UICC – SIM-Card

Paradigm: a SIM card = a Smart Card

Tor Hjalmar

New functionality

New services and

New business opportunities

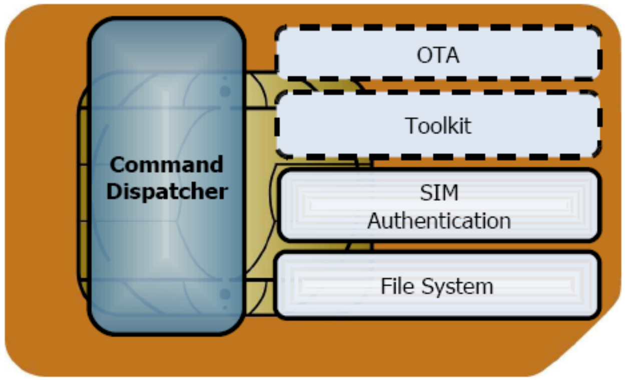
telenor

SIMcard → UICC

Basic rationale:

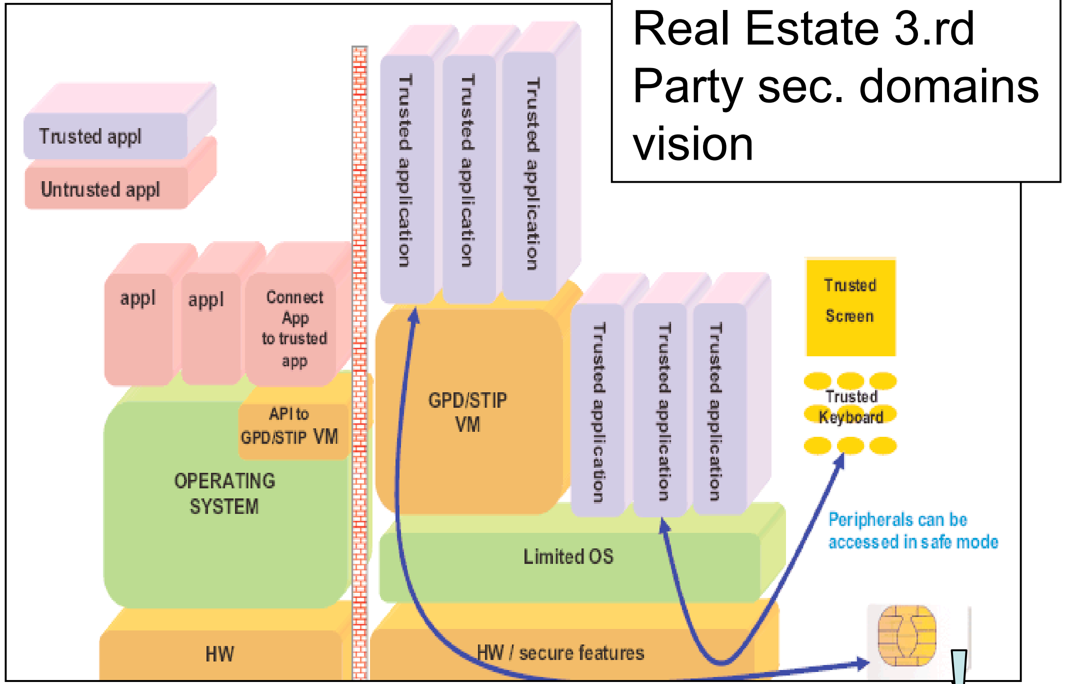
- To comply with 3G networking requirements (USIM)
  - Security features (algos and protocols)
    - singleS auth → mutual auth
    - → milenage algorithm – longer key lengths etc.
    - ISIM application (IMS)
      - private user identity
      - one or more public user identities
      - Long term secret

New visions
for mobile / UICC



Current Telenor SIM (UICC) card (from 2001)

