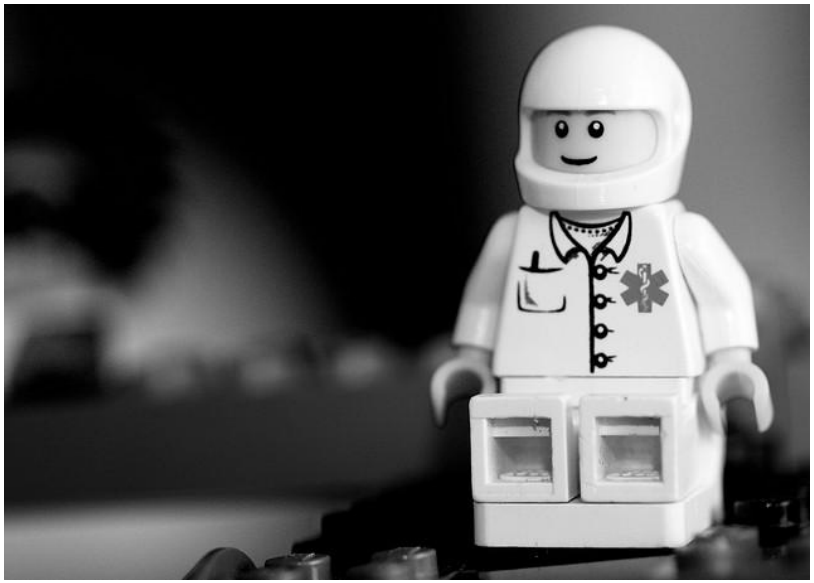
Security Enablers : Trends

Virginie GALINDO
September 2014

Virginie Galindo …

http://fr.linkedin.com/in/virginiegalindo



L'indémodable by EquinoxeFr (Creative Common rights)

gemalto

Security Enablers ? What are we taking about ?

- Anything with a dedicated chips to perform secure calculation and secure storage of sensitive credentials …
- Yes, it means, SIM cards (micro, nano, ..), ID card, corporate or loyalty cards, banking card, USB token, TPM chips, embedded Secure Element, stacked chips with unbelievable packaging, HSM (on server side, in readers)…
- Yes, all of it…

Security Enablers Markets

- Banking & Payment
- Government
- Mobile
- Corporate
- M2M (car industry, smart city, starting)
- IoT (not yet, really)

All those markets are enjoying tremendous transformation

8 trends challenging the secure enablers

- All is (open) mobile
- New connectivity
- Welcome to the online world
- Value proposition move
- From native to mobile to web
- From integration to desperation
- Security alternatives
- New customer power balance

Hum…

- 8 reasons that could put the secure enablers in danger ?
- What can we do about it ?

This is all about adapting, pivoting, moving, shifting, buying, gathering, innovating (my fav' ones)

1. Revisit the security value

- We need to position the value proposition of the security in the different markets we address and the new market to attack
  - SE versus TEE versus software
  - NFC : Android app accessible via HCE versus Secure Element

- We need to have a consistent and real life based value proposition
  - Don’t use a smart card to protect a mobile app having a 2 months life

- Re-assess the security certification virtues
  - EAL4+ means something
  - See http://www.ssi.gouv.fr/fr/produits-et-prestataires/produits-qualifies/
  - Security certification is the only mean to guarantee secure functions

2. Promote and develop TEE

- TEE is a good technology that makes the security job
  - Secure storage and secure execution
  - Trusted UI (coming soon …)
  - Certified EAL2+ (or similar), resistant to software attacks
  - Integrated in recent smart phones
  - Standardized in Global Platform with all actors (device makers, smart card vendors, chipset vendors, service providers), see http://www.globalplatform.org/specificationsdevice.asp
  - Requires remote management (that we can offer)
  - An open source TEE project exists https://github.com/OP-TEE to support Linaro Security Working Group

- It is a good (best) companion for Secure Enablers
  - TEE standard API to access the Secure Element
  - Secure Channel between applications in TEE and Secure Element

3. Enter mobile

- Join force in SIM Alliance (gathering SIM card vendors)
  - Defining an interoperable API to access Secure Element
  - Allowing to access any Secure Element
  - Read the Open Mobile API
- Support mobile vendors and mobile network operators to integrate it
  - Now present in major NFC enabled platforms
- Build a consistent offer for all Secure Enablers
  - Offer around the embedded Secure Element
  - And make sure several Secure Element can co-exist
- Do not ignore HCE

3. Enter web

- Becoming W3C, OWASP, FIDO Alliance members

- Starting to talk with browser makers
  - Look at recent FF OS, it does embed an access to Secure Element https://bugzilla.mozilla.org/show_bug.cgi?id=879861
  - By the way, Tizen too, https://developer.tizen.org/dev-guide/2.2.0/org.tizen.web.device.apireference/tizen/se.html

- Supporting development of sensitive use cases such as
  - Payment : http://www.w3.org/2014/04/payments/webpayments_charter.html
  - Cryptography : http://www.w3.org/2012/webcrypto/
  - Online authentication : https://fidoalliance.org/specifications
  - Security in general : https://www.w3.org/Security/wiki/IG

4. Seek new opportunities

- New markets
  - Automotive,
  - Smart City,
  - E-banking,
  - New form factors (Wereable…)

- Strengthening our eco-system
  - Connecting service providers and customers with trust
  - Administrating services for them with security

5. Innovation …

- Experimenting (and creating) new objects and services,
- Changing manufacturing process
- Joining IP free (today's) world

So what …

This is really interesting to see this industry moving, creating new value and new services

Thanks !

gemalto