Secure Element API

An introduction
Objectives and use cases

• “An API enabling the discovery, introspection, and interaction with hardware tokens (Secure Elements) that offer secure services such as tamper-proof storage, cryptographic operations, etc.”

• Secure Elements:
  – Smart card (contact or contactless)
  – SIM/ UICC card
  – Smart/Secure microSD cards
  – Embedded Secure Elements

• Clients
  – PC
  – Mobile
  – Tablet
  – …
Use Case #1: Web Authentication with SE

- PC, with contact or contactless PC/SC reader
- Government eID card with contacts
- User goes to an eGov web site, and is asked to authenticate
  - E.g. https://tax.myeservices.net/
- User inserts her eID card in PC reader, and types PIN code
- User is authenticated
- User digital signs a document (eg Tax declaration) using her ID card
Use Case #2: “Card present” mCommerce

- Mobile with NFC
- UICC or NFC Visa card
- User navigates to a merchant web store in mobile browser
- User pays with Visa app preloaded on UICC or in contactless Visa banking card
- This triggers a system application, which prompts user for confirmation and optionally payment issuer (if multiple available), PIN code, asks SE for “payment credential”, and forward it to payment server
- When payment confirmation is received, it is forwarded to originating merchant in the browser, which displays confirmation message
Use Case #3: Reloading transportation card

- Mobile with NFC
- Public transportation card (e.g. London’s Oyster card)
- User opens the mobile browser, and navigates to the card’s emitter web site (e.g. https://oyster.tfl.gov.uk)
- User buys a ticket and loads it on her transportation card by tapping it on the mobile
- Transportation card now holds the tickets, it can be presented to “touch” readers when travelling
Use Case #4: Mobile ID (OOB auth)

• 2 devices:
  – Web application used on PC browser (no SE)
  – Out-of-band authentication on Mobile with NFC
• Company ID card with embedded Auth Certificate
• User opens a session on a web application in a PC browser
• The server opens a session and waits for credential (a signature) from a pre-registered mobile
• User opens a pre-installed authentication application on mobile, and tap her NFC corporate card
• Authentication application computes the credential using the embedded card certificate, and sends it to server
• Server validates session on PC browser and let user in
Status

• In W3C: SE planned in Phase 2 of SysApp WG

• Adoption in Web industry:
  – Tizen
    • Open source, standards-based software platform supported by leading mobile operators, device manufacturers, and silicon suppliers for smartphones, tablets, netbooks, in-vehicle infotainment devices, smart TVs, etc.
  – Webinos
    • EU funded project delivering a platform for web applications across mobile, PC, home media (TV) and in-car devices

• Adoption In Mobile Industry
  – SIMAlliance’s Open Mobile API
    • Non-profit trade association working mobile community seeking to create a secure, open and interoperable mobile environment
  – Deployed devices (NFC):
    • 180+ models by more than 15 manufacturers
    • Android, BlackBerry (BB OS 10), Windows Phone (7.5)
Commercial devices examples

- Acer: Liquid Express C6
- Alcatel (TCL): Smart III-4
- BlackBerry: Z10
- HTC: One X
- LG: P940 (Prada)
- Nokia: Lumia 610 NFC
- Motorola: Droid RAZR (XT926)
- Samsung: Galaxy S2, Galaxy S3, Galaxy S4
- Sony: Xperia Z
- ZTE: P728

...
Roadmap

• Editorship offer: 2 co-editors
  – Gemalto (Olivier Potonniée)
  – Intel (Tran Dzung D.)

• Ready to draft
  – Start with Use Cases
  – Contributions welcome

• Requirements
  – How should we manage them?