LAUREA
UNIVERSITY OF APPLIED SCIENCES
Prime Mover

Tracking cross-border criminals with satellites

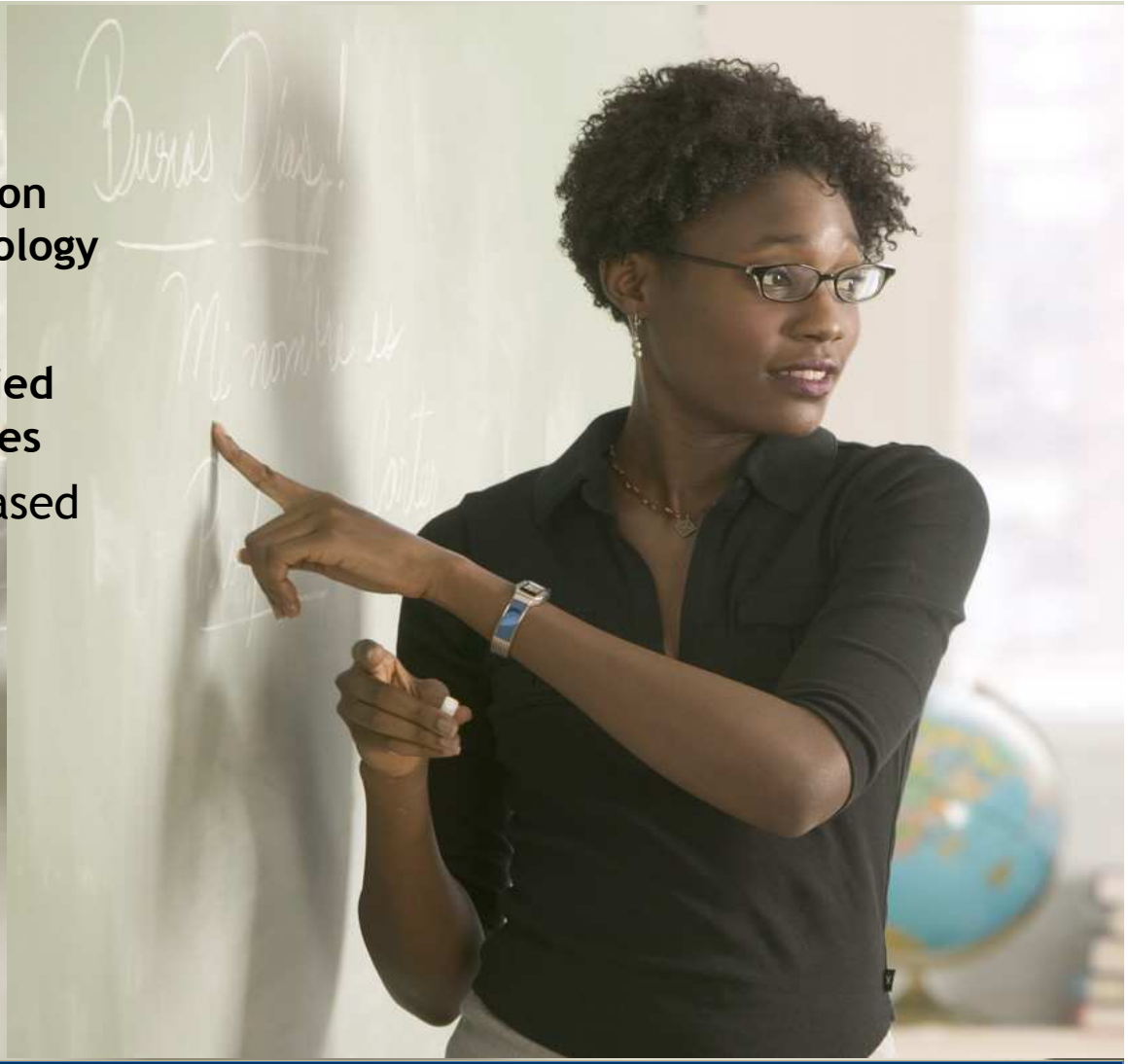
SATERISK project - *Jyri Rajamäki*
MACICO project – *John Holmström*

