

Proposed SIs for Security WG in 2020

Zhimin Du/Yan Li
Qualcomm

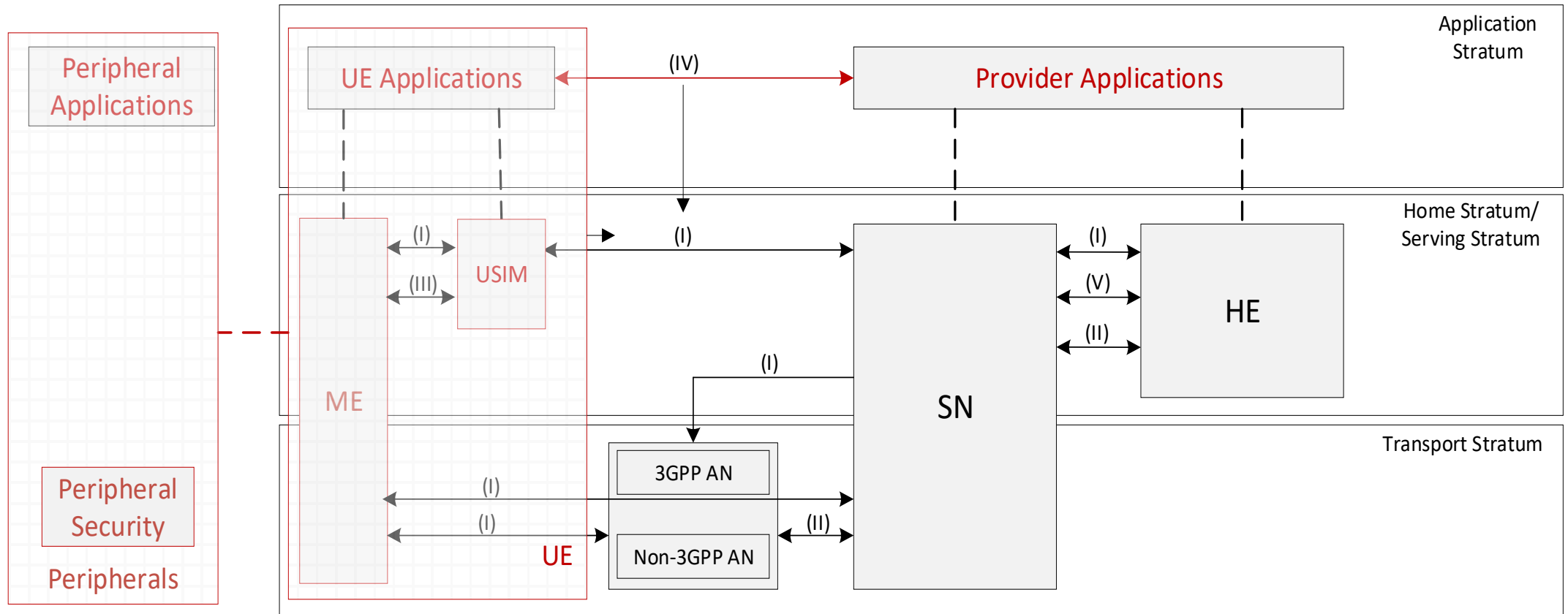
Contents

- UE-Centric 5G Security Whitepaper 2.0
- New Study on 5G Slicing Security

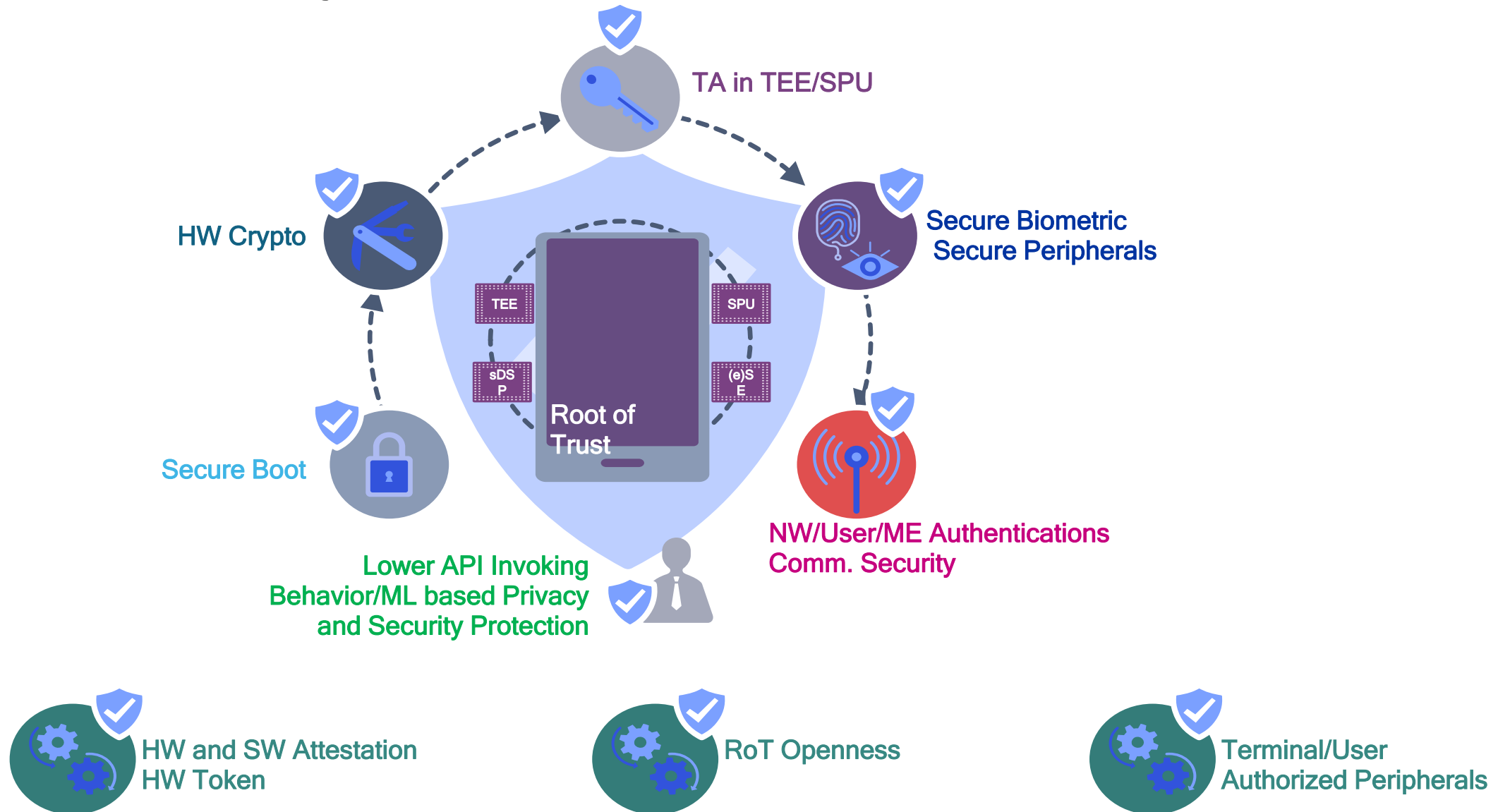
Contents in Whitepaper 1.0

- Chapter 1: Preface and General Introduction
- Chapter 2: 5G Applications and Terminal
 - Focusing on security relevant use cases
- Chapter 3: Security Threats in Aforementioned Use Cases
- Chapter 4: Security Solutions
 - Traditional solutions
 - Emerging solutions (5G SUCI/Authentication)
- Chapter 5: UE-Centric Security
 - UE as RoT
 - Remote Authentication and Attestation
 - Hardware Token
 - Openness of UE RoT and Security Capabilities
 - Multi-role Isolation

