|  |
| --- |
| 3GPP TS 26.531 V1.1.0 (2022-02) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group SA;Data Collection and Reporting;General Description and Architecture(Release 17) |
|  |
|  |  |
|  |
| 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.© 2021, 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 7

3.3 Abbreviations 7

4 Reference architecture for data collection and reporting 7

4.1 General 7

4.2 Functional entities for data collection and reporting 8

4.3 Reference points for data collection and reporting 11

4.4 Service-based architecture for data collection and reporting 13

4.5 Information security model 14

4.6 Domain model 16

4.6.1 General 16

4.6.2 Provisioning information for data collection and reporting 18

4.6.3 Configuration information for data collection clients 18

4.6.4 Information included in data reports to the Data Collection AF 19

5 Procedures for data collection and reporting 20

5.1 General 20

5.2 Procedures for data collection and reporting provisioning 21

5.3 Procedures for Data Collection AF subscription 22

5.4 Procedures for configuring data collection client 23

5.5 Procedures for reporting to the Data Collection AF 24

5.6 Procedures for Data Collection AF data exposure 24

5.7 Procedures for Data Collection AF unsubscription 25

5.8 Procedures for event consumer authorization 25

Annex A (informative): Collaboration scenarios for data collection and reporting 27

A.1 General 27

A.2 Collaboration A 28

A.3 Collaboration B 29

A.4 Collaboration C 30

A.5 Collaboration D 31

A.6 Collaboration E 32

Annex B (informative): Change history 33

# Foreword

This Technical Specification 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 defines a generic architecture for collecting and reporting data in the 5G System as defined in TS 23.501 [2], TS 23.502 [3] , TS 23.288 [4] and TS 29.517 [5].

# 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 23.501: "System architecture for the 5G System (5GS)".

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

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

[5] 3GPP TS 29.517: "5G System; Application Function Event Exposure Service; Stage 3".

[6] 3GPP TS 29.510: "Network function repository services; Stage 3".

[7] 3GPP TS 29.532: "Data Collection and Reporting; Protocols and Formats".

[8] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[9] 3GPP TS 33.501: "Security architecture and procedures for 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], TS 23.501 [2], TS 23.502 [3], TS 23.288 [4], TS 29.517 [5] 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 collection client:** functional entity that collects data and reports it to the Data Collection AF, *viz.* Direct Data Collection Client, Indirect Data Collection Client or AS

**direct reporting:** method of sending a data report from the Direct Data Collection Client to the Data Collection AF

**indirect reporting:** method of sending a data report from a UE Application to the Data Collection AF via an Indirect Data Collection Client function of an Application Service Provider

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] , TS 23.501 [2], TS 23.502 [3], TS 23.288 [4], TS 29.517 [5] 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].

AF Application Function

AS Application Server

CAPIF Common API Framework for 3GPP Northbound APIs

DCAF Data Collection AF

DN Data Network

NEF Network Exposure Function

NF Network Function

NWDAF Network Data Analytics Function

UE User Equipment

# 4 Reference architecture for data collection and reporting

## 4.1 General

Clause 6.2.8 of TS 23.288 [4] envisages a set of high-level procedures by which data is collected by a Network Data Analytics Function (NWDAF) from UE Application(s) via an intermediary Application Function. This clause defines a generic reference architecture for data collection and reporting that satisfies those procedures, including the logical functions involved and the logical reference points between them. The intermediary Application Function envisaged in [4] is here named the *Data Collection AF*. It is intended that this reference architecture be instantiated in domain-specific ways to suit the needs of different features of the 5G System. The reference architecture may be instantiated separately in different slices of a network.

The Data Collection AF may support CAPIF [8] to provide APIs to other applications (i.e. API invokers). When CAPIF is supported, then:

- the Data Collection AF shall support the CAPIF API provider domain functions as part of a distributed CAPIF deployment, i.e. Ndcaf and Naf via CAPIF‑2/2e; and CAPIF‑3, CAPIF‑4 and CAPIF‑5, as specified in clause 7.3 of TS 23.222 [8];

- the Data Collection AF shall support the CAPIF Core Function and API provider domain functions as part of a centralised CAPIF deployment, i.e. Ndcaf and Naf via CAPIF‑2/2e, as specified in clause 7.2 of TS 23.222 [8].

The CAPIF and associated API provider domain functions are specified in TS 23.222 [8].

## 4.2 Functional entities for data collection and reporting

Editor’s Note: Different realisations of the reference are currently under consideration by SA4, including SEAL-based and CAPIF-based models.

Figure 4.2‑1 below shows the reference architecture for data collection and reporting using reference point notation.



NOTE: The Data Collection AF may be deployed outside the trusted domain, in which case the services it exposes to API invokers are mediated by the NEF. The logical relationships denoted by the reference points are unaffected by such deployment choices.

Figure 4.2‑1: Reference architecture for data collection and reporting in reference point notation

The functional entities illustrated in the figure are described as follows:

1. Data collection and reporting functionality is provisioned at reference point R1 by a *Provisioning AF* of the *Application Service Provider* that may be deployed either inside or outside the trusted domain.

2. The *Data Collection AF* may be deployed inside or outside the trusted domain. It is responsible for managing the provisioning state for data collection and reporting. When its provisioning state changes, the Data Collection AF updates the set of available NF profile(s) in the NRF by invoking the Nnrf\_NFManagement service defined in clause 5.2.7.2 of TS 23.502 [3] according to the usage defined in clause 6.2.8.2.2 of TS 23.288 [4] and specified in clause 6.1 of TS 29.510 [6].

NOTE 1: If the Data Collection AF is deployed outside the trusted domain, this registration occurs via the NEF, as described in clause 6.2.2.3 of TS 23.288 [4].

