draft-irtf-hiprg-rfid-00

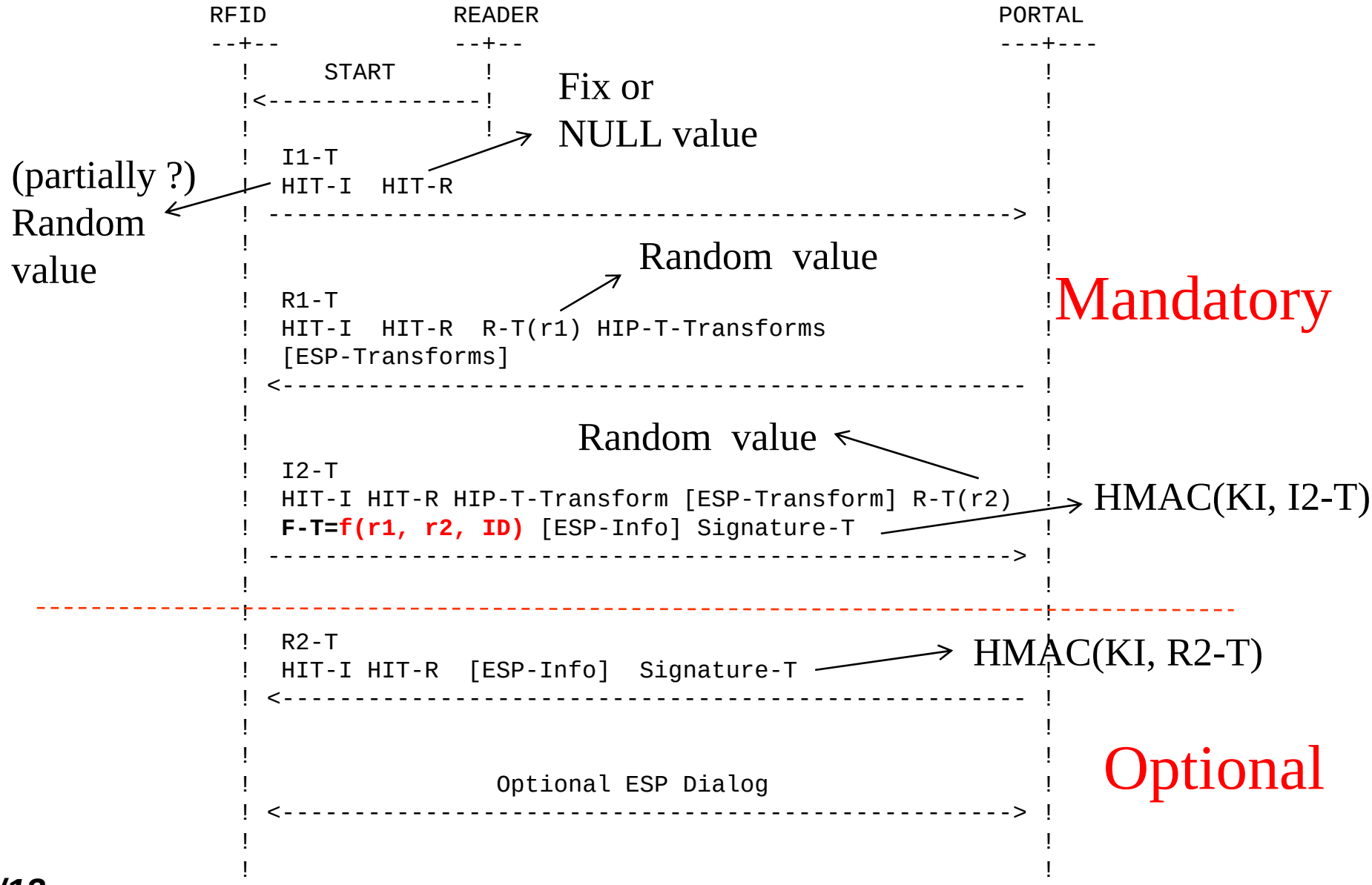
HIP support for RFIDs

Pascal.Urien@telecom-paristech.fr

About RFIDs

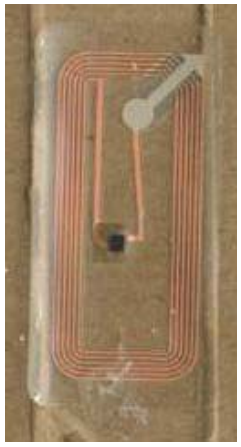
- **What is an RFID ?**
  - An RFID is an electronic device that delivers an identity (ID) thanks to radio means.
- **Link with the Internet Of Things (IoT)**
  - A Thing is associated with a RFID
- **RFID have limited computing resources**
  - Electronic chip, whose area ranges from 1mm^2 to 25mm^2
  - 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.

