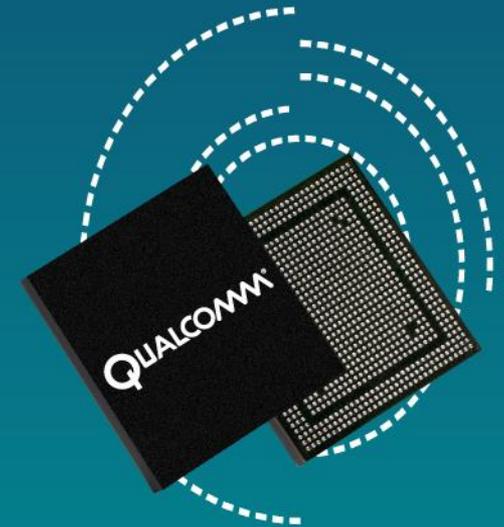




ProSe usage information storage in UICC C6-150026



Confidential and Proprietary – Qualcomm Technologies, Inc.

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm or its subsidiaries without the express approval of Qualcomm's Configuration Management.

Requirement for storage in UICC

- When ProSe charging data is stored in the UICC, some security aspects shall be considered that can give advantage over storage on ME.
- Make sure that data cannot be deleted
 - Storing data simply in a file in the USIM is not a feasible solution
 - Any external module/attacker could easily overwrite the data, deleting the data before it is transmitted.
 - Data shall be deleted only after it is successfully transmitted to the charging server.
- Read the data
 - One of the purposes of storing the data in UICC is security offered by UICC platform
 - Once the data is written (need to trust the terminal during this phase), reading it back to send it to the server adds an additional hop where data can be attacked. So, it is preferable that stored data shall not be readable from the UICC.
- Limitations (derived from LS [C6-140646](#) from SA3)
 - The UICC – ME interface is in clear
 - There is a need to trust the ME that correct information is passed to the UICC (as highlighted by SA3)
 - Not possible to prevent fake data to be sent to the UICC

Proposal

Move entire logic of ProSe reporting into UICC when the UICC supports it.

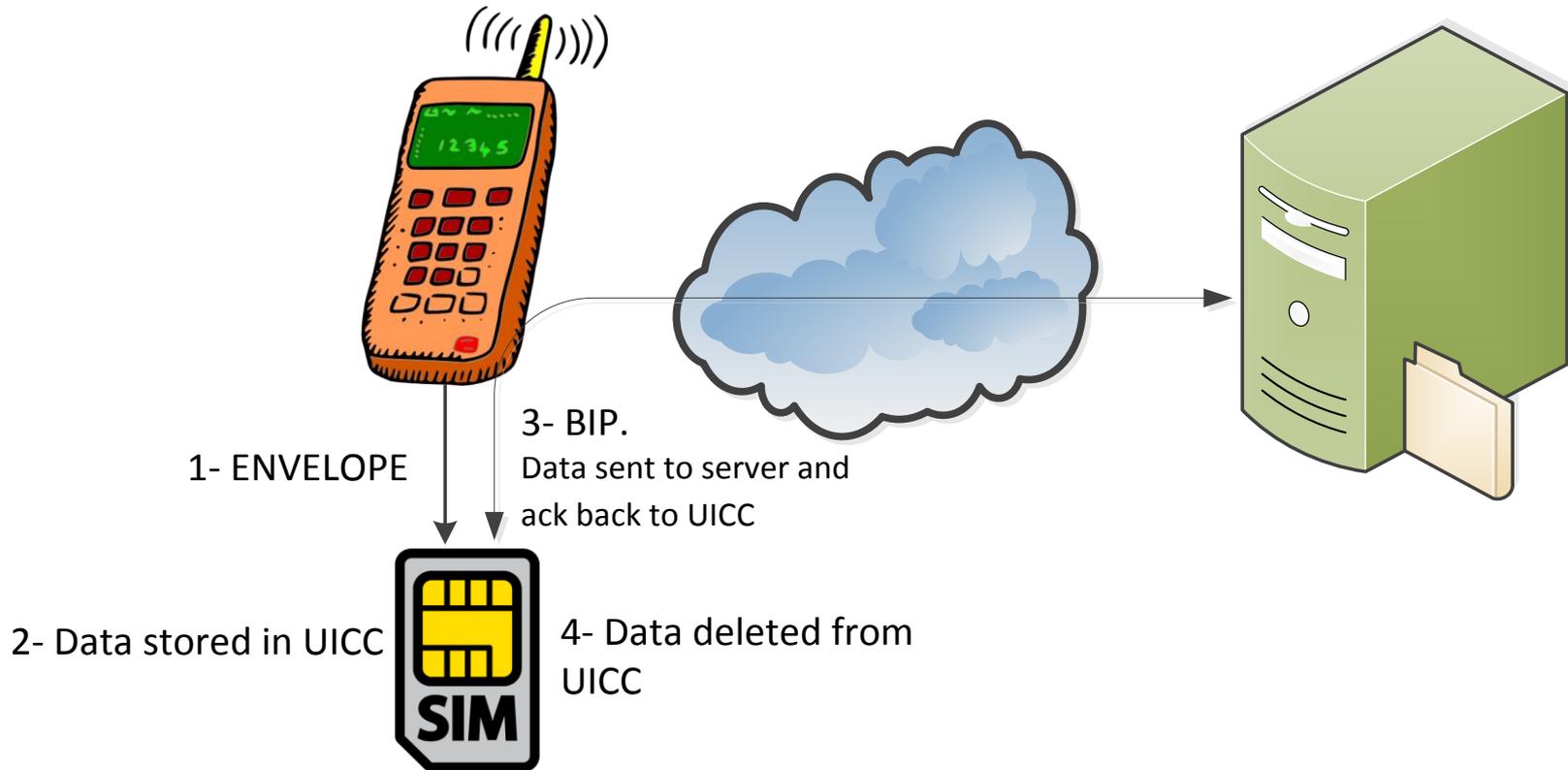
- 1- Terminal pushes data to UICC as it happens
 - Introduce a new 3GPP ENVELOPE for this operation.
 - Information can be written to the UICC, but not read back

- 2- UICC stores the information securely in its internal storage
 - UICC already has commands to retrieve the IMEI of the device and can optionally associate the ProSe data with the IMEI, if this is required.
 - Handling of the case where UICC storage is full is operator dependent, implemented inside the UICC
 - Ideally speaking, this information is not communicated externally to the terminal (possible security issue)
 - The operator can decide which data might need to be deleted (older or newest), depending on regional requirements.

- 3- UICC takes care of transmitting the data to the server using BIP mechanism when in coverage
 - Transmission over BIP uses the same protocol as if data is stored in the ME (protocol to be defined by CT1 during this meeting)

- 4- UICC deletes the information after successfully sending it to server
 - UICC prevents risk that data is deleted before it is communicated

Proposal



Questions?

<https://support.cdmatech.com>

