Hewlett Packard Enterprise

Business white paper

Implementing mobile electronic identity

A Hewlett Packard Enterprise approach based on hardware token microSD card

Technical composition of mobile devices

Mobile electronic identity, or MeID, is a complementary concept combining the advantages of electronic ID (eID) and mobile devices. It represents the integration of existing eID functionality into a mobile device—for example, a smartphone or tablet. And it uses standardized components such as secure element and near-field communication.

Table of contents

Secure Element form factors in mobile devices

According to the European Union Agency for Network and Information Security (ENISA), mobile devices need a secure element (SE) to achieve a high level of end-to-end security. SE is a tamper-resistant platform capable of keeping data confidential and supporting cryptographic functions. It is an obvious choice for realizing identification and authentication solutions for mobile devices.

Currently, the technological composition of mobile devices can work with the SE form factors shown in Figure 1.

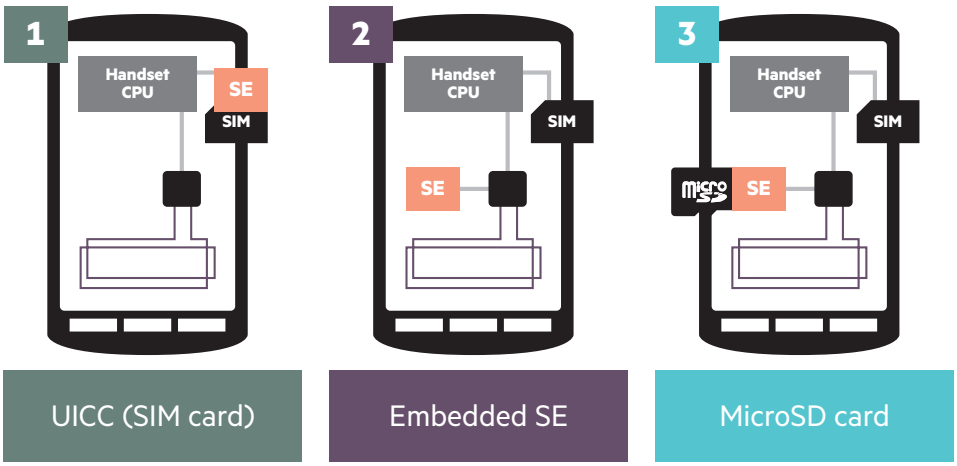

Figure 1: Secure element form factors

Here are descriptions of each form factor:

- **SE as universal integrated circuit card (UICC)–SIM**—Some European Union (EU) member countries, such as Estonia and Finland, have introduced MeID using this concept. Disadvantages of this approach include a complicated implementation and higher costs—because distributing special SIM cards requires collaboration between issuing authorities and various mobile network operators. Additionally, some mobile devices lack a SIM slot, such as tablets and ultrabooks, yet are still highly portable and often connected via Wi-Fi. Moreover, GSMA released a remote-provisioning specification, which introduces embedded SIM (eSIM)—implanted directly into the mobile device. This specification may result in a gradual but complete substitution of removable SIM cards in the next few years. **The technological director of T-Mobile Slovakia said** that the first models of mobile devices with eSIM should appear on the market this year, and massive penetration is expected in 2017 and 2018.Taking into account our previous findings, we are convinced that the removable SIM card model is considered obsolete.

Key principles for MeID realization include:

- Identical functionality as implemented in national identification scheme
- A high level of security and reliability for MeID that is equal to eID
- Already existing infrastructure and logistical processes used for MeID lifecycle management
- Availability on a broad spectrum of mobile platforms—such as Android, iOS, and Windows®

- **SE embedded in the mobile device**—Embedded SE probably will replace removable SIM cards in the near future.
- **MicroSD card as SE**—This is an open concept supported by renowned mobile device manufacturers. Based on Hewlett Packard Enterprise (HPE) analysis, a microSD slot is present in 85 percent of smartphones and 80.8 percent of tablets available on the Slovak market as of 25 April 2016. Except for Apple,® all major producers now include a slot for microSD cards into their product designs; they consider it a relevant and stable part of their development plans.

HPE cooperates with partner company Plaut Slovakia in the field of mobile identification. As the result of our investigation we propose pursuing the third option—microSD card for implementing MeID. In this case, the owner of the microSD card decides which applications can be activated or added. From the product point of view, we highly recommend innovative microSD card designed by the SMK-Logomotion Corporation. Refer to the appendix of this document for more details.
Compliance with BSI and ANSSI eIDAS token specification (TR 03110) and adherence to EU Regulation 910/2014—on electronic identification and trust services for electronic transactions in the internal market (eIDAS)—are cornerstones of the presented option.

Other alternatives for implementing MeID

Software token

The software token solution keeps private key and certificates in the operation system while the storage space is usually a file or storage provided by the system itself. Such storage is typically protected by encryption. To work with the saved keys, the user must enter the password as part of system login or when accessing a file with the keys.

The advantage of the solution is its low price, as you don't need to purchase security hardware for storing key pairs and associated certificates. An additional benefit is easy integration into the application, avoiding any installation and integration by using drivers supplied by the device manufacturer.

But from a security perspective, software storage typically has a low or intermediary security level. Software storage can be remotely "stolen", such as through malware, and then the key value retrieved by applying a brute-force attack.

