Hewlett Packard
Enterprise

Implementácia mobilnej elektronickej identity

Navrhovaný prístup na báze hardvérového tokenu - microSD karty

Technické zloženie mobilných zariadení

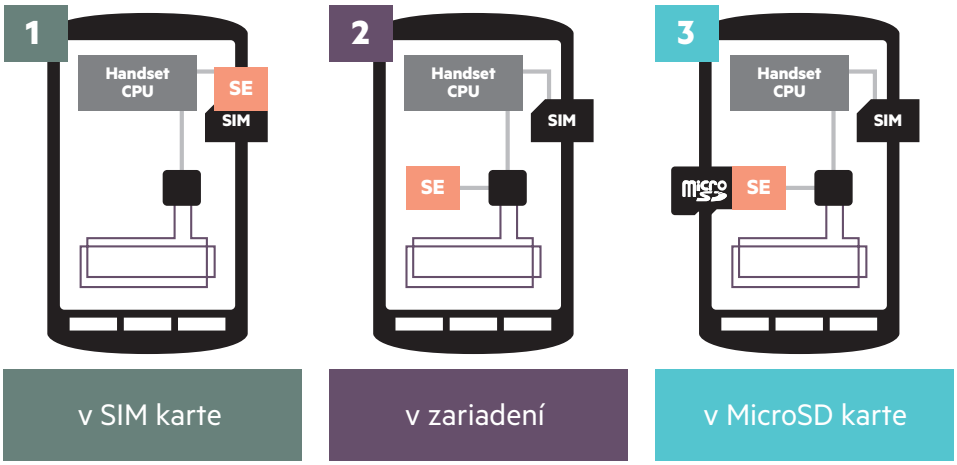
MeID je komplementárny koncept, ktorý spája výhody eID a mobilného zariadenia a je integráciou existujúcej funkcionality eID do mobilného zariadenia (smartphone, tablet) s využitím jeho štandardizovaných komponentov ako bezpečnostný čip (SE – secure element) a NFC.

Obsah

Možnosti zabudovania SE v mobilných zariadeniach

Podľa Európskej agentúry pre sieťovú a informačnú bezpečnosť (ENISA) je pre dosiahnutie vysokej miery zabezpečenia vyžadovaná prítomnosť SE (Secure Element) v mobilnom zariadení. SE predstavuje bezpečnú platformu pre uchovávanie dôverných údajov a podporu kryptografických funkcií a je prirodzenou voľbou pre realizáciu identifikačných a autentifikačných riešení na báze mobilných zariadení.

V súčasnosti technologické vyhotovenie mobilného zariadenia podporuje nasledovné možnosti zabudovania SE:



Obrázok 1: Možnosti zabudovania SE

Popis jednotlivých možností zabudovania EF:

- **1. SE zabudovaný v SIM karte**
  Niektoré krajiny zaviedli MeID na tomto koncepte (napr. Estónsko, Fínsko). Nevýhodou je značne komplikovaná implementácia a vysoké náklady, keďže nevyhnutná distribúcia špeciálnych SIM kariet vyžaduje náročnú koordináciu medzi vydávajúcou autoritou a mobilnými operátormi pôsobiacimi na lokálnom trhu. Okrem toho, niektoré druhy mobilných zariadení (napr. tablety) nedisponujú slotom pre SIM kartu. Rovnako **GSM asociácia** (GSMA) oznámila **vydanie špecifikácie vzdialenej správy**, ktorá zavádza do reálneho používania pevne zabudované SIM karty (eSIM – embedded SIM) v mobilných zariadeniach. **Podľa vyjadrení technologického riaditeľa T-Mobile** sú prvé modely mobilných zariadení s eSIM očakávané už tento rok a masívny prienik eSIM je predpokladaný v rokoch 2017 a 2018. Preto sa koncept odnímateľných SIM kariet pokladá za koncept minulosti.

Kľúčové navrhované princípy pre realizáciu MeID:

- Párovanie s národnou schémou eID (rovnaká funkcionalita, elektronická identifikácia a QEP)
- Rovnaký stupeň bezpečnosti a dôveryhodnosti MeID ako pre eID
- Dostupnosť na širokom spektre mobilných platforiem (Android, Windows Phone, iOS)
- Zdieľanie existujúcej infraštruktúry MV a zavedených logistických procesov pre správu životného cyklu MeID

- **2. SE zabudovaný výrobcom do zariadenia**
  V blízkej budúcnosti pravdepodobne substituuje dnešné odnímateľné SIM karty.

