Workshop on Authentication, Hardware Tokens and Beyond

Discovery and connection API for Proximity Security Devices

Philip Hoyer – Director Strategic Innovation

September 10th, 2014

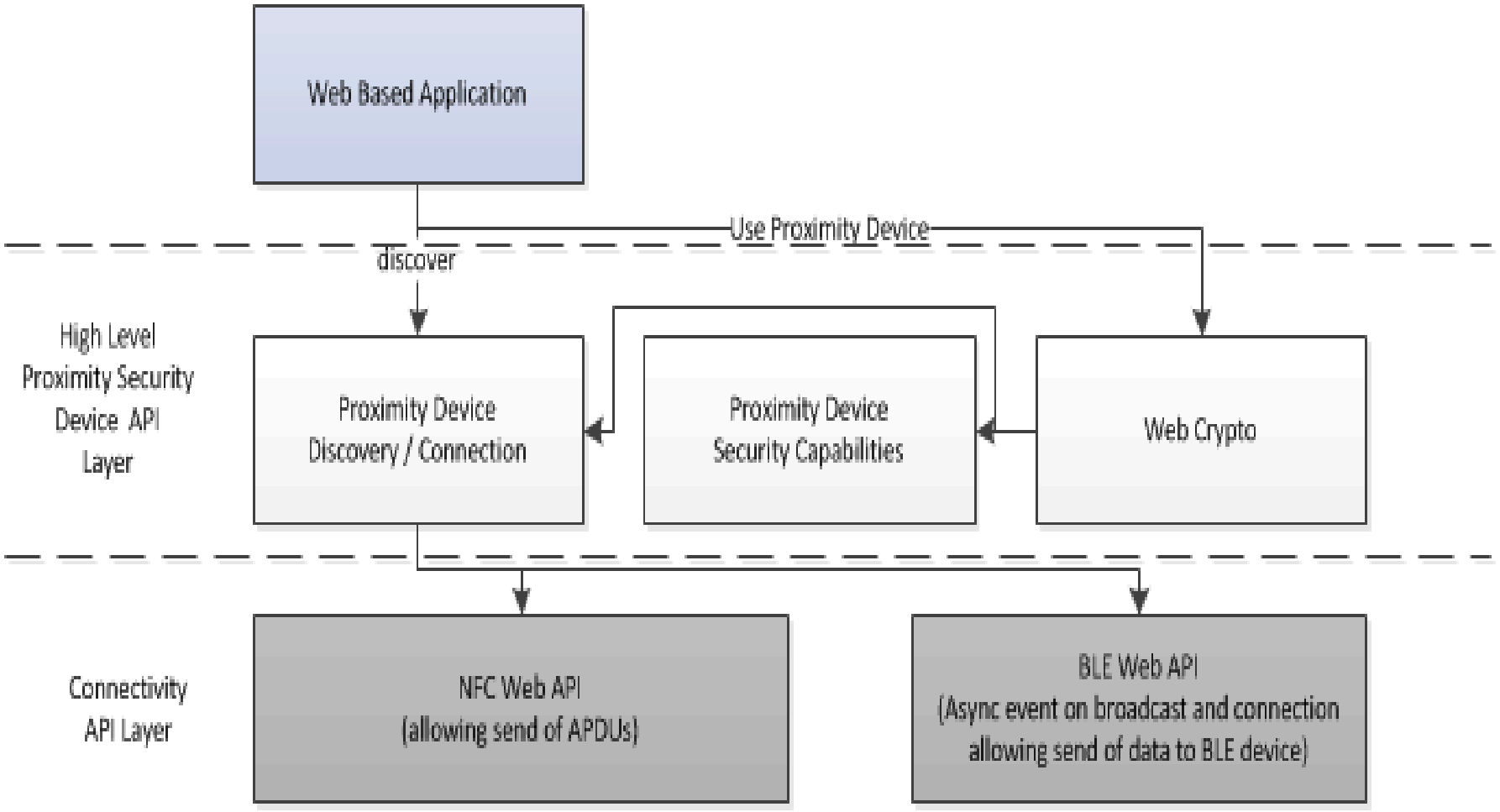
New proximity technologies and security capable or security dedicated devices

Application terminal device hosting browser app – Proximity device interaction

Proposal – proximity API: two layers

- **Communication oriented API**, to be able to communicate with the device from a web based application – high priority / fundamental
  - ***NFC*** - W3 has done some forays into NFC with the Web NFC API (http://www.w3.org/TR/nfc/) limited to reading NFC forum tags no APDUs send/receive support needed for contactless smart card for example (PIV 201-2 smart card or an HID Seos Access Card)
  - ***BLE*** There seems no current web API for BLE
- **Proximity Devices API** - Higher level API (uses Comm API) :
  - ***Discovery / Connection*** and listing of known Proximity Security devices independent of transport (abstract NFC / BLE, etc as much as possible)
  - ***Retrieval of the security capabilities*** of known Proximity Security Devices
  - ***Connection API*** to the security devices at an abstraction level that would then map it to the existing W3C Crypto API Level (e.g. ability to retrieve a handle to a SubtleCrypto interface from a connected device handle)

Layer diagram



Conclusion

- In the quest to get rid of passwords, contactless proximity interface based security devices present one of the best and convenient user experience.
- By enabling browser based application to leverage them for security (authentication and crypto function) processes through a set of layered Proximity Device APIs we will see new generation of user convenient and secure web applications.
- We feel that this proposal is ideally aligned and builds on the initial work of the W3C Crypto API charter.