Depending on the provisioning information provided by the Application Service Provider (see clause 4.6.2), the Data Collection AF provides a data collection and reporting configuration to the *Direct Data Collection Client* at reference point R2, to the *Indirect Data Collection Client* at reference point R3 or to the Application Server (*AS*) instances at reference point R4, and receives data reports from them respectively at those same reference points.

The Data Collection AF processes received data reports according to processing instructions in its provisioning state. The processing activities include, but are not limited to, reporting format conversion, data normalisation, domain-specific anonymisation of data and (dis)aggregation of data into reports to be exposed as events.

Editor’s Note: Currently-defined 3GPP event types are specified in TS 23.502 and TS 23.288. Additional types of UE application level information available at the AF – for example content hosting logs, QoS and charging policy modification, network assistance and consumption reports as defined in TS 26.501 and TS 26.512 for 5G Media Streaming may also be deemed suitable as event exposure services for subscription by the NWDAF in performing related data analytics, based on further discussion with SA2.

Finally, the Data Collection AF is responsible for exposing processed UE data to event notification subscribers both inside the trusted domain (such as the NWDAF) and outside it (such as the *Event Consumer AF* in the Application Service Provider). In this role, the Data Collection AF realises the Event Exposure Service as defined in clause 6.2.2.1 of TS 23.288 [4] and as specified in TS 29.517 [5]. Subscribers fulfil the role of NF consumers of this service in the service-based architecture [2, 3].

The set of UE data to be collected and exposed by the Data Collection AF is determined by the intersection[[1]](#footnote-1) between its provisioning state provided at R1 and the current set of subscriptions. This is reflected in the data collection and reporting configuration exposed at reference points R2, R3 and R4, and the subscription-driven event notifications sent to consumer entities such as the NWDAF or Event Consumer AF of an Application Service Provider over reference points R5 and R6. The Data Collection AF is responsible for ensuring that access to UE data is controlled according to the rules indicated in its provisioning state.

NOTE 2: When the Data Collection AF is deployed outside the trusted domain, the NWDAF uses the procedure defined in clause 5.2.6.2 of TS 23.502 [3] and further elaborated by clause 6.2.2.3 of TS 23.288 [4] to collect data from the externally deployed Data Collection AF via the NEF.

NOTE 3: The Data Collection AF is intended to be instantiated inside another Application Function in order to satisfy the domain-specific data collection and reporting requirements corresponding to particular features in the 5G System. As such, there may be several domain-specific Data Collection AF instances operating simultaneously in a particular 5G System, each one performing a different role. The definitions of these instantiations are beyond the scope of the present document.

3. The *Direct Data Collection Client* is responsible for collecting relevant data in the UE and for sending data reports to the Data Collection AF via reference point R2 using the Ndcaf\_DataReporting service according to a data collection and reporting configuration that it has previously obtained from the Data Collection AF by invoking the same service at reference point R2.

NOTE 1: This method of reporting corresponds to the direct data collection procedure defined in clause 6.2.8 of TS 23.288 [4].

NOTE 2: In the case where the Data Collection AF is deployed in a different trust domain than the UE, the Direct Data Collection Client instead invokes the equivalent Nnef\_DataReporting API via the NEF.

NOTE 3: The Direct Data Collection Client function is intended to be instantiated inside other UE functions in order to satisfy the domain-specific data collection and reporting requirements corresponding to particular features of the 5G System. As such, there may be several domain-specific Data Collection Client instances operating simultaneously on a given UE, each one performing a different role. One valid deployment option is to combine these instances in a common middleware component. Another option is to provide the Direct Data Collection Client as an integral part of each relevant UE Application. The definitions of these instantiations are beyond the scope of the present document. The realisation of these logical functions is implementation-dependent.

4. The *UE Application* is responsible for sharing relevant data with the Direct Data Collection Client via reference point R7. This may be achieved as a combination of application design, application configuration via R8 and/or application configuration via R7.

5. An Application Service Provider may also collect data from UE Applications via reference point R8 and employ an *Indirect Data Collection Client* subfunction to then send data reports to the Data Collection AF via reference point R3 by invoking the Ndcaf\_DataReporting service according to a data collection and reporting configuration that it has previously obtained from the Data Collection AF by invoking the same service at reference point R3.

NOTE 1: This method of reporting corresponds to the indirect data collection procedure defined in clause 6.2.8 of TS 23.288 [4].

NOTE 2: In the case where the Application Service Provider server is deployed in a different trust domain than the Data Collection AF, the Indirect Data Collection Client instead invokes the equivalent Nnef\_DataReporting API via the NEF at reference point R3.

NOTE 3: Collection of UE data via reference point R8 and processing by the Application Server Provider are outside 3GPP scope. The Indirect Data Collection Client may modify the collected UE data to satisfy the requirements of its data collection and reporting configuration.

Editor’s Note: Need to check with SA2 about stage 2 definition of the Nnef\_DataReporting service (and possibly as follow-up with CT3 on corresponding stage 3 specification) which is currently absent in TS 23.502 [3] and TS 23.288 [4].

6. Application Server instances (labelled *AS*) inside or outside the trusted domain may also collect data and report it to the Data Collection AF via reference point R4 by invoking the Ndcaf\_DataReporting service, according to a data collection and reporting configuration previously obtained from the Data Collection AF by invoking the same service at reference point R4.

Editor’s Note: Need to check with SA2 about stage 2 definition of the Nnef\_DataReporting service (and possibly as follow-up with CT3 on corresponding stage 3 specification) which is currently absent in TS 23.502 [3] and TS 23.288 [4].

