ITS – Safety, Security and Privacy

Scott Cadzow, i-Tour partner, ETSI ITS WG5 Chairman

ITS Security “*tutorial*” agenda

- ITS security/safety/privacy in context
- The security process
  - TVRA – what we analysed and the key results
  - CIA paradigm – what we follow
- Privacy and data protection in ITS
  - Regulatory obligations and consequences
- Main standards effort
  - Requirements
    - the stage 1 and stage 2 services
  - Architecture
    - the framework for the stage 2 services and the stage 3 definitions of them
  - Protocols
    - the stage 3 process

Primary role of ETSI TC ITS WG5

- To provide sufficient standardisation that ITS when deployed is:
  - Legally compliant (privacy, data protection, LI, DR)
  - Interoperable and interworkable
  - Presents low risk to the user of exploit of their behaviour
  - Presents low risk to the OEM and the “ITS Operator”
- To provide guidance to the ITS community on the risks in ITS
  - TVRA process
- To assist ITS in identifying security mechanisms to meet operational requirements

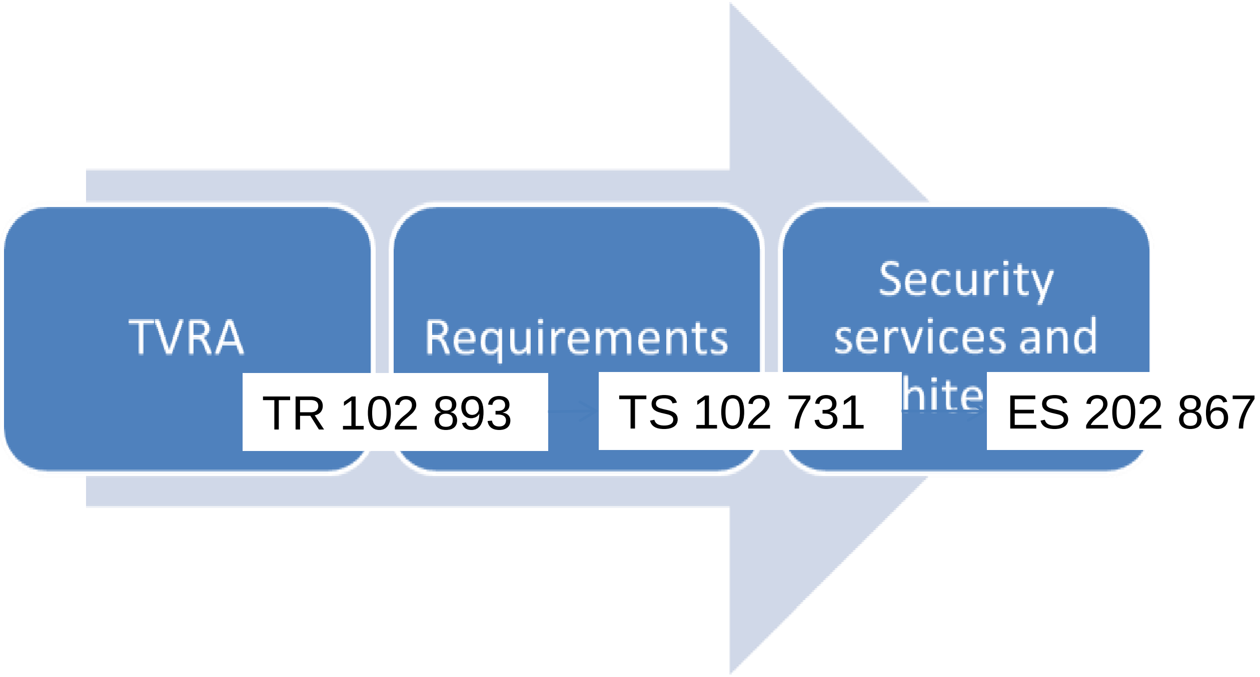
ETSI ITS versus ITS in general

- ITS are often classified into the following categories:
  - Advanced Traveller Information Systems (ATIS)
  - Advanced Traffic Management Systems (ATMS)
  - ITS-Enabled Transportation Pricing Systems
  - Vehicle-to-Infrastructure Integration (VII)
  - Vehicle-to-Vehicle Integration (V2V)
- ETSI’s current focus is:
  - V2V and V2I (*VII*) cooperative awareness in support of safer transport
  - ITS-S as source of data and as processor of data
  - Communications links via IEEE 802.11p (5.9GHz, Wireless Ethernet, ad-hoc *and infrastructure* modes)

Basic concepts in ETSI ITS

- ITS stations send environmental (event) and (vehicle) status data to other ITS stations
  - DNN, CAM
- ITS stations may exist in vehicles
- ITS stations may exist in roadside furniture
- ITS stations may be networked together
- Interpretation of received data may assist in driver safety
  - E.g. Collision avoidance
- Interpretation of received data may assist in regulatory compliance
  - E.g. Speed limit notification and adherence
- Different data has different authority
  - E.g. Speed limit notification from an authority versus speed assertion from an ITS station

