draft-irtf-hiprg-rfid-04

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 04

- **Section 6, Security Considerations**
  - Data exchanged between readers and portals MUST be protected by appropriate means (IPSEC, …)
  - I1-T and R1-T packets are not protected by cryptographic features, but respectively deliver r1 and r2 value
  - I2-T packet is HMACed with a key computed from the RFID EPC-Code (i.e. g(r1,r2,EPC-Code))
  - Although HIP-T-TRANSFORMs detailed in this draft only deal with I2-T integrity, other transforms MAY use different schemes

To Be Done

- **We suggest a last call for the final review of this draft**
  - An open test platform has been released for Java, Android and javacards components, see http://www.enst.fr/~urien/hiprfid/index.html
- **Items that are not defined by this draft**
  - The HEP (HIP Encapsulation Protocol) protocol
  - ESP secure channels and associated ESP-T-TRANSFORMs
- **HIP-RFID could be extended by a new IRTF draft**
  - This item could be discuss in the next IETF meeting in Paris

HIP-RFID in a Nutshell

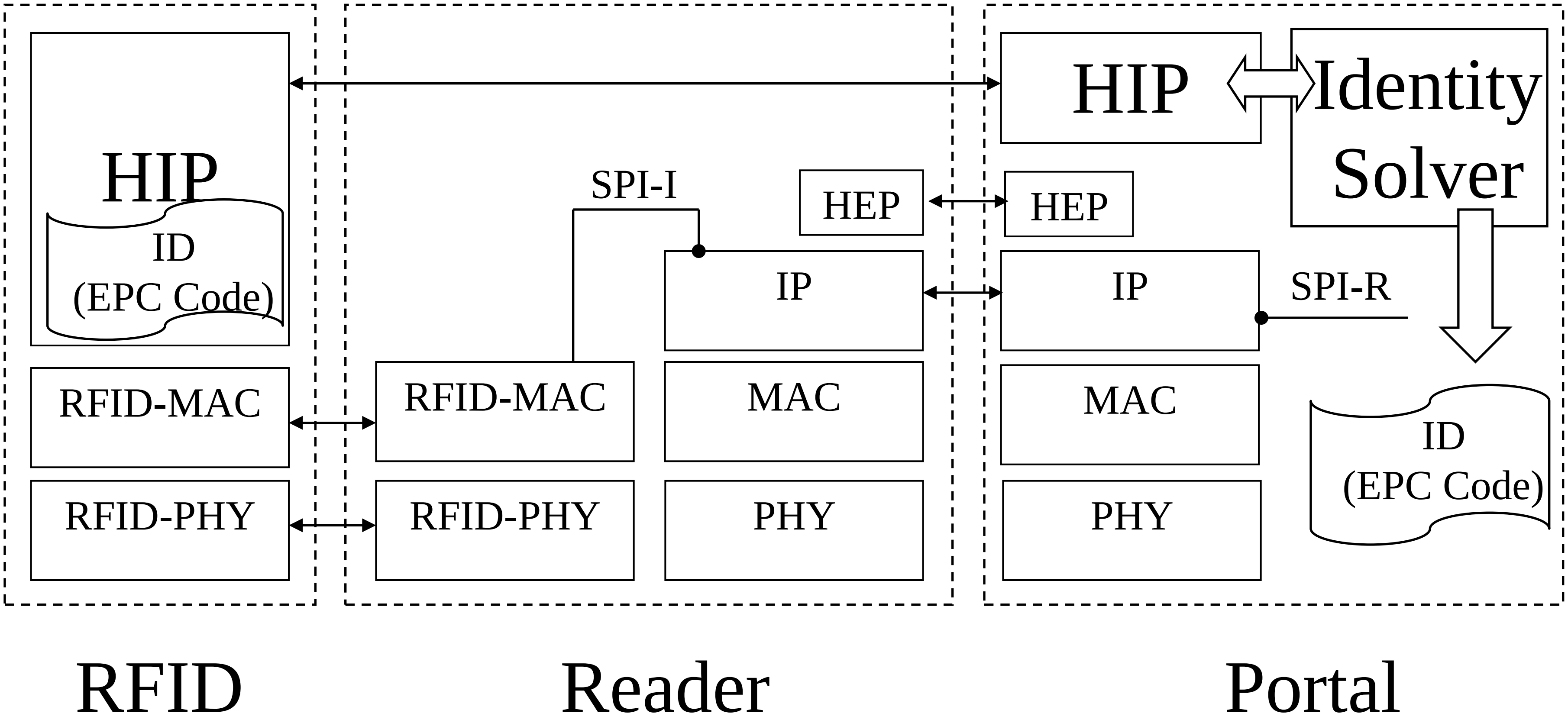
About RFIDs

- **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

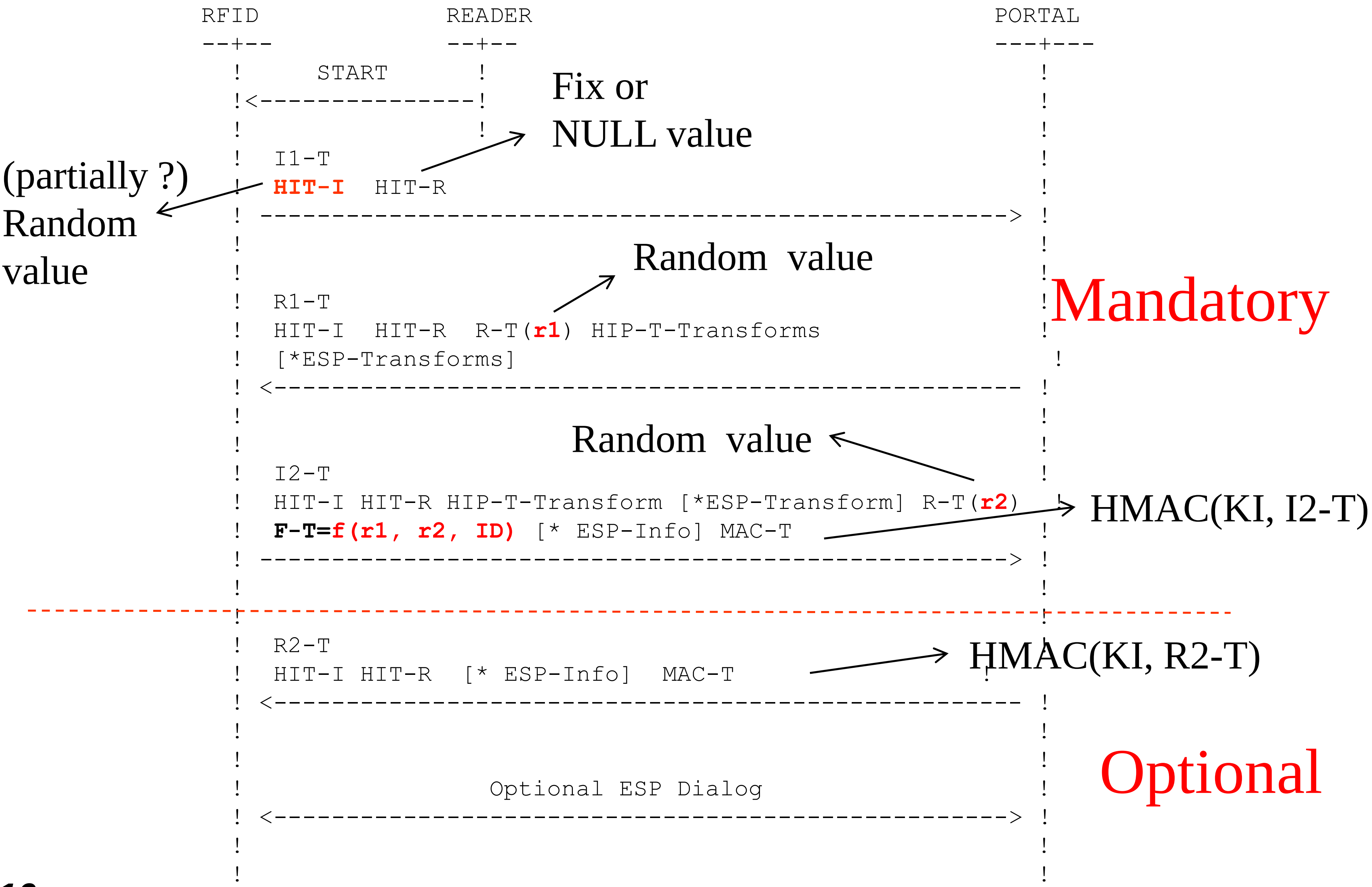
- **Modified BEX exchange**
  - Negotiation of the security scheme (HIT-T-TRANSFORM attribute).
  - Third and fourth message are MACed (typically with a HMAC function)
  - Fourth message is optional, only mandatory when a secure ESP channel has been negotiated.
    - This SHOULD be specified in a new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

