draft-irtf-hiprg-rfid-02

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 02

- **Editorial issues**
  - Typographic corrections
- **Java code for NFC RFIDs added to the draft**
  - Only support the T-TRANSFORM 0001
- **Experimental platforms**
  - Tests with NFC (javacards) RFIDs
  - Tests with smart phone equipped with the NFC technology and (U)SIM (java) cards
  - In progress, tests with Android platform
  - More Info http://perso.telecom-paristech.fr/~urien/hiprfid/
- **Comparison between HMAC or Key-Tree T-Transforms**
  - Paper published at IEEE CCNC 2011
  - For N RFIDs, N small, HMAC is more efficient
  - For N RFIDs, N= p^n big, Keys Tree is more efficient, with p big and n small

Conclusion: To be done

- **HIT structure for pseudo-random coding**
  - Proposal ?
  - Done in an other draft ?
- **Secure Channel establishment**
  - To be specify by an other draft.
- **HEP (HIP Encapsulation Protocol)**
  - To be specify by an other draft.
- **Java code for RFIDs to be improved**
  - T-TRANSFORM 0002 support

HIP-RFID in a Nutshell

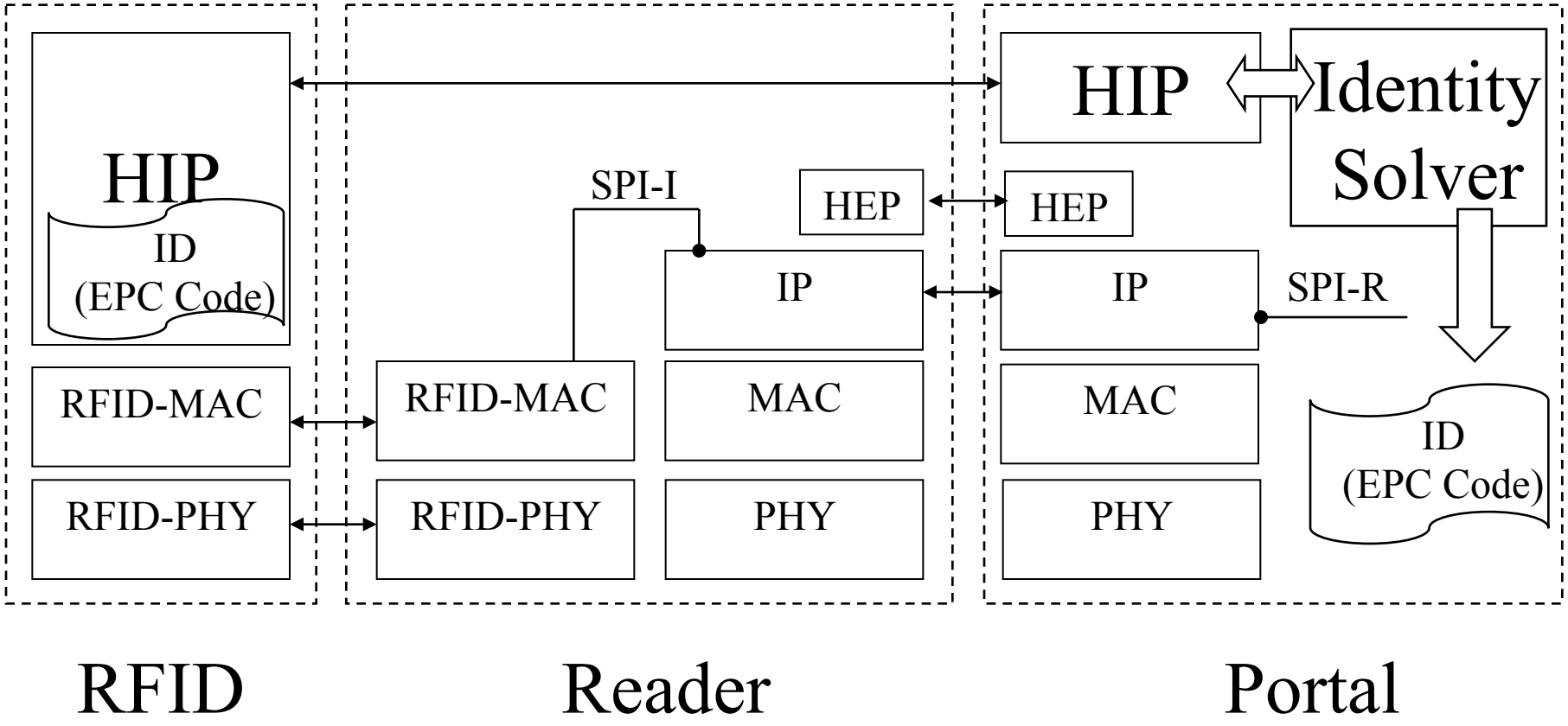
About RFIDs

- **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.
  - Managing **secure channel** with RFIDs (Optional)
  - **Crypto Agility**: cryptographic procedures adapted to RFIDs computing resources.

