3RD GENERATION PARTNERSHIP PROJECT 2 "3GPP2"

TSG-AC Correspondence

Dr. Edward G. Tiedemann, Jr.
Chair, 3GPP2 TSG-AC
Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
USA
tsgac_chair@3gpp2.org

5 December 2014

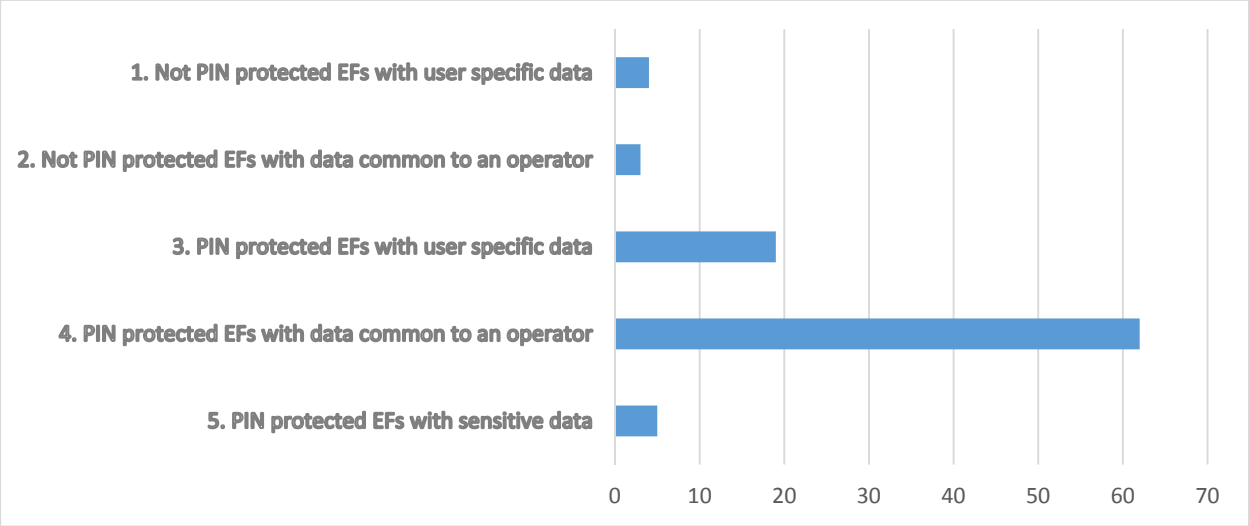
Mr. Paul Jolivet
Chair, ETSI SCP TEC
paul.jolivet@lge.com

Re: UICC Access Optimization

Dear Mr. Jolivet:

Thank you for your liaison to 3GPP2 TSG-AC regarding UICC Access Optimization. After reviewing the LS and related documents, 3GPP2 TSG-AC agrees that the "File Update Counter Mechanism" described in SCPTEC(14)000146r5 can improve UICC initialization time.

Below is an analysis of the 3GPP2 EFs widely used by operators. There are five categories of EFs that may be impacted by the mechanism described in SCPTEC(14)000146r5.



©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.

Only seven (7) EFs, out of all the EFs widely used, are not PIN protected. The majority of EFs are PIN protected. However, most of the PIN protected EFs carry data common to each operator. This common data are known, and therefore, it is not sensitive.

For categories 1 through 4, the security concerns described in the LS are not a concern. However, there is a concern for a small number of EFs in category 5 that contain sensitive data related to Cipher & Integrity Keys and Card Personalization. Since the file size of the EFs in this category is small, and the number of files concerned is small, such EFs can be excluded from the list of EFs supporting the File Update Counter TLV to avoid caching sensitive data in the device.

3GPP2 TSG-AC discussed possible solutions to the security concerns,

1. PIN protected EFs with sensitive data shall be excluded from the list of EFs supporting the File Update Counter TLV or shall be saved in a secure area in the device if the File Update Counter TLV is present.
2. The Device shall complete PIN verification before reading data from PIN protected EFs cached in the memory.
3. The File Update Counter Mechanism proposal shall clarify when to delete the cache and how to use the file update counter.

3GPP2 TSG-AC appreciates ETSI SCP TEC's consideration of our suggestions, and we look forward to continued collaboration in the future.

Regards,

Edward G. Tiedemann, Jr.
Chair, 3GPP2 TSG-AC

cc:	Ms. Jane Brownley	3GPP2 Steering Committee Chair	sc_chair@3gpp2.org
	Ms. Victoria Mitchell	Director, 3GPP2	vmitchell@tiaonline.org
	Dr. Xiaowu "Frankle" Zhao	Chair, 3GPP2 TSG-SX	tsgsx_chair@3gpp2.org
	Dr. Klaus Vedder	Chair, ETSI SCP	Klaus.Vedder@de.gi-de.com
	Mr. Xavier Piednoir	ETSI SCP and 3GPP Secretariat	Xavier.Piednoir@ETSI.ORG
	Mr. Heiko Kruse	Chair, 3GPP CT6	heiko.kruse@morpho.com

©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.