3GPP TSG-SA WG3 eMeeting #105-e
E-meeting, 08th Nov– 19th Nov 2021

S3-213965

Discussion on Data Integrity Service in IoT

China Unicom

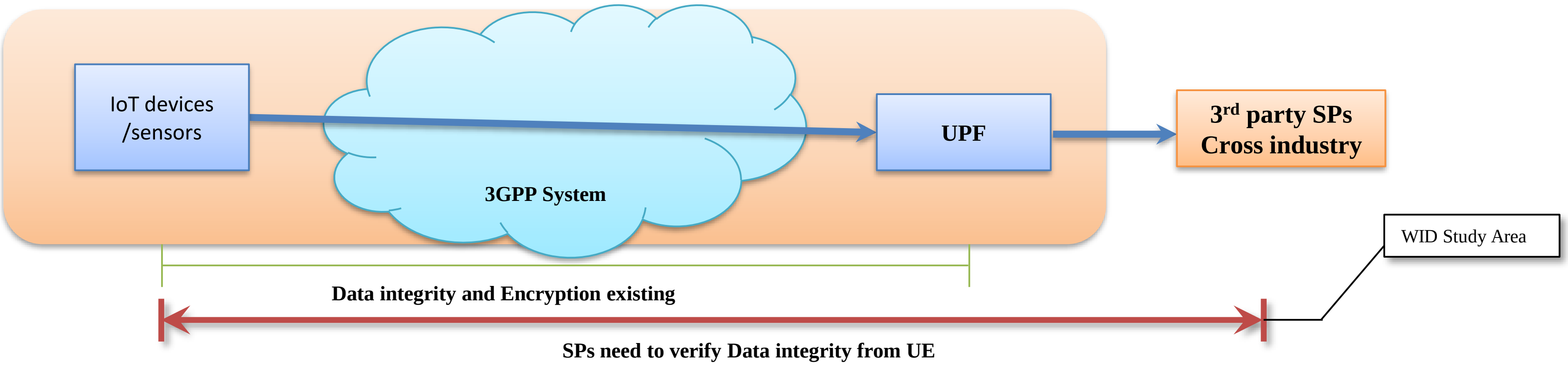
Xing tianqi

Why

The requirement of data integrity in verticals

- Data collected from IoT devices/sensors is mostly sent to service platform directly, e.g. position data in logistics services.
- However IoT data for finance related services may be very crucial. Hence verticals such as supply chain finance and insurance have strict requirements for data integrity, e.g. environment data(e.g. temperature and windspeed) for agricultural insurance and warehouse data (e.g. number and weight of goods) for inventory financing. Those services requi to data exchange from IoT devices/sensors to the third party SP（service provider).

Gap between 3GPP and requirement of verticals


IoT devices /sensors
3GPP System
UPF
3rd party SPs Cross industry
WID Study Area
Data integrity and Encryption existing
SPs need to verify Data integrity from UE

- While data integrity methods are provided within the 3GPP network, there are gaps of how to verify data integrity as a service between a UE to 3rd party Service Providers using the 3GPP Network.
- Moreover, data integrity is important for data verification services(e.g. an insurance claim)
- In any case, all kinds of IoT UEs and SPs of the enterprises above are connected to MNO’s networks, especially the more extensive cross industry SP business model.
- Need to get ready to provide a mechanism to realize data integrity verify service for the community in the interest alliance.

Related Requirement

- **22.261's CR: TS 22.261 descrbe Data Integrity Service Requirements in 5GS to assure the integrity of the data exchanged between the 5G network and a third-party service provider:**