Working methods in ETSI TC ITS WG5



TVRA

Requirements

Security services and

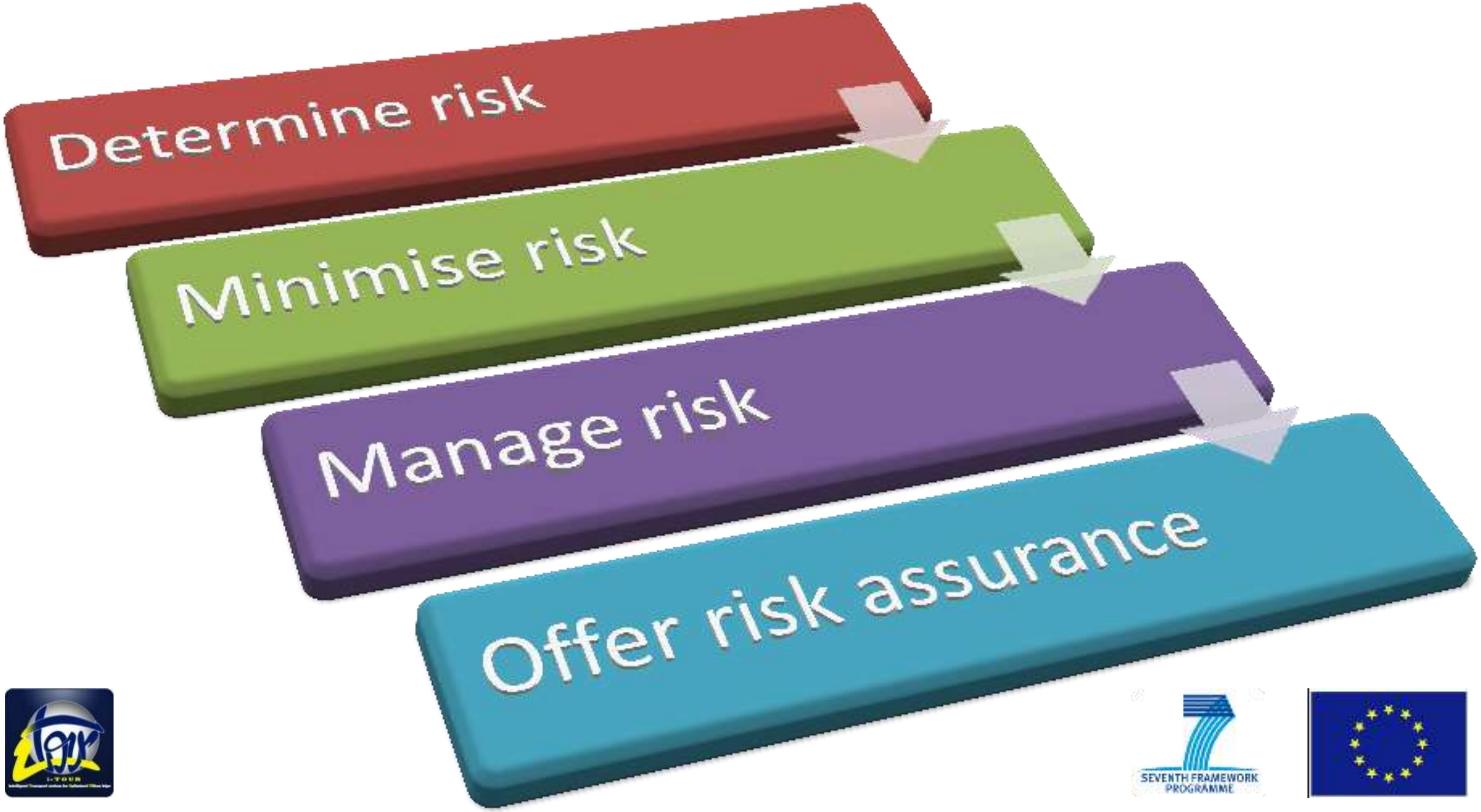
hite

TR 102 893

TS 102 731

ES 202 867

The (ITS) approach to security



- Determine risk
- Minimise risk
- Manage risk
- Offer risk assurance

ITS aim: Improved safety to aid survivability

ITS aim: To reduce or eliminate congestion

ITS data source

ITS data source

ITS data source

ITS data source

ITS data source

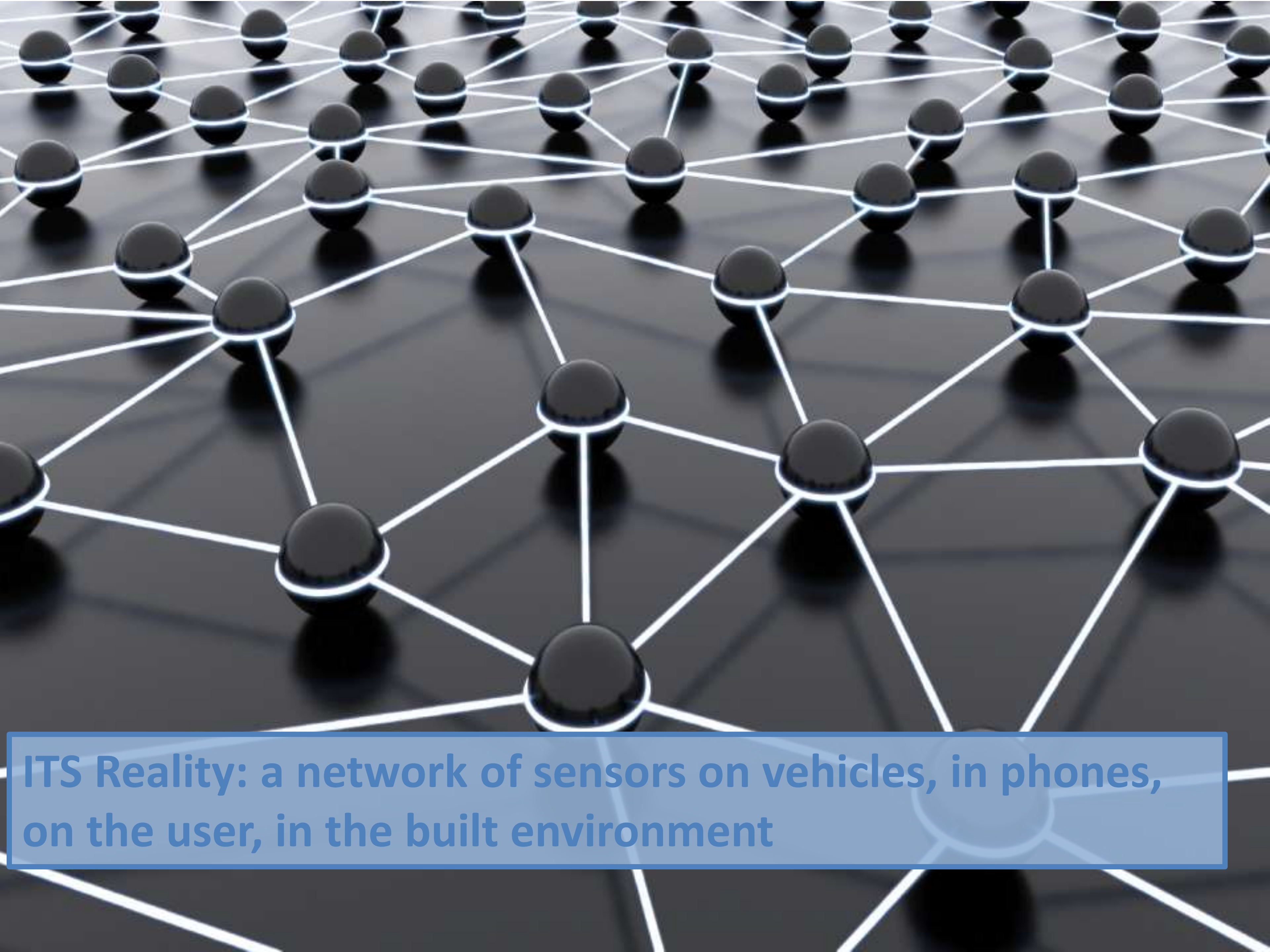
ITS data source

ITS data source

ITS Aim: Reduce impact of transport on the environment

ITS aim: To encourage the use of public/shared transport

ITS reality: Travel patterns and behavior mark us as members Virtual Communities



ITS Reality: a network of sensors on vehicles, in phones, on the user, in the built environment

ITS reality: A network of people for people

ITS data source

ITS da
sourc

ITS data source

ITS data source

ITS data source

ITS data source

ITS data source

ITS data source

ITS data source

Safety

A closer look?

Safety – global challenge

- Every year, 1.3 million people are killed and 50 million injured on the world's roads.