PSC Europe
Public Safety Communication Europe

PSC Europe Forum Conference, 30 & 31 May 2012, Helsinki, Finland

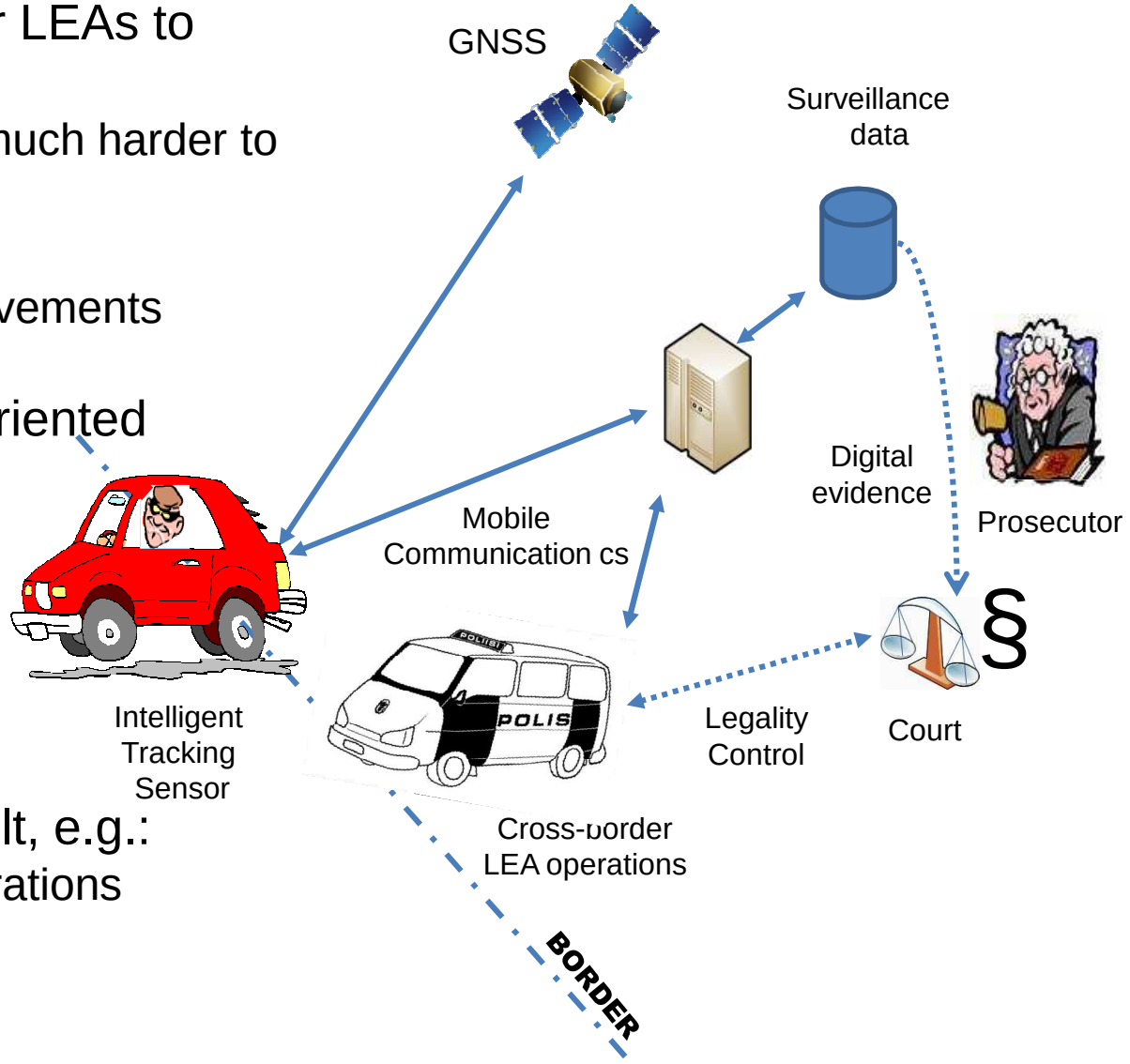
Contents

1. Introduction
   - Operational environment
   - Why LEAs need Global Navigation Satellite Systems (GNSS) technology
2. Empirical case
   - Why Laurea University of Applied Sciences researches these issues
   - SATERISK project - SATEllite-based tracking RISKs
3. Tracking challenges for LEAs
   - GNSS sensors
   - Cross-border operations
   - Mobile communications
   - Digital evidence
   - Legality control
4. Future work