- **3. SE zabudovaný na microSD karte**
  Otvorený koncept podporovaný renomovanými výrobcami mobilných zriadení. Podľa prieskumu HPE je microSD slot prítomný v 85% smartfónov a 80,8% tabletov v predaji na slovenskom trhu ku 25.4.2016. S výnimkou Apple, signifikantní výrobcovia smartfónov podporujú slot pre microSD a je stabilnou súčasťou ich rozvojových plánov.

Z vyššie uvedených dôvodov HPE pri implementácii MeID odporúča alternatívu 3, teda využiť microSD kartu. V tomto prípade vlastník microSD rozhoduje o aplikáciách, ktoré budú na nej aktivované. Z podhľadu produktu odporúčame inovatívnu microSD kartu od spoločnosti SMK-Logomotion Corporation (SLC).

Bázovým východiskom pre implementáciu je súlad so štandardom BSI and ANSSI eIDAS token specification (TR 03110) a direktívou EU eIDAS platnou od 1.7.2016.

Iné alternatívy pre implementáciu MeID

Softvérový token
Riešenie softvérového tokenu spočíva v uložení privátneho kľúča a certifikátu v rámci operačného systému, pričom miestom uloženia je zvyčajne súbor alebo úložisko poskytované samotným operačným systémom. Takéto úložisko je obvykle chránené šifrovaním a pre prístup k práci s uloženými kľúčmi je potrebné zadať prístupové heslo, či už v rámci prihlásenia sa do operačného systému alebo explicitne pri prístupe k súboru s kľúčmi.

Výhodou riešenia softvérového tokenu je jeho nízka cena, nakoľko nie je nutné zakupovať bezpečné hardvérové zariadenia pre ukladanie kľúčových párov a súvisiacich certifikátov. Výhodou je aj ľahká integrácia do aplikácie bez potreby inštalácie a integrácie s ovládačmi od výrobcu daného zariadenia.

Z hľadiska bezpečnosti však softvérové úložisko predstavuje nízku alebo strednú úroveň bezpečnosti. Softvérové úložisko je možné na diaľku „ukradnúť“ (napr. pomocou malware-u) a následne prostredníctvom brute-force útoku získať hodnotu uloženého kľúča.

Táto úroveň bezpečnosti je omnoho nižšia ako poskytujú certifikované hardvérové tokeny, ktoré pre ochranu kľúčov používajú najmodernejšie technológie zabezpečenia ako napr. odolnosť voči SDA/DPA (Simple/Differential Power Analysis), active shield a self-destruction, bus scrambling, šifrovanie údajov v pamäti, na zbernici a aj v CPU, dual CPU pre detekciu zlyhania (napr. pri snahe ovplyvniť činnosť procesora laserom alebo iným žiarením), scrambling dát a adresného priestoru v pamäti, random wait-states, zablokovanie prístupu po viacnásobne nesprávne zadanom PIN a iných.

Preto v zmysle definície úrovní zabezpečenia podľa nariadenia Európskeho parlamentu a rady (EÚ) č. 910/2014 (nariadenie eIDAS) môže byť úroveň bezpečnosti schémy elektronickej identifikácie založenej na softvérovom úložisku hodnotená ako „nízka“ alebo najviac „pokročilá“. Naopak, hardvérové tokeny dosahujú úroveň zabezpečenia „vysoká“.

Uložené kľúčové páry je možné použiť v nasledujúcich scenároch:

- Elektronická identifikácia a autentifikácia používateľov pri prístupe ku službám poskytovateľov elektronických služieb – používateľ svojím vzdialeným privátnym kľúčom, na ktorý má vydaný certifikát, podpíše autentifikačný a identifikačný token, alebo
- Vytvorenie kvalifikovaného elektronického podpisu (KEP resp. angl. QES) – používateľ svojím vzdialeným privátnym kľúčom, na ktorý má vydaný kvalifikovaný certifikát, podpíše príslušný elektronický dokument

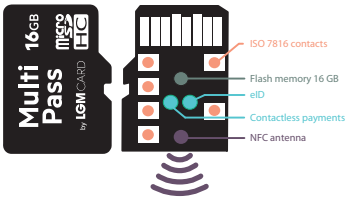
Aplikácia na vzdialenom serveri
Ďalším možným riešením pre elektronickú identifikáciu a autentifikáciu používateľov je riešenie Server Signing , v ktorom sú kľúčové páry a certifikáty používateľov uložené v bezpečnom hardvérovom module (HSM) poskytovateľa dôveryhodných služieb. Server Signing riešenie (resp. SSCS – Secure Signature Creation Service) vychádza z požiadaviek normy CEN/TS 419241:2014 – Security Requirements for Trustworthy Systems Supporting Server Signing.