Saved key pairs can be used in these scenarios:

- Electronic identification and authentication of users accessing electronic service provider services—The user signs the authentication and identification token by a remotely available private key to which there is a corresponding certificate.
- Creation of a qualified electronic signature—The user signs an electronic document by a remotely available private key to which there is a corresponding qualified certificate.

This security level is considerably lower than the one offered by certified hardware tokens, which use state-of-the-art techniques for key protection. These include resistance to simple/differential power analysis, active shield, bus scrambling, and memory encryption.

Therefore, in terms of assurance-level classification corresponding with eIDAS regulation, the security level of the eID scheme, based on software storage, is rated "low" or "substantial" at the most. Comparatively, the hardware token assurance level is assessed as "high."

Server Signing

Another conceivable solution for eID and user authentication is the Server Signing solution, where key pairs and associated certificates are stored in a hardware security module (HSM) of a trusted service provider. Server Signing Secure Signature Creation Service (SSCS) originates from CEN/TS 419241:2014—Security Requirements for Trustworthy Systems Supporting Server Signing.

Access to keys stored in an HSM is granted exclusively to its user—an owner of the key pair and certificate. This access right is based on authentication by means of identificator, password, and additional authentication. This involves using a one-time password obtained via short message service on a registered phone number.

The availability of electronic identification and authentication that extends to mobile platforms is seen as advantageous in this case. That's because for application, it is not necessary to install and integrate any peripheral security device—you only need an application for a specific mobile platform.

Appendix

SMK-Logomotion Corporation (SLC) was established on May 7, 2015 as a joint venture of Slovak company Logomotion and Japanese company SMK Corporation. The SLC head office is located in Tokyo, with a branch office in Bratislava, Slovakia. It specializes in developing innovative NFC (Near Field Communication) products and aims to maximize the potential of patented technology to support secure NFC payments and Internet of Things applications.

The microSD architecture distinguishes itself by specific elements and patented technologies (see Figure 2):

- Two separate and independent secure elements
- High-performance miniature near-field communication antenna that communicates even through the microSD slot's metallic casing
- ISO7816 contacts on the card surface

In addition to the properties mentioned, this microSD card is certified as a Mobile MasterCard™ PayPass® product and also provides conventional data storage.

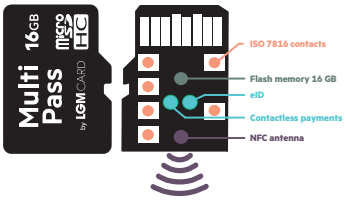

Figure 2: MicroSD architecture

On the other side, this solution's weakness lies in the security of the authentication process at the moment a user remotely accesses stored keys. Most of all, considering all well-known attacks, OTP (one time password) cannot be graded today as the "high" assurance level defined in eIDAS.

In line with statements made by the German Bureau of Information Safety (BSI, or Bundesamtes für Sicherheit in der Informationstechnik), OTP mechanisms should not be used in solutions where a high assurance level is required. This is because of the recent discovery of new types of malicious software focused on capturing OTP and delivering it to an intruder.

Despite the fact that online banking is the primary target, it shows that such an attack on the Server Signing concept also could be effective. BSI advises that a plausible alternative for securing Server Signing is employing hardware tokens—such as a USB token or MeID microSD card—instead of the OTP.

Moreover, applying an electronic signature for identification and authentication conflicts with eIDAS legislation, as the **European Commission pronounced** that: "Since 1st of July 2016, when the trust services' provisions under the eIDAS regulation entered into application, an eSignature can only be used by a natural person to 'sign,' that is, mainly to express consent on the data the eSignature is put. This represents a significant difference from the eSignature Directive where the eSignature, which could also be used by legal persons, was defined as a means for authentication."

MicroSD card—a natural enabler

Innovative solutions based on the microSD card introduce a capacity to securely retain multiple documents on a single carrier in digitized form and generate development impulse for establishing mobile government in the Slovak republic. Currently, various countries—including the U.S., UK, and Australia—are considering digitizing driving licenses. And it appears that doing the same with **other types of official documents or government-issued licenses will be next**. Other countries probably will follow this trend. So adding a mobile electronic driving license as the next application to our microSD card solution seems to be reasonable, with a high potential for success.

The goal is to integrate various documents in adherence to legislative conditions. In the end, a citizen would possess a mobile device containing a microSD card capable of accumulating all relevant documents in digitized form. It would be significantly beneficial for citizens to have key electronic documents readily available in their mobile device—and the ability to display them to authorities on request. Additionally, authorities could conduct a real-time inspection of electronic documents by means of a mobile device in proximity mode.

For citizens, MeID provides the required convenience, flexibility, and mobility on all major platforms—Android, iOS, and Windows. For governments, this technology boosts use of e-government services. And for businesses, it delivers higher security at a lower cost. Should the Slovakian government start to pioneer MeID solutions, it will realize an additional benefit: This technology is proving to be a natural enabler for public-private sector cooperation and collaboration, benefiting banking, e-commerce, e-health, transportation, tourism, and many other areas of operation.

Sign up for updates

Hewlett Packard Enterprise

4AA6-8167ENW, October 2016