Introduction

- Tracking is an essential tool for LEAs to prevent and investigate crimes
  - A GNSS-sensor under car is much harder to find than a tailing car
- Crime has internationalized
  - European integration; free movements
  - Organized crime
- Criminals are more technical oriented
  - Jamming
  - Learn to check their vehicles
- Change has been rapid and LEAs have failed to create protocols for international tracking issues
- Cross-border operations difficult, e.g.:
  - Lack of Interoperability of operations (distrust)
  - Lack of roaming of PSC



Laurea University of Applied Sciences

- New competences in the field of service innovations
- Professionally orientated and education – 500 personnel and 8 000 students
- Development and R&D activities
- Vast contact network with actors operating in public and private safety & security, civil protection and crises management.
- MA Programme in Security Competence & BA Business Administration: focusing on Private Security, Risk Management and International Security Management

Laurea's best hidden assets are their in-house officer and top management level students with 5-15 years of working experience from police, security police, rescue service, customs, intelligence, military etc. or from private sector, who have returned for another degree in Safety and Security Management.

SATERISK – SATEllite-based tracking RISKs

Tracking is used to increase safety of logistics and optimize work flow, but does it always work that way? Do we know the risks? – ***Are we creating new risks?***

- Joint project with Laurea, University of Lapland, international universities, industrial partners and end-users
- 563.000€ (Tekes 60%) / 1.9.2008 – 31.12.2011

Pasi Kämppi's Master's thesis " Grounded View to Technical Risks of Satellite Based Tracking Systems: A Multi methodology Research" won best thesis of the year 2011 award in Finland (20.000 thesis/20 awards)

Here *Tracking* means: Remotely following the target with help of *GNSS*

Who is being tracked?
- private person
- employee
- criminal
- vehicle, ship
- property

Who is tracking?
- private person himself
- service provider
- employer
- authorities (police etc.)
- owner of the target

What are supporting systems?
- applications
- communication elements
- transferring position data
- encryption
- tracking devices

How?
- GPS
- GLONASS
- Galileo
- Compass

Where?
- National region
- EU/Schengen regions
- Outside EU (eg. Russia)
- Cross border tracking
- Crossing multiple countries