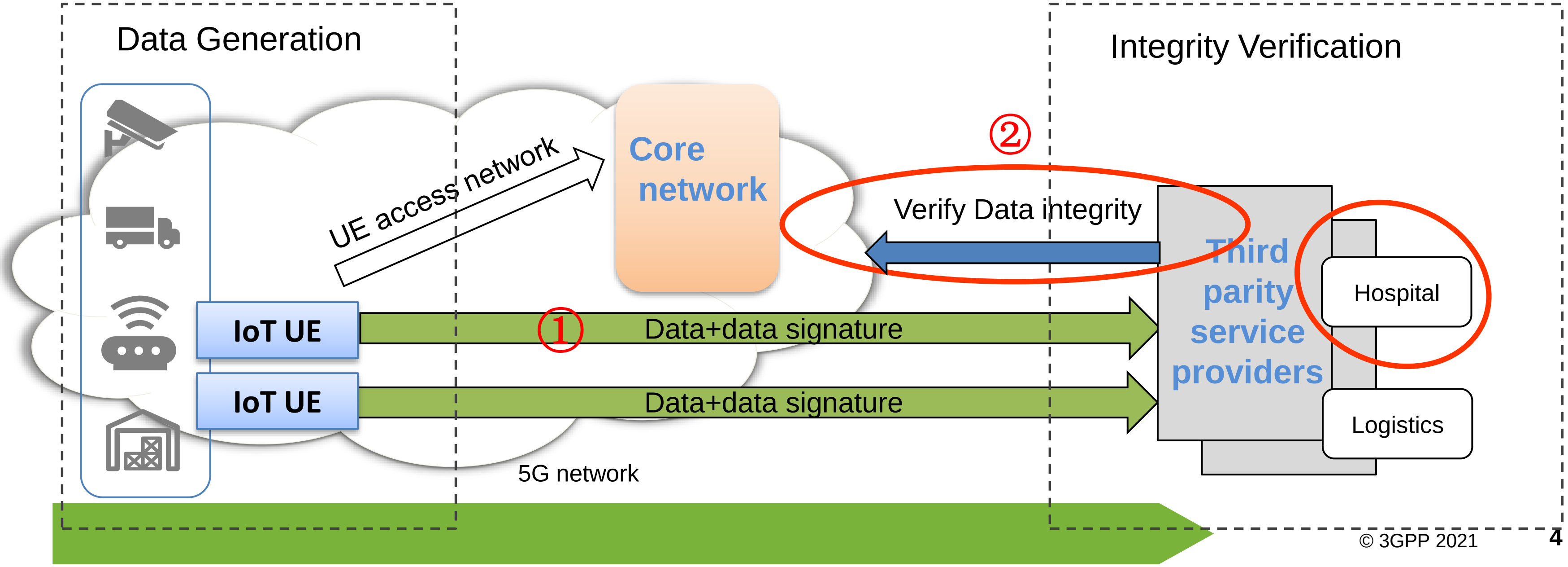
Subject to regulatory requirements and based on operator policy, the 5G system shall provide a mechanism to support data integrity verification service to assure the integrity of the data exchanged between the 5G network and a third-party service provider.

NOTE: This requirement could apply to mechanisms supported over the interface between 5G core network and an external application, with no impact on RAN and UE.

Case Example

Cold Chain Logistics

- ①During the transportation of vaccines/drugs, vaccines/drugs containers in cold chain logistics may be equipped with IoT sensors which send data to the vehicles. Those vehicles connect to a SP platform by 3GPP network for data gathering and processing. Monitoring is very critical since the products in the container may exceptionally sensitive to changes in pH, temperature and even light conditions.
  - Ensuring the collected environment data unchanged in each container/sensor is necessary to the service in order to guarantee vaccine/drug activity.
  - In this use case, the requirements are to achieve the data integrity for the environment data.
- ②Moreover, If problems arose, SP (hospital or vaccine company) would claim to verify the environment data of transportation.



Requirement Gap Analysis

AKMA（SA3）

- 3GPP TS 33.535 specifies the security features and mechanisms to support authentication and key management aspects for applications based on subscription credential(s) in 5G system.
- GAP1: AKMA is an authentication mechanism in 5G network layer.
- GAP2: Identify new Network Element AAnF and protocols .

GBA（SA3）

- 3GPP TS 33.220 describes the security features and mechanisms to bootstrap authentication and key agreement for application security.
- GAP1:GBA provide an authentication mechanism in 4G network layer
- GAP2:Identify new Network Element BSF and protocols.

Study on Data Integrity Service in IOT of SA6

- This SID is designed to provide Data Integrity Service in from IoT UE to a third party SP in application layer.
- Have no impact on UE’s chip/physical layer.

