draft-irtf-hiprg-rfid-03

HIP support for RFIDs

Pascal.Urien@telecom-paristech.fr

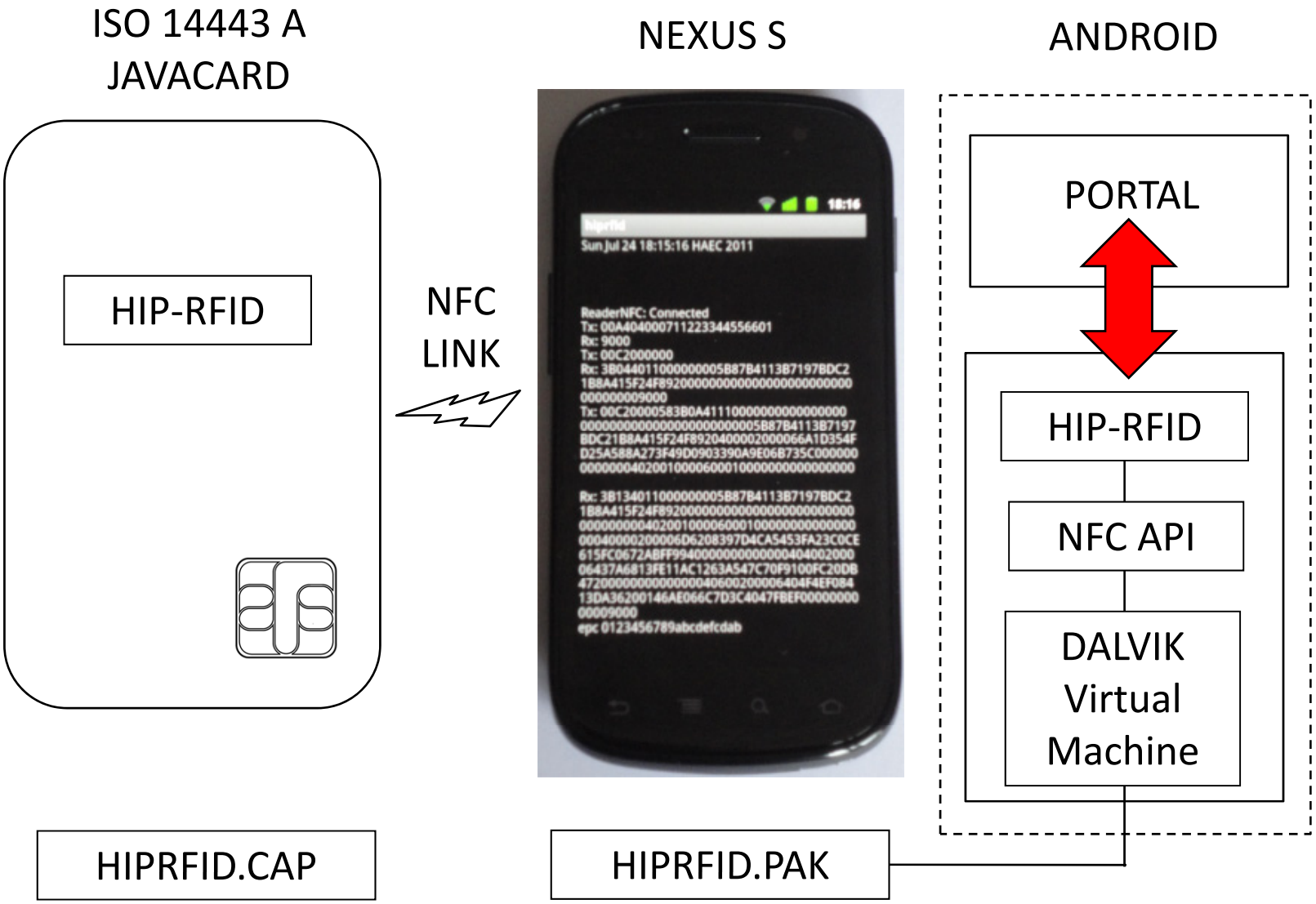
http://perso.telecom-paristech.fr/~urien/hiprfid/

http://www.telecom-paristech.fr

What is new in version 03

- **Review from Thomas R. Henderson**
  - Thanks Tom !
- **Editorial issues**
  - Typographic corrections
- **Experimental platforms**
  - Tests with Android platform (Nexus S) and NFC (javacards) HIP-RFIDs
  - More Info http://perso.telecom-paristech.fr/~urien/hiprfid/