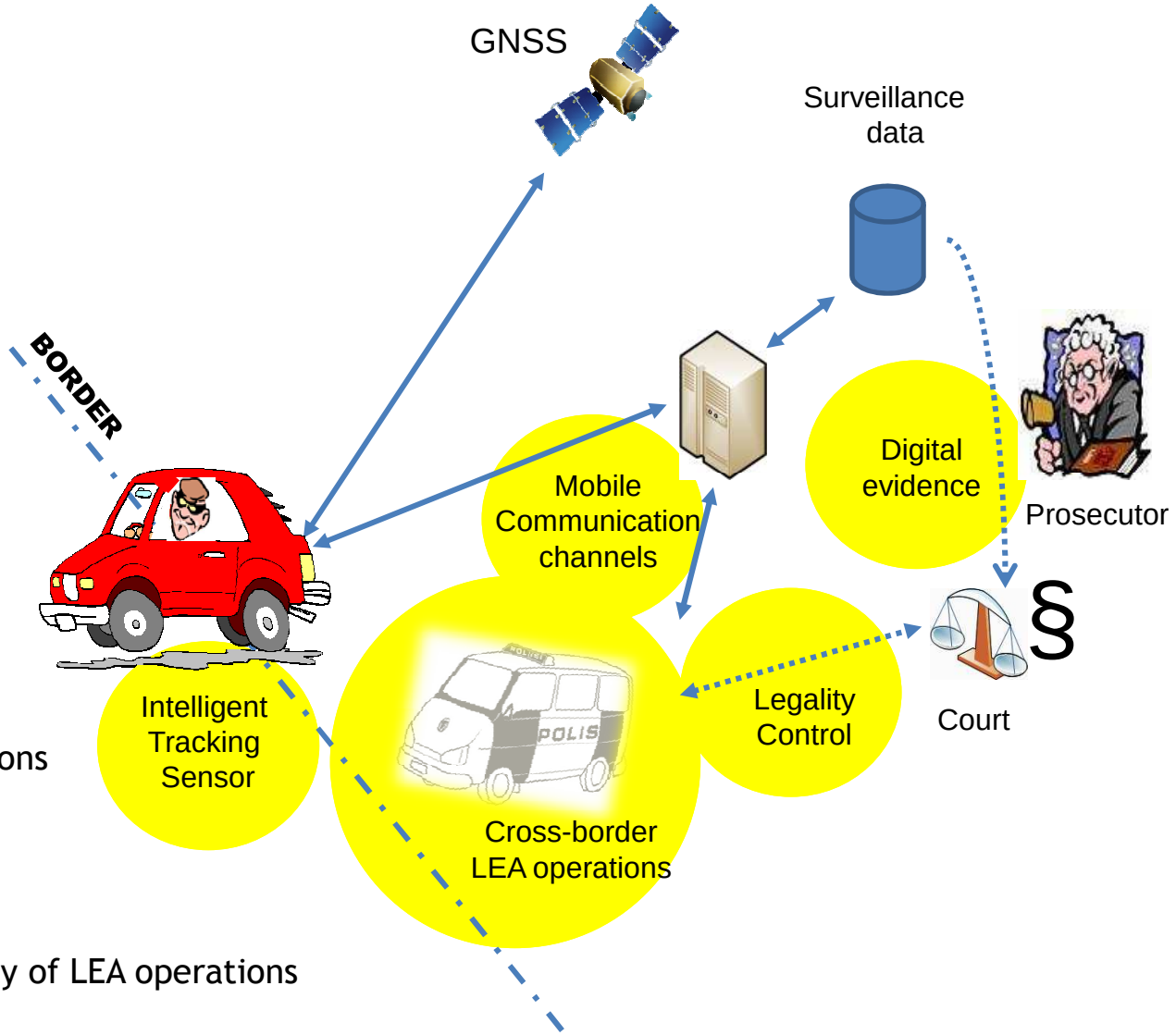
Source of risks?
- technology
- operation
- legislation

Why?
- navigation
- offering service
- commercial use
- increasing efficiency
- security
- investigation
- rescuing
- protecting property
- entertainment

Source: http://www.saterisk.fi

Tracking Challanges for LEAs

1. GNSS sensors
   - Concealing
   - Power consumption
   - Intelligence
   - Communications
2. Cross-border operations
   - Legislation
   - Co-operations
   - Technology
3. Mobile communications
   - Tracking sensor
   - LEAs on the field
   - Especially in cross-border operations
4. Digital evidence
   - Chain of evidency
5. Legality control
   - New technologies vs. Transparency of LEA operations