SA6 proposed way of Application

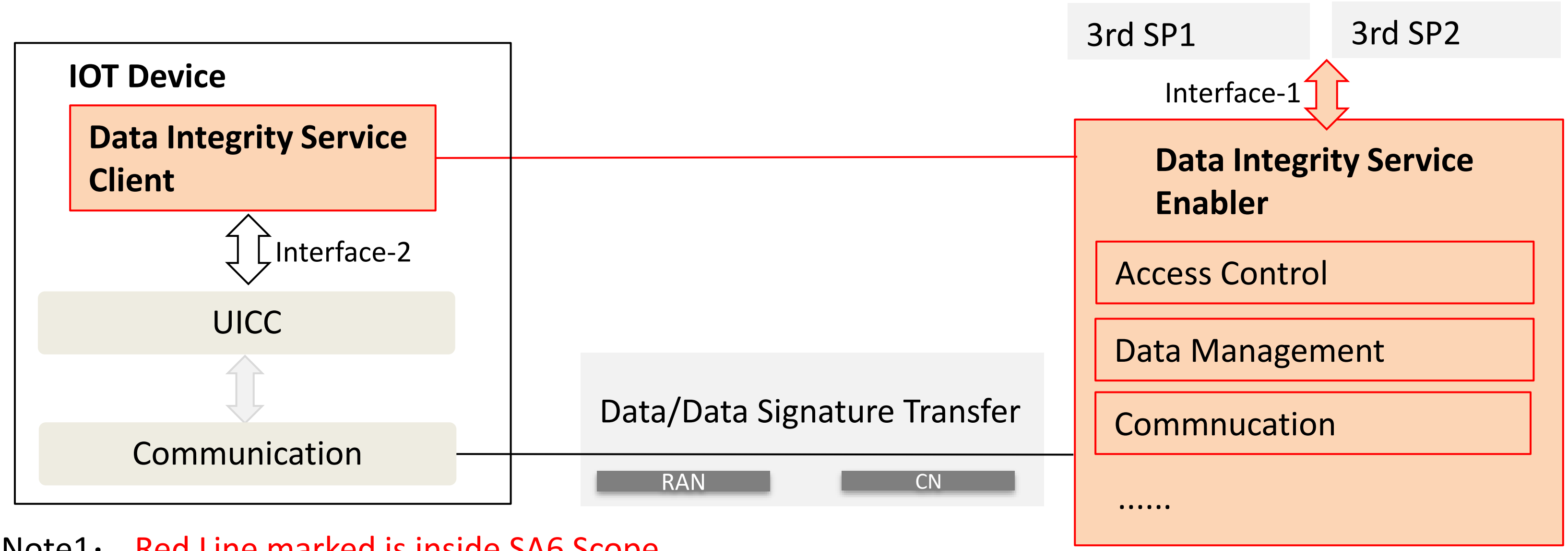
Data Integrity Service in IoT

1)Analyze existing requirements of data integrity service based on TS 22.261 Subclause 8.9.

2)Evaluate application architectural requirements and application layer architectures for data integrity service.

3)Analyze the re-use of functionalities from SA6 specifications for the solutions, where applicable.

4)Identify key issues and develop solutions based on 1) -3) .



Note1： Red Line marked is inside SA6 Scope

Note2： Application solutions have no impact on UE chip/physical layer.

MisAlignment with SA1 requirement?

- *Subject to regulatory requirements and based on operator policy, the 5G system shall provide a mechanism to support data integrity verification service to assure the integrity of the data exchanged between the 5G network and a third-party service provider.*
  - *NOTE: This requirement could apply to mechanisms supported over the interface between 5G core network and an external application, with no impact on RAN and UE.*

---TS 22.261

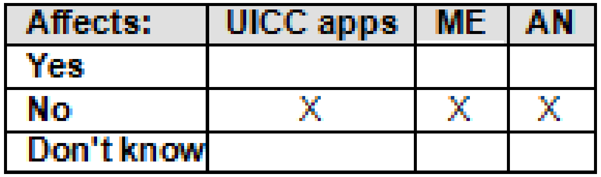
1-The requirement refers to **5G system** to support **DI verificarion service** within 5G system.

2-For it is a **SERVICE** requirement， the **client-server service model** could be the reasonable assumption(which is SA6’s scope), and the related data generated or collected from the UE and then transmitted to the SP through the 5G network.

3-The requirements are clear to state no impact on the chip and physical layer of UE.

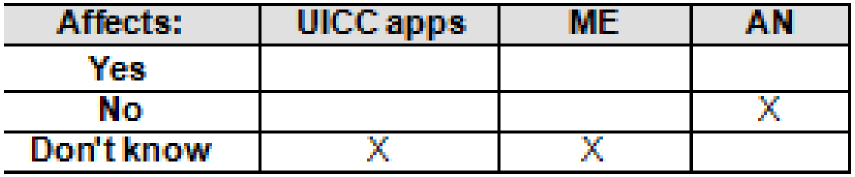
However, the difference of scopes are reasonable, because SA6 discusses the content including UE client.