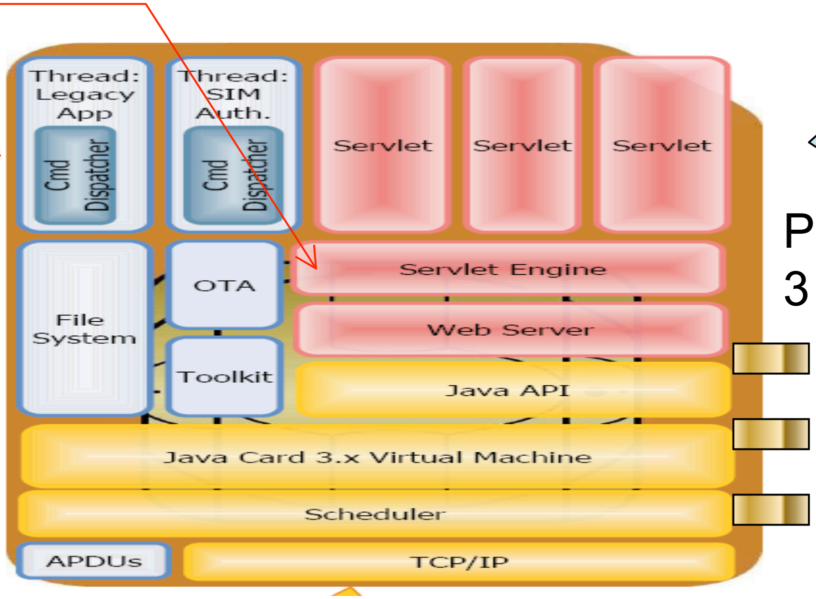
GlobalPlatform's Real Estate 3.rd Party sec. domains vision



On-board WEB server !

Multi-Thread

SUN 2009? (Java)



Plus ETSI SCP 3 new phys IFs:

12 Mb/s USB

NFC (SWP)

