draft-irtf-hiprg-rfid-01

HIP support for RFIDs

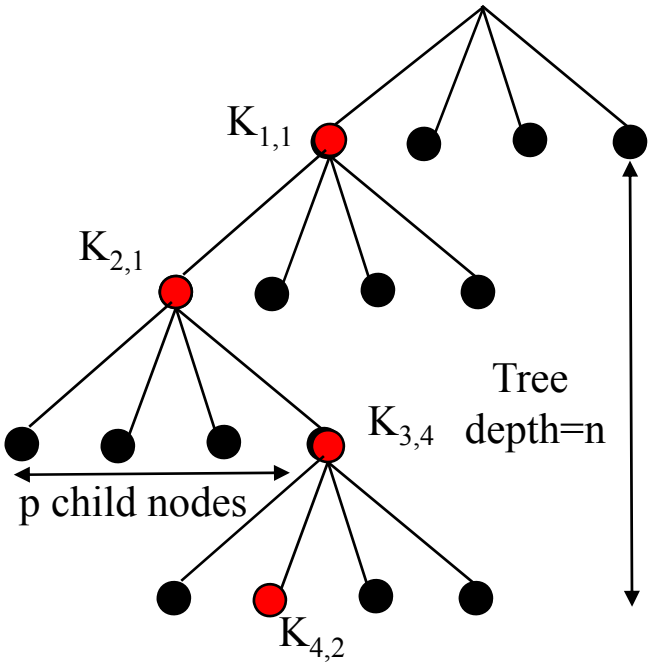
Pascal.Urien@telecom-paristech.fr

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

What is new in version 01

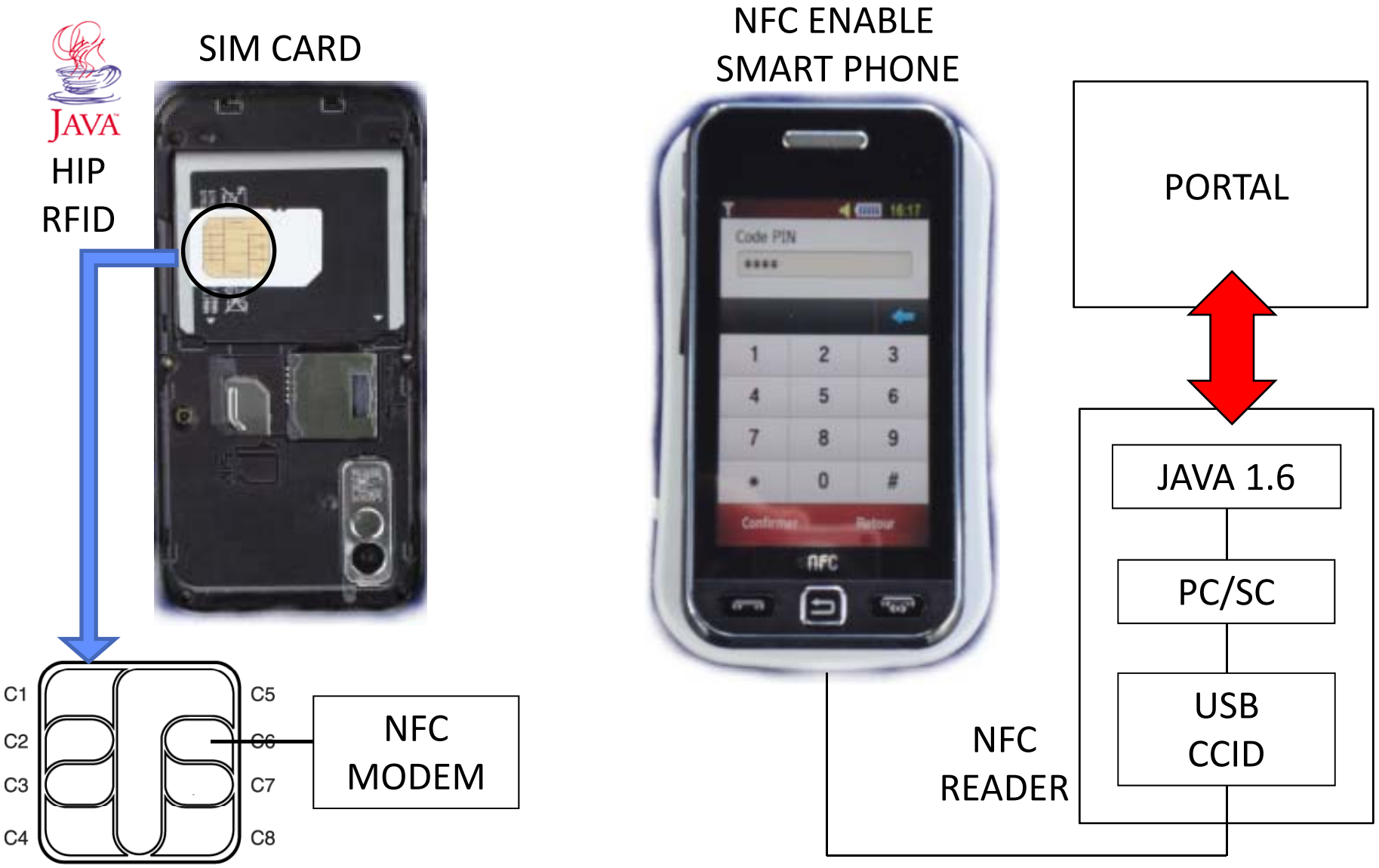
- **Editorial issues**
  - Replace the word TAG (inherited from the previous draft HIP-TAG) by RFID
  - The Signature-T attribute is renamed MAC-T
  - The HAT (HIP Address Translation) protocol is renamed HEP (HIP Encapsulation Protocol)
- **Keys-Tree improvement**
  - Simulations of various scenarios show that a tree of depth n, with p**n elements (p child nodes per node) is optimized for p a big integer (10^6, …) and n small integer (<10)
    - RFID have small computing resources
    - PORTAL have powerful computing resources
  - Paper to be published
- **Experimental platforms**
  - Tests were performed with smart phone equipped with the NFC technology and SIM (java) cards
  - Paper to be published