Android Experimental Platform



Conclusion

- **To be done**
  - Section on security
- **To be defined by an other draft**
  - HIT-I structure for pseudo-random coding
  - Secure Channel establishment
  - HEP (HIP Encapsulation Protocol)

HIP-RFID in a Nutshell

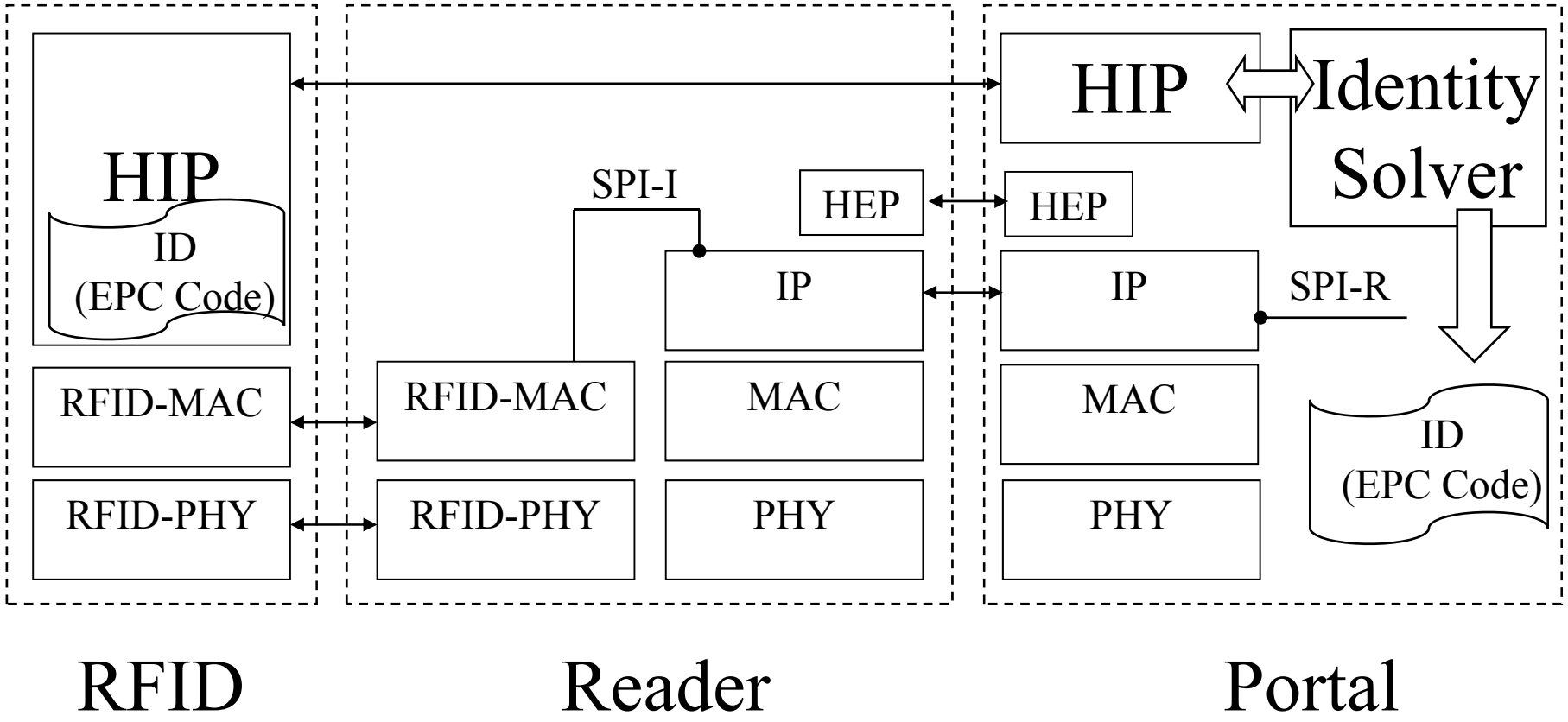
About RFIDs

- **What is an RFID ?**
  - An RFID is an electronic device that delivers an identity (ID) thanks to radio means.
- **Link with the Internet Of Things (IoT)**
  - A Thing is associated with a RFID
- **RFID have limited computing resources**
  - Electronic chip, whose area ranges from 1mm^2 to 25mm^2
  - RFIDs are usually powered by readers.
  - Very low power consumption.
- **Objective of this draft**
  - Defining **a protocol for RFIDs**, compatible with the IP ecosystem.
  - Enforcing **strong privacy**, i.e. no information leakage for unauthorized ears.
  - **Crypto Agility**: cryptographic procedures adapted to RFIDs computing resources.