NOTE 1: In the case where the Application Server is deployed in a different trust domain than the Data Collection AF, the AS instead invokes the equivalent Nnef\_DataReporting service via the NEF.

NOTE 2: The data collection and reporting requirements for such Application Servers are domain-specific and therefore beyond the scope of the present document.

7. The NWDAF is the primary consumer of processed UE data. This is exposed to the NWDAF by the Data Collection AF in the form of data reporting event notifications via reference point R5 using the Naf\_EventExposure service (as specified in TS 29.517 [5]) after any processing by the Data Collection AF has been performed according to its provisioned processing instructions.

NOTE: If the Data Collection AF is deployed outside the trusted domain, this interaction occurs instead by invoking the Nnef\_EventExposure service via the NEF, as defined in clause 5.2.6.2 of TS 23.502 [3] and as further elaborated by clause 6.2.2.3 of TS 23.288 [4].

8. By means of appropriate data collection and reporting provisioning, certain UE data may also be exposed in the form of data reporting events by the Data Collection AF to an *Event Consumer AF* residing in the Application Service Provider via reference point R6 using the Naf\_EventExposure service defined in clause 5.2.19 of TS 23.502 [4] and specified in TS 29.517 [5].

NOTE: In the case where the Application Service Provider server is deployed outside the trusted domain, the Nnef\_EventExposure service, as defined in clause 5.2.6.2 of TS 23.502 [3], is invoked instead.

## 4.3 Reference points for data collection and reporting

The purposes of the reference points in the functional architecture defined in clause 4.2 above are as follows:

- **R1** supports the following interactions between a Provisioning AF in the Application Service Provider and the Data Collection AF:

- Used by the Application Service Provider to provision data collection and reporting in a Data Collection AF instance by means of the Ndcaf\_DataReportingProvisioning service defined in clause 4.4 of the present document (or else the equivalent service exposed by the NEF if the two functions are deployed in different trust domains). The provisioning information specifies what data is to be collected by Data Collection Clients, how it is to be processed by the Data Collection AF and how it is to be exposed to event notification subscribers. A generic provisioning envelope for data collection and reporting is defined in clause 4.6 of the present document, but this is expected to be extended by individual reporting domains.

- **R2** supports the following interactions between the Direct Data Collection Client in the UE and the Data Collection AF:

- Used by a Direct Data Collection Client instance to obtain its data collection and reporting configuration from the corresponding Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document. A generic data collection and reporting configuration envelope is defined in clause 4.6.3 of the present document, but details of the configuration are specific to individual reporting domains and are specified elsewhere.

- Subsequently used by the Direct Data Collection Client to send reports to its Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document. A generic data reporting envelope is defined in clause 4.6.4 of the present document, but details of the reporting format are specific to individual reporting domains and are specified elsewhere.

NOTE 1: This method of reporting corresponds to the direct data collection procedure defined in clause 6.2.8 of TS 23.288 [4].

- **R3** supports the following interactions between the Indirect Data Collection Client in the Application Service Provider Server and the Data Collection AF.

- Used by an Indirect Data Collection Client instance to obtain its data collection and reporting configuration from the corresponding Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document (or else the equivalent service exposed by the NEF if the two functions are deployed in different trust domains). A generic data collection and reporting configuration envelope is defined in clause 4.6.3 of the present document, but details of the configuration are specific to individual reporting domains and are specified elsewhere.

- Subsequently used by the Indirect Data Collection Client in the Application Service Provider server to send data reports to its Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document (or else the equivalent service exposed by the NEF if the two functions are deployed in different trust domains). A generic data reporting envelope is defined in clause 4.6.4 of the present document, but details of the reporting format are specific to individual reporting domains and are specified elsewhere.

NOTE 2: This method of reporting corresponds to the indirect data collection procedure defined in clause 6.2.8 of TS 23.288 [4].

- **R4** supports the following interactions between the Application Server (AS) and the Data Collection AF:

- Used by an AS instance to obtain its data collection and reporting configuration from the corresponding Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document (or else the equivalent service exposed by the NEF if the two functions are deployed in different trust domains). A generic data collection and reporting configuration envelope is defined in clause 4.6.3 of the present document, but details of the configuration are specific to individual reporting domains and are specified elsewhere.

- Subsequently used by the AS instance to send data reports to its Data Collection AF instance by means of the Ndcaf\_DataReporting service defined in clause 4.4 of the present document (or else the equivalent service exposed by the NEF if the two functions are deployed in different trust domains). A generic data reporting envelope is defined in clause 4.6.4 of the present document, but details of the reporting format are specific to individual reporting domains and are specified elsewhere.

NOTE 3: The AS plays the role of a Network Function when it invokes the Ndcaf\_DataReporting service at reference point R4.

- **R5** supports the following interactions between the NWDAF and the Data Collection AF:

 Used by an NWDAF instance to subscribe to data reporting events exposed by a Data Collection AF instance, according to the Naf\_EventExposure\_Subscribe procedure defined in clause 5.2.19.2.2 of TS 23.502 [3], as further elaborated in step 3a of clause 6.2.8.2.3 in TS 23.288 [4], and as specified in TS 29.517 [5] (or else the equivalent Nnef\_EventExposure\_Subscribe service exposed by the NEF if the two functions are deployed in different trust domains).

 Subsequently used by the Data Collection AF to expose data reporting events to the NWDAF, according to the Naf\_EventExposure\_Notify procedure defined in clause 5.2.19.2.2 of TS 23.502 [3], as further elaborated in step 5a of clause 6.2.8.2.3 in TS 23.288 [4], and as specified in TS 29.517 [5] (or else the equivalent Nnef\_EventExposure\_Notify service exposed by the NEF if the two functions are deployed in different trust domains).

