Using the SIM for the next generation pass for students and staff of research and education institutions

Authors: Frans Panken and Joost van Dijk, SURFnet
Keywords: E-SIM, student and employee pass, mobile service offering, temper-resistant hardware-based isolated environments.

Summary

Most institutions have passes / badges for students and staff. These badges are sealed pieces of plastic with a photo and are equipped with a smartcard. They serve as the base to authenticate the user's identity and are used for accessing printing facilities, coffee machines, lockers, library, identification during exams, giving employees access to buildings, parking lots, laboratories, elevators, etcetera. New developments within the standardization of SIM cards allow using the SIM card as the smartcard in a traditional piece of plastic and/or in a smartphone. This opens opportunities that are currently restricted to large players such as credit card organizations, Apple, and Google.

During the presentation at TNC2018, we will reveal the opportunities for the research and education community that stem from new developments in (and changes of) the SIM. The presentation shows the potentials of using the SIM as the smartcard on the traditional student and employee pass as well as the opportunities that this brings when the SIM is removed from the plastic card and inserted in a smartphone or tablet. The presentation explains that this potentially realizes an open market distribution model for secure applications in smartphones. If time allows, we can demonstrate one or two use cases of applets stored on the smartcard that also hosts the SIM. Examples of demonstration include: using the SIM to gain access to eduroam (as an alternative for username/password) and using an applet on an E-SIM to realize two-factor authentication as a more user-friendly and safer alternative for sending one-time passwords via SMS.

New developments of the SIM

A subscriber identification module (SIM) is an application on a smart card that is used to identify and authenticate subscribers on mobile telephony devices. If users change from one mobile operator to another, the SIM from the old provider has to be replaced by one from the new provider. Mobile operators see a huge potential in the machine-to-machine and the Internet of Things markets. They want to use the same infrastructure and authentication mechanisms as used for the phones but they realize that the swapping of SIMs blocks the uptake of those new markets. The costs of swapping a SIM in a machine for another one is estimated to €50-€100 per machine/thing. In addition, the size of a SIM is too large to include on a small device such as a sensor. The solution is found in a new SIM design that can be embedded on a main board of a device, named the embedded SIM (E-SIM). The E-SIM is still a SIM; it just not replaceable. Changing operators is realised by altering operator profiles that are stored on the E-SIM. This process can be realised over the air and hence does not require physical access to the device that hosts the E-SIM.

For a device, the E-SIM has the same capabilities as a traditional SIM. So, if we place an E-SIM with operator profiles on a form factor that is used by a phone, it is recognized by the phone and can be used as a regular SIM. During the presentation at TNC2018, we will explain how we successfully changed one operator to another without physically touching the SIM in the phone: we used an E-SIM and changed the operator profile over the air.

Potentials of the E-SIM

The E-SIM is an application on a smartcard. Other applications can be placed next to the E-SIM applet without disturbing one another's functionalities. Hence, we can separate the card that hosts the E-SIM in two separate domains: a telecom domain (that contains the operator profiles) and a security domain that is compliant to the Global Platform specifications and hosts applets that are commonly stored on an employee or student pass. These domains can be managed independently from one another, over the air. The ability to change the applets in the security domain over the air is one of the obvious advantages of using a SIM in a smartphone for the student/employee pass over using of a smartcard that is sealed in a piece of plastic. The operator profiles are neither uploaded nor activated if we seal an E-SIM in plastic and used as student or employee pass as we know it today.

The new advances of the E-SIM make it possible that an NREN buys E-SIM compatible smartcards from a company that can manage them. The NREN becomes the owner of the smartcard, including the E-SIM applet and the associated security keys needed to write the applets on the smartcard. This allows an NREN to make a first step in the process of extending its fixed network offerings with mobile services without making any investments in a mobile infrastructure. The NREN subsequently selects a mobile operator for voice and data services and places the profiles of this operator on the E-SIM. In time, the NREN may select another mobile operator to realize its mobile service offerings and realizes this by replacing the existing operator profiles on the E-SIM by profiles of the newly selected operator. As soon as this happened, the E-SIM uses the cellular and backend infrastructure (including the authentication server) of the new operator. It also allows using the smartcard that hosts the SIM for the functionalities of today's student and employee passes. The owner's photo can be stored on the card and displayed on the device that reads the E-SIM. Finally, the smartcard can be used for securing applications used on the phone. The next section explains in short how we realize the latter.

We stress that the true merit of the ownership of the E-SIM lies neither in the potential for NRENs to offer a mobile service without an operator lock-in, nor in offering an alternative for the student and employee cards. The true merit of the ownership of the E-SIM lies in realizing a common future-proof architecture for a hardware-based isolated environment that can be used in various devices (including plastic cards) and allows building a common and tamper-resistant security solution that can be audited.