Keys-Tree



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

HIP-RFID for NFC Smart phone



Conclusion: To be done

- HIT structure for pseudo-random coding
- Secure Channel establishment
  - To be specify by an other draft
- HEP (HIP Encapsulation Protocol)
  - To be specify by an other draft
- Open code for Keys-Tree
- Other ?

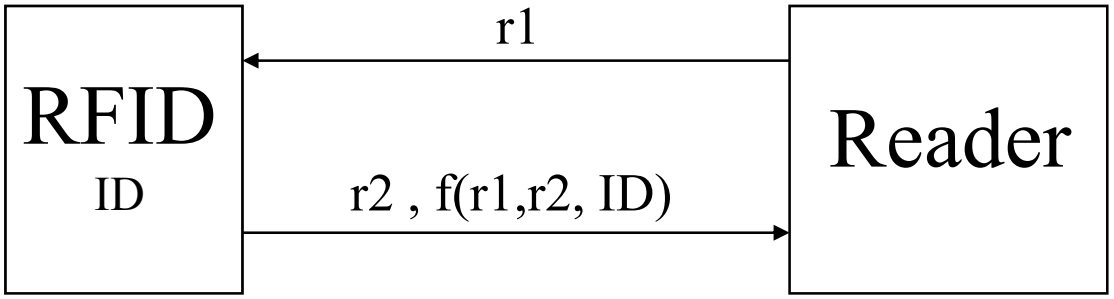
HIP-RFID in a Nutshell

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.