Based on 3GPP Security Architecture with Extensions

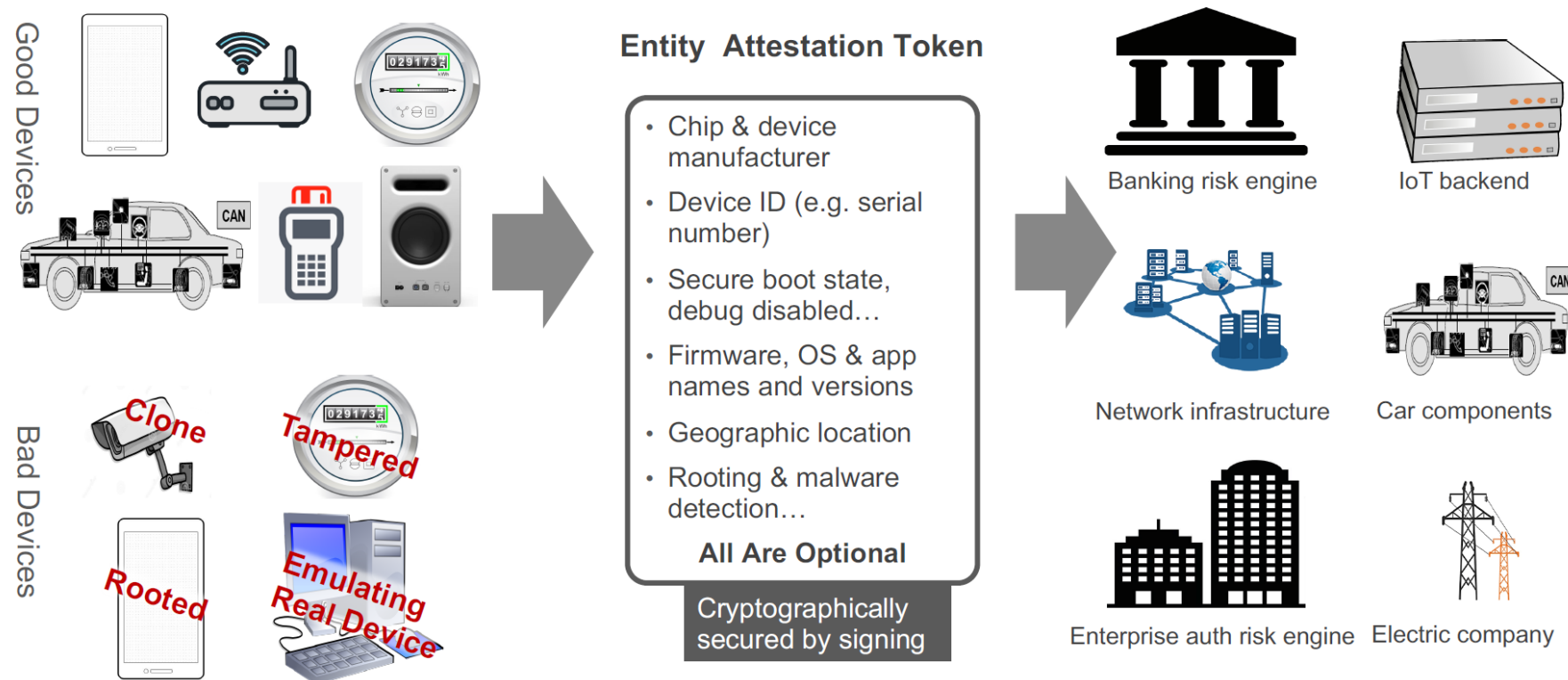


UE-Centric Security Framework as the Foundation



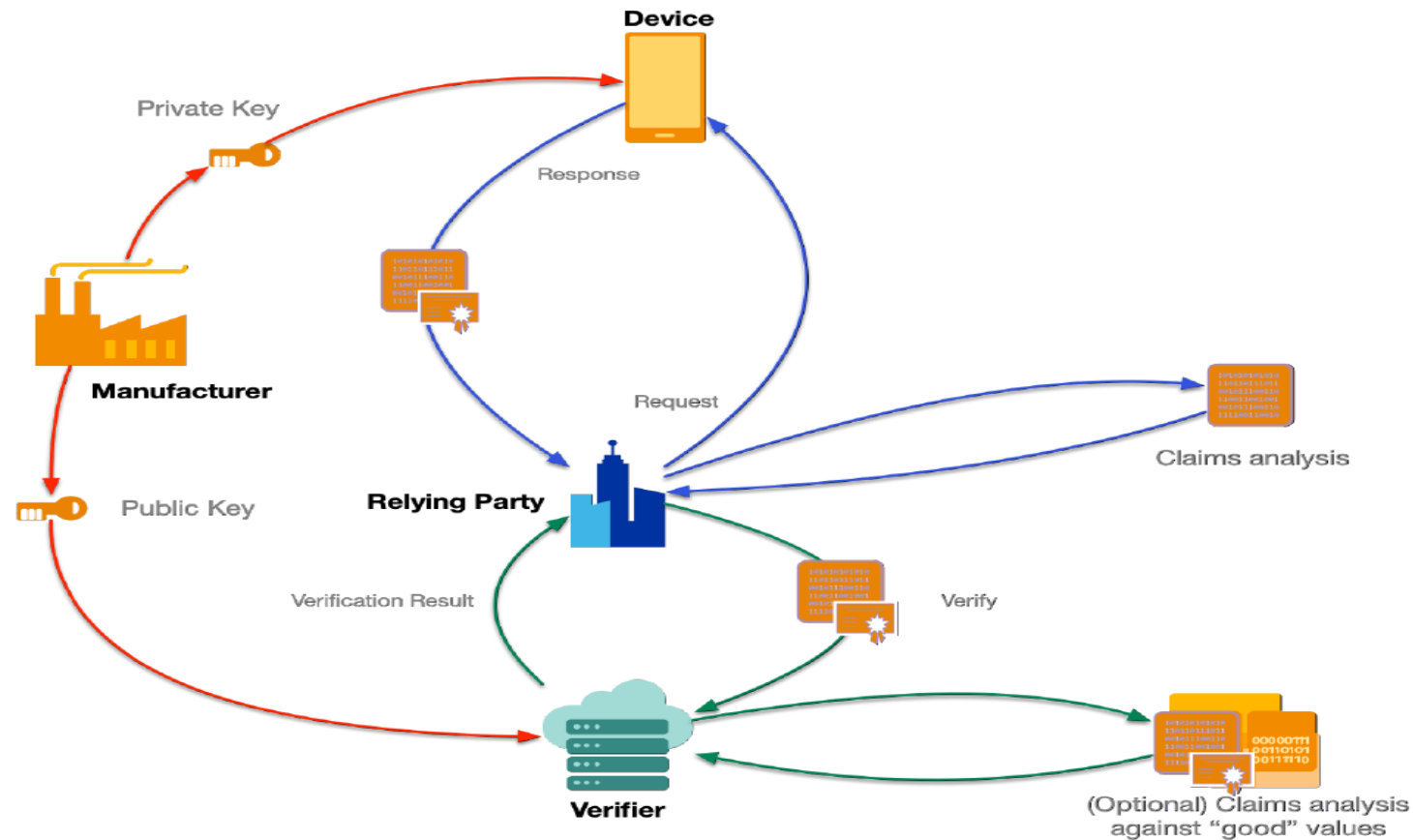
Candidate Contents for Whitepaper 2.0 (1/3)