- **R6** supports the following interactions between the Event Consumer AF in the Application Service Provider and the Data Collection AF:

- Used by an Event Consumer AF instance to subscribe to data reporting events exposed by the Data Collection AF, according to the Naf\_EventExposure\_Subscribe procedure defined in clause 5.2.19.1 of TS 23.502 [3] and specified in TS 29.517 [5] (or else the equivalent Nnef\_EventExposure\_Subscribe service exposed by the NEF if the two functions are deployed in different trust domains).

- Subsequently used by the Data Collection AF to expose data reporting events to the Event Consumer AF according to the Naf\_EventExposure\_Notify procedure defined in clause 5.2.19.1 of TS 23.502 [3] and specified in TS 29.517 [5] (or else the equivalent Nnef\_EventExposure\_Notify service exposed by the NEF if the two functions are deployed in different trust domains).

Editor’s Note: Need to check with SA2/CT3 about the security aspects of event exposure to External AFs via the NEF. Exposure of events to external parties via NEF is not explicitly described in TS 23.288, although it is envisaged as a possibility in TS 23.502.

- **R7** is a client API offered by the Direct Data Collection Client to the UE Application.

NOTE 4: When the Direct Data Collection Client is embedded in the UE Application, reference point R7 is not used.

NOTE 5: Interactions at reference point R7 are not fully specified in this release.

- **R8** supports data collection and reporting interactions between the UE Application and the Application Service Provider server.

NOTE 6: Interactions at reference point R8 are beyond the scope of 3GPP standardisation.

## 4.4 Service-based architecture for data collection and reporting

Editor’s Note: Different realisations of the reference architecture are currently under consideration by SA4, including SEAL-based and CAPIF-based models.

Figure 4.4‑1 below shows the reference architecture for data collection and reporting in service-based architecture notation. It depicts the case where the Data Collection AF is deployed inside the trusted domain, while the Application Service Provider and the AS may be deployed independently either inside or outside the trusted domain.



NOTE 1: In its role as an event exposure service provider Application Function, the Data Collection AF provides the (un)subscription operations of the Naf\_EventExposure (or Nnef\_EventExposure) service for use by Network Function service consumers. As Network Function service consumers, the NWDAF and the Event Consumer AF provide the event notification operation of the Naf\_EventExposure (or Nnef\_EventExposure) service for use by the Data Collection AF.

NOTE 2: The UE-based Direct Data Collection Client interacts with the Data Collection AF in the user plane, and so the interaction at reference point R2 does not traverse the service bus.

Figure 4.4‑1: Reference architecture for data collection and reporting in service‑based architecture notation when the Data Collection AF is deployed in the trusted domain

The following service-based APIs are used in connection with data collection and reporting:

1. The Ndcaf\_DataReportingProvisioning service is provided by the Data Collection AF. It is defined by the present document and is specified in TS 26.532 [7]. This service is used by Provisioning AF instances to provision data collection and reporting in the Data Collection AF.

2. The Nnrf\_NFManagement service is provided by the NRF. It is defined in clause 5.2.7.2 of TS 23.502 [3] and specified in clause 6.1 of TS 29.510 [6]. This service is used by the Data Collection AF to register an available NF profile with the NRF for each set of data collection and reporting provisioning information held by the former.

NOTE: As described in clause 6.2.8.2.2 of TS 23.288 [4] the NF profile in this case includes the External Application Identifier (used by clients when reporting data to the Data Collection AF), the Internal Application Identifier (used for event exposure to the NWDAF) and the Event ID. These NF profile parameters are in addition to those specified in clause 5.2.7.2 of TS 23.502 [3].

3. The Ndcaf\_DataReporting service is provided by the Data Collection AF. It is defined by the present document and is specified in TS 26.532 [7].

a. This service is used by the Direct Data Collection Client, by the Indirect Data Collection Client in the Application Service Provider server and by AS instances to obtain their data collection and reporting configuration from the Data Collection AF.

b. Subsequently, this service is used by the Direct Data Collection Client, by the Indirect Data Collection Client and by AS instances to send data reports to the Data Collection AF.

NOTE: Trusted AS instances play the role of a Network Function when invoking the Ndcaf\_DataReporting service (or equivalent) and are therefore depicted in figure 4.4‑1 as being directly attached to the service bus.

4. The Naf\_EventExposure service is provided by the Data Collection AF. It is defined in clause 5.2.19.2 of TS 23.502 [3] and TS 23.288 [4], and is specified in TS 29.517 [5].

a. Used by the NWDAF to subscribe to data reporting events exposed by the Data Collection AF and subsequently used by the Data Collection AF to notify these events to the NWDAF, as described in clause 6.2.2.2 or 6.2.2.3 (as appropriate) of TS 23.288 [4].

b. Used by an Event Consumer AF in the Application Service Provider server to subscribe to data reporting events exposed by the Data Collection AF and subsequently used by the Data Collection AF to notify these events to the Application Service Provider server, as described in clause 6.2.2.2 or clause 6.2.2.3 (as appropriate) of TS 23.288 [4].

Figure 4.4‑2 depicts the case where the Data Collection AF is instead deployed outside the trusted domain, along with the Application Service Provider and the (external) AS. In this case, the subfunctions of the Application Service Provider and the (external) AS do not interact with the Data Collection AF via the 5G System service bus. The Ndcaf service is therefore not required in such deployments. The interactions at the relevant reference points are outside the scope of 3GPP and are depicted as R1′, R3′, R4′ and R6′ to reflect this.



Figure 4.4‑2: Reference architecture for data collection and reporting in service‑based architecture notation when the Data Collection AF is deployed outside the trusted domain

## 4.5 Information security model

An encrypted data transfer protocol shall be employed at reference point R2 to protect the secrecy and integrity of collected UE data in transit between the Direct Data Collection Client and the Data Collection AF.