Privacy issues for RFIDs

- ID MUST be protected
- HIP-RFID: ID is a solution of f(r1,r2,ID)



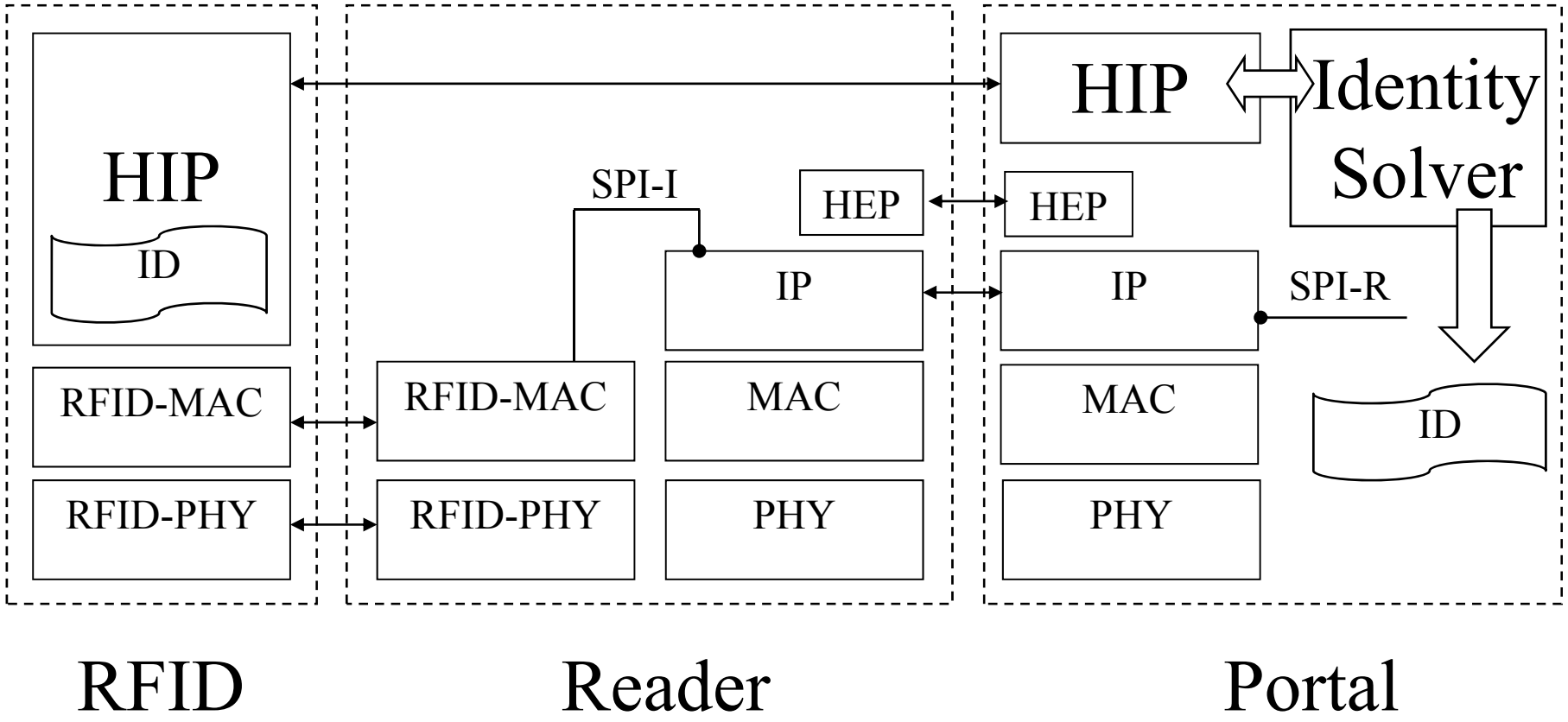
- Example
  - Many proposal in the scientific literature
    - Example: f(r1,r2, ID) = hash (r1 | r2 | ID)

S. Weis, S. Sarma, R. Rivest and D. Engels. "Security and privacy aspects of low-cost radio frequency identification systems." In D. Hutter, G. Muller, W. Stephan and M. Ullman, editors, International Conference on Security in Pervasive Computing - SPC 2003, volume 2802 of Lecture Notes in computer Science, pages 454- 469. Springer-Verlag, 2003.

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 is not yet detailed in this draft
    - ESP MAY be used for read write operation.
- **The HIT is a random number**
- **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