**3GPP TSG-SA3 Meeting #107-e *S3-220791***

**e-meeting, 16 - 20 May 2022**

**Source: China Mobile, CableLabs, Huawei, Hisilicon, Xiaomi**

**Title: New SID on Study on security aspects for XR and media services**

**Document for: Approval**

**Agenda Item: 6**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study on security aspects for XR and media services

Acronym: FS\_XRM\_sec

Unique identifier: xxx

Potential target Release: Rel-18

# 1 Impacts

{For Normative work, identify the anticipated impacts. For a Study, identify the scope of the study}

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | X |  |
| No |  |  |  |  |  |
| Don't know | X | X | X |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

{Tick one box. "**Feature** / **Building Block** / Work Task" form a hierarchical structure. E.g. no Building Block can be proposed without a corresponding parent Feature. The full structure of all existing Work Items is shown in the 3GPP Work Plan in ftp://ftp.3gpp.org/Information/WORK\_PLAN}

|  |  |
| --- | --- |
|  | Feature |
|  | Building Block |
|  | *Work Task* |
| X | Study Item |

## 2.2 Parent Work Item

|  |
| --- |
| Parent Work / Study Items  |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
|  |  |  |  |

### 2.3 Other related Work Items and dependencies

|  |
| --- |
| Other related Work /Study Items (if any) |
| Unique ID | Title | Nature of relationship |
| 900027 | Study on supporting tactile and multi-modality communication services (Release 18) | Study of requirement about tactile and multi-modality communication services  |
| 800014 | Study on Audio-Visual Service Production (Release 17) | Multiple devices collecting data for the same task with strict KPI requirements. |
| 940068 | Study on XR (Extended Reality) and media services (Release 18) | SA2 study on the architecture of XR and media services |
| 940016 | Study of privacy of identifiers over radio access | SA3 study on privacy of identifiers over radio access |

# 3 Justification

Mobile media services with high bandwidth, low latency and mass connection requirements such as XR (eXtended Reality) based healthcare, self-driving, industrial automation and gaming etc pose fundamental challenges to 5G network. It is relatively easy to configure the 5G network to meet one of above requirements for XR, but it's difficult to satisfy all of them.

From the security perspective, XR services also attract more security attacks because of its coexistence with potential adversary entities in an open environment and its increased points of attacking with data from multiple sources and sensors. Some of the security and privacy threats include the following:

Device compromise: As XR very likely deploys devices and sensors in open environment as in the case of IoT, XR devices are in more danger of being compromised through physical contact or visual observation by adversaries. As a result of device compromise, user’s credentials can be stolen or directly accessed. As such, it becomes crucial to design systems which can prevent an adversary from directly exploiting such a compromise. For instance, it should not be possible to directly replay an obtained credential, nor should adversaries be able to use the compromised clients for further, more damaging attacks.

Privacy of biometric data: in XR applications biometrics based authentication is more widely used, such as finger print, eye scan, face recognition etc. It's a larger security and privacy problem if biometrics data are leaked due to their irrevocability. Users would face the nightmare of security threat once their biometrics data are compromised. Therefore, biometric privacy becomes a very important issue in designing security architectures, algorithms and procedures for XR.

Denial of service attack: XR applications are very resource intensive, so the XR servers and 5G processing nodes at the core or at the edge would be under high load. If attacks find out a node along the path and start DoS/DDoS attack on it, it would be relatively easy to bring down the whole XR service to its knee, or at least causing it not useable by failing to meet the required bandwidth and latency.

Current security mechanisms in 5GS are helpful in dealing with security threats faced by XR applications, but the overhead imposed by current 5G security mechanisms could become a main roadblock. As stated before, XR will push 5G network to its limit by requiring both high bandwidth and low latency, the high demand of computational and network processing from current security mechanisms may cause the latency and bandwidth requirement to fail. To reduce security overhead, lightweight or selective/adaptive security mechanisms can be brought into play. Security and QoS modules, or AF and 5GS could also coordinate to dynamically adjust the security resource consumption to favour XR's bandwidth and latency demands if needed.

For example, coordination between security protection and QoS handling of XR multi-modality data flows can be considered. In order to better utilize radio resources, 5GS may perform filtering on PDU sets to selectively discard the packets from data flows with low priority based on radio utilization, which may interfere with 5GS UP integrity policy depending on how data packets are processed at UPF, gNB or UE. In order to help classify PDU sets, data packets are appended with extra information such as PDU set ID, importance level, correlation sequence number etc, it's also to be investigated whether these classification fields need to be protected for confidentiality and integrity.

Moreover, XR may require further information exposure from 5GS to AF that hosts XR applications (especially for the media services with large traffic burst) to help application adapt to network congestion and provide better QoE. It needs to prevent sensitive information of the 5GS and users from being exposed and whether they need security and privacy protection.

Considering the above security challenges, it is important to start SA3 research to identify security issues brought by XR related services, investigate on the security solutions to mitigate the security threats and issues to help the further advancement of XR services and their wide deployment.

# 4 Objective

The study item aims at identifying the security and privacy threats associated with XR media services, investigating approaches to mitigate security threats being identified, and providing security recommendations to better support advanced XR media services.

This study may include but not limited to the following objectives:

1. Investigate the security optimization for XR services in 5GS.

 - Lightweight security mechanisms to meet the URLLC scenarios for XR media services

 - Fine granularity security policy based on PDU set to provide security protection for multi-modal data (such as video, audio and haptic etc) in XR applications to improve user’s QoE.

2. Investigate security protection needed for enhanced XR QoS.

- Security protection needed for the important information which may be appended to the XR PDU packets e.g. PDU set ID, importance level of the PDU set, correlation sequence number of the PDU set, etc

3. Investigate the privacy and security protection of information exposure between 5GS and XR applications.

 - Identify the security/privacy issues of 5GS network information (e.g., NF ID, S-NSSAI(s) etc.) to be exposed to XR applications and their protection mechanisms.

 - Identify sensitive information (such as biometrics data) from XR applications being exposed to 5GS and their privacy protection.

NOTE: Coordination with the Privacy Study in TR 33.870 may be needed for the above bullets.

# 5 Expected Output and Time scale

|  |
| --- |
| New specifications {One line per specification. Create/delete lines as needed} |
| Type  | TS/TR number | Title | For info at TSG#  | For approval at TSG# | Rapporteur |
| Internal TR | 33.xxx | Study on security aspects for XR and media services | TSG SA#97 | TSG SA#98 | Hua Song, China Mobile, songhua@chinamobile.com  |

|  |
| --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} |
| TS/TR No. | Description of change  | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

Hua Song, China Mobile, songhua@chinamobile.com

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

Potential interactions with SA2 for the architectural aspects, and RAN 2/3 for the RAN architectural aspects.

9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| China Mobile |
| CableLabs  |
| CATT  |
| Huawei |
| HiSilicon |
| Interdigital |
| Lenovo |
| Xiaomi |
| ZTE |
|  |
|  |
|  |
|  |
|  |
|  |
|  |