telenor

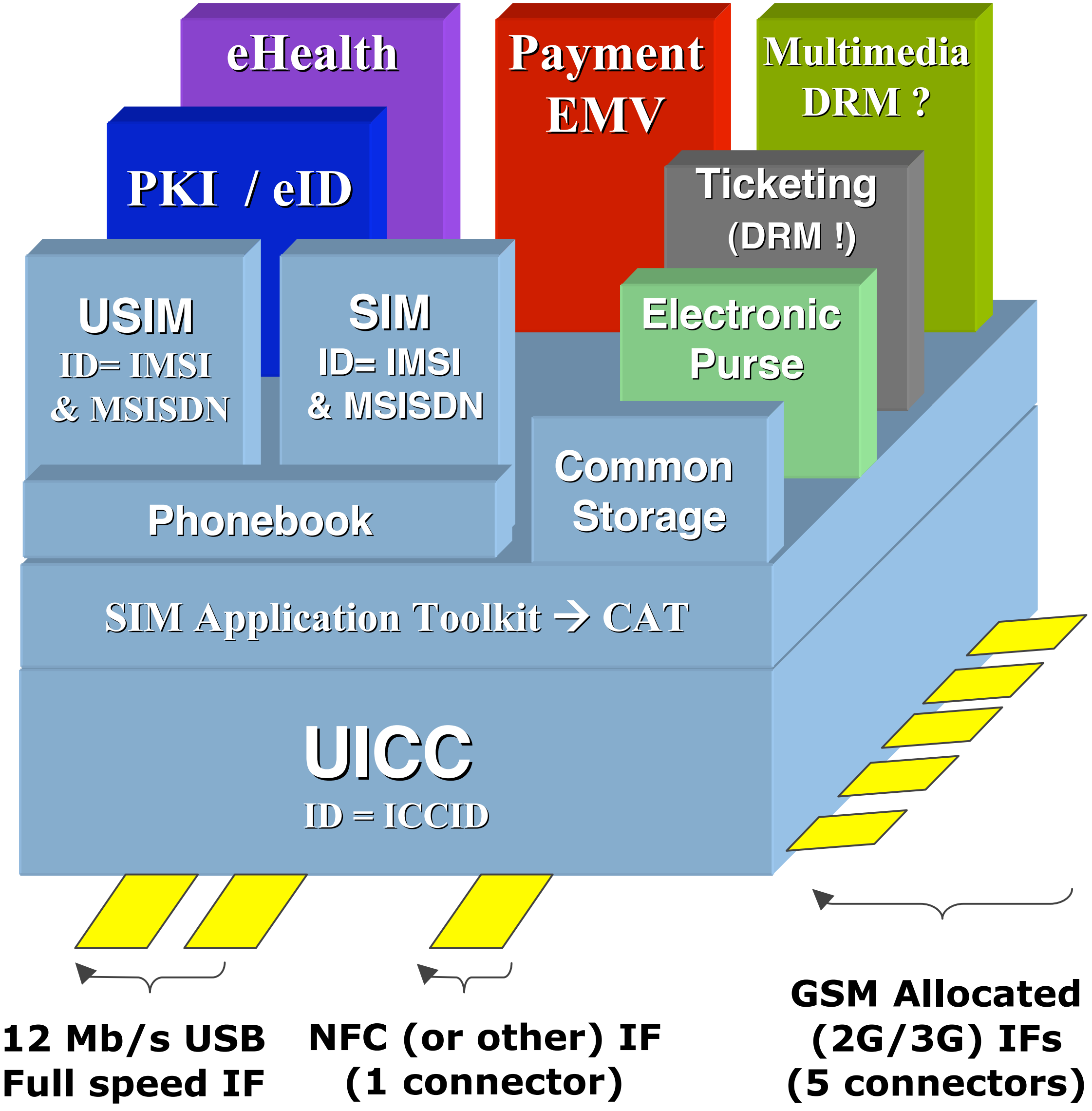
New SIM/UICC features 1

- **ETSI SCP**
  - New: USB 12 MB/s interface (for multimedia)
    - 2 dedicated physical pins on the chip = full duplex
  - New: NFC/SWP (Near Field Comm / Single wire Protocol)
    - 1 dedicated physical pin on the chip = half duplex
  - Improved OTA and Sim Applic. Toolkit (SAT)
    - BIP protocol and CAT
    - For remote download and management of new applications, including 3.rd party
      - EMV (ePayment), eID, eBanking etc)

Challenge: onboard verification of downloaded applications

UICC = hw platform for the SIM, USIM, ISIM applications + more (3.rd party)

New UICC Architecture / SIM advances



New SIM/UICC features 2

- **NFC Forum / GlobalPlatform:**
  - Dedicated OTA channels for 3.rd parties remote control of own onboard applications
  - Especially NFC-oriented ones

New SIM/UICC features 3

- **Java cards**
  - Java Virtual Machine (JVM)
    - Scheduler to provide concurrency among multiple applications
    - Operating on top of UICC own OS
    - Big question: memory management & firewalling to protect applications from each other

Obvious tasks: Protection profiling of platforms and OS to comply with 3.rd party operators with high requirements.

New SIM/UICC features 4

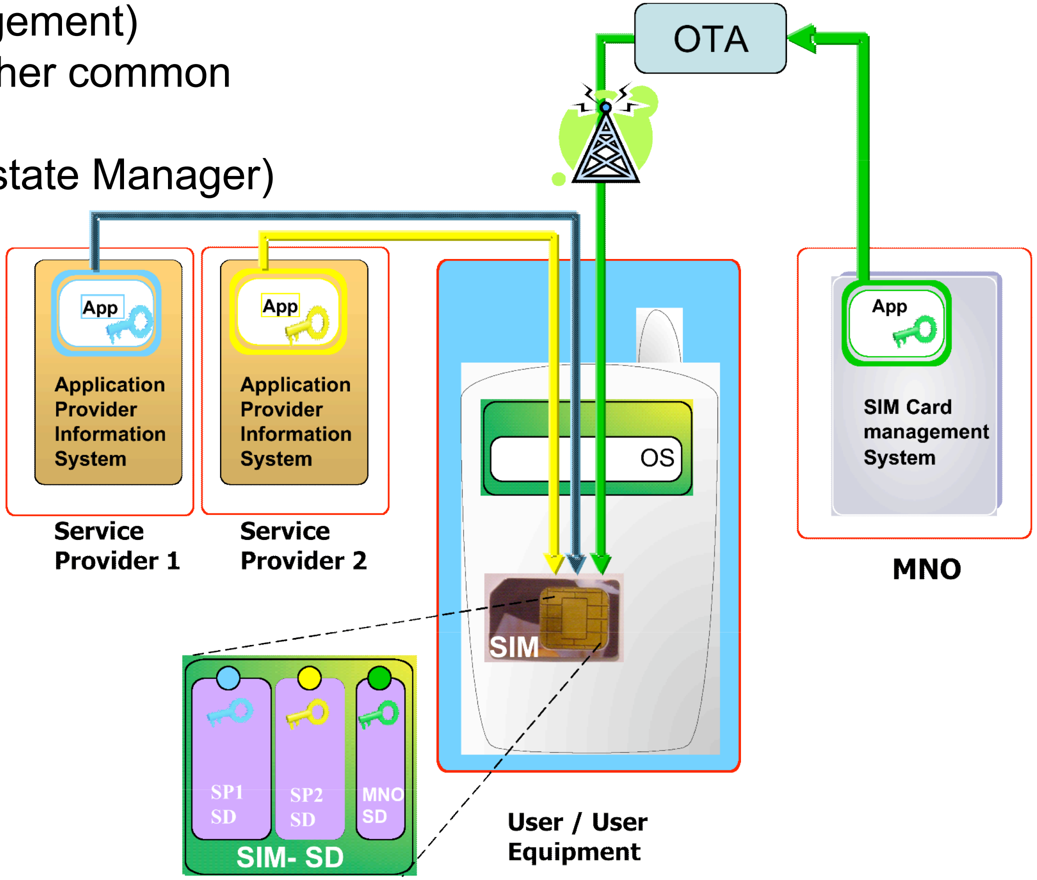
- General technological evolution
  - EEPROM (Byte R/W) → FlashEEPROM (Block R/W)
  - Larger capasity: 8-32 Kbyte → 128 Kbyte
    - and also to the multi MByte RAM capasity (1Gbyte?) when commercially acceptable pricing. (available today!)
  - One low speed half duplex 9600b/s I/O
    → three I/O including full duplex highspeed
  - Increased processor clock
  - Batteries may be a problem, but interesting reports from Stanford Univ. 10x capasity nanotech inventions.