Appendix
Spoločnosť SMK-Logomotion vznikla 7. mája 2015 spoločnou majetkovou účasťou slovenskej spoločnosti Logomotion a japonskej spoločnosti SMK Corporation. SLC sídli v Tokiu a má pobočku na Slovensku v Bratislave. Špecializuje sa na vývoj inovatívnych NFC produktov s cieľom maximalizovať potenciál využitia ich patentovaných technológií podporujúcich bezpečné NFC platby a aplikácie v oblasti IoT (internet of things).

Architektúra microSD karty sa odlišuje prítomnosťou špecifických prvkov a patentovaných technológií:

- dva samostatné a nezávislé SE,
- vysokovýkonnou miniatúrnou NFC anténou schopnou komunikovať aj cez kovom vystlaný slot pre microSD karty a
- kontakty na karte v súlade s normou ISO7816

Okrem toho je táto microSD karta certifikovaná ako Mobile MasterCard™ PayPass® produkt a poskytuje aj funkciu konvenčného dátového úložiska (pamäť až 16 GB).



Obrázok 2: Architektúra microSD karty

Prístup ku kľúču uloženom v HSM má výlučne len príslušný používateľ – ako vlastník kľúčového páru a certifikátu – pričom tento prístup je zvyčajne založený na autentifikácii používateľa prostredníctvom identifikátora, hesla a doplnkovej autentifikácii na základe OTP – one time password - odoslaného v SMS na registrované telefónne číslo.

Slabinou tohto riešenia však je zabezpečenie procesu autentifikácie pri prístupe ku vzdialeným kľúčom používateľa. Najmä použitie OTP, vzhľadom na známe útoky, už dnes nie je možné považovať za dostatočne bezpečné pre úroveň zabezpečenia „vysoká" v zmysle nariadenia eIDAS. **Na základe stanoviska nemeckého úradu pre bezpečnosť v informatike BSI**, mechanizmus OTP nemá byť už viac použitý pre nové riešenia s požadovaným stupňom zabezpečenia „vysoký", nakoľko „sa medzičasom objavili nové typy škodlivých softvérov, ktoré sa zameriavajú na odchytenie OTP a jeho odoslanie útočníkovi. Aj keď je ich cieľom zvyčajne Online-Banking, ukazuje sa, že takéto útoky by boli použiteľné aj pri koncepte Server Signing. Možnou alternatívou zabezpečenia mechanizmu Server Signing by podľa BSI bolo (namiesto OTP) použitie hardvérových tokenov, napr. USB token alebo tu navrhované riešenie MeID na báze microSD karty.

Navyše, použitie elektronického podpisu pre účely identifikácie a autentifikácie by bolo v rozpore s legislatívou eIDAS, nakoľko **podľa stanoviska európskej komisie** použitie elektronického podpisu je možné len na podpisovanie údajov a nie autentifikáciu. Podľa tohto stanoviska "Od 1.7.2016, keď legislatíva eIDAS nadobudne účinnosť, elektronický podpis môže byť použitý iba fyzickou osobou na podpisovanie, najmä na vyjadrenie súhlasu a schválenie údajov, ku ktorým je podpis pripojený. Toto predstavuje rozdiel od smernice 1999/93/ES o elektronickom podpise, kde el. podpis – ktorý mohol byť používaný aj právnickými osobami – bol definovaný aj ako prostriedok pre autentifikáciu."

Záver

Navrhované inovatívne riešenie na báze microSD karty má potenciál bezpečného uchovávania viacerých dokladov na jednom nosiči v digitalizovanej podobe a vytvára rozvojový impulz pre budovanie inovovaného mobilného eGovernmentu v SR. **V súčasnosti sa v zahraničí (USA, VB, Austrália) formuje trend digitalizácie vodičských preukazov** a ďalšie druhy dokladov budú pribúdať. S najväčšou pravdepodobnosťou budú ostatné krajiny nasledovať túto ideu a realizovať obdobné riešenia v blízkej budúcnosti, preto sa zdá byť vhodné pridať mobilný elektronický vodičský preukaz ako prvú ďalšiu aplikáciu k aplikácii eID.

Cieľom je postupne integrovať jednotlivé doklady v závislosti od legislatívnych podmienok tak, aby občan disponoval mobilným zariadením s vloženým prostriedkom schopným akumulovať všetky relevantné doklady v digitalizovanej podobe. Zdá sa byť nespornou výhodou pre držiteľa mať všetky doklady vždy poruke a okamžite ich použiť v elektronickom prostredí resp. ich zobraziť autoritám na požiadanie. Z pohľadu autorít môže byť prínosom vykonávanie inšpekcie dokladov v reálnom čase prostredníctvom mobilného zariadenia v proximity režime.

Registrujte sa pre aktualizácie

Hewlett Packard Enterprise

4AA6-8167ENW, October 2016