Some statistics

- Deaths on EU27 roads:
  - Dropped from 56,247 in 2000 to 34,500 in 2009
    - Downward trend is persistent and ITS should aim to accelerate the trend
- Vehicles on EU27 roads:
  - Increased from 334/1000 inhabitants in 1991 to 473/1000 in 2009
    - Assertion: Manufacturers want to continue this increase
    - Assertion: Social mobility pressures will cause this to increase
- Public transport use:
  - Flat at 7% for train use in EU27
  - Flat at 9% for bus use in EU27

Safety – UK roads

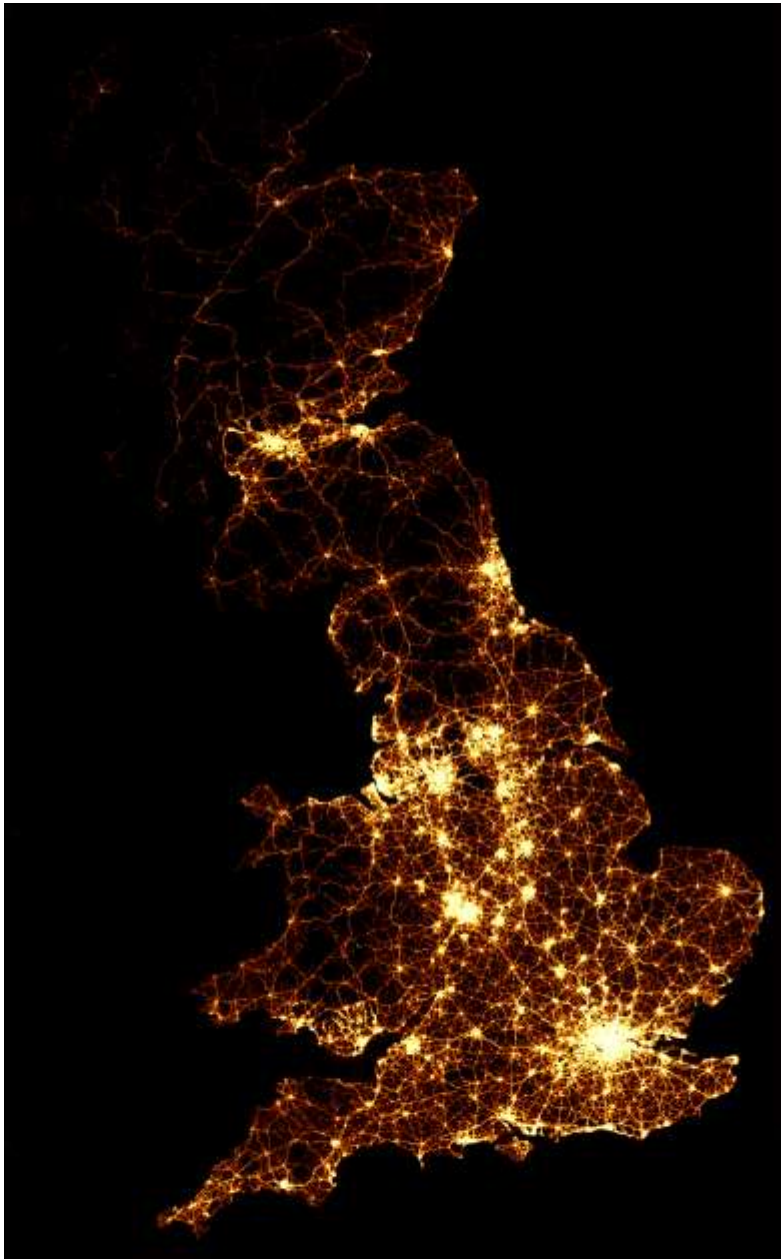
- In 2010, the police recorded:
  - 1,850 deaths,
  - 22,660 people seriously injured, and
  - 184,138 who received light injuries.
- Due to under-reporting Government estimates suggest that 730,000 are either killed or hurt every year (i.e. 3½ times the official recording).
- According to the Department for Transport, the annual economic burden of road casualties is between £15bn and £32bn.
  - Population of 64 million paying £32 billion? £500/head/year?

Safety – global challenge

- Every year, 1.3 million people are killed and 50 million injured on the world's roads.
  - Population of 7 billion? Cost (extrapolated from UK figures) of £3.5 trillion?

Safety

- **The location of 2,396,750 road crashes in Great Britain from 1999 to 2010. Each light point is an individual collision which resulted in a casualty. The intensity of brightness shows where collisions are more frequent.**
- http://www.bbc.co.uk/news/uk-15975724



Top causes of crashes

Contributory factors*	Fatal	All
*RECORDED BY POLICE AT SCENE. PERCENTAGES MAY NOT TALLY AS MULTIPLE CATEGORIES CAN BE SELECTED. SOURCE: DEPT FOR TRANSPORT		
1. Driver/rider error	70%	70%
2. Injudicious action	29%	25%
3. Behaviour or inexperience	29%	23%
4. Road environment	11%	16%
5. Pedestrian error	17%	13%

Mitigation - rationale

- The US Insurance Institute for Highway Safety has *estimated* that four of the currently available features - lane departure warning, forward collision warning, blind spot detection and adaptive headlights - could prevent or mitigate one out of every three fatal crashes and one out of every five crashes that result in serious or moderate injury
- A 2008 EU study by the Finnish VTT Technical Research Centre found that mandating lane departure warning systems could reduce deaths by about 15%.
- Functions warning drivers they were exceeding the speed limit and of other potential hazards would cut fatalities by 13%
- Emergency braking assistance could potentially reduce deaths by 7%
- Driver drowsiness warnings could potentially reduce deaths 5%
- Research at the University of Leeds has found that speed-limiting technology can reduce crashes causing injuries by almost 28%.

ITS and ICT in cars

- Source of distraction
  - Cited by the US DoT as a problem to be addressed by **regulation**
- Addressed by ETSI TC HF
  - Guidance on the use and application of ICT in cars in TR 102 762 from April 2010
  - The approach is compatible with the European Statement of Principles on the Design of Human Machine Interaction

What is "ICT in cars"?

- Information and communication equipment and related services which are used within the car environment.
- For ITS the interest is where ICT in cars interacts with the car occupants.
- This therefore includes the impact of both Intelligent Transport Systems (ITS) and pure entertainment systems such as radio, music and video on the driver and passengers.

The in-car ICT environment

- The driver has a number of potentially competing issues to deal with whilst driving:
  - issues related to the immediate task of controlling the car;
  - awareness of the immediate environment (including other road users, road signs, etc.);
  - issues related to the long-term goal of the journey.

Human task switching

1. when a new event occurs, the alerting network detects an event that may require attention;
2. the alerted brain then has to disengage the attention that is allocated to the current ongoing task;
3. the brain then has to switch focus to the new task and identify the relevant brain processes to deal with such a task;
4. the rules that apply to processing the new task are activated.