Compartmentalisation of the UICC

3.rd party on-board applications featuring

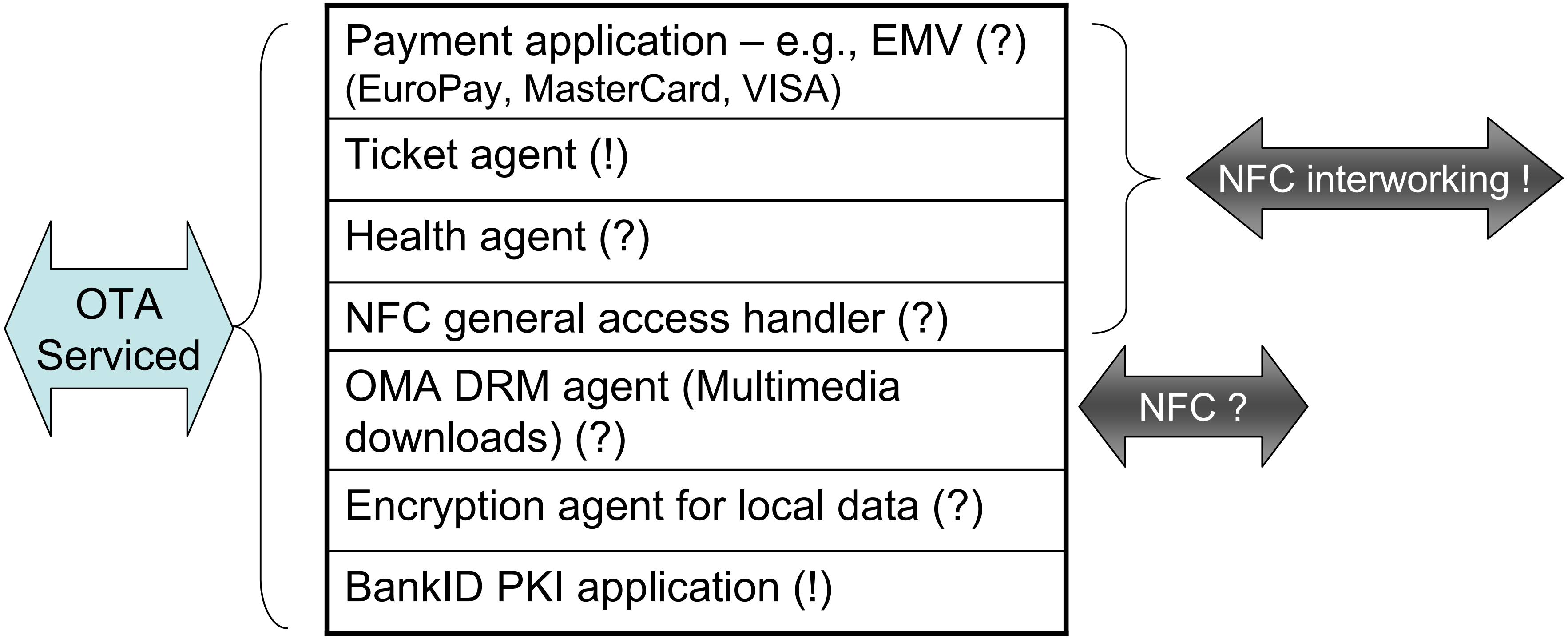
- Internal and segregated Security domains
- Private entrances for SP to applications (own keys and key management)
- Use of NFC, USB IF or other common resources

-MNO as house-keeper (Real Estate Manager)


OTA
App
Application Provider Information System
Service Provider 1
App
Application Provider Information System
Service Provider 2
OS
SIM
User / User Equipment
App
SIM Card management System
MNO
SP1 SD
SP2 SD
MNO SD
SIM- SD

Potential Real Estate Residents

& new services including 3.rd party



Payment application – e.g., EMV (?) (EuroPay, MasterCard, VISA)

Ticket agent (!)