Tracking Sensors

CURRENT

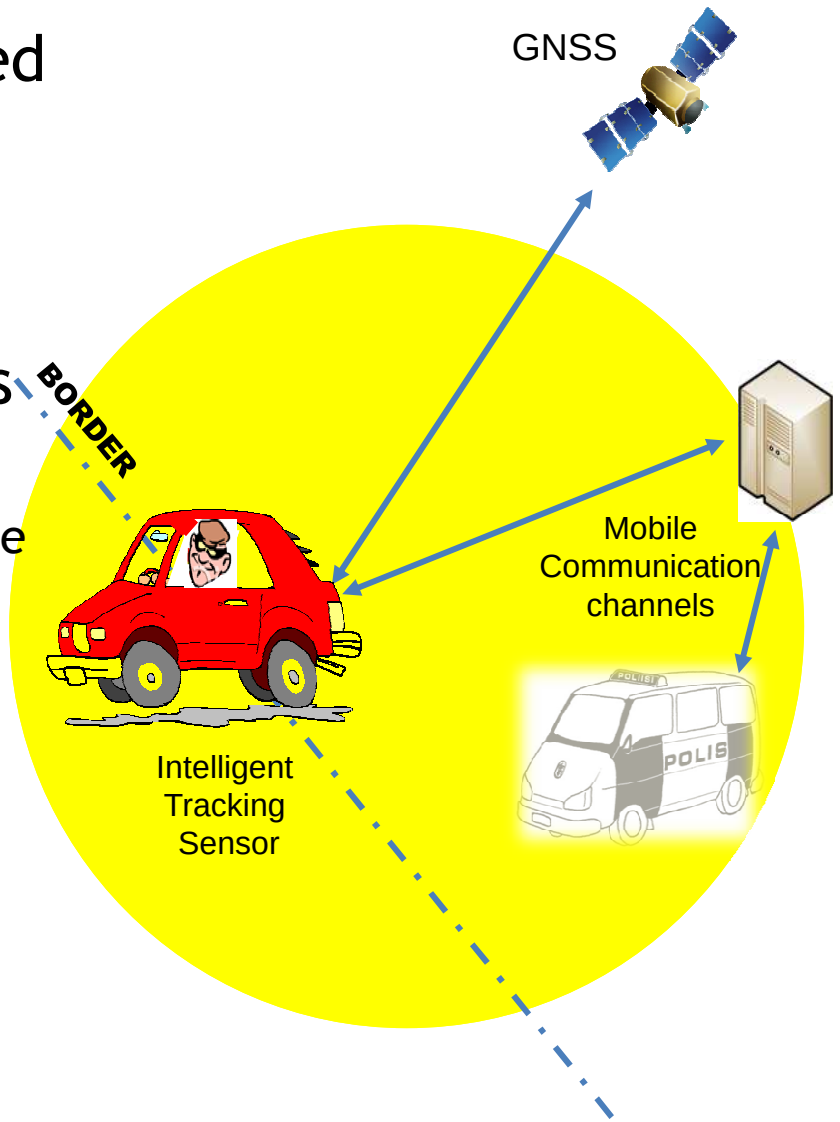
- Too big
- Hard to disguise
- Energy consuming
- GPS and GSM dependent
- No cross-over possibilities, e.g. positioning be based on known WLAN networks, mobile phone cell location, RF/DF
- Intelligence is lacking from the systems
  - they can be commanded but they do not have the capability of self-reacting and alerting
  - Vulnerable to jamming without jamming detection

FUTURE

- *Multi GNSS capability* (Galileo, GPS, CLONASS)
- Battery is biggest part of sensors, *miniaturizing* will mainly be achieved by optimizing power consumption, utilizing energy harvesting and new high energy rechargeable battery technologies
- *For easy concealment*, recharging should be wireless
- For improving *legal, policy and social acceptance* issues, tracking sensors should need *authentication permission* token to operate
- *Encryption* should be done in the first possible phase, so that there will be no plain information stored in the system.
- Self-protection and counter measure protection as well as jamming detection should be included.