SA1: WID Scope



Affects:	UICC apps	ME	AN
Yes			
No	X	X	X
Don't know			

SA6: SID Scope

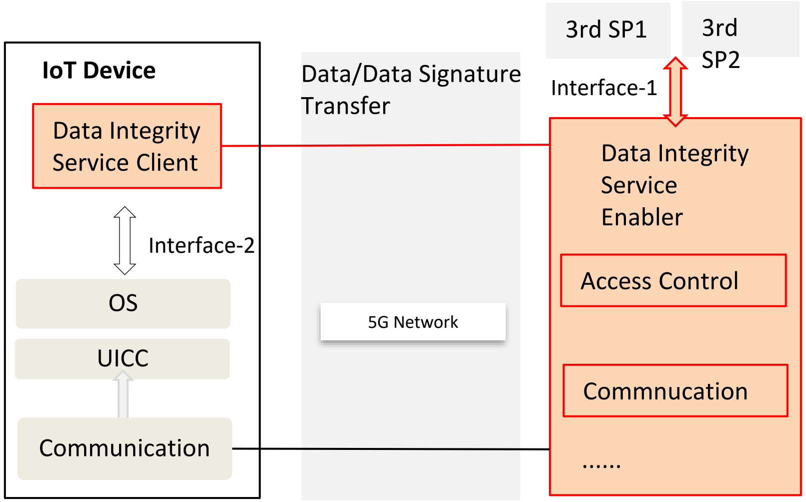


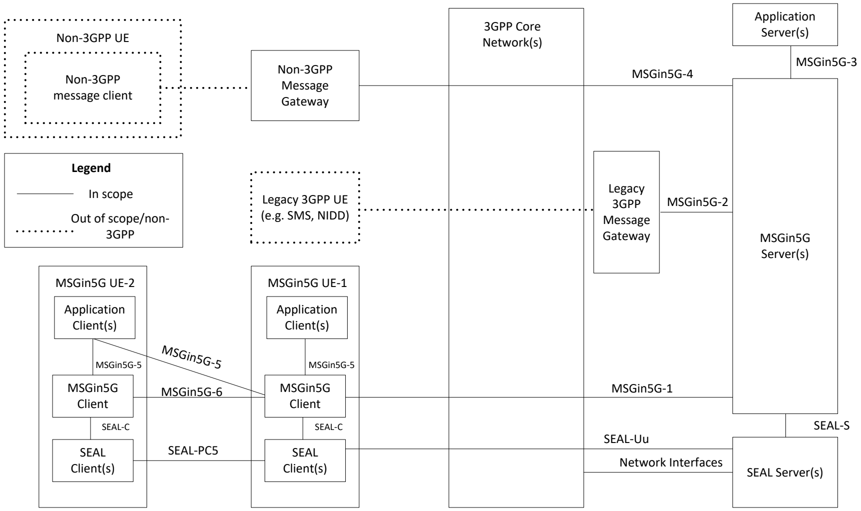
Affects:	UICC apps	ME	AN
Yes			
No			X
Don't know	X	X	

Note: Concept reference could be found on the attached page.

ME Affect Analysis

Data Integrity Service in IoT





Application Airchitecture of MSGin5G Service from TS.23.554

The ME of SA6 affect ONLY in the application layer(Data Integrity Service Client is an App client), has NO effect on UE chip

- Worked as APP Client-Server Model,similar as MSGin5G Service(3GPP TS 23.554 etc.)
- The Interface from Client to OS, UICC and etc. can reuse the existing mechanisms.

Note1： Red Line marked is inside SA6 Scope.

Thank you

Definition related to ME and UE

- PS: definition in TS 21.905
  - **Mobile Equipment (ME)**: The Mobile Equipment is functionally divided into several entities, i.e.one or more Mobile Terminations (MT) and one or more Terminal Equipments (TE).
  - **Mobile Termination (MT)**: The Mobile Termination is the component of the Mobile Equipment (ME) which supports functions specific to management of the PLMN access interface (3GPP or non-3GPP). The MT is realized as a single functional entity..
  - **Terminal Equipment (TE)**: Equipment that provides the functions necessary for the operation of the access protocols by the user. A functional group on the user side of a user-network interface (source: ITU-T I.112).
  - **User Equipment (UE)**: Allows a user access to network services. For the purpose of 3GPP specifications the interface between the UE and the network is the radio interface. A User Equipment can be subdivided into a number of domains, the domains being separated by reference points. Currently the User Equipment is subdivided into the UICC domain and the ME Domain. The ME Domain can further be subdivided into one or more Mobile Termination (MT) and Terminal Equipment (TE) components showing the connectivity between multiple functional groups.