**SA WG2 Meeting #162 S2-2405394**

**15 April – 19 April, 2024, Changsha, China (revision of S2-2404806)**

**Source: Apple, ZTE, InterDigital**

**Title: KI#3: Interim Conclusion Principles**

**Document for: Approval**

**Agenda Item: 19.8**

**Work Item / Release: FS\_UIA\_ARC / Rel-19**

*Abstract of the contribution:* *This paper proposes conclusion principles for Key Issue #3 “Exposure of User Identity Profile Information”*

# 1 Discussion

This paper proposes interim conclusion principles for Key Issue #3 “Exposure of User Identity Profile Information”.

# 2 Proposal

It is proposed to include the following changes in TR 23.700-32 V0.2.0.

 **\* \* \* \* Start of Changes – All New Text \* \* \* \***

## 8.X Key Issue #3 Conclusions

The following conclusion principles are agreed for key issue #3.

* User consent aspects about any potential exposure of user identity information (including verification result) should be checked by SA WG3.
* User identifier verification result can be exposed by a NEF API to an authorized AF.
	+ This is to enable a service, where a 3rd party AF can trust a User accessing its services using the User Identifier based on the verification result (i.e. success or failure) obtained from MNO.

NOTE: How an AF is authorized to receive information about user identity will be addressed by SA WG3.

Editor’s Note: The above conclusion principles are only tentatively agreed.

Editor’s Note: Exposure of other content of user identity profile will be justified with relevant use cases or service requirements once the contents of user identity profile is finalised.

**\* \* \* \* End of Changes \* \* \* \***