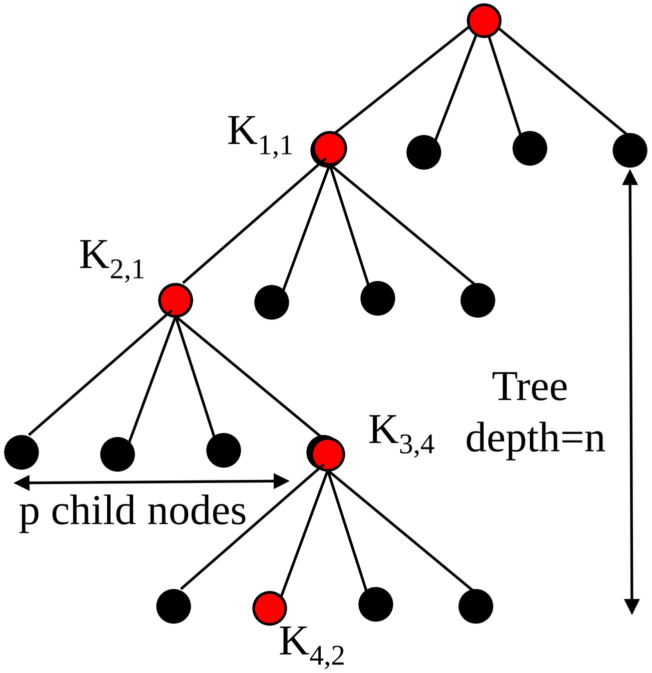


```
RFID             READER                                 PORTAL
--+--            --+--                                  ---+---
  !      START     !                                       !
  !<---------------!                                       !
  !                !                                       !
  !  I1-T                                                  !
  !  HIT-I  HIT-R                                          !
  ! -----------------------------------------------------> !
  !                                                        !
  !                                                        !
  !  R1-T                                                  !
  !  HIT-I  HIT-R  R-T(r1) HIP-T-Transforms                !
  !  [*ESP-Transforms]                                      !
  ! <----------------------------------------------------- !
  !                                                        !
  !                                                        !
  !  I2-T                                                  !
  !  HIT-I HIT-R HIP-T-Transform [*ESP-Transform] R-T(r2)  !
  !  F-T=f(r1, r2, ID) [* ESP-Info] MAC-T                  !
  ! -----------------------------------------------------> !
  !                                                        !
  !                                                        !
  !  R2-T                                                  !
  !  HIT-I HIT-R  [* ESP-Info]  MAC-T                     !
  ! <----------------------------------------------------- !
  !                                                        !
  !                                                        !
  !                 Optional ESP Dialog                    !
  ! <----------------------------------------------------> !
  !                                                        !
  !                                                        !
```

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 $K_{i,j}$
  - $1\leq i \leq n$
  - $0\leq j \leq p-1$
  - $j= a_i$
- $f(r1,r2,\text{EPC-Code})= H_1|H_2 |\ldots|H_n$
  - $Hi = HMAC(r1|r2, K_{i,j})$