The role of the smartphone

A major obstacle for allowing third parties to utilize hardware-based isolated environments in phones/tablets is the fact that underlying secure hardware is under the control of their stakeholders. Trusted applications, applets or trustlets must first be admitted (and signed) by the respective stakeholder in order to be executed within the smart card. This requires developers to collaborate with large stakeholders. As a result, the usage of hardware-based security in phones is currently restricted to large players (Samsung, Apple, Google, credit card companies). Ownership of

the E-SIM changes this. We envision the smartcard that also hosts the E-SIM as the temper-resistant secure hardware environment.
To remove the obstacles, we envision an open market code distribution model for the distribution of code (applets, trustlets and trusted apps) for secure hardware. Part of this process is that the owner of the secure hardware publishes an approachable process (e.g., a website) for application developers to upload their application and applets for code inspection and signing. Mobile app markets have successfully bridged the gap between app developers and large OS vendors, and thus could also serve in the same way between developers and secure hardware stakeholders. The following figure illustrates what such an ecosystem could look like (the E-SIM is on the right and the smartphone on the left):

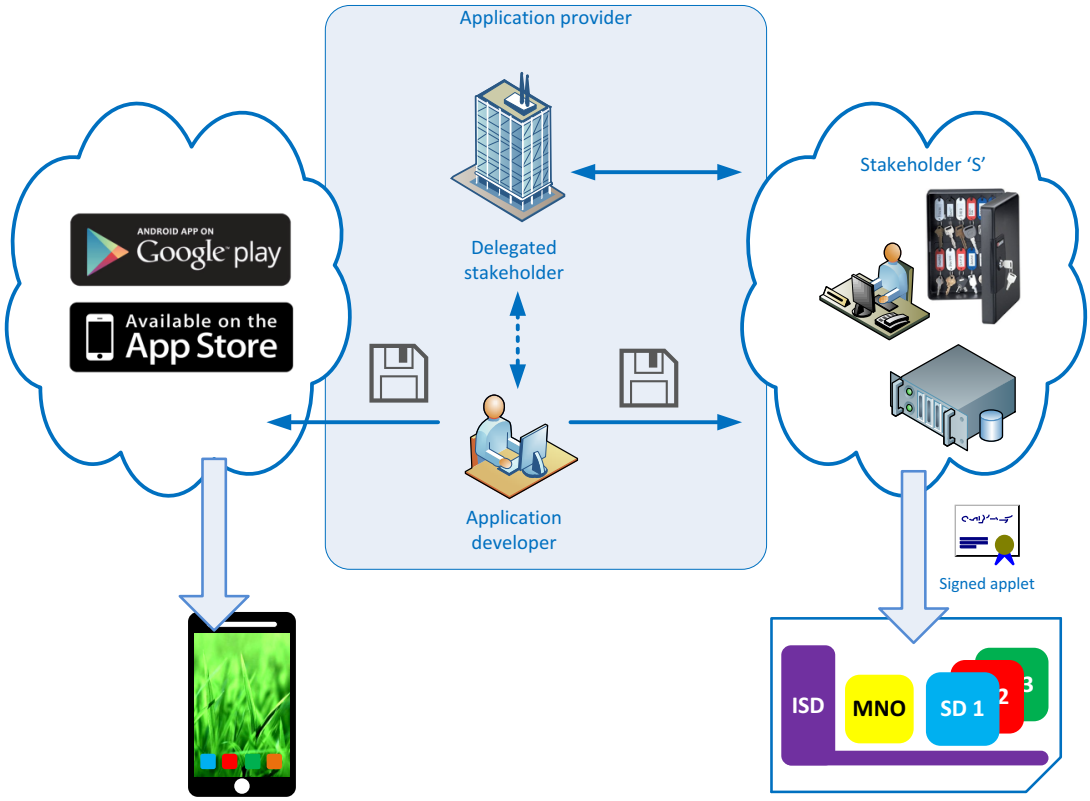

Figure 1 Visualization of the open market code distribution model. ISD= issuer security domain (NREN's domain), MNO = profile of mobile operator, SD = security domain of institution.

Please note that the application developer in our model may include the companies that offer their service to realize today's student card and employee passes.

The introduction of the open mobile API (by SIM alliance) that allows communication between applications on a phone and applets on the smartcard that hosts the E-SIM strengthens our beliefs that our vision can become reality soon.

Please note that we do not imply that institutions will offer students a mobile subscription (although in time they might do so to facilitate mobile learning). In time (when operators allow), students may select the operator that services their E-SIM and place their student card in their smartphone. This is how the LTE variants of the smart watches (e.g., Apple smart watch and the Samsung's Gear S3) are connected to the cellular network.