Mobile Payments with Linux

Samuel Ortiz
Intel Open Source Technology Center

September 16th, 2013
Agenda

- What's a mobile payment?
- How does it work?
- Missing and existing Linux bits
- A proposal
Mobile Payment?

- Money transaction from a mobile device
- SMS payments
- Direct billing
- Contact-less payments
Contact-less Payments

- NFC as the carrier
- Coupons, Loyalty
- Key-less rental cars, hotels...
A widely deployed technology

Storage

Smartcard OS

Metro Reader

UNDERGROUND

oyster

FROM
What we want

- Phone as a smartcard
- NFC card emulation
- At least as secure
- One device, multiple services
What Card Issuers want

- Tamper resistant platform
- Security domain
- Secure storage
- FIPS and CC certified crypto
- Not your typical mobile SoC...
Secure Elements

• Secure platform
  • Stores and runs application
• 3 form factors
  • SIM, NFC embedded, μSD
• Smartcard OS
• EMV compliant
• Space for rent
How does all this work?

- The POS sees the mobile device as a card
- The POS selects an application on the SE
- Transaction between the SE and the POS
  - ISO7816 APDUs
- The SE notifies the host, if needed
- The NFC controller becomes a pass-through
So what's needed on Linux?

- Secure elements manager
- But there are more requirements:
  - Host must be able to send ISO 7816 APDUs
  - Host must implement access control
  - Host must be able to route notifications
  - Host should provide SIM alliance APIs
Do we have that?

- SEEK for Android is open source
- But:
  - Specifically designed for Android
  - Very limited HW support
  - SIM centric
  - Java APIs
  - This is NOT your Google Wallet
Our proposal

- NFC netlink API
  - Discover and enable/disable secure elements
  - Forward NFC events
- Secure element daemon
  - Access control, ISO 7816 I/O
- D-Bus API
  - SIM Alliance compatible
Netlink API

- SE discovery and enablement
  - Upstream, implemented for pn544
- NFC ISO 7816
  - Implemented on nfc-next
- NFC events
  - Events defined, not implemented yet
Secure Element Daemon

- ISO 7816 abstraction
  - Support for NFC and telephony
- Access control list
  - Global Platform specification
  - Enforcement done on the host
  - Fall back mechanism not implemented
- NFC events
  - Not supported yet
Secure Element Daemon

- D-Bus API
  - To be compatible with the SIM Alliance API
  - Lists, enables and disables SEs
  - Access to the basic channel
  - Opens a logical channel linked to an AID
  - Logical channel I/O
- Will be part of neard
Next Steps

- Software secure elements (TEEs)
- Reader/POS mode
- Cloud based payments
- Access control fall back mechanism
- NFC events
- Provisioning
Questions?

sameo@linux.intel.com