The Provisioning AF restricts the exposure of UE data over reference points R5 and R6 by configuring a set of Data Access Profiles for each Event ID to be exposed. A Data Access Profile specifies a set of data processing operations that need to be performed by the Data Collection AF on the collected UE data in order to synthesize the event data that will be exposed to the NWDAF and/or Event Consumer AF.

When subscribing to event exposure notifications for a particular Event ID, an NWDAF or Event Consumer AF goes through an authorisation procedure (see clause 5.8) with an Authorisation AS that determines the level of access the event subscriber is allowed to have by selecting one of the provisioned Data Access Profiles for the Event ID in question. If successful, the Authorisation AS supplies an access token to the subscriber which is presented to and validated by the Data Collection AF as part of the event subscription procedure.

NOTE: The procedure for selecting an appropriate Data Access Profile is not specified in the present document.

Figure 4.5.2-1 depicts the static data model for the data collection provisioning with Data Access Profiles to restrict data exposure access.



Figure 4.5.2-1: Data exposure restriction domain model

The Data Access Profile defines restrictions along the time, user, and location dimensions:

- Restrictions along the time dimension determine the granularity of access to UE data along the time axis. The finest granularity allows access to events as they take place in time. The coarsest level of access aggregates all event data along the time axis to produce a single aggregated value.

- Restrictions along the user dimension allow the Provisioning AF to restrict access to UE data related events based on groups. The finest granularity allows the event consumer to access events related to single users. Coarse granularity access exposes aggregated collected event data based on user groups. The coarsest granularity access exposes the data being aggregated for all users.

- Restrictions along the location dimension allow the Provisioning AF to restrict access to UE data related events based on the geographical location of the data collection client during the event. The finest granularity allows the event consumer to access events individually, irrespective of the location. Coarse granularity access exposes aggregated collected event data based on a geographical area. The coarsest level of access aggregates all event data along the location axis to produce a single aggregated value for all locations.

The baseline set of aggregation functions is listed in table 4.5.2‑1:

Table 4.5.2‑1: Baseline aggregation functions

|  |  |
| --- | --- |
| Aggregation function | Description |
| None | No aggregation is applied, and all reported data records are exposed as individual events. |
| Count | The number of reported data records is exposed to event consumers. |
| Mean | The mean average of the values in reported data records is exposed to event consumers. |
| Maximum | The maximal observed value in reported data records is exposed to event consumers. |
| Minimum | The minimal observed value in reported data records is exposed to event consumers. |
| Sum | The sum of the values in reported data records is exposed to event consumers. |

The authorization URL, if present in the data exposure restrictions, is used to redirect subscription requests without a valid access token to an authorization server, which will perform the authorization for the requested Data Access Profile.

Upon successful authorization, the consumer entity obtains an access token, which contains an identifier of the Data Access Profile that is allowed for the event consumer. Upon successful subscription, the Data Collection AF shall apply the indicated aggregation functions of the corresponding Data Access Profile along the time and user dimensions on the collected data prior to exposing it to the event consumer.

## 4.6 Domain model

### 4.6.1 General

Figure 4.6.1‑1 depicts the static data model for the data collection and reporting domain. It is further described below.



Figure 4.6.1‑1: Static domain model

The *Provisioning AF* provisions zero or more sets of *provisioning information* in the Data Collection AF at reference point R1. The baseline set of information provisioned is described in clause 4.6.2. Each set of provisioning information pertains to one application, identified by its *external application identifier*, and one type of exposed *event*, uniquely identified in the 5G System by its *Event ID*, as defined in clause 4.15.1 of TS 23.502 [3]. There may be more than one set of provisioning information for a particular external application identifier, but the combination of the external application identifier and Event ID shall be unique for a given Data Collection AF instance.

The *data processing instructions* and *data exposure restrictions* are expressed as a set of Data Access Profiles (see clause 4.5.2). The data exposure restrictions limit the types of event consumer that are authorised to subscribe to the Event ID provisioned for the application and the data processing instructions specify aggregation functions that are applied to UE data prior to exposure to those event consumers.

Each set of provisioning information is manifested as a *data collection client configuration* that the Data Collection AF makes available to Direct Data Collection Client instances at reference point R2, to Indirect Data Collection Client instances at R3 and to AS instances at R4.

Once configured, these data collection clients then send *data reports* to the Data Collection AF associated with the data collection client configuration. Each data report provides the external application identifier associated with the UE Application and also includes a non-empty list of *data reporting records* containing the parameters collected by the data collection client. These parameters typically include a sampling timestamp.

NOTE: It is the responsibility of the data collection client to discover its external application identifier by means outside the scope of the present document.

Depending on the *data processing instructions* provisioned in the Data Collection AF, a data reporting record contributes to zero or more events exposed to subscribers at reference points R5 and/or R6. Conversely, an exposed event arises from one or more data reporting records. In the case of events synthesised by the Data Collection AF from multiple data reporting records, the timestamp of the event shall indicate when it was synthesised. Otherwise, the timestamp of the event shall be identical to the timestamp of the data reporting record from which it arose.

The Data Collection AF exposes a batch of recent events to consumers (the NWDAF and/or Event Consumer AF) as an *event exposure notification*.