  - Managing **secure channel** with RFIDs (Optional)

HIP -RFID Overview

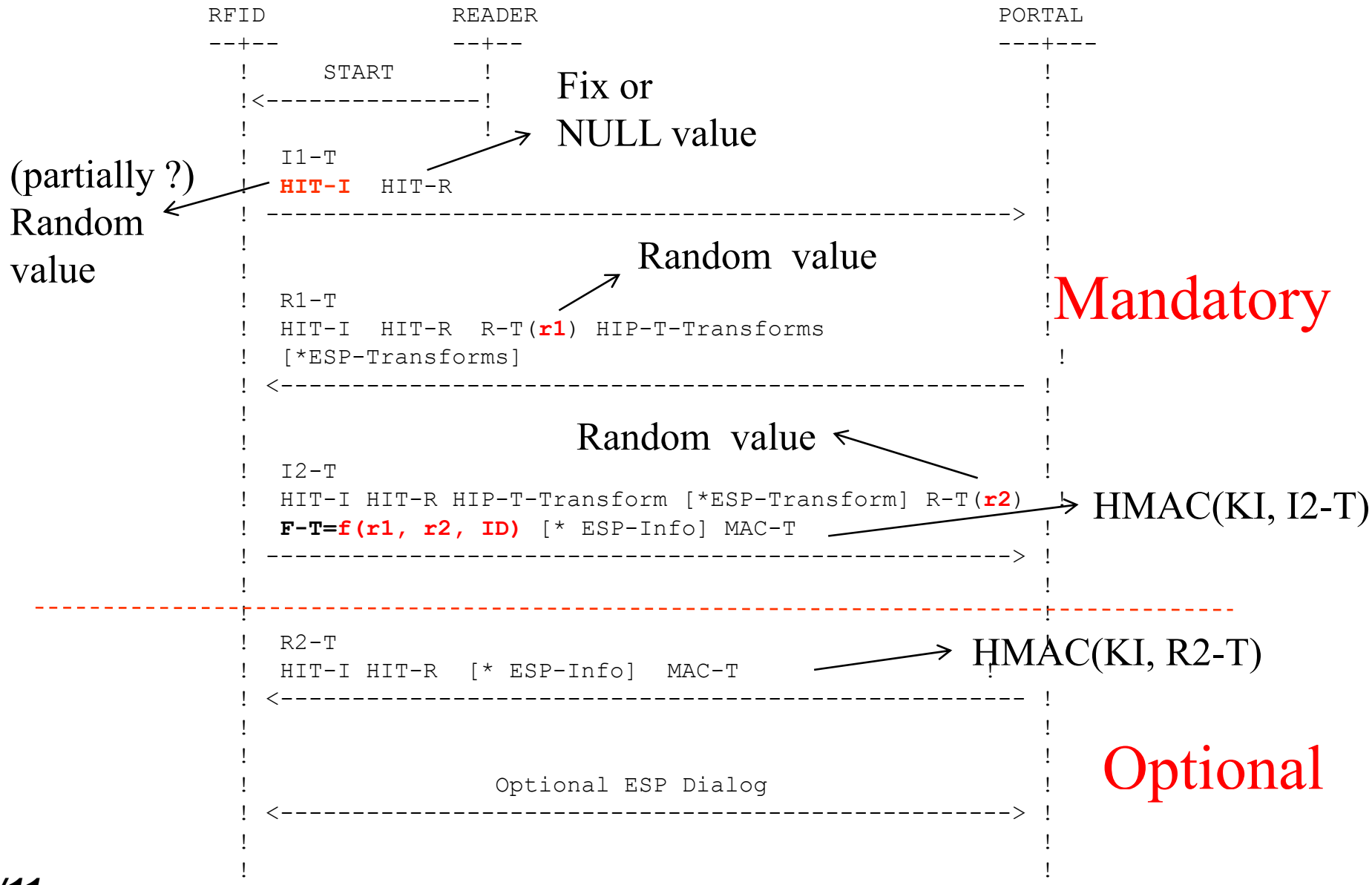
- **Modified BEX exchange**
  - Negotiation of the security scheme (HIT-T-TRANSFORM attribute).
  - Third and fourth message are MACed (typically with a HMAC function)
  - Fourth message is optional, only mandatory when a secure ESP channel has been negotiated.
    - This SHOULD be specified in a new draft
    - ESP MAY be used for read write operation.
- **The HIT is a 16 bytes random number**
  - MAY include a fix part
  - To be fixed
- **RFIDs never expose their identity in clear text, but hide this value (typically an EPC-Code) by a particular equation (f) that can be only solved by a dedicated entity, referred as the PORTAL.**
  - f(r1,r2, ID)
  - *f can be anything that works*
  - *An integrity key is computed from KI-AUTH-KEY = g(r1,r2,ID)*
- **HIP exchanges occurred between RFIDs and PORTALs; they are shuttled by IP packets, through the Internet cloud.**

