From RFID to the Internet of Things
6-7 March, Brussels

How to secure visible, physical, (of only one holding) objects through a digital trustworthy infrastructure ? :

privacy issues for citizens, enterprises, states

Michel Riguidel
riguidel@enst.fr

TELECOM PARIS
école nationale supérieure des télécommunications

Increased sovereignty & dignity for better digital living

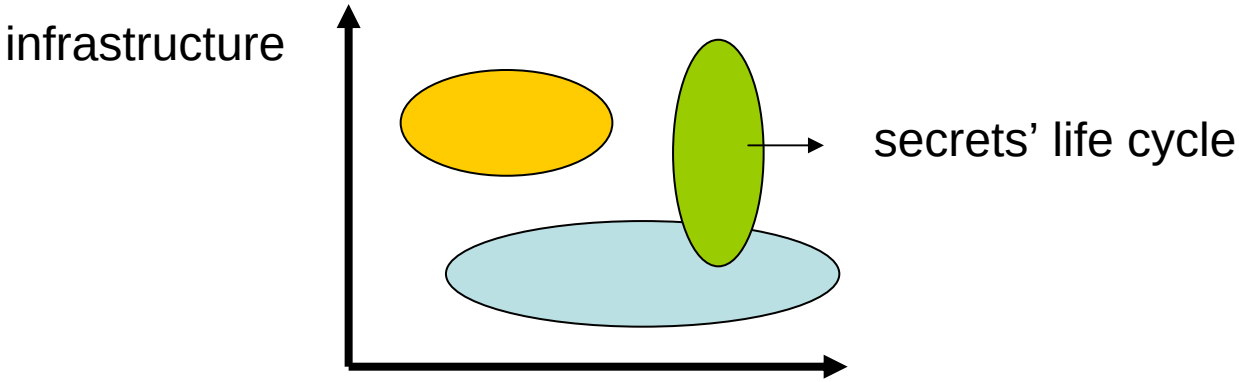
- Digital Sovereignty : Security versus Privacy Dialectic
  - Digital Marks & Traces everywhere : dirty digital world used as alibis
  - Privacy of Astrid versus the organization
    - I want my intimacy protected & I accept to be observed up to this limit
    - georeferenced data attached to subjects & objects
  - Security of the organization versus Astrid
    - I want guaranty your safety, security…against enemies, errors & I protect infrastructures, services, data … & I do some surveillance to observe Astrid
    - network of surveillance with cameras and sensors in cities
- Digital Dignity : "behind the scenes" versus "out in the open" security
  - Security in obscurity (software editors)
    - how to trust security mechanisms ? (TPM, TCG, RFIds "standards"…)
  - New infrastructures
    - RFIDs & Tags : physical objects
    - Galileo : trustworthy clock and positioning system in Europe
    - Opportunity
      - new security mechanisms (small scale security)
      - new cryptographic protocols taking into account time, space, objects
    - Threats (traceability)

ICT Morphology evolution & Security

- Before 1995 : Systems have convex architectures, **salient** morphology
  - **Salient** into the environment : plants, campus
  - Convex, ICT islands
    - Private part important, public part minimum
  - Security function at the boundaries (“walls”) : access control
    - Firewall, conditional access
- 1995 - 2005 : Infrastructures occupy a field
  - **Pregnant (Pervasive)** into an environment : nets, branches
    - Telecom, Electricity : flows, Distribution : just in time
- 2005 – 2010 : Ambient Intelligences & autonomous objects
  - **Pregnant** morphology : pervasive & intelligent ambiance
    - Graphs, capillarity, communication infrastructures
  - Security functions: intrusion detection, flow sensors
    - What are the rules for the ambient intelligence?
  - **Physical objects attached** and connected to networks : massive population with scarce resources
  - Security functions : identification, traceability, …
    - an Identifier, a message or a program
- After 2010 : "**Smart dust**" (nanotechnologies)
  - Invisible autonomous grains (nanotechnology, cells)
  - Security functions: traceability (tags, …), audit