Situation awareness mental processes

- Level 1 situation awareness is where we look and perceive basic information.
- Level 2 situation awareness is where we think about and understand the meanings of that information.
- Level 3 situation awareness is where we use the meanings in order to anticipate what will happen ahead in time and space.

Safety – a conclusion

- Transport is not safe enough
- ITS challenge is to improve safety
  - Whilst respecting that ICT can increase distraction
  - Whilst recognising that human decision engines are at the start and end of most ITS chains

Privacy

A closer look

Privacy, data protection and security

- Privacy is a fundamental right
  - Article 12 UDHR:
    - No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks
  - Article 8 EU Convention for the Protection of Human Rights and Fundamental Freedoms: Right to respect for private and family life
    - Everyone has the right to respect for his private and family life, his home and his correspondence.
    - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Privacy, data protection and security

- Assigns rights to citizens on how data related to them is protected
  - Enshrined in law in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
  - Supplemented by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Privacy, data protection and security

- Personal data
  - shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- Processing of personal data
  - shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
- “data subject’s” consent
  - shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

Privacy, data protection and <u>security</u>

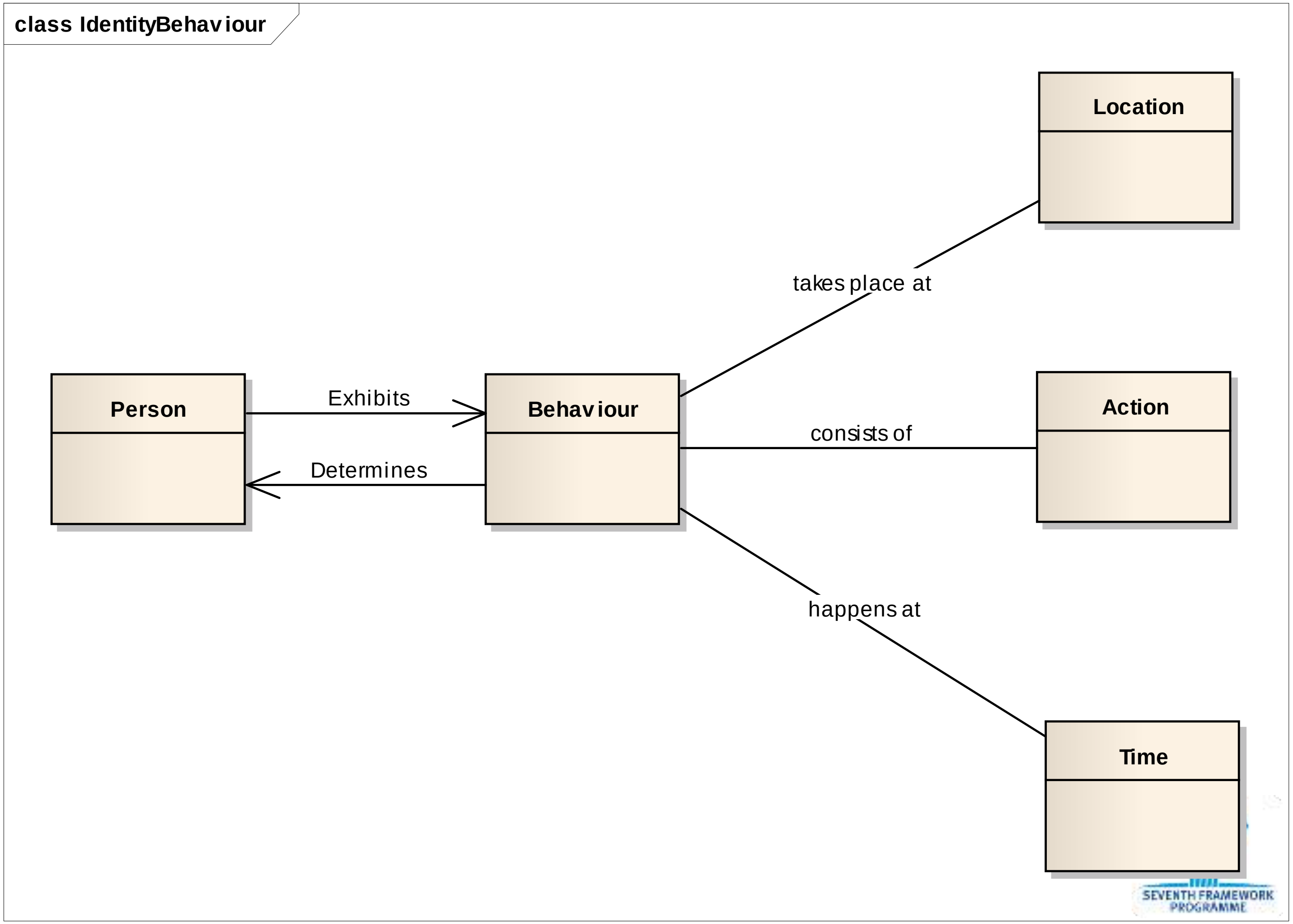
- The means to give assurance of the confidentiality, integrity and availability of data and services
  - Offers technical and procedural means to support regulation

- Security supports …
  - Privacy (Privacy Enhancing Technologies)
    - COM(2007) 228 final: "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs)"
  - Data protection