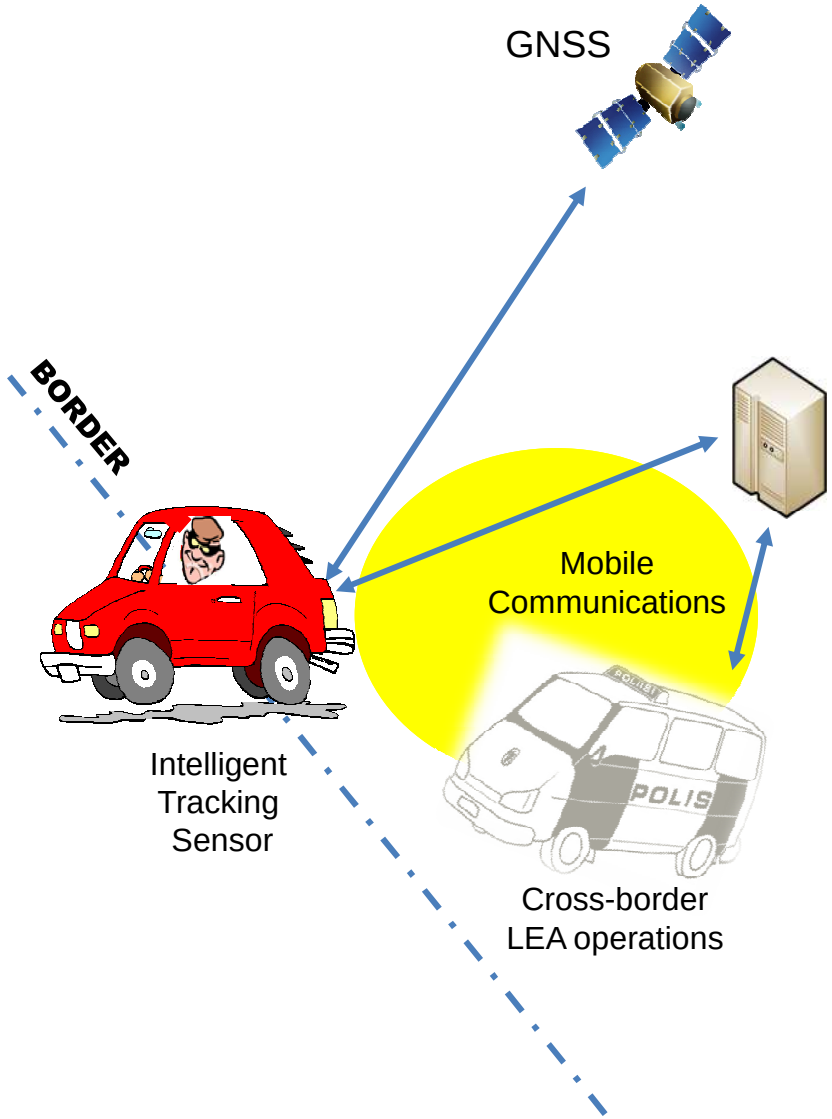
Cross-border LEA Operations

- European integration has increased the transport of illegal goods and other criminal activities
- Today, LEAs' practices, technologies and legal procedures differs from country to country
  - Slow and/or hindered information exchange
- Need: How to exchange time critical data between multinational organisations?
  - To use of m2m tracking across borders
  - To create a timely situational picture in joint multinational and interagency operations



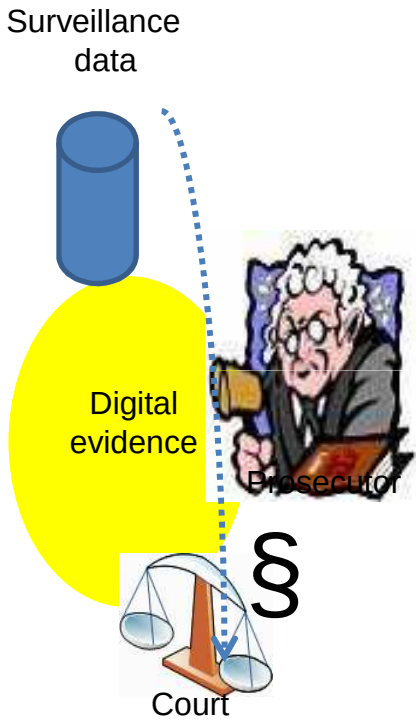
Mobile Communications

- Tracking sensor
  - 2G/3G
  - No proprietary radio channels
- LEAs on the field
  - TETRA networks have no roaming abilities
  - 2G/3G reliability?
  - Satellite communications: cost, bandwidth
  - Multichannel (TETRA+2G/3G+Sat) communications