Morphology : Geography, Organization, Operations

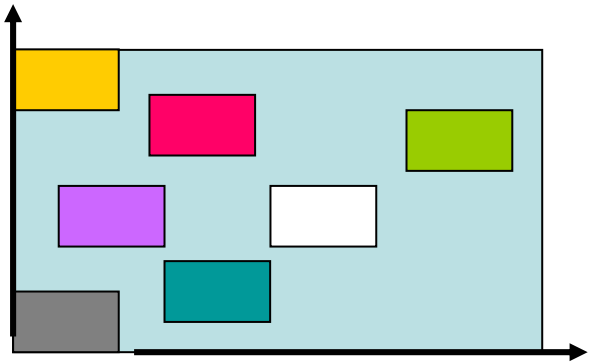
Security : the art of sharing secrets (along 2D)



interoperability does not mean unique

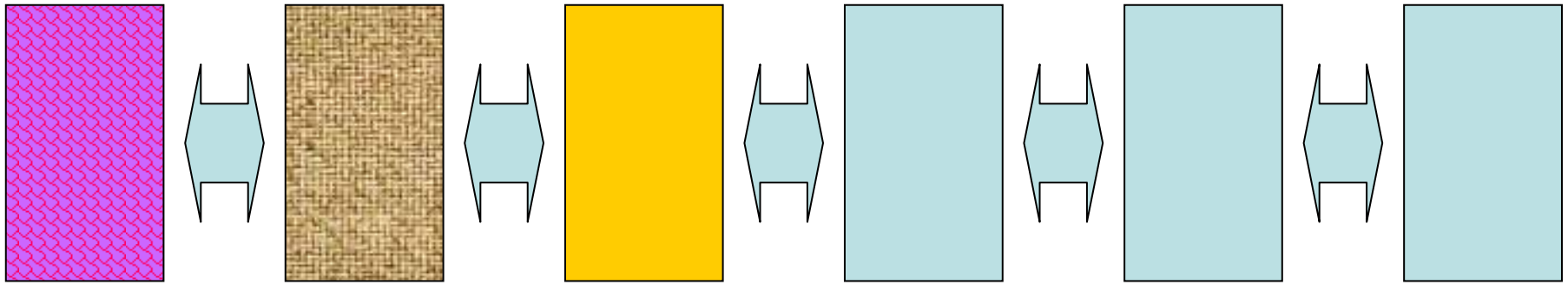
a unique constant identifier

not an identifier : a volatile program



"any reader can read all the rfids" is not the requirement
"only the authorized readers can read the relevant labels" is the need

RFIDs infrastructure : how to protect the interfaces and to attain a security continuum