Health agent (?)

NFC general access handler (?)

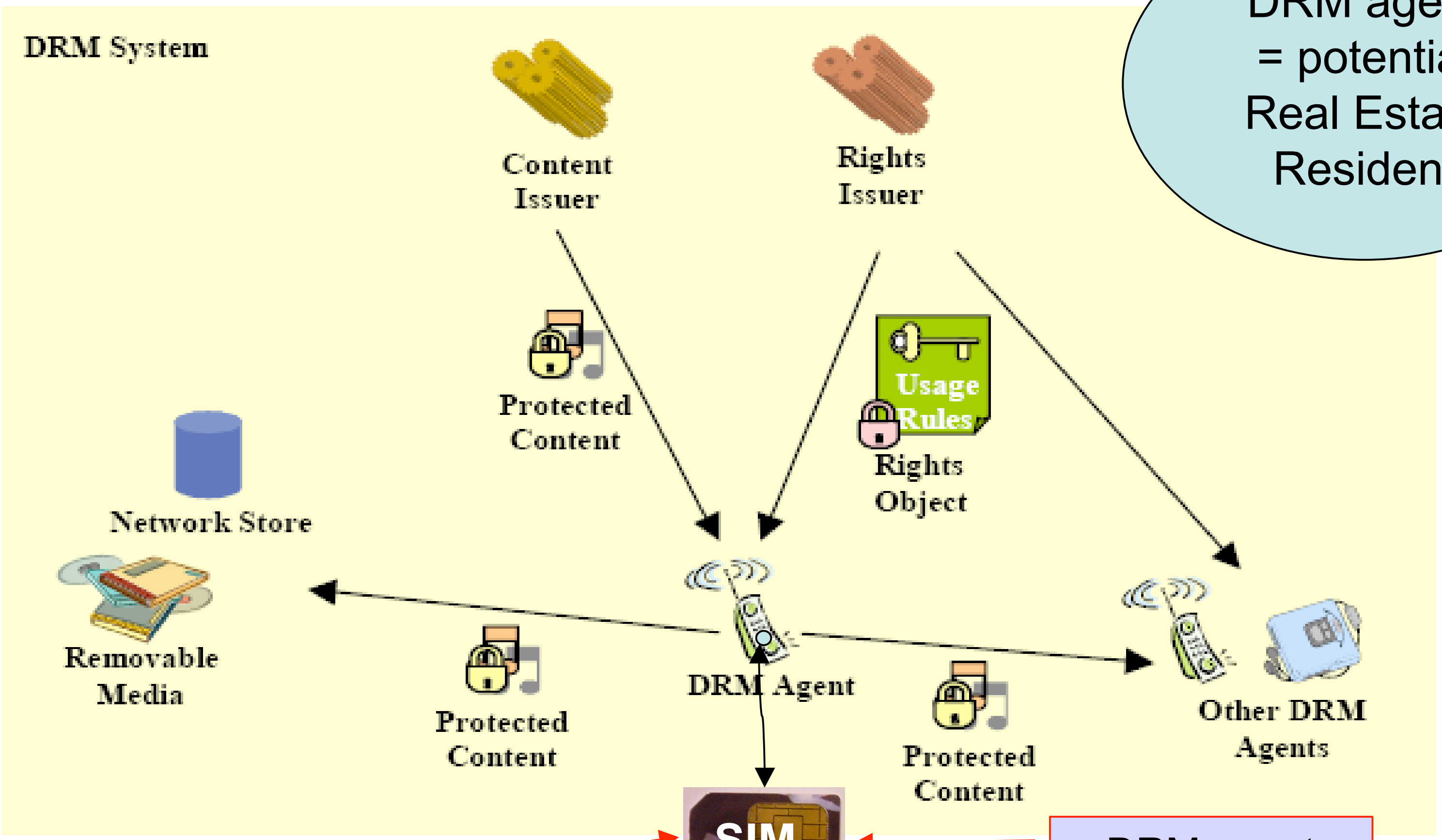
OMA DRM agent (Multimedia downloads) (?)