### 4.6.2 Provisioning information for data collection and reporting

A separate set of provisioning information shall be provided to the Data Collection AF at reference point R1 for each Event ID it is to expose. This provisioning information embodies the Service Level Agreement between the network operator and the Application Service Provider envisaged in clause 6.2.8.1 of TS 23.288 [4]. The provisioning information shall include at least the parameters defined in table 4.6.2‑1 below:

Table 4.6.2‑1: Baseline provisioning information for data collection and reporting

|  |  |  |
| --- | --- | --- |
| Parameter | Cardinality | Description |
| External Application Identifier | 1..1 | The identifier to be used in reports sent to the Data Collection AF by data collection clients. (This needs to be mapped to the Internal Application Identifier when exposing events to the NWDAF.) |
| Internal Application Identifier | 1..1 | The identifier to be used by event consumers (including the NWDAF and the Event Consumer AF) when subscribing to events in the Data Collection AF. |
| Event ID | 1..1 | The identifier of an AF event that will be exposed to event consumers as a result of the provisioning. |
| Data collection client type | 1..1 | The type of data collection client that will submit data reports to the Data Collection AF. |
| Valid targets | 1..1 | A parameter to control whether event consumers are permitted to filter events by External UE identifier or External Group Identifier when subscribing, instead of receiving events relating to all UEs. |
| Parameters to be reported | 1..\* | The subset of domain-specific parameters associated with the specified Event ID to be reported to the Data Collection AF (subject to user consent). |
| Data processing instructions | 1..\* | A set of operations to be performed by the Data Collection AF on the parameters reported according to clause 4.6.4 prior to exposure as an event at a particular access level.The set of supported operations shall include at least those listed in table 4.5.2‑1. |
| Data exposure restrictions | 1..\* | A set of restrictions on the exposure of the collected data after any data processing, each corresponding to a different access level. |

### 4.6.3 Configuration information for data collection clients

All clients of the Data Collection AF wishing to report data shall first obtain a data collection and reporting configuration from the Data Collection AF at reference point R2, R3 or R4 (as appropriate). For each Event ID, the data collection and reporting configuration shall include at least the parameters defined in table 4.6.3‑1 below:

Table 4.6.3‑1: Baseline information for data collection and reporting configuration

|  |  |  |
| --- | --- | --- |
| Parameter | Cardinality | Description |
| External Application Identifier | 1..1 | Identifies the UE Application to which this data collection and reporting configuration pertains.Quoted in reports sent to the Data Collection AF. |
| Parameters to be collected | 1..\* | The subset of domain-specific parameters associated with the specified Event ID to be collected by the Data Collection AF (subject to user consent). |

Editor’s Note: When *requesting configuration*, additional information needs to be passed across the R7 client API (then R2) to realise the "authentication information that enables the [Data Collection] AF to verify the authenticity of the UE's Application that provides data" as envisaged in clause 6.2.8.1 of TS 23.288 [4].

### 4.6.4 Information included in data reports to the Data Collection AF

For each Event ID, the data report shall include at least the parameters as defined in table 4.6.4-1 below:

Table 4.6.4‑1: Baseline information for data reporting

|  |  |  |
| --- | --- | --- |
| Parameter | Cardinality | Description |
| External Application Identifier | 1..1 | Identifies the UE Application to which this data report pertains. |
| Collected parameters | 1..\* | The set of parameters collected by the data collection and reporting client. |

Editor’s Note: When *reporting data*, additional information needs to be passed across the R7 client API (then R2) to realise the "authentication information that enables the [Data Collection] AF to verify the authenticity of the UE's Application that provides data" as envisaged in clause 6.2.8.1 of TS 23.288 [4].

# 5 Procedures for data collection and reporting

## 5.1 General

This clause defines the high-level procedures for data collection and reporting.

Figure 5.1-1 below depicts the case where all functional entities lie inside the trusted domain. The detailed steps for each phase are further elaborated in the following clauses.



Figure 5.1‑1: High-level procedures for data collection and reporting

## 5.2 Procedures for data collection and reporting provisioning

Editor’s Note: High-level definition of how data collection and reporting is provisioned, including, but not limited to:

1. Access controls relating to user privacy protection and/or differential exposure of collected data in reports to different parties.

2. Manipulation of collected data for subsequent reporting (e.g. summarisation, anonymisation, etc.).



Figure 5.2‑1: High-level procedures for AF registration and provisioning phases

Initially, the different types of AF register themselves with the NRF using the Nnrf\_NFManagement\_NFRegister service operation defined in clause 5.2.7.2.2 of TS 23.502 [3]:

1. The NWDAF registers itself with the NRF.

2. The Data Collection AF registers itself with the NRF. This registration includes a list of Event IDs that it is capable of exposing to event consumers.

At some later point, Data Collection and Reporting features are provisioned by the Application Service Provider's Provisioning AF:

3. The Provisioning AF discovers the Data Collection AF by following the Nnrf\_NFDiscovery procedure defined in clause 5.2.7.3 of TS 23.502 [3].

4. The Provisioning AF provisions data collection and reporting in the Data Collection AF for a specific Event ID, using the Ndcaf\_DataReportingProvisioning procedures defined in the present document. The provisioning information may vary depending on the data reporting method, i.e. direct reporting or indirect reporting.

## 5.3 Procedures for Data Collection AF subscription

Editor’s Note: It appears that the specification of the *Naf\_EventExposure* service to NF consumers residing outside the trusted domain is outside the current scope of SA2. Therefore, it is unclear whether SA2 will wish to take the lead on the design of the Naf\_EventExposure API in support of subscription by and event notification to an ASP (i.e. its Event Consumer AF) located in an external DN. To be confirmed by LS exchange with SA2, SA4 may be responsible for defining *Naf\_EventExposure*, and whereby close coordination with SA2 and perhaps CT3 will be necessary to ensure appropriate handling and ownership of the stage 2 and stage 3 specifications of the associated *Naf\_EventExposure* and *Nnef\_EventExposure* service APIs.

Subsequently, one or more of the two types of event consumer discover the Data Collection AF and subscribe to events from it.