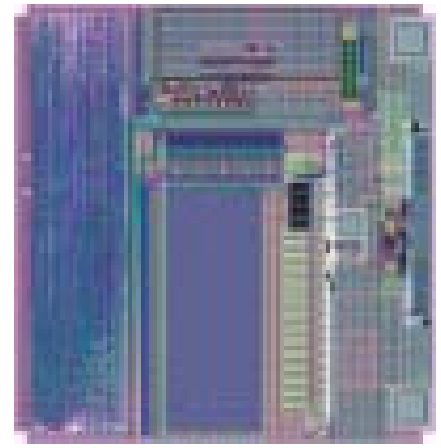
Protocol Overview



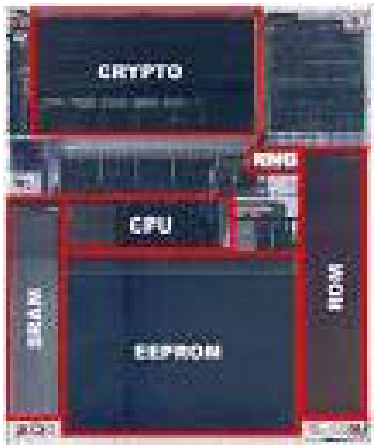
About RFIDs

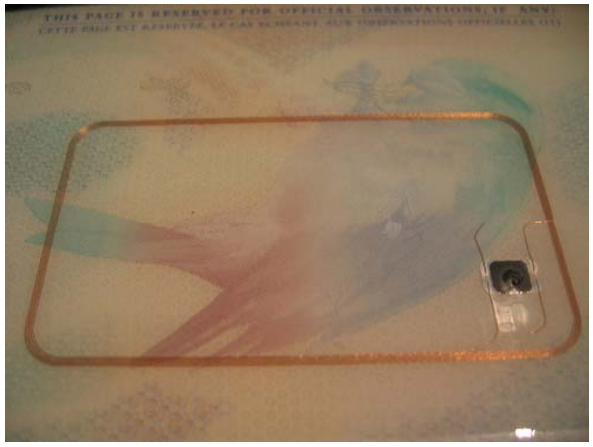
- **An RFID is a slice of silicon whose area is about 1 mm² for components used as cheap electronic tags, and around 25 mm² for chips like contact-less smartcards inserted in passports.**
- **We divide RFIDs in two classes,**
  - First comprises electronic chips based on cabled logic circuits.
  - Second includes devices that embed CPU and memories (RAM, ROM, E²PROM) such as contact-less smart cards.





ISO18000-3 Mode2 RFID Chip





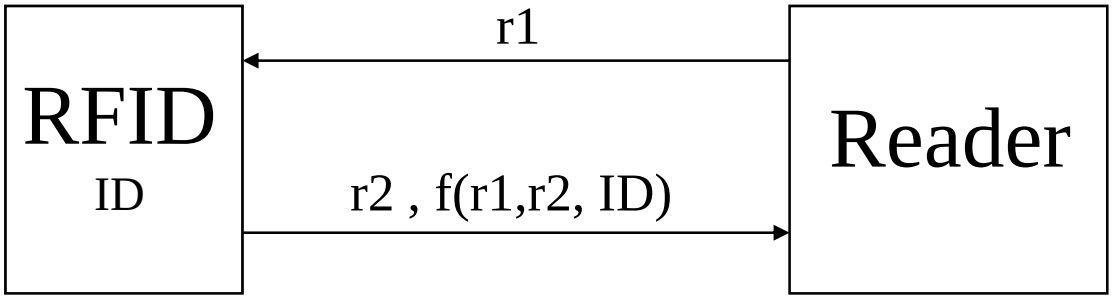
ISO 14443 Contact-less Smart Card

Some physical standards

- **The ISO 14443 standard introduces components dealing with the 13,56Mhz frequency that embed a CPU and consume about 10mW; data throughput is about 100 Kbits/s and the maximum working distance (from the reader) is about 10cm.**
- **The ISO 15693 standard also uses the same 13,56 MHz frequency, but enables working distances as high as one meter, with a data throughput of a few Kbits/s.**
- **The ISO 18000 standard defines parameters for air interface communications associated with frequency such as 135 KHz, 13,56 MHz, 2.45 GHz, 5.8 GHz, 860 to 960 MHz and 433 MHz.**
  - The ISO 18000-6 standard uses the 860-960 MHz range and is the basis for the Class-1 Generation-2 UHF RFID, introduced by the EPCglobal consortium.
- **NFC standards for mobile phones.**
  - Based on ISO 14443.