Encryption agent for local data (?)

BankID PKI application (!)

The OMA DRM v2.0

functional architecture



DRM agent = potential Real Estate Resident

Content
via 12Mb USB

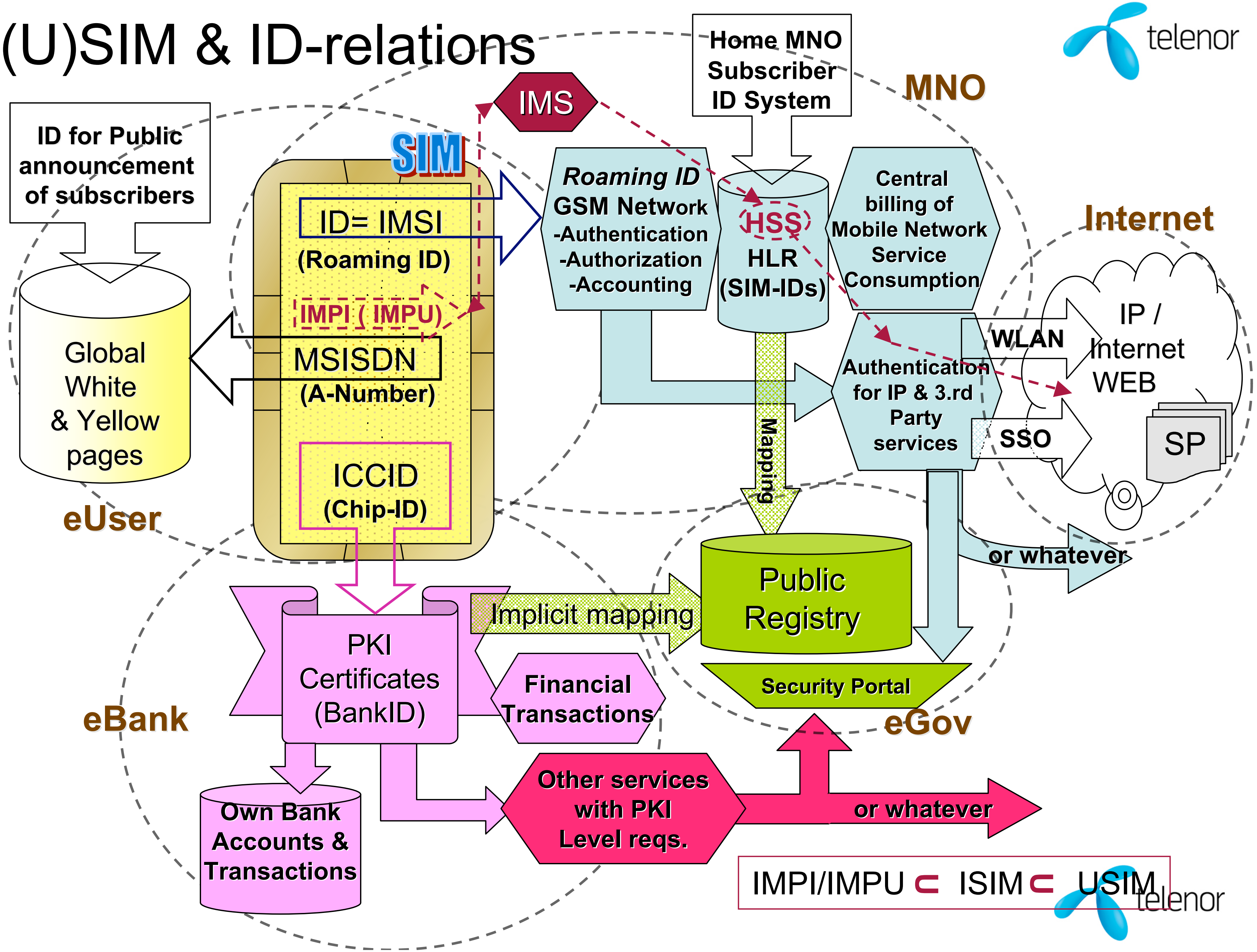
”Set-top box” ?

DRM agent
Access Controls:
- **Display**
- **Play**
- **Print**
- **Execute**

Ongoing tasks

- Extension of the usage of existing IdM system of mobile operations interworking

(U)SIM & ID-relations



IMPI/IMPU ⊂ ISIM ⊂ USIM