physical
item
thing

physical
person
/animal

packaging
envelope
packing case
container
pallet

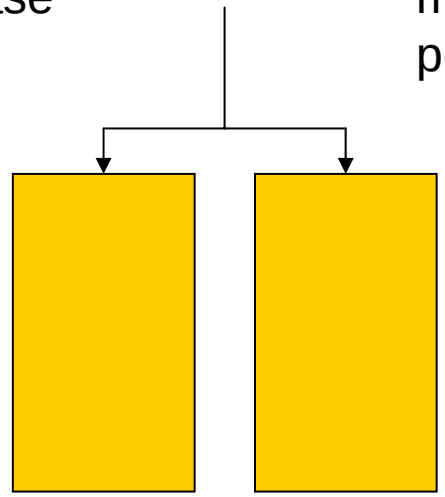
RFID
smart label

RFID reader

mobile phone
pda

Private
Information
system
middleware

Public
Internet
3G telecom



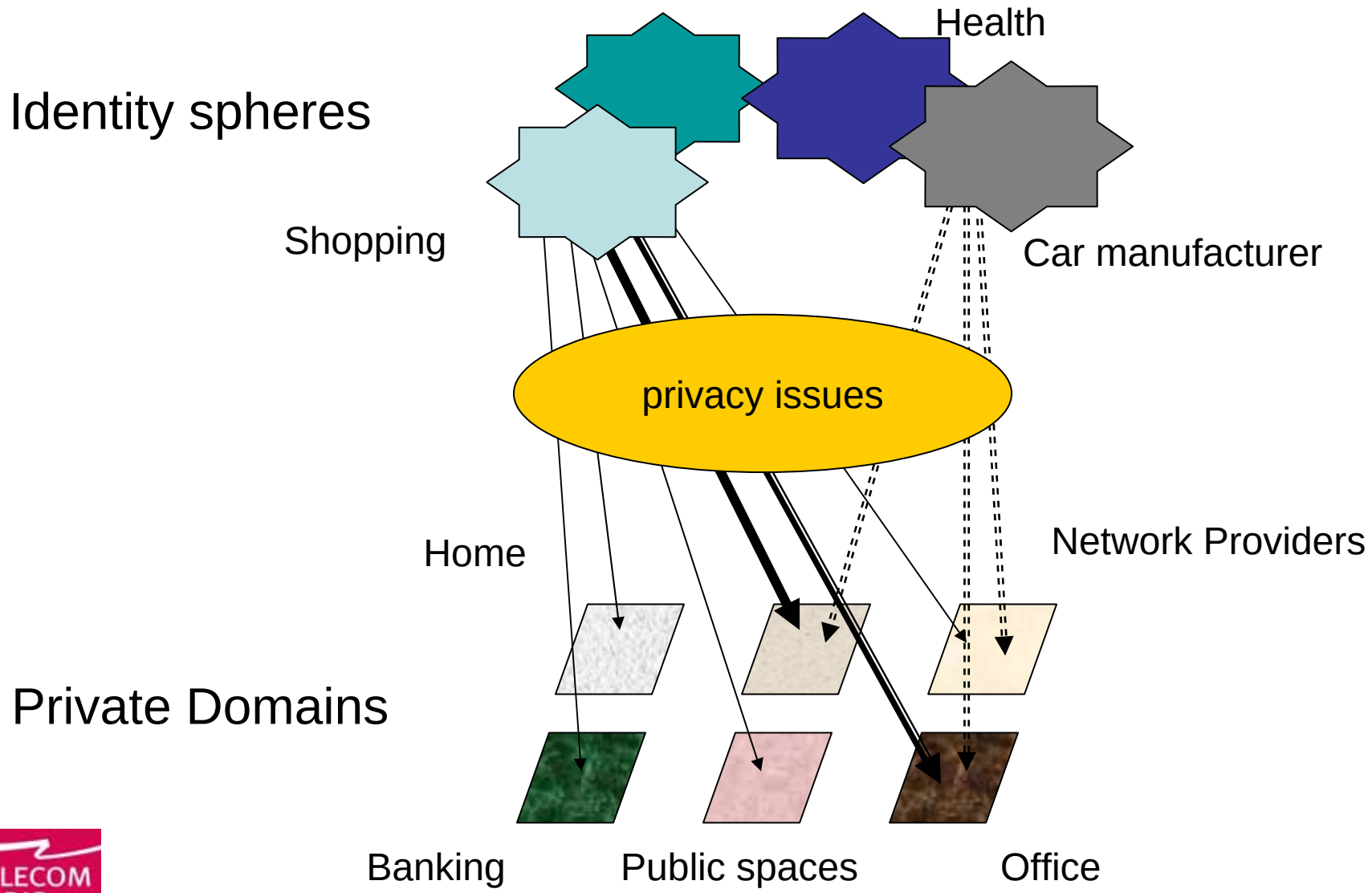
smart sensor

GPS/Galileo/Zigbee
positioning systems

Life cycle of Objects with smart Labels

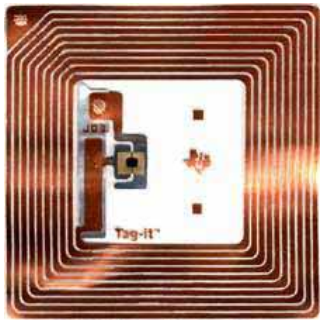
- Creation
  - factory
  - trusted infrastructure to avoid clones, corruption of smart labels
- Distribution
  - tracability, inventory, storage, billing, etc
  - usurpation, falsification, lost of smart labels
  - espionage, surveillance, economic intelligence
- Exploitation
  - End-user, consumers, citizen utilization
  - penetration in the private sphere, privacy invasion
    - private objects can be seen during transportation (nomadic people)
    - private objects can be seen indoor by a visitor or a passer by
    - profiling
- Maintenance, storage
  - direct link with vendors (cars, etc)
- Destruction
  - recycling, obsolescence

Identity spheres & ownership domains



Threats (not exhaustive)

- On physical Labels (RFIDs)
  - Counterfeiting, Forgery
    - wrong item with its “true” label
  - Usurpation, Spoofing
    - right item with its wrong label (or with no label)
  - Decoy, lure, deception
    - false object with its “right” label
  - Disruption, vandalism
    - right object with its right label
    - and jamming item or several false labels attached to one item