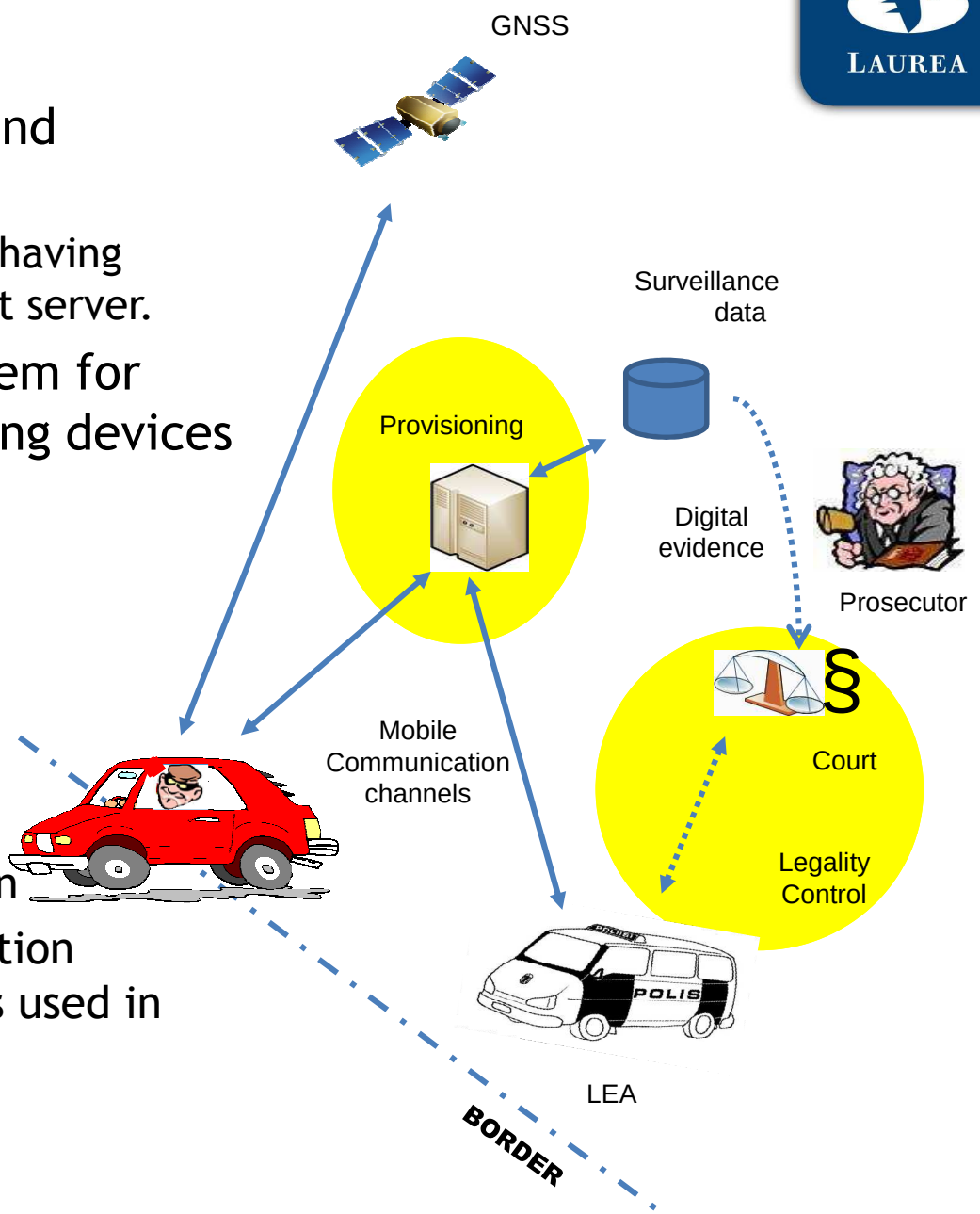
Digital Evidence

- At present, LEAs use point to point investigation tools and tracking systems, where the information is transmitted from the sensor to e.g. a laptop of the surveillance team for monitoring
- These systems creates neither watermarks nor log file marks
  - the system only retrieves the information and stores it locally
- Neither chain-of-custody nor social acceptance by transparency comes true
- Gathering, conservation, communication and presentation of the computer-derived evidence must fulfill legal requirements with regard to the admissibility of the evidence; they should be admissible, authentic, complete, reliable and believable.
- Electronic evidence not gathered in accordance with the law will be inadmissible and be ruled out of court.
- Today's main evidence authentication system is the hash value
  - Proves: data is original and no one has tampered with it
  - Problem: when, where and by whom data is produced