Privacy issues for RFIDs

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



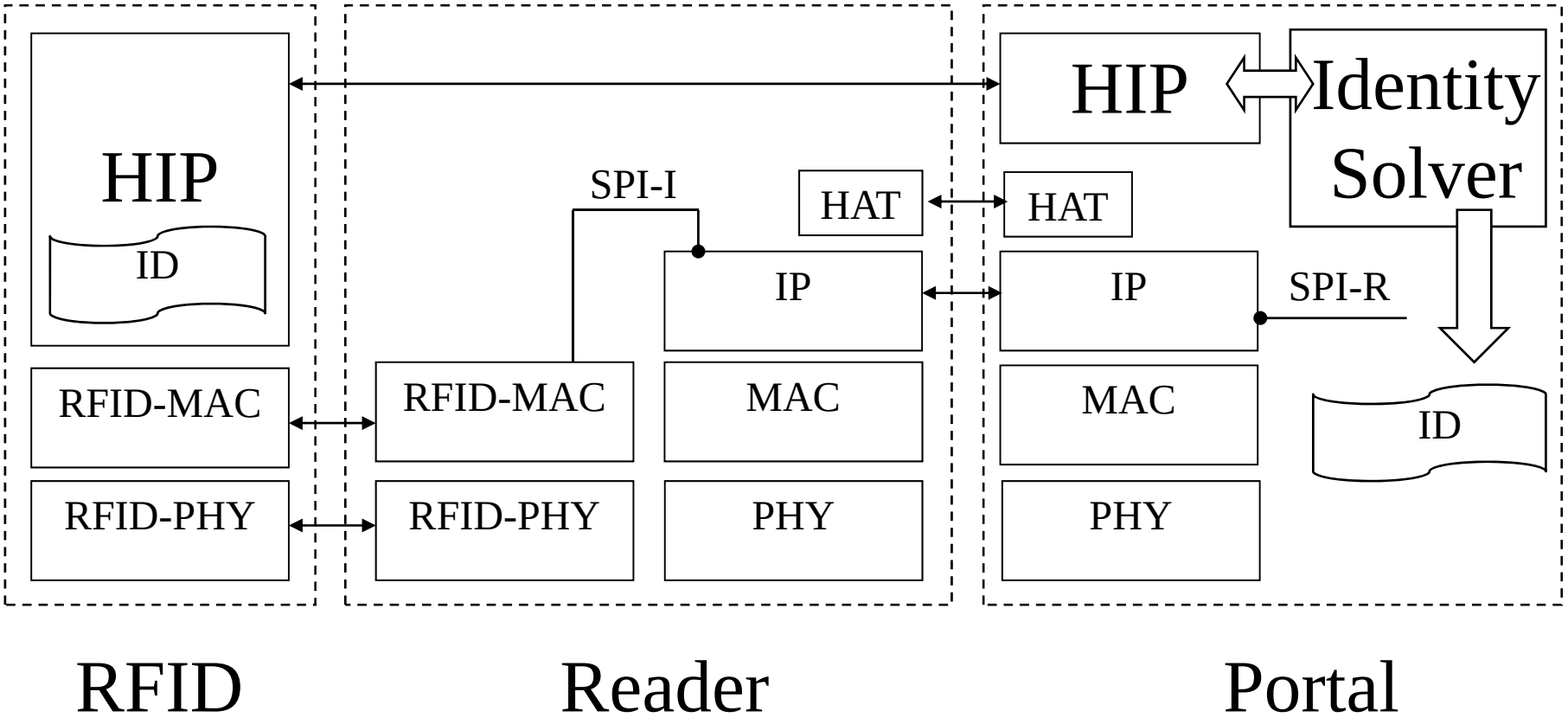
- Example
  - Many proposal in the scientific literature
    - Example: f(r1,r2, ID) = hash (r1 | r2 | ID)

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 Main Ideas

- **The RFID runs a modified version of HIP**
  - IN HIP, HIT is a fix value
    - HIT = hash(Public-Key)
    - **For RFID this *fix identifier* is a privacy issue**
  - In HIP-RFID
    - HIT-RFID is a random value
    - On the mailing list it has been suggested that only part of the HIT could be a random value, for example 96 bits for IPV6 addressing scheme compatibility.
- **The RFID Reader is an IP node**
  - It acts as a docking host for HIP RFIDs
  - The Reader is not able to solve the **f** equation
  - The *identity solver* entity is located in a node called the PORTAL
- **HIP dialog between the RFID and the Portal**
  - HIP packets **MAY** be encapsulated by a HAT (*HIP Address Translation*) layer.
    - HAT could be an UDP transport of HIP packets
    - On the mailing list it has been suggested that this name is not adequate