- Combination of Remote Attestation and Hardware Token
 - Hardware token based remote attestation
 - IETF RATS WG is developing a new RFC EAT



Candidate Contents for Whitepaper 2.0 (2/3)

- Combination of Remote Attestation and Hardware Token



Candidate Contents for Whitepaper 2.0 (3/3)

- More scenarios and solutions on Openness of UE RoT and Security Capabilities
- 3GPP AKMA study
- Transfer/Relay of Trust
 - Tsinghua Uni. inputs?
 - Hop-by-Hop, E2E, 3GPP IAB Security study?
- New UE-involved and security-required use cases (if any)?
- Also open to other proposals

Contents

- UE-Centric 5G Security Whitepaper 2.0
- New Study on 5G Slicing Security

5G Slicing Security Study (1/3)

- Network Slicing deemed as the critical feature to enable 5G SA usage for Verticals
- What 3GPP has done on 5G Slicing Security

Key issue	Solution1	Solution2	Solution3	Solution4	Solution5	Solution6	Solution7	Solution8	Solution 9	Solution 10
#1 Authentication for access to specific Network Slices	Yes	Yes	NA	Evaluation pending	NA	NA	NA	NA	NA	NA
#2: AMF Key separation	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
#3: Security features for NSaaS	NA	NA	Evaluation pending	NA	NA	NA	NA	NA	NA	NA
#4: Security and privacy aspects related to the solution for Network Slice specific access authentication and authorization	Evaluation pending	NA	NA	NA	Evaluation pending	Evaluation pending	Evaluation pending	NA	NA	NA
#5: Access token handling between Network Slices	NA	NA	NA	NA	NA	NA	NA	NA	Evaluation pending	NA
#6: Confidentiality protection of NSSAI and home control	NA	NA	NA	NA	NA	NA	NA	Evaluation pending	NA	Evaluation pending

5G Slicing Security Study (2/3)




- What 3GPP has done on 5G Slicing Security
 - Focus on Network Slice Specific Authentication and Authorization (NSSAA)
 - **General conclusions**
 - *Slice specific authentication is optional to use*
 - *Slice specific authentication uses a User ID and credentials, different from the 3GPP subscription credentials (e.g. SUPI and credentials used for PLMN access) and takes place after the primary authentication.*
 - *AMF confirms, locally or based on ARPF/UDM, whether slice authentication is required for each S-NSSAI*
 - *Slice specific authentication is based on EAP framework where AMF takes the role of the passing through Authenticator*
 - **Conclusions for key issues**
 - *For Key Issue #1 Authentication for access to specific Network Slices, a merge of Solution#1, solution#2 and Solution#4 are recommended as the basis for the normative work.*
 - *For Key Issue#2, AMF key separation, it is concluded not to consider in the present document, since the use case that this key issue is addressing, is not concluded in TR 23.740 [5].*
 - *For Key Issue #4, it is recommended that no normative work is required.*
 - *For Key Issue #5, it is recommended that Solution #9 is used as the basis for normative work.*

5G Slicing Security Study (3/3)

- Suggest to also study other parts beyond 3GPP scope, e.g.
 - Appropriate ID and credential management for NSSAA
 - Slice specific and vertical services oriented security other than NSSAA
 - Application management, policy mapping, slice selection for different verticals
 - Charging?
 -



Thank you

Follow us on:    

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

©2018 Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes Qualcomm’s licensing business, QTL, and the vast majority of its patent portfolio. Qualcomm Technologies, Inc., a wholly-owned subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of Qualcomm’s engineering, research and development functions, and substantially all of its product and services businesses, including its semiconductor business, QCT.