Figure 5.3‑1: High-level procedures for subscription phase

The steps are as follows:

5. The NWDAF discovers the Data Collection AF by following the Nnrf\_NFDiscovery procedure defined in clause 5.2.7.3 of TS 23.502 [3]...

6. ...and then subscribes to event(s) of interest by invoking the Naf\_EventExposure\_Subscribe service operation defined in clause 5.2.19.2.2 of TS 23.502 [3] on the discovered Data Collection AF.

7. The Event Consumer AF discovers the Data Collection AF by following the Nnrf\_NFDiscovery procedure defined in clause 5.2.7.3 of TS 23.502 [3]...

8. ...and then subscribes to event(s) of interest by invoking the Naf\_EventExposure\_Subscribe service operation defined in clause 5.2.19.2.2 of TS 23.502 [3] on the discovered Data Collection AF.

## 5.4 Procedures for configuring data collection client

At some later point, one or more of the three types of data collection client obtain their configuration from the Data Collection AF by invoking the Ndcaf\_DataReporting service defined in the present document and specified in TS 26.532 [7]. The intersection between the above provisioning information and current event consumer subscriptions determines the contents of this configuration.



Figure 5.4‑1: High-level procedures for data collection client configuration phase

The steps are as follows:

9. The Direct Data Collection Client acquires its data collection and reporting configuration from the Data Collection AF, if relevant.

10. The Indirect Data Collection Client acquires its data collection and reporting configuration from the Data Collection AF, if relevant.

11. The AS acquires its data collection and reporting configuration from the Data Collection AF, if relevant.

Whenever the provisioning information changes, or the set of event exposure subscriptions changes, a new set of data collection and reporting configuration shall be made available to data collection clients by the Data Collection AF.

## 5.5 Procedures for reporting to the Data Collection AF



Figure 5.5‑1: High-level procedures for data reporting and exposure phase

The different data collection clients proceed as follows:

12. The Direct Data Reporting Client may submit a data report to the Data Collection AF via reference point R2 by invoking the Ndcaf\_DataReporting service defined in the present document and specified in TS 26.532 [7].

13. The UE Application may send application-specific data reporting to the Application Service Provider...

14. ...and the Indirect Data Collection Client may, as a result, submit a data report to the Data Collection AF by invoking the Ndcaf\_DataReporting service defined in the present document and specified in TS 26.532 [7].

15. The AS may submit a data report to the Data Collection AF by invoking the Ndcaf\_DataReporting service defined in the present document and specified in TS 26.532 [7].

## 5.6 Procedures for Data Collection AF data exposure

In response to receiving a data report:

16. The Data Reporting AF processes the data report.

Reception of a data report by the Data Collection AF may result in an event being exposed to subscribed event consumers:

17. The Data Collection AF may expose an event to the NWDAF by invoking the Naf\_EventExposure\_Notify service operation on the latter, as defined in clause 5.2.19.2.4 of TS 23.502 [3].

18. The Data Collection AF may expose an event to the Event Consumer AF by invoking the Naf\_EventExposure\_Notify service operation on the latter, as defined in clause 5.2.19.2.4 of TS 23.502 [3].

## 5.7 Procedures for Data Collection AF unsubscription



Figure 5.7‑1: High-level procedures for unsubscription phases

Finally:

19. The NWDAF unsubscribes to events from the Data Collection AF by invoking the Naf\_EventExposure\_Unsubscribe service operation, as defined in clause 5.2.19.2.3 of TS 23.502 [3].

20. The Event Consumer AF unsubscribes to events from the Data Collection AF by invoking the Naf\_EventExposure\_Unsubscribe service operation, as defined in clause 5.2.19.2.3 of TS 23.502 [3].

## 5.8 Procedures for event consumer authorization

The procedure for authorising access to the events exposed by the Data Collection AF is depicted by the following call flow:



Figure 5.8‑1: High-level procedures for event consumer authorization

The steps are:

1. The Provisioning AF provisions the data collection and the report exposure functionality at reference point R1, per the procedures in clause 5.2, including a set of Data Access Profiles.

2. An event consumer sends a subscription request to the Data Collection AF to receive events via reference point R5 or R6, per the procedures in clause 5.3, indicating the Event ID of interest. The subscription request may nominate a specific Data Access Profile by citing its unique identifier.

3. In return, the Data Collection AF redirects the event consumer to the Authorization AS in order to obtain access based on the requested Data Access Profile.

4. The event consumer contacts the Authorization AS (according to the procedures for authorization of NF service access defined in clause 13.4 of TS 33.501 [9]) with a set of valid credentials and optionally the requested Data Access Profile.

5. If access is granted, the Authorization AS responds with an access token that is valid for the authorised Data Access Profile for a specific period of time. The response may redirect the event consumer to the Data Collection AF using the initial subscription request URL, enhanced with the access token.

6. The event consumer resends the subscription request to the Data Collection AF, this time with the access token.

7. The Data Collection AF may verify the access token with the authorization server, or it may verify it locally.

8. If verification is successful, the Data Collection AF approves the subscription request for the requested Access Profile

9. The Data Collection AF sends event notifications to the event consumer, per the procedures in clause 5.6.

10. The event consumer cancels its event subscription using the procedures in clause 5.7.

Annex A (informative):
Collaboration scenarios for data collection and reporting

# A.1 General

This annex documents a set of collaboration scenarios that illustrate potential deployments of the data collection and reporting architecture as defined in the present document.