Legality control

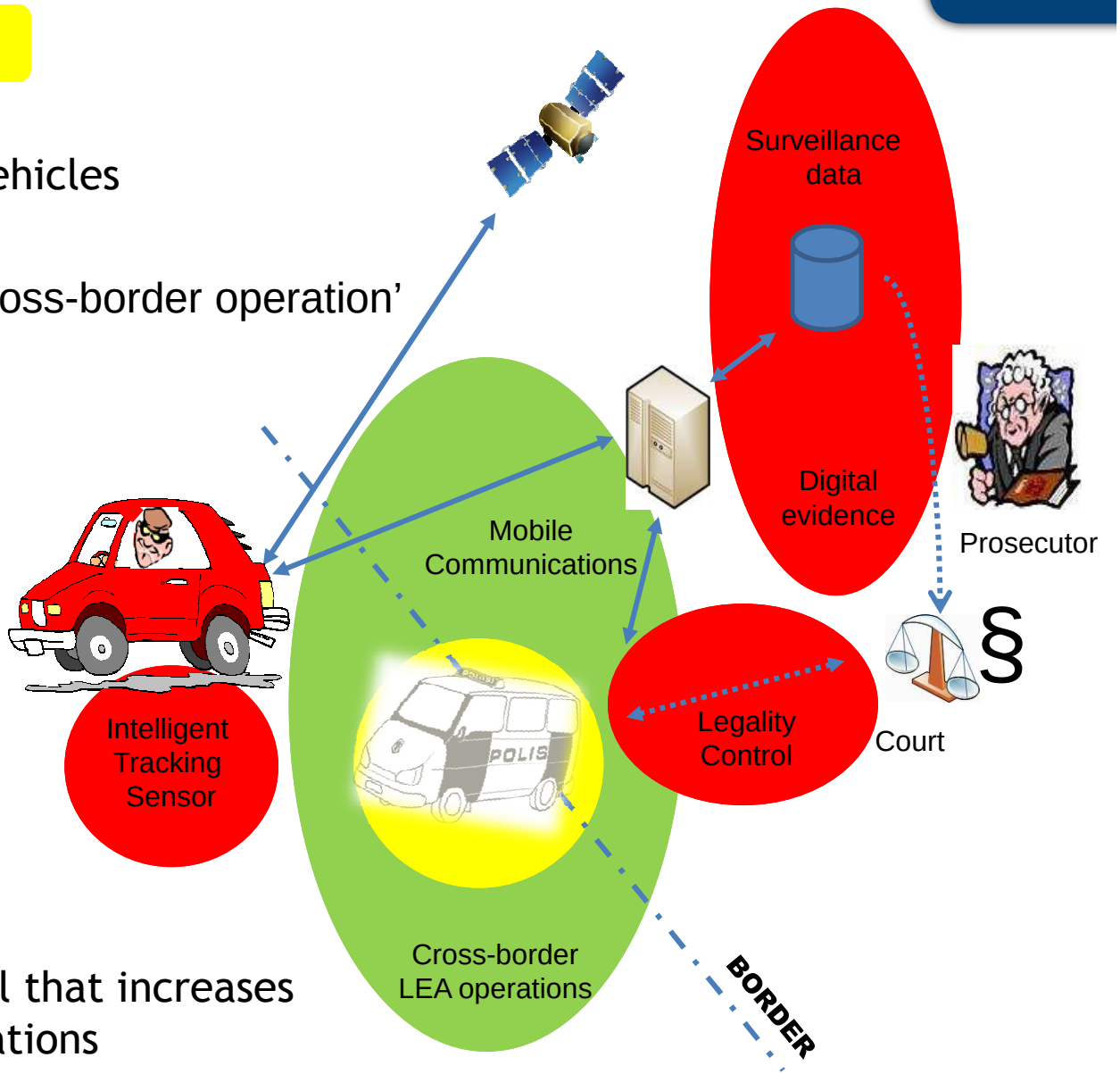
- Strong authentication mechanisms and provisioning system is needed
  - enables the sensor to work only when having permission from the central legal audit server.
- Open standardized provisioning system for covert investigation tools and tracking devices is missing!
- Provisioning server should
  - Authorize devices to operate
  - Define legal and technical limits for surveillance nodes
  - Legal monitoring
  - Evidence trail and temper evaluation
  - Unify authorization and legal inspection functions over wide range of sensors used in surveillance



Future work

1. Finnish national project *MOBI*
   - Sep. 2010 – Aug. 2013
   - ICT integration of PPDR vehicles
2. CELTC+ project *MACICO*

   'Multi-agency cooperation in cross-border operation'
   - France, Spain, Finland
   - Dec. 2011 – May 2014
   - Mobile cross-border communications
3. ARTEMIS project proposal *EVISENSING*
   - Intelligent, miniturized tracking sensors
   - Surveillance data that fulfils the requirement of digital evidence
   - System for legality control that increases transparency of LEA operations



LAUREA
UNIVERSITY OF APPLIED SCIENCES
Prime Mover

Thank You

jyri.rajamaki@laurea.fi

www.saterisk.fi
www.laurea.fi