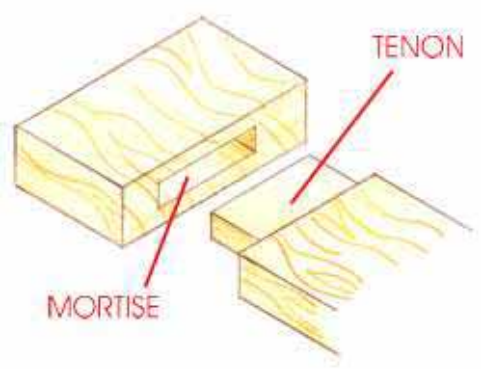


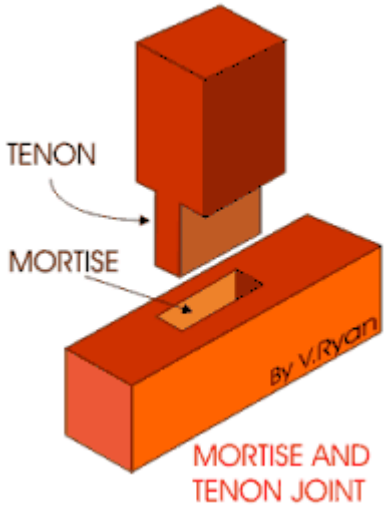
- On Readers & protocols
  - unauthorized readers
  - covert channels, replay, man-in-the middle, …
- On the infrastructure
  - Middleware
    - => same as Grids in a public environment
    - => same as digital link
  - Universal, Unique Identifier : Major vulnerability
    - the identification is unique, public, universal
    - similar to a permanent static unique IPv6 address

A security solution with scarce resources

- Ambient security : peer to peer approach
  - it works if there is enough resources (for cryptography)
- Small scale security : the mortice and tenon joint security
  - the whole security of an RFID must not only embedded on this device

security created by **solidarity** and assembly of several elements

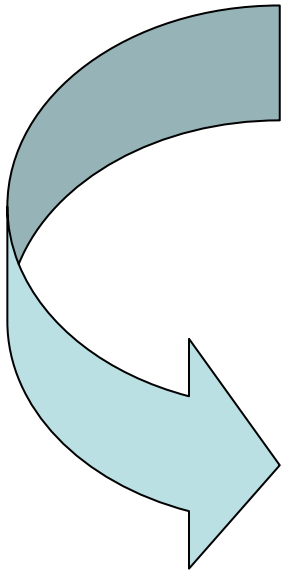




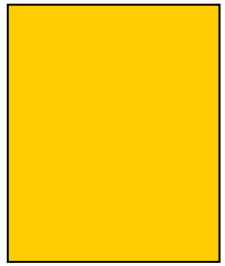
- RFID stands for identification
  - identification is not necessarily a **name**
  - it could be a **program** (nano-applet) – cf. intentional architecture

Scalable Security with scarce resources

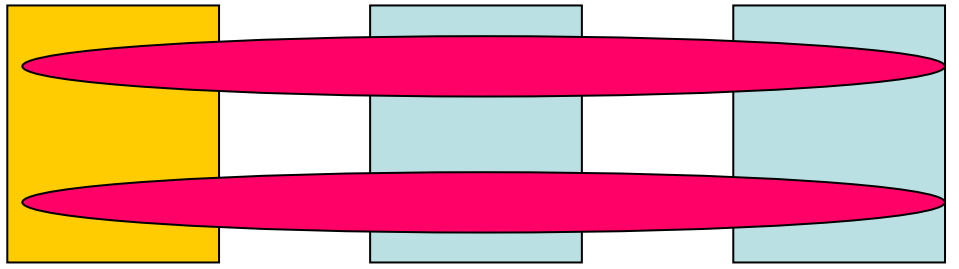
- Piecewise & transitive security is impossible
- Security models must works at a higher level than autonomous objects
- Security must be orthogonal to the physical objects



open security of a standalone rfid : impossible



secrets are shared by the various elements of the infrastructure



The boundary between physical space & cyberspace will fade away (~2010)

- Geostrategic threats
  - Digital urbanization goes on up to capillary irrigation of visible things (except very short life duration items and very cheap goods)
  - Economical : Standard, Normalization dependency
    - prevent technological (& political) putsch of providential solutions
  - Social :Transparency & visibility of the private sphere
    - personal, enterprise, state, government
  - Cyberterrorism related with Internet of Things will appear by 2008 (~)
    - connection of daily things with computing world & networks
    - new attacks to kill remotely in a distributed manner with networks
- Technological Challenges for the Internet security of Things
  - we do not have yet neither the models nor the tools
- Heightened confidence & security in the ambient Intelligence
    - Security on a large scale
      - Resilience of critical infrastructures, services, information
      - Securing & making reliable the complex digital landscape
    - Security on a small scale
      - Security with scarce resources
      - Protecting the end-user's digital realm & infrastructure extremities