HIP-RFID Architecture



*HEP: HIP Encapsulation Protocol

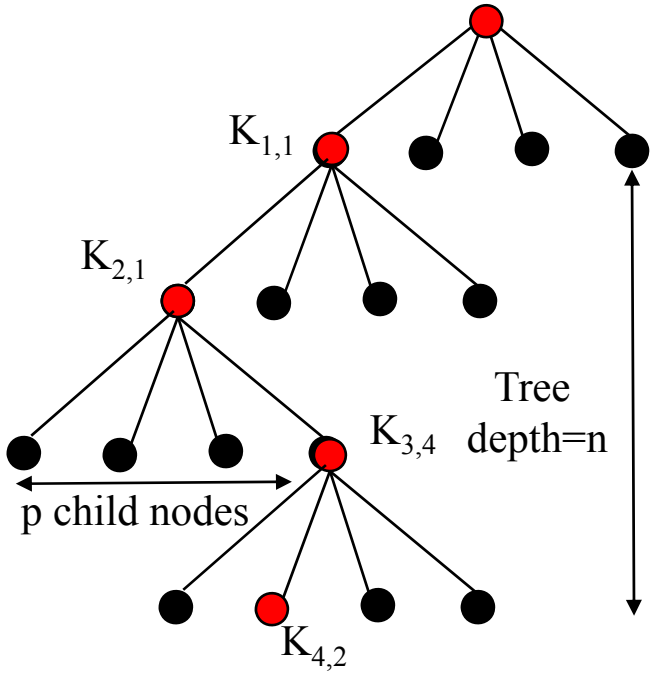
Protocol Overview



T-TRANSFORM 0001, HMAC

- K = HMAC-SHA1(r1 | r2, ID)
- F-T = HMAC-SHA1(K, CT1 | "Type 0001 key ")
  - CT1 = 0x00000001 (32 bits)
- KI-AUTH-KEY = HMAC-SHA1(K, CT2 | "Type 0001 key")
  - CT2 = 0x00000010 (32 bits)

T-TRANSFORM 0002, Keys-Tree



- A Keys-Tree manages a maximum of p^n RFIDs, with np keys
- Each RFID stores n keys
- RFID-Index = I= Function(EPC-Code)
  - $I= a_n\ p^{n-1} + a_{n-1}\ p^{n-2} +\ldots + a_1$
- Each term a_i is associated with a key $K_{i,j}$
  - $1 \le i \le n$
  - $0 \le j \le p-1$
  - $j= a_i$
- $f(r1,r2,\text{EPC-Code})= H_1 | H_2 | \ldots | H_n$
  - $Hi = HMAC(r1|r2, K_{i,j})$