E-SIM: ONE CARD FOR PRINTING, ACCESS AND CALLING?

Words
Judith
Verhoeven
SURFnet

A SIM is a security element used in the authentication of subscribers before granting them access to the mobile network. The potentials of the internet-of-things market was the motivation to introduce the embedded SIM (E-SIM), allowing to change the subscription to a different mobile operator without touching the SIM card. From the perspective of a phone, however, the E-SIM is a regular SIM and does not need to be embedded on a circuit board to use its capabilities. Technically, the E-SIM is an applet with SIM card functions on a smart card. The E-SIM allows you to integrate the functions of a SIM card with those of a smart card already used by education and research institutions, for instance for student and employee cards. If you place a smart card in a phone's SIM card slot, the user is given access to the mobile network while the apps on the phone can also use the crypto functionalities of that smart card. This opens the door to a whole host of new possibilities.

SIM card and smart card in one

Education and research institutions currently use smart cards for student and employee cards. The E-SIM allows smart card functionality to be expanded by adding a SIM card functionality, and to integrate this into the phone. This means that apps running on your phone, for security purposes, are using the smart card with integrated E-SIM.

The E-SIM has its own management and maintenance methods, which have been prescribed by the telecommunications industry. Telecommunications profiles are added to the E-SIM for telephone, SMS/M2M and data communication purposes. Today, SIMs use these profiles to authenticate users and steer phones to the correct mobile network. The difference with the E-SIM is that it offers flexibility: a profile doesn't have to be placed on a smart card in a factory, as it can be uploaded. It can later be replaced by a profile from another telecommunications provider.

By placing a telecommunications profile on a smart card that is also used for the technical functionalities offered by the student and employee card, you open the door to a whole host of integrated functionalities. You can add functions to a smart card that, for example, provide access to buildings and coffee machines, but you can also add access to eduroam. The applications on the phone will then outsource the security functions to the smart card, where the telecommunications profiles are also located.

Better security than a phone

A smart card can be used as a sort of vault where you keep your passwords. An application on the phone sends a 'challenge' to the applet on the smart card, which then sends a response. Should the right response be received, the security is deemed to be acceptable. This is more secure than saving credentials on your phone.

On the way to a joint security architecture

In order to use the smart card's 'vault functionality' correctly, SURF develops a joint hardware security architecture with their member institutions. The technical and functional requirements for the hardware (the smart card) should be documented in this architecture. By making these choices together, you can convince suppliers of parking facilities, cards and printers to name a few, but also software developers to use this architecture for their products. You can then lower your procurement costs, for instance, and you will only need one card (or your phone). But there is another, more important benefit: as all the suppliers fulfil the joint architecture specifications, we can audit the whole system for security aspects. In addition, we are able to take better action in the event of security issues: with everyone using the same architecture, we can provide information on solutions centrally in the event of hacks, for example.

Integrating a smart card... or not

As mentioned above, it is possible to integrate this smart card into a phone (after all, the 'E' in E-SIM stands for 'embedded'), but you don't have to. It can also be placed in other types of devices, such as smart watches and toys. By adding NFC functionality to the smart card, you can place it in a card the size of a credit card, which is then used just like the traditional student or employee card. You can still use the smart card as a SIM card later: simply remove the smart card element from the card, place it in the SIM card slot of your phone and then push a user profile to it for communication purposes. In the pilot we previously carried out with the E-SIM, we showed that telephones operate with a regular SIM that obey all E-SIM functionalities and capabilities. Hence the E-SIM doesn't necessarily need to be integrated into the phone but can be placed on a smart card that fits in the SIM slot of a phone.

The smart card may either remain in the plastic card or could be place in a phone/tablet. The advantage of placing a smart card in a phone is that it can always be managed remotely as long as there is a network connection. Institutions can manage the smart card from a central location - making use of their own security domain - and invite mobile operators to place telecommunication profiles within the E-SIM on their smart card.

http://www.surf.nl/en/e-sim