In deployment, it is possible that some UE data is provided to the Data Collection AF using the direct data reporting method at reference point R2, while other (application-private) UE data is collected via reference R8 and provided to the Data Collection AF via the indirect data reporting method at reference point R3 (R3′ in Collaboration D). In certain domains, UE data is collected in the first instance by an AS and therefore needs to be provided to the Data Collection AF at reference point R4 (R4′ in Collaboration D). Hence, all three data reporting reference points are potentially in scope for all of the documented collaboration scenarios.

NOTE 1: In all of the documented collaboration scenarios, reference point R2 traverses the data plane between the Direct Data Collection Client and the Data Collection AF regardless of whether the latter is deployed inside or outside the trusted domain.

NOTE 2: In all of the documented collaboration scenarios, reference point R8 traverses the data plane between the UE Application the Application Service Provider. The traffic carried at this reference point is tunnelled transparently through the trusted domain without interacting with any control plane entities.

# A.2 Collaboration A

In this collaboration scenario all of the functions are deployed inside the trusted domain. This corresponds to the case where the functional entities of the Application Service Provider as well as the Application Server (AS) are internal to the 5G System.

NOTE: Although deployed within the trusted domain, and granted privileged access to certain Network Functions in the 5G System, the Application Service Provider and/or the AS may or may not be under direct control of the MNO in this collaboration scenario. For example, management of one or more of the functional entities may be delegated to a trusted third-party service provider.



Figure A.2‑1: Collaboration A with all functions deployed inside the trusted domain

# A.3 Collaboration B

In this collaboration scenario the functional entities of the Application Service Provider are deployed outside the trusted domain. Interactions between these functions and the Data Collection AF must therefore be mediated by the NEF.

Editor's Note: Need to check with SA2 that the proposed new Ndcaf service can be exposed via NEF.



Figure A.3‑1: Collaboration B with all functions of Application Service Provider
deployed outside the trusted domain

# A.4 Collaboration C

This collaboration scenario illustrates the case where the Application Server (AS) is also deployed outside the trusted domain (in addition to the functional entities of the Application Service Provider per Collaboration B). In this case, the AS must therefore additionally interact with the Data Collection AF via the NEF.

Editor's Note: Need to check with SA2 that the proposed new Ndcaf service can be exposed via NEF.



Figure A.4‑1: Collaboration C with all functions of Application Service Provider
and Application Server deployed outside the trusted domain

# A.5 Collaboration D

In this collaboration scenario, the Data Collection AF itself is deployed outside the trusted domain and interactions with functions inside the trusted domain occur via the NEF. This scenario corresponds to the "Procedure for Data Collection from AF via NEF" defined in clause 6.2.2.3 of TS 23.288 [4]. Specifically:

- The externally deployed Data Collection AF registers with the NRF inside the trusted domain using the Nnef\_NFManagement service via the NEF.

NOTE: In practice, the Data Collection AF is instantiated as a subfunction of a domain-specific Application Function. The enclosing Application Function should include data collection and reporting capabilities in its own registration with the NRF on behalf of the enclosed Data Collection AF rather than making a separate registration for the subfunction.

- The NWDAF inside the trusted domain uses the Nnef\_EventExposure service (as specified in clause 5.2.6.2 of TS 23.502 [3]) to subscribe to and receive events exposed by the externally deployed Data Collection AF.



Figure A.5‑1: Collaboration D with Data Collection AF deployed outside the trusted domain

The functional entities of the Application Service Provider, as well as the Application Server (AS), interact with the externally deployed Data Collection AF using interfaces that are outside the scope of 3GPP specification. However, the interactions at reference points R1′, R3′, R4′ and R6′ are expected to be functionally equivalent to those at R1, R3, R4 and R6 respectively.

# A.6 Collaboration E

In this collaboration scenario, the Data Collection Client is deployed as a subfunction of the UE Application. As a consequence of this arrangement, reference point R7 is subsumed into the UE Application.

This collaboration may be combined with any of the preceding collaboration scenarios. Hence, only reference points R2 and R8 are depicted in the figure in the interests of brevity.



Figure A.6‑1: Collaboration E with Data Collection Client deployed as part of the UE Application

The Direct Data Collection Client could, for example, be realised as a software library that implements the appropriate protocol at reference point R2. In such a realisation, the procedures defined in the present document at reference point R7 would likely form the API of the Data Collection Client library.

Annex B (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2021-06 | Post-SA4#115-e ad hoc |  |  |  |  | Initial skeleton document. | 0.0.1 |
| 2021-08 | SA4#115-e | S4-211037S4-211218S4-211232 |  |  |  | Addition of reference architecture and collaboration scenarios.References to CAPIF as an implementation option. | 0.1.0 |
| 2021-10 | Post SA4#115-e ad hoc | S4aI211226S4aI211227S4aI211233 |  |  |  | Additional collaboration scenario.Additional service-based reference architecture figure.Informative note declaring R7 for future study. | 0.1.1 |
| S4aI211236S4aI211242S4aI211244 |  |  |  | Domain model.High-level procedures.Corrections and updates to editor’s notes. | 0.1.2 |
| 2021-11 | SA4#116-e | S4-211590S4-211591 |  |  |  | Clarification of direct and indirect reporting.Miscellaneous clarifications and corrections. | 0.2.0 |
| 2021-12 | SA#94-e | SP-211342 |  |  |  | Presentation to SA plenary for information | 1.0.0 |
| 2021-12 | Post-SA4#116-e ad hoc | S4-aI211254 |  |  |  | Domain model revisited. | 1.0.1 |
| 2022-02 | SA4#117-e | S4-200243 |  |  |  | S4-220240: Data exposure restriction model. | 1.1.0 |

1. In the event that provisioning data and subscription data contain similar rules, the permissible information to be exposed by the Data Collection Function shall be governed by the rule with more restrictive semantics. [↑](#footnote-ref-1)