Immigration Department clarifies rumours on remote access of chip data of new smart identity cards

â€‹â€‹ Regarding the recent rumours relating to remote access of chip data of new smart identity cards, the Immigration Department (ImmD) yesterday (July 18) issued the following clarification:

â€‹â€‹ The ImmD reiterated that the new smart identity card has adopted multi-level safeguards to ensure comprehensive protection of the privacy of personal data stored in the chip of the identity card, and the identity verification process is absolutely secure and accurate.

â€‹â€‹ Under the Next Generation Smart Identity Card System (SMARTICS-2), only authorised optical card readers are able to read the personal data from the chip of new smart identity cards. Readers are not possible to access the chip data if they are not authorised with certificate and equipped with the specific algorithm, no matter how sophisticated they are.

â€‹â€‹ Moreover, access to chip data must be initiated by the cardholder through taking out his/her smart identity card and placing it onto an authorised optical card reader. The reading process is conducted with the combination of optical card reader and wireless transmission technology. Before communication and data reading, the identity of the chip and the optical card reader must be defined and mutually authenticated. All communication and data transmission would be encrypted throughout the whole process. The chip in the new smart identity card is a passive type which means it is not powered by any standalone battery. Without power, it is not able to send out any signal by itself. During the whole communication and data transmission process, the distance between the chip and the optical card reader must be less than 2 cm. As such, if the cardholder does not take out the new smart identity card, it is impossible for others to remotely read the chip data of the new smart identity card without notice by the cardholder.
â€‹â€‹
At different stages of the implementation of the SMARTICS-2, the ImmD has engaged independent consultants to conduct assessments on privacy impacts and information technology security with a view to ensuring that the system design and work flow comply with the Personal Data (Privacy) Ordinance as well as the relevant standards and guidelines laid down by the Office of the Government Chief Information Office. The assessments conducted by independent consultants have confirmed that the safeguards adopted by the new smart identity card have effectively prevented unauthorised access to personal data stored inside the chip of the smart identity card through contactless interface.

â€‹â€‹ The ImmD noted that several individual groups in the community had distributed card protectors to the public free of charge, claiming it would block radio frequency identification (RFID) to prevent unauthorised access to

personal data stored in new smart identity cards. The ImmD reiterated that there is no case of unauthorised access to the new smart identity card. The relevant message is misleading and thus clarified as above.