HIP -RFID Overview

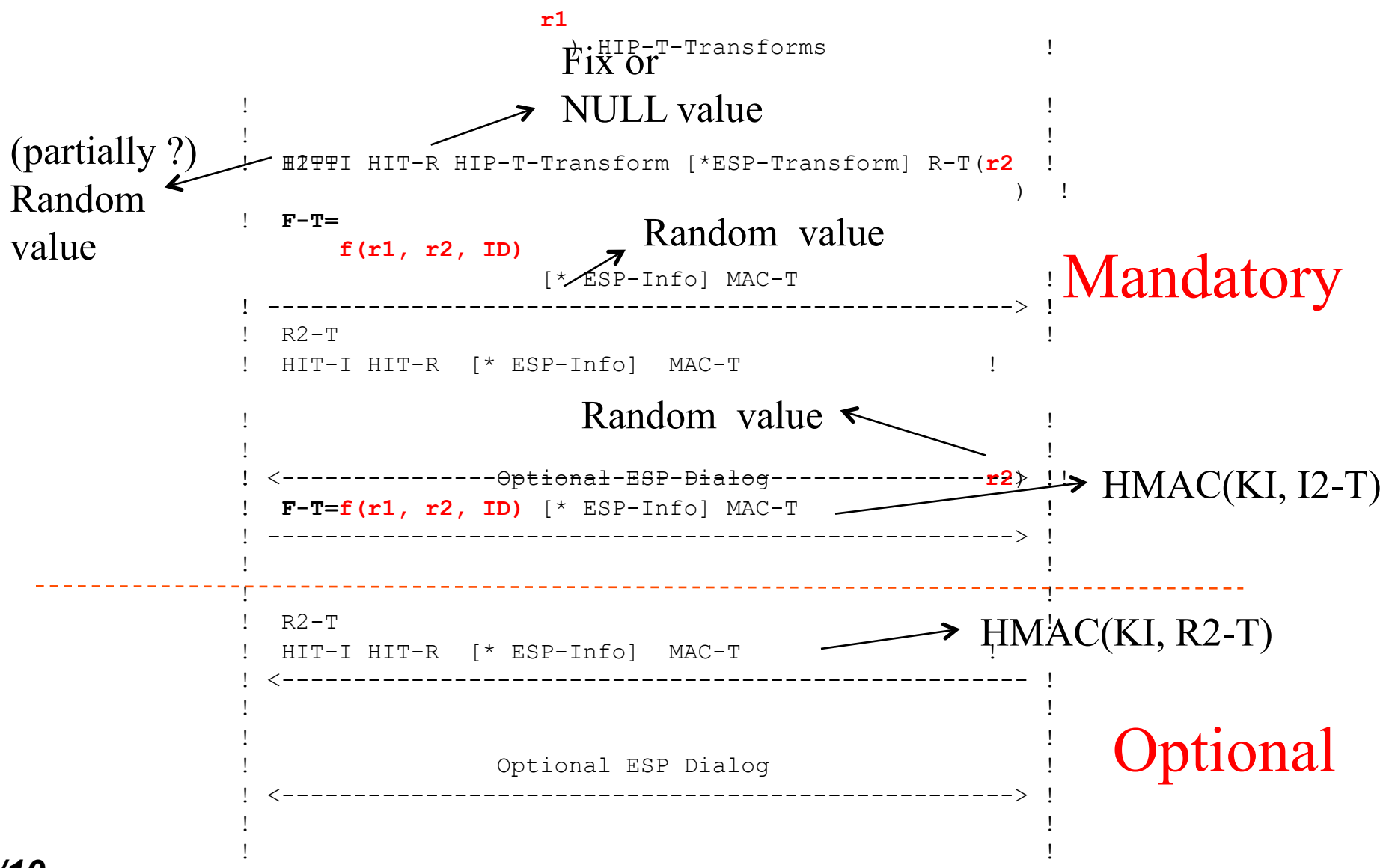
- **Modified BEX exchange**
  - Negotiation of the security scheme (HIT-T-TRANSFORM attribute).
  - Third and fourth message are MACed (typically with a HMAC function)
  - Fourth message is optional, only mandatory when a secure ESP channel has been negotiated.
    - This SHOULD be specified in a new 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

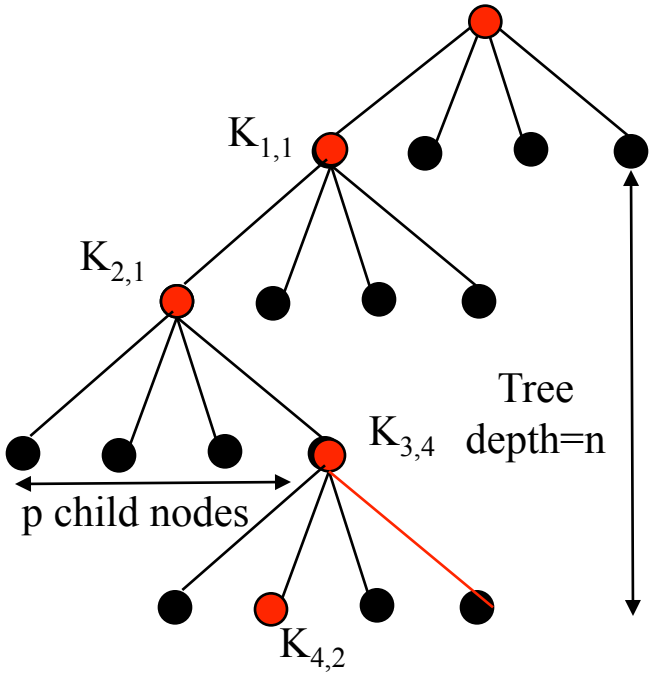
Protocol Overview



T-TRANSFORM 0001, HMAC

- K = HMAC-SHA1(r1 | r2, ID)
-
  -
-
  -

T-TRANSFORM 0002, Keys-Tree



- Code)
  -
- key $K_{i,j}$
  -
  -
  -
-
  - Hi = HMAC(r1|r2, $K_{i,j}$)