

TSG-SX Correspondence

Dr. Xiaowu (Frankle) Zhao
Chair, 3GPP2 TSG-SX
ZTE Corporation
tsgsx_chair@3GPP2.org

November 4, 2014

To:

Dr. Klaus Vedder
Chairman, ETSI TC SCP
klaus.vedder@gi-de.com

Subject: RE: Network Access Algorithm Support for the Embedded UICC (ETSI TC SCP(14)000266)

Dear Dr. Vedder,

3GPP2 would like to thank ETSI SCP for informing us about the progress of your work on Embedded UICC (eUICC) and the issue of network access algorithm support. The standards developed by ETSI SCP in this area would greatly help expand the adoption of 3GPP2 access technologies in Machine-to-Machine (M2M) applications.

We would like to provide the following responses on your 4 actions to 3GPP2 TSG-SX WG4.

Action 1. To consider whether Embedded UICCs that are intended for use on 3GPP or 3GPP2 networks should support a standardised network access algorithm, and if so, which one

With respect to the support of cryptographic algorithm(s) for AKA authentication over 3GPP2 access networks, as currently specified, we would like to note that there are two possible scenarios:

1. Use of CSIM as a Network Access Application (NAA) to access services provided by 3GPP2 core network, using CDMA 1xRTT or High Rate Packet Data (HRPD) access technologies.
2. Use of USIM as a Network Access Application (NAA) to access services provided by the 3GPP Evolved Packet Core (EPC) network, using evolved HRPD (eHRPD) access technology.

In case of scenario 1, the AKA algorithm used would depend on the algorithm supported by the 3GPP2 core network (e.g., HLR /AuC or AAA) and the CSIM. This is typically determined by the

©2014 3GPP2

This correspondence represents "working papers". Therefore, the contents cannot be viewed as reflecting the corporate policies or the views of the Third Generation Partnership Project 2 or of any company. The Partnership Project, the companies and individuals involved take no responsibility in the application of contents of this document.

3GPP2 network operator issuing the CSIM. SHA-based example AKA algorithm is specified in 3GPP2 [S.S0055](#) and 3GPP2 [S.S0078](#).

In case of scenario 2, the AKA algorithm used would depend on the algorithm supported by the 3GPP network operator (i.e., HSS) and the USIM. The AKA algorithms that are used by these entities are under the scope of 3GPP TSG SA3.

Therefore, unless all operators agree to implement and use AKA for authentication, using e.g. USIM, CSIM, ISIM and other relevant applications on the eUICC platforms, with the same standardized authentication algorithm for network access authentication, it might not be possible to mandate support of a specific network access algorithm for all cases.

In addition to the use of AKA for authentication, we would like to also note that the CSIM may need to support other cryptographic algorithms for authentication in order to access certain services provided by 3GPP2 core networks (e.g., CAVE algorithm specified in [S.S0053](#) for CDMA 1x circuit-switched access, algorithms for CHAP / digest response calculations for certain IP data services such as Simple IP or Mobile IP). Whether any of these algorithms would need to be supported by the eUICC would likely depend on the application/services provided by the terminal that uses eUICC.

As an example, an M2M terminal with CSIM application on the eUICC that is intended to operate only over a 3GPP2 network and is using CAVE for access authentication, may not need support for a standardized AKA algorithm.

For the above stated reasons, 3GPP2 would prefer that no network access algorithm is mandated by eUICC specifications defined by the ETSI SCP, and the 3GPP2 mandates any eUICC-based network access algorithm required to support 3GPP2 applications and services.

Action 2. To consider whether Embedded UICCs that are intended for use on 3GPP or 3GPP2 networks should support a second network access algorithm, and if so, which one

With respect to the support of a second algorithm on eUICC, in order to mitigate potential compromise of the primary algorithm, we agree it is a prudent security practice. However, 3GPP2 specification currently do not support in all cases the use of second authentication algorithm for network access authentication.

We would also like to kindly note that whether support for second algorithm is needed could be decided based on the application(s)/service(s) that the terminal is intended to provide and its security risk profile. For example, a smart meter with eUICC that is intended to be in service for 10 years or more, may require support for a second algorithm, whereas a consumer electronics

device with eUICC that may reasonably be expected to be in service for only a few years may not require support for a second algorithm.

Action 3. To consider how best to formalize any decisions related to items 1) and 2), such as (for example) changes to 3GPP and 3GPP2 specifications or industry recommendations

One option to address item 1) is to profile the Network Access Application for use with eUICC. For example, CSIM profile listing mandatory and optional algorithms (and potentially EFs) in order to support interoperability of CSIM applications on eUICCs could be developed either by 3GPP2 or an industry fora that serves the needs of 3GPP2 ecosystem.

For item 2, specifications may need to be developed (or enhanced) in order to a) specify the second algorithm; b) securely trigger the algorithm switch.

- For a), 3GPP2 is aware that 3GPP has recently published TUAK as the second example AKA algorithm and this can be used when USIM is used for AKA authentication and a support for second algorithm is deemed to be needed. However, when CSIM is used for authentication, as noted in response to action 2), a second algorithm may not be available in all cases.
- For b), a mechanism may need to be specified such that the use of the second algorithm is securely indicated by the home network to the eUICC as such capability is not currently available for AKA. Alternatively, the MNO Profile (per ETSI TS 103 383) on the eUICC could include information on the algorithm to use, which could be later updated in order to trigger the algorithm switch.

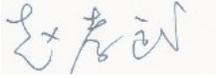
Action 4. Advise ETSI TC SCP of any progress on these topics

Until now, 3GPP2 has not actively discussed these topics. We will keep ETSI SCP and other groups abreast of any progress on these topics.

ETSI SCP (and the other groups working in this area) is kindly requested to take these responses into account in their work on eUICC.

We are looking forward to the continued fruitful cooperation with ETSI TC SCP.

Sincerely,



Dr. Xiaowu (Frankle) Zhao
Chair, 3GPP2 TSG-SX

Attachments: None

cc:

Ms. Jane Brownley	Chair, 3GPP2 Steering Committee	sc_chair@3gpp2.org
Ms. Victoria Mitchell	Director, 3GPP2	vmitchell@tiaonline.org
Dr. Ed Tiedemann	Chair, 3GPP2 TSG-AC	tsgac_chair@3gpp2.org
Mr. Anand Palanigounder	Chair, 3GPP2 TSG-SX WG4	apg@qti.qualcomm.com
Dr. Anand Prasad	Chair, 3GPP TSG SA3	anand@bq.jp.nec.com
Mr. Paul Jolivet,	Chair, 3GPP TSG CT6	paul.jolivet@lge.com
Mr. Xavier Piednoir	Technical Officer, ETSI SCP	xavier.piednoir@etsi.org
Mr. Paul Jolivet,	Chair, ETSI SCP TEC	paul.jolivet@lge.com
Mr. Davide Pratone	Chair, ETSI SCP REQ	davide.pratone@telecomitalia.it
Mr. James Moran	SG Director, GSMA Security Group	jmoran@gsma.com
Ms. Gloria Trujillo	SIM Director, GSMA SIM Steering Group	gtrujillo@gsma.com
Mr. Ian Pannell	SIM Co-Coordinator, GSMA	ipannell@gsma.com