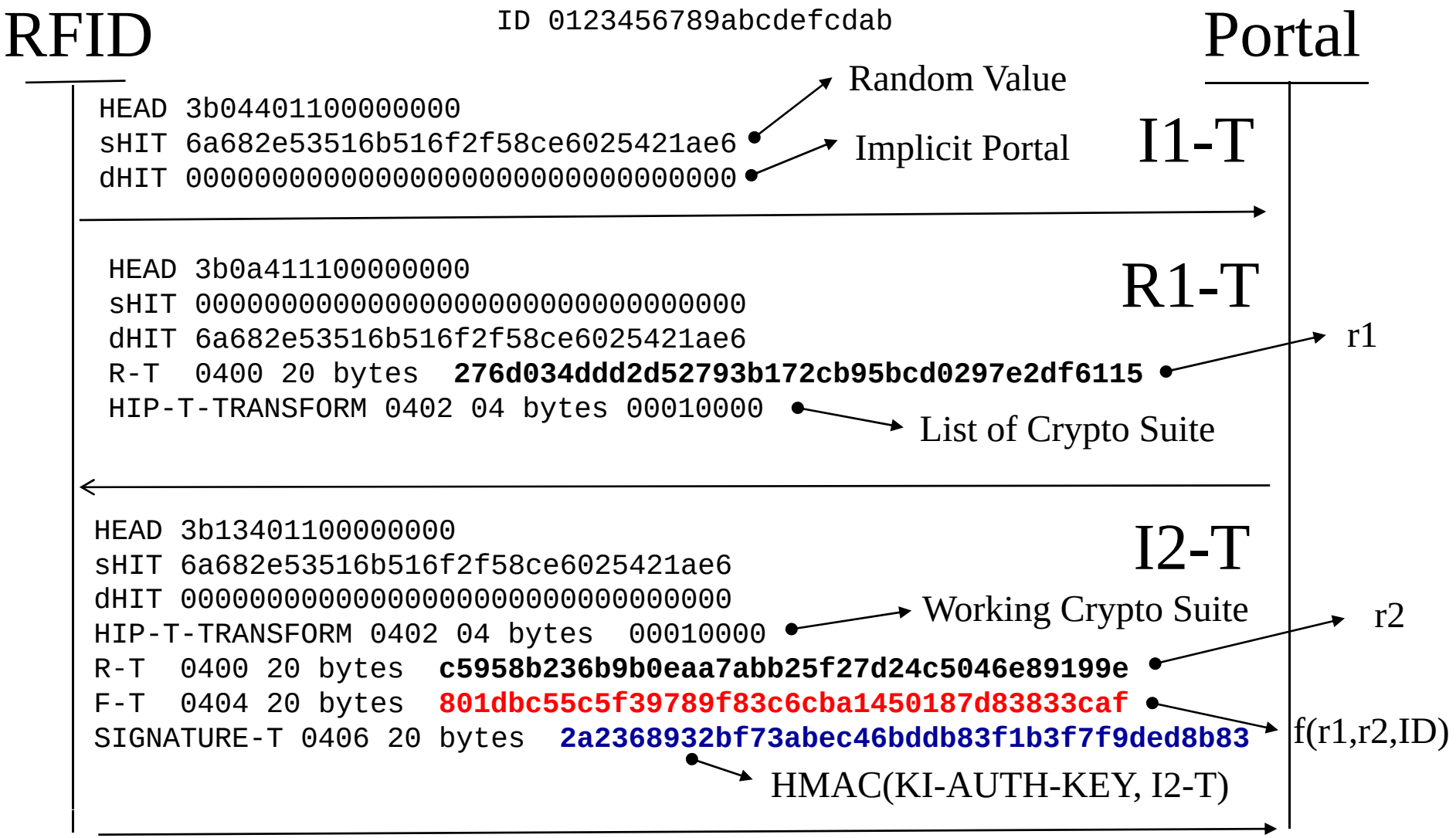
HIP-RFID Architecture



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.**

BEX Example, with T-Transform = 0001



T-Transform

- **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 = 0x00000002 (32 bits)
- **T-TRANSFORM 0002 (TREE)**
  - F-T = H1 | H2 | Hi | Hn
    - Hi = HMAC-SHA1(r1 | r2, Ki | CT1),or
    - Hi = HMAC-SHA1(r1 | r2, Ki | CT2)
      - **CT1 = 0x00000001, CT2 = 0x00000002**
    - Notation: $H_i^{CTk}{}_{Ki}$ k=1,2 i=1…n
  - KI-AUTH-KEY = HMAC-SHA1(K, CT1 | "Type 0002 key")
    - K = HMAC-SHA1(r1 | r2, EPC-Code)
      - **CT1 = 0x00000001 (32 bits)**

Questions ?

- Ideas for T-TRANSFORMs ?
- What structure for the HIT-RFID ?
- HAT name and functionality ?
- ESP Secure Channel ?