, processor ID, purpose of processing, user consent result to the Intermediate NF. UE ID is relevant to the subscriber ID, e.g. SUPI, GPSI, processor ID refers to a data processor who processes data for the UE, can be PLMN ID, AF ID, or more generic, e.g. “3rd party” or “all”. Purpose of processing is linked to the revoked services. User consent result refers to consent for data processor to process the data according to purpose of data processing, e.g. allowed or not allowed.

Once receiving the request, the intermediate NF shall delete the data subject to the consent, if the intermediate NF has the processing data functionalities, such as analysis, collection functionalities, intermediate NF shall stop processing the data subject to the consent.

Step 3: If the Data Consumer accesses the Data Provide via intermediate NF, the intermediate NF shall additionally send user consent revocation request message to the Data Consumer. Upon receiving the request, the Data Consumer shall delete the data subject to the consent, if the intermediate NF has the processing data functionalities, such as analysis, collection functionalities, intermediate NF shall stop processing the data subject to the consent.

Step2b: UDM shall send out the Nudm\_SDM\_Notify message to Data Consumer directly. The message is the same as provided to the intermediate NF.

Once receiving the request, the Data Consumer shall delete the data subject to the consent, if the intermediate NF has the processing data functionalities, such as analysis, collection functionalities, intermediate NF shall stop processing the data subject to the consent.

Editor’s Note: How to handle scenarios where the target NF is not available is FFS.

### 7.6.3 Solution evaluation

There is no impact on UE side.

# 8 Conclusions

## 8.1 Conclusion on KI #1 User's consent for exposure of information to Edge Applications

## 8.2 Conclusion on KI #2: User consent for UE data collection

In the use case of UE related analytics in NWDAF, the following specific aspects are concluded for normative work:

* The NWDAF determines whether to allow the NF service consumer to request for analysis using data subject to user consent based on user consent parameters.
* The NWDAF retrieves user consent parameters in NWDAF’s UE context or invokes UDM service to retrieve user consent parameters.

Editor’s Note: This conclusion is only sufficient for cases in which NWDAF and the data providing NF are operated by the same legal entity, other situations are FFS.

## 8.3 Conclusion for Key Issue #3: Modification or revocation of user consent

The following specific aspects for use case#1 (NWDAF) are concluded for normative work:

* NWDAF shall subscribe the service for notification of revocation of user consent if the NWDAF processes data subject to user consent, and shall be notified if user consent is changed.
* If user consent is revoked, the NWDAF shall halt analyzing and collecting of data subject to the user consent.
* If user consent is revoked, the NWDAF shall notify NF service consumers to halt processing of data subject to the user consent.

Editor’s Note: This conclusion is only sufficient for cases in which NWDAF and the data providing NF are operated by the same legal entity, other situations are FFS.

Editor’s Note: How to delete data subject to the user consent is FFS.

## 8.4 Conclusion on KI #4: Relationship between the subscriber and the end-users

For the KI #4 on relation between the subscriber and the end-users, it is concluded that:

The user consent is obtained from the end-users. The end-users may be the subscriber or may authorize the subscriber to provide consent on behalf of the end-users or the end-users are authorized by the subscriber to provide the consent. How authorization is provided between the subscriber and the users is out-of-scope of 3GPP.

End-users cannot retroactively make the user consent setting more permissive, i.e., If end-user accepts processing of data for purpose 1, and later also accepts purpose 2 (making the consent more permissive), the data collected before end-user have given consent for purpose 2 can not be used for purpose 2. If end-user revokes consent for purpose 1 (making end-user consent setting more restrictive), that also applies to data collected before the change in consent setting.

## 8.5 General Conclusions

### 8.5.1 UDM Service for User Consent Check

The following aspects are concluded for normative work:

* UDM service is used to retrieve user consent parameters for NF to check of user consent. This service is used for service consumer to obtain user consent parameters if user consent parameters are not available on the service consumer.
* User consent parameters are stored in UDM as subscription data.

Editor’s Note: How the UDM decides whether the service consumer is allowed to request user consent information is FFS.

Editor’s Note: service consumer needs further clarification.

Editor’s Note: user consent parameters are FFS.

### 8.5.2 General Conclusion on Generic Requirement for the Procedures for User Consent Check

The following generic aspects are concluded for normative work:

* How to check of user consent in a generic way shall be specified. This will provide guideline for new use cases (i.e. other than NWDAF and MEC), that need to check of user consent. Generic statement will be made for:
* If a service is invoked by NF service consumer directly, NF service provider shall check user consent based on user consent parameters in UE context or the NF service provider shall use UDM service to retrieve the user consent parameters.

### 8.5.3 UDM Service for User Consent Revocation

The following aspects are concluded for normative work:

* UDM service is used to notify about user consent change. If user consent parameters are changed, the service consumer shall be notified.
* Upon receiving notification of user consent revocation, the service consumer shall halt processing of data subject to the user consent.
* User consent is effective until revoked.
* User consent shall only be effective for data collected after the point in time that user consent was given.

Editor’s Note: How to delete data subject to the user consent is ffs.

### 8.5.4 Generic Requirement for the Procedures for User Consent Revocation

The following generic aspects are concluded for normative work:

* How to handle user consent revocation shall be specified in a generic way. This is to provide guideline for new use cases that need notification of revocation of user consent.
* If a service is invoked by NF service consumer directly, NF service provider subscribes UDM service which can be notified that user consent is changed.
* If user consent is revoked, the NF service provider halts processing of data subject to the user consent.
* If there is an intermediate NF which is involved in service invocation, e.g. NWDAF, NEF, etc., the intermediate NF subscribes UDM service which can be notified that user consent is changed
* If user consent is revoked, the intermediate NF halts processing of data subject to the user consent, if available.
* If user consent is revoked, the intermediate NF notifies NF service consumers to halt processing of data subject to the user consent.

Editor’s Note: How to delete data subject to the user consent is ffs.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*