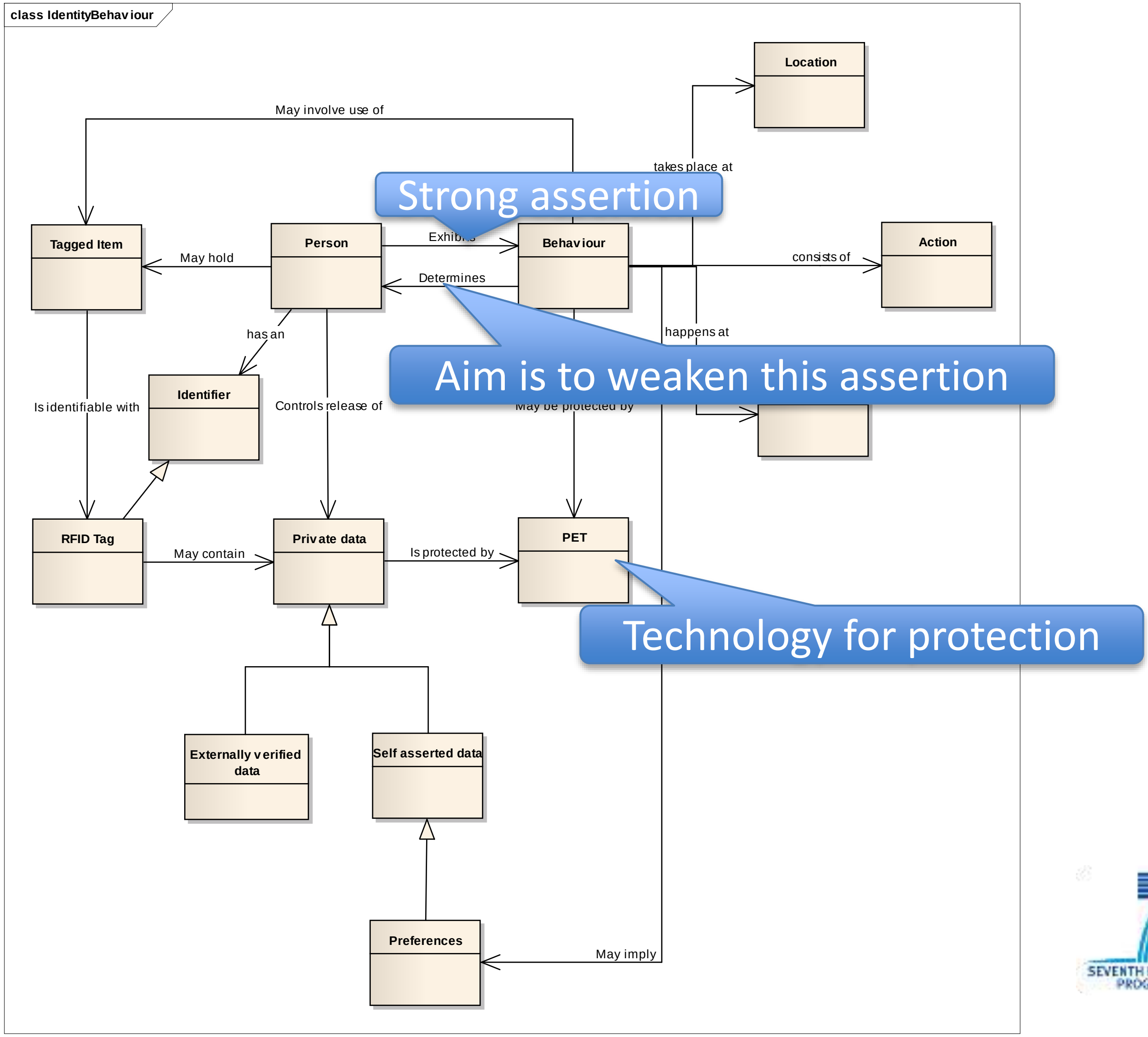
Protecting User Privacy

- Privacy protection protects a person.
- A person is described by what they do, where they do, when they do it, what they do it with, and with whom they do it
- ITS users share their activity with each other and with the system
  - Need to protect exploit of that data by other parties

Wider concept



A model or ontology for privacy



Strong assertion

Aim is to weaken this assertion

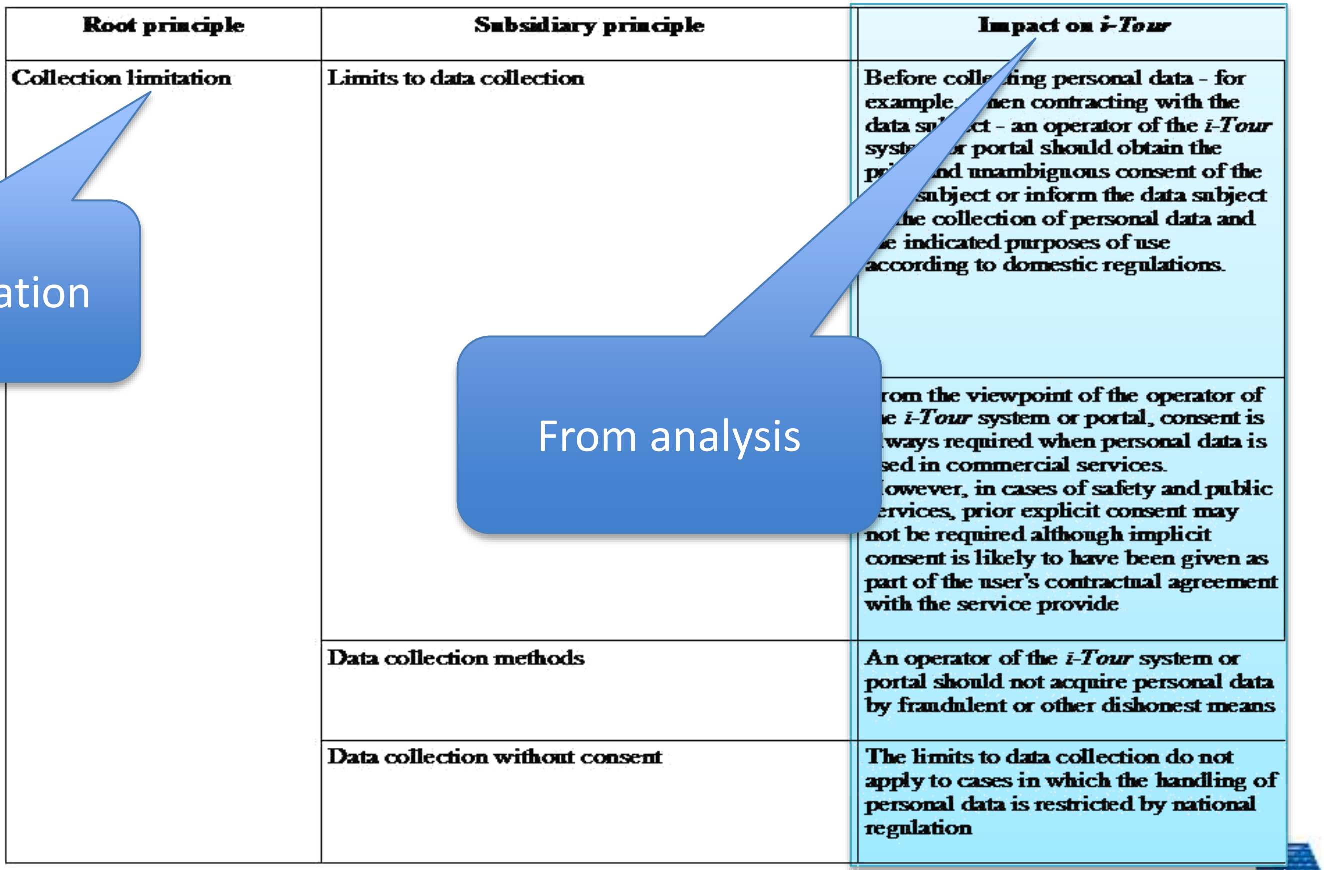
Technology for protection

User Privacy versus User security

- Security is not a synonym for privacy
  - But security techniques will give some protection of privacy
  - Security techniques counter risk of
    - Interception, Masquerade, Manipulation, Repudiation

Objectives from directives

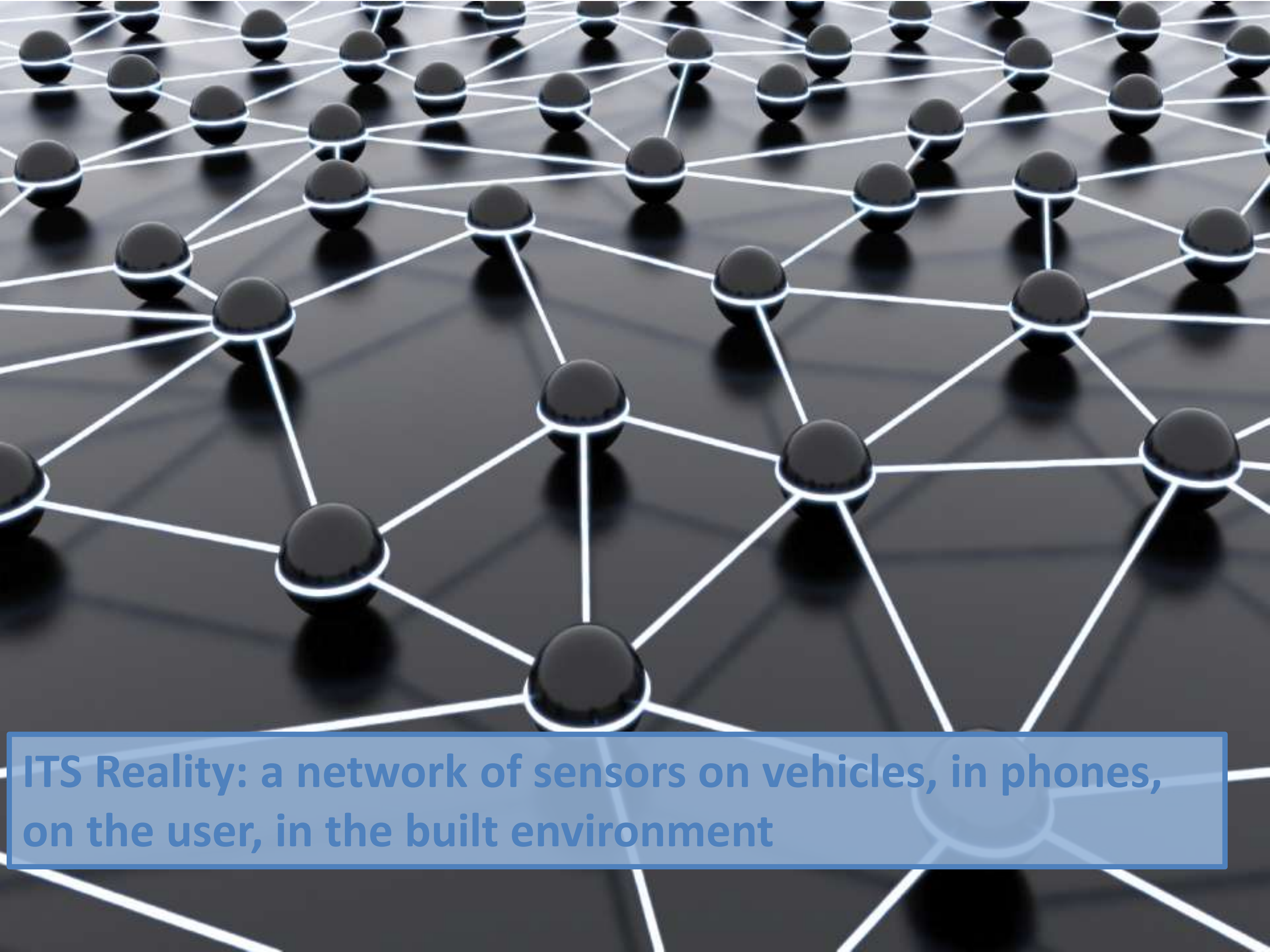
Table 1: Objectives arising from OECD guidelines and EC Data Privacy directives.



Root principle	Subsidiary principle	Impact on *i-Tour*
Collection limitation	Limits to data collection	Before colle ting personal data - for example, hen contracting with the data su ct - an operator of the *i-Tour* syste r portal should obtain the pr nd unambiguous consent of the subject or inform the data subject he collection of personal data and e indicated purposes of use according to domestic regulations.
		rom the viewpoint of the operator of e *i-Tour* system or portal, consent is ways required when personal data is sed in commercial services. owever, in cases of safety and public ervices, prior explicit consent may not be required although implicit consent is likely to have been given as part of the user's contractual agreement with the service provide
	Data collection methods	An operator of the *i-Tour* system or portal should not acquire personal data by fraudulent or other dishonest means
	Data collection without consent	The limits to data collection do not apply to cases in which the handling of personal data is restricted by national regulation

From regulation

From analysis



ITS Reality: a network of sensors on vehicles, in phones, on the user, in the built environment

Concerns of ITS as a sensor network

- Using mobile devices as sensors
  - Who does it give its sensor data to? Does it trust the receiver will use it well? Can the sensor function be switched off?
- Using people as sensors
  - What are you sensing? Is this going to come back and adversely affect me?
- Using mobile devices as computing nodes
  - Is this realistic?
  - For example how much excess computing power is a car maker going to install?
- Using people as data sources
  - Not just sensor data but opinions too? How to develop trust in their input

Concerns expressed in i-Tour

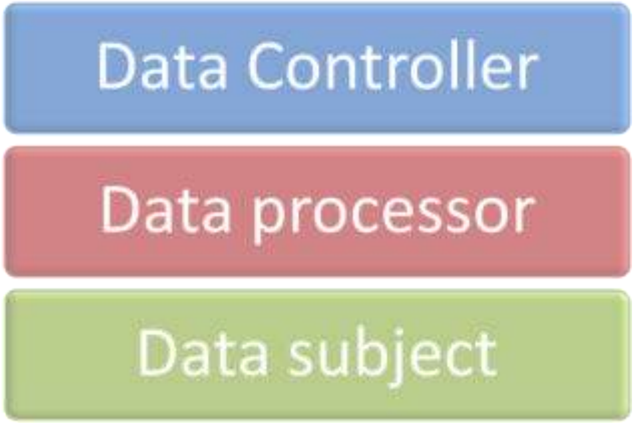
- The reason for travel is often personal
  - Leisure, work, family travels are not open for all to see and exploit
- A traveller’s viewpoint is too low to see the “right path”
  - Needs help from a trusted authority with a better viewpoint
- Asking for directions is naturally a verbal/aural process
  - Often doesn’t just concern the shortest/quickest route but the one that fits to the person (e.g. via this type of shop, suitable for a baby buggy, with indoor secure bike parking close to the destination, …)

Building trust in i-Tour

- Trust is developed over time from the analysis of actions, reactions, and contributions
  - Requires observation and interaction over time
  - Requires contextual knowledge
  - Trusting party-A in context-X does not mean having to trust party-A in context-Y

Privacy roles and locations

- Roles are identified in legislation (for EU)
- Data controller and data processor roles are embedded in the “core”
- Consent for data use is managed through the “core”



Data Controller

Data processor

Data subject

Risk analysis in ITS

Review of work done and in hand

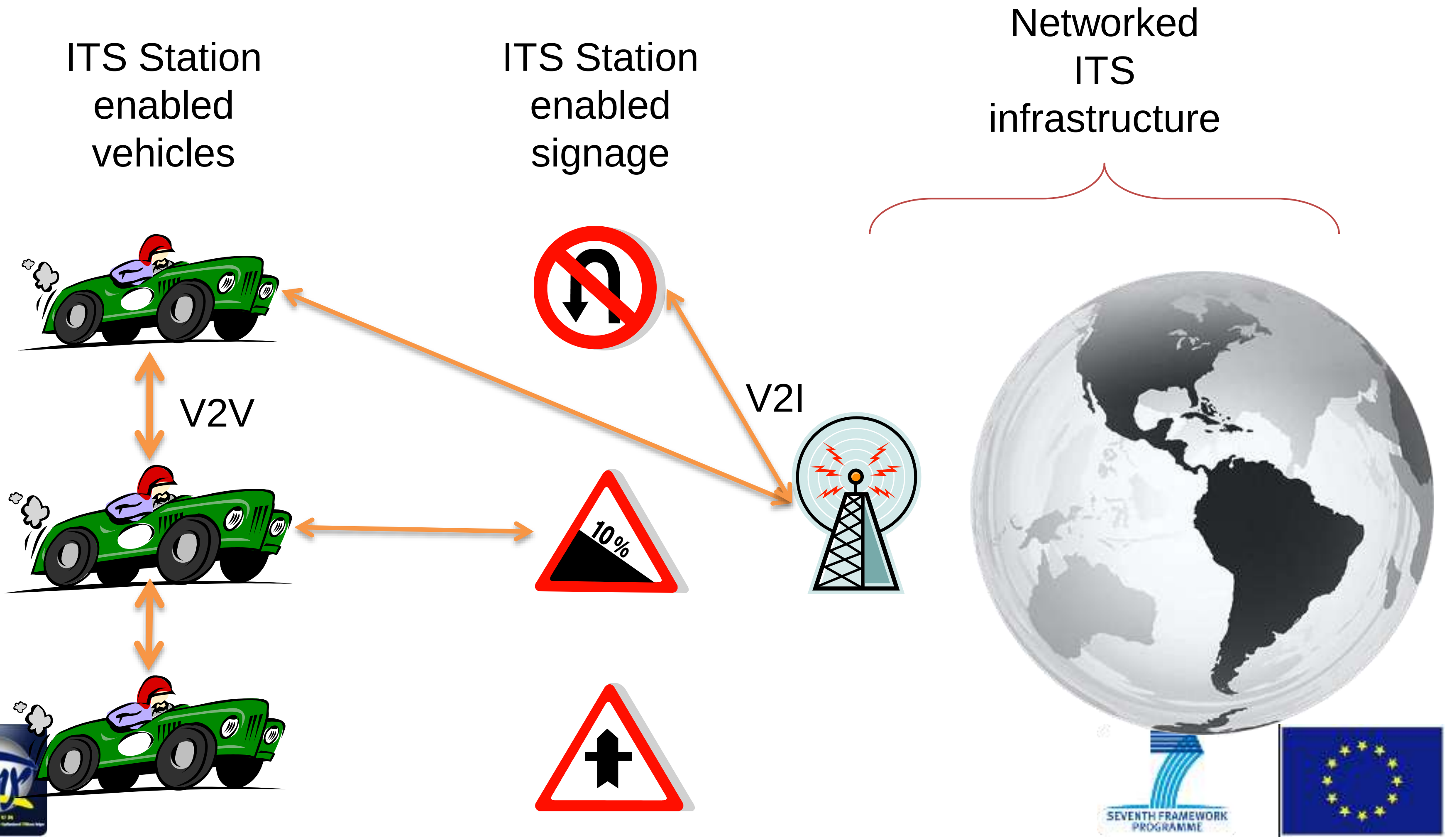
Use cases considered in TVRA

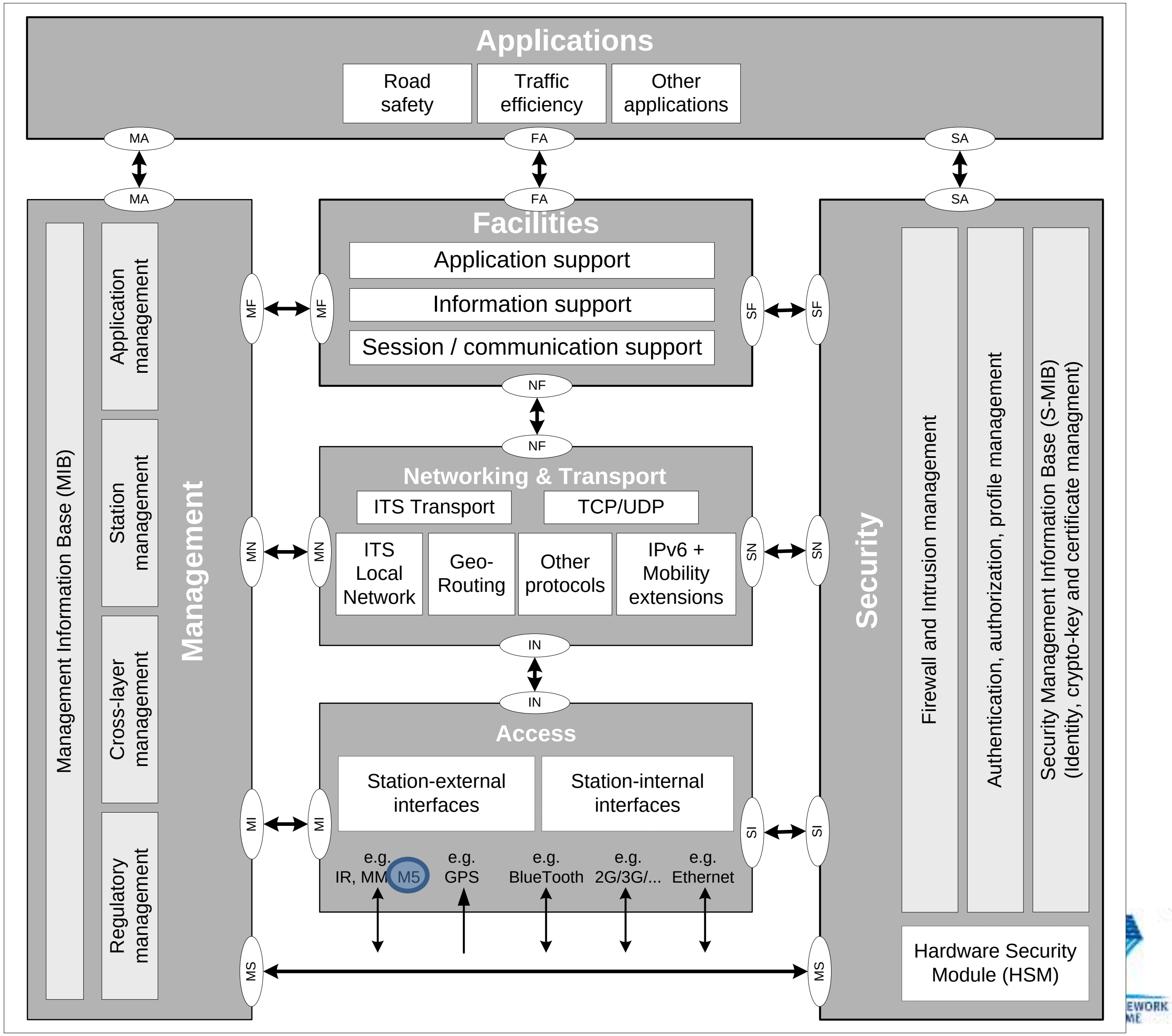
- The use cases in the BSA and included in the TVRA are as follows:
  - Stationary vehicle warning - accident/vehicle problem.
  - Traffic condition warning (includes traffic jam ahead warning).
  - Signal violation warning (includes stop sign violation).
  - Road work warning.
  - Collision Risk Warning from RSU.
  - Decentralized Floating Car Data - Precipitations/Road Adhesion/Visibility/Wind.
  - Regulatory/Contextual speed limits.
  - Traffic information & Recommended itinerary.
  - Limited access, detour notification.
  - In-vehicle signage.

Review of BSA

- The ITS BSA use cases send and receive two fundamental message types which are:
  - Cooperative Awareness Message (CAM):
    - Periodically transmitted containing transient data on the vehicle status.
  - Decentralized environmental Notification Message (DNM):
    - Generated upon detecting an event and contain information about this event.
    - DNM messages are typically relevant for a defined geographic area.

Use cases and scenarios


ITS Station enabled vehicles
ITS Station enabled signage
Networked ITS infrastructure
V2V
V2I
10%
SEVENTH FRAMEWORK PROGRAMME



Applications

Road safety

Traffic efficiency

Other applications

Facilities

Application support

Information support

Session / communication support

Networking & Transport

ITS Transport

TCP/UDP

ITS Local Network

Geo-Routing

Other protocols

IPv6 + Mobility extensions

Access

Station-external interfaces

Station-internal interfaces

e.g. IR, MM M5

e.g. GPS

e.g. BlueTooth

e.g. 2G/3G/...

e.g. Ethernet

Management

Management Information Base (MIB)

Application management

Station management

Cross-layer management

Regulatory management

Security

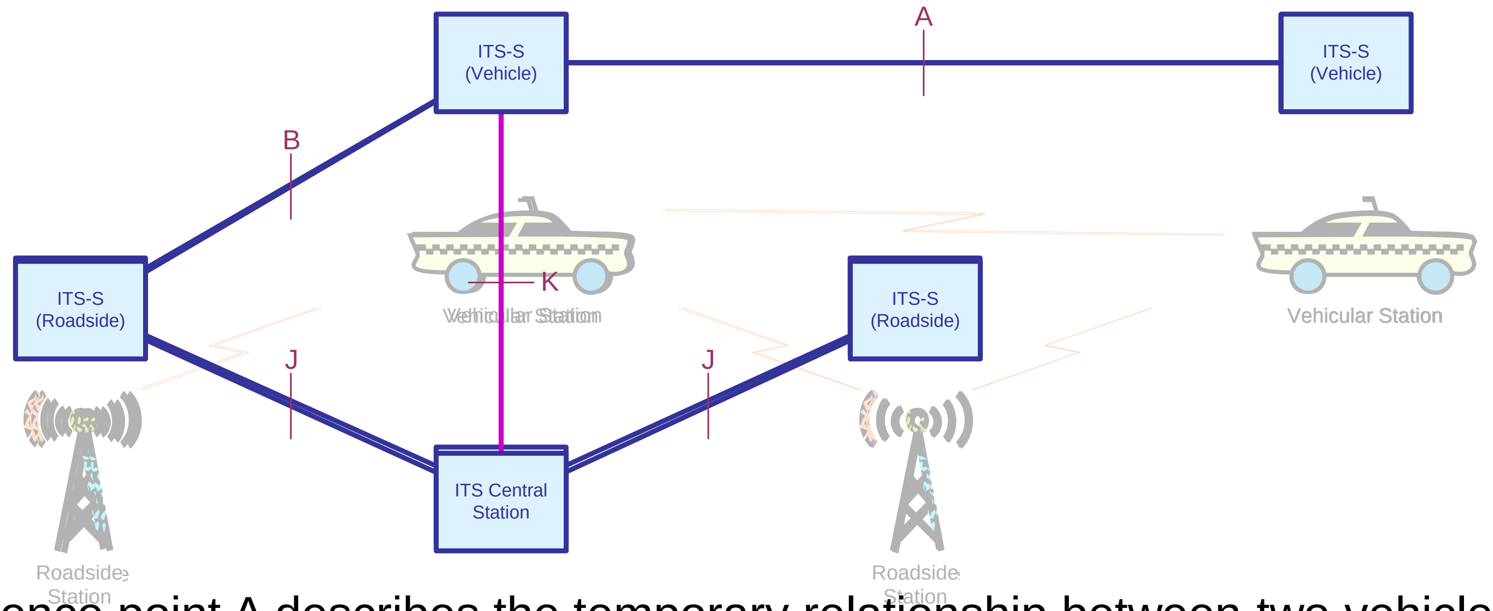
Firewall and Intrusion management

Authentication, authorization, profile management

Security Management Information Base (S-MIB) (Identity, crypto-key and certificate managment)

Hardware Security Module (HSM)

The abstract view of ITS



Reference point A describes the temporary relationship between two vehicles.

Reference point B describes the temporary relationship between a vehicle and a roadside station.

Reference point J describes the relationship between an ITS roadside station and the ITS network infrastructure.

Reference point K describes the relationship between an ITS vehicle station and the ITS network infrastructure.

Threats considered in the TVRA

- Basic principles and assumptions:
  - Radio communications will be intercepted
  - Radio path facets will introduce manipulation
  - Radio paths are unreliable and messages will be lost
  - Attackers do not need to be in line of sight
  - Attackers may use more than one vector to attack the ITS system
  - Attackers may act in concert against single stations or against single locations

NOTE: Most of these radio problems have to be sorted by the PHY and MAC (maybe with LLC) and not be security features

- Concept of trusted domain
  - The ITS-S is assumