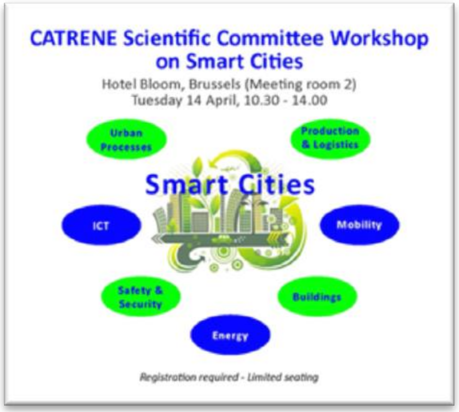
CATRENE workshop on SmartCities

Security chapter



CATRENE Scientific Committee Workshop on Smart Cities

Hotel Bloom, Brussels (Meeting room 2)
Tuesday 14 April, 10.30 - 14.00

Smart Cities

Urban Processes

Production & Logistics

ICT

Mobility

Safety & Security

Buildings

Energy

Registration required - Limited seating

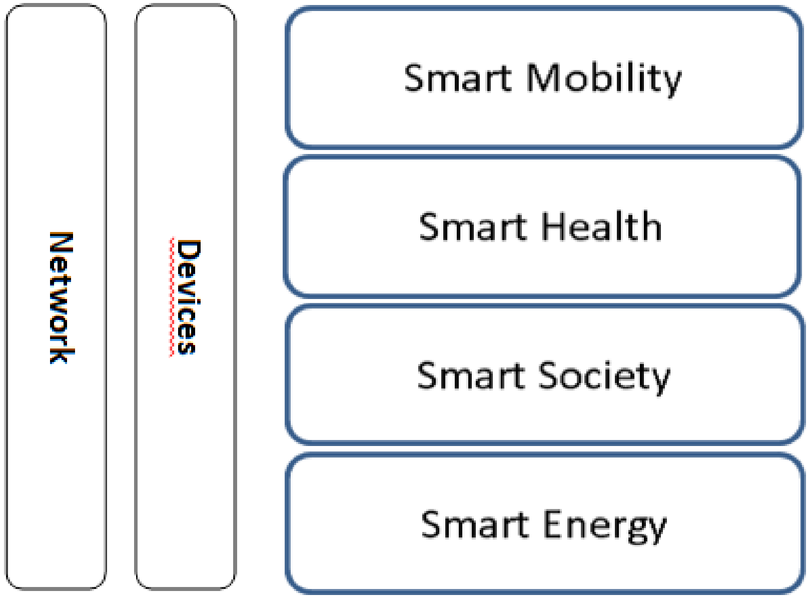
PEBAY-PEYROULA Florian (CEA-Leti)
AMBACHER Oliver (Fraunhofer IAF)
HENNEBERT Christine (CEA-Leti)
MAURER Anne-Julie (Fraunhofer IAF)
TUOT François (Gemalto)
VUICINIC Malisa (ST)

CATRENE workshop on SmartCities – Security

FUTURE KEY PRODUCTS

Smart domains and security requirements

- Smart domains
- Security requirements
  - – Secure identification
  - – Secure firmware
  - – Secure communication
  - – Component integrity
  - – Quality of service, availability
  - – Resilience (in case of a major event)
  - – Secure deployability



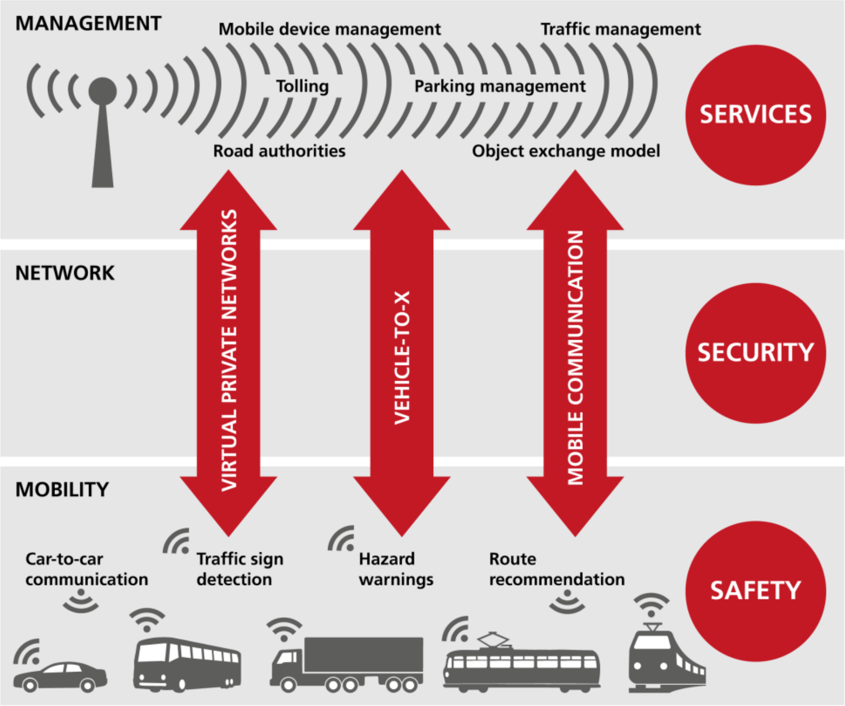
Domain / security matrix

Domain	Item	Threats	Risks	Main security requirements
		Tamper of meter (modify consumption, recover keys...)	Fraud with economic loss Power loss	Hardware electronic integrity Secure identification
		Eavesdropping of consumption and billing data	User privacy violation User Behavior recording	Secure communication
	Heating sensor at home	Tamper of sensor (modify consumption)	Fraud with economic loss	Hardware sensor integrity
Smart Health	Air pollution sensor	Eavesdropping of communication	Extraction of information for other purposes	No security requirements
		Tamper device configuration Non trusted firmware	False information reported Inappropriate decision taken	Secure firmware Secure identification
	Medical file privacy	Cyber-attacks on servers	Access to sensitive personal data User privacy	Secure identification Linkability to a person
		Eavesdropping during connections	Identity usurpation	Secure communication
Smart Energy	Heating sensor at home	Tamper of sensor (modify consumption)	Fraud with economic loss	Hardware sensor integrity
	individuals		User privacy	Hardware electronic integrity
		Modification of various sensors	Wrong information reported to system	Hardware sensor integrity
Smart Society	e-Administration	Network attacks	Untrusted websites collecting user credentials for fraud	Secure communication
		Phishing	Identity usurpation User privacy	Secure identification
	Safe city	Denial of service of a security device	Public security attempt Economic loss	Quality of service, availability Resilience
		Tamper device configuration Non trusted firmware Sensor cloning	False information reported Inappropriate decision taken	Secure deployability Secure firmware Hardware electronic integrity

CATRENE workshop on SmartCities – Security

TECHNOLOGICAL REQUIREMENTS

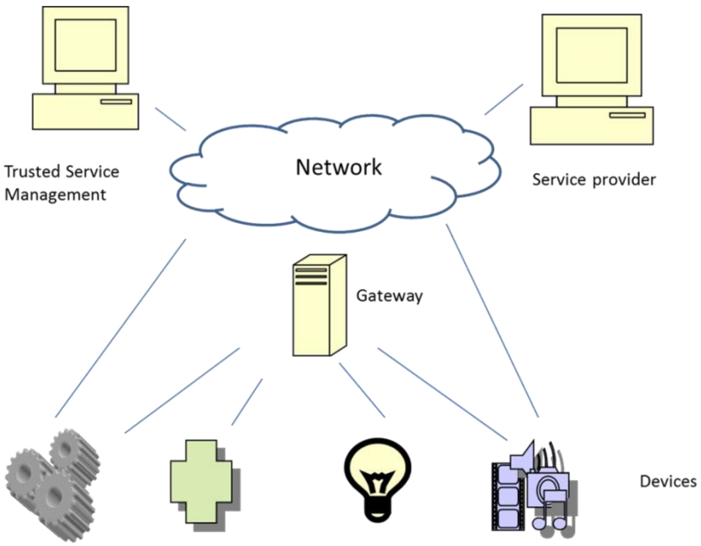
Secure generation of information



- Sensor needs
  - high data rates
  - secure measurement
  - secure transmission
  - high reliability & robustness
  - low acquisition and operation costs
- Safe & secure cities
  - Eg. traffic management
    - Secure vehicle navigation
    - Efficient traffic opimization
    - Vehicle automation
    - Pedestrian safety avoiding collisions

Authentication, Authorization, Access control and Privacy

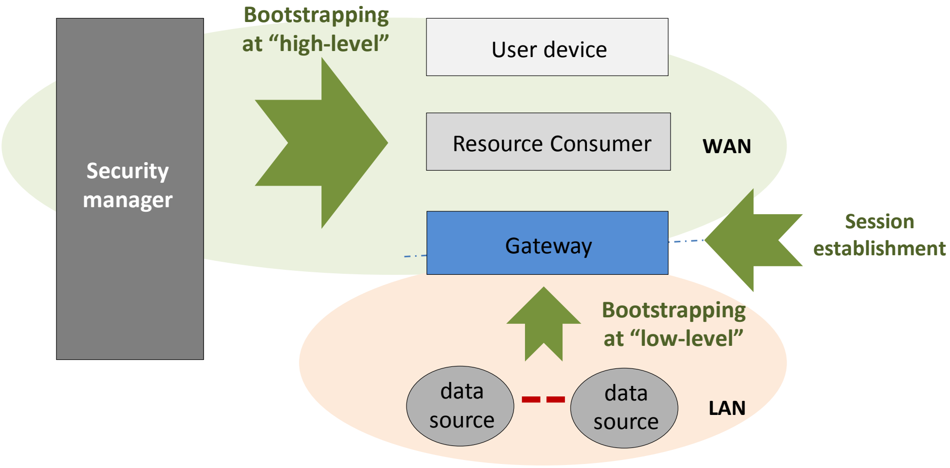
- Network topology
  - People
  - Devices
- Need strong authentication
  - Not: login/password
- Consistent access control
  - Network heterogeneity
- Privacy always a challenge
  - Business is on data also



Bootstraping and deployment

- How an user to personalize a virgin node into his network?
  - Lowlevel boostraping: local credentials (eg. network access)
  - Highlevel bootstraping: access to the resources (eg. Service)

- Directions
  - In-band pairing
  - Out-band pairing
  - Secure storage
  - Preshared certificates



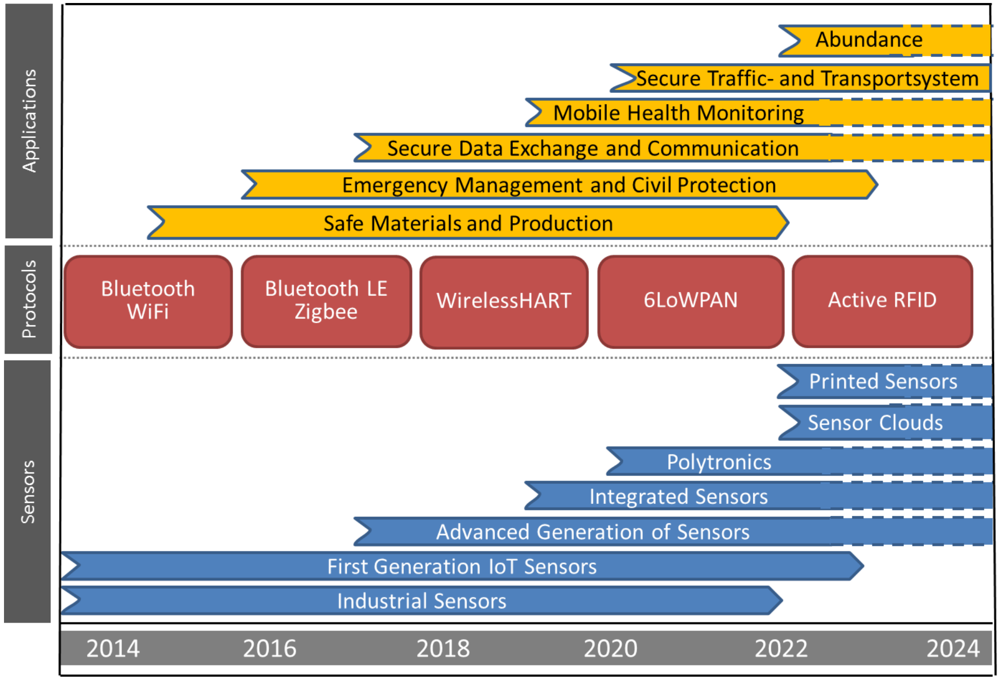
Need for secure anchors in small & cheap objects

- Peer Authentication with DTLS
  - End to end security
  - Important need of memory for each session key
  - Handshake performance in radio duty-cycled networks
- Authorization with OAuth 2.0
  - Strong link with IETF
  - Application Level Security: CoAP
- Trust Anchor Provisioning and Ownership Management
  - TPM like for constrained objects

CATRENE workshop on SmartCities – Security

ROADMAP & ECONOMIC IMPACT

Roadmap



- Microeletronic needs
  - Modern concepts
    - Algorihms
    - Filters
    - Chemistry sensors
  - Novel materials and technos
    - Printable
    - Nano-tubes/catalysts
  - New devices
    - Energy
    - datarate vs range
    - Robustness
  - Innovative systems
    - Data exchange btw infrastuctures
    - Monitoring…

Strategic Research & Economic Impact

- Research areas to be investigated in future calls
  - Bootstrapping using out-of-band channels and standard IP protocols
  - Handshake performance & memory session management improvements
- Economic impact for component manufacturer
  - Market SmartCities: 8.1B in 2010 -> 39.5B in 2016
  - Security market: 60M in 2018 -> 1.8B in 2024
- Perceived insecurity of wireless sensors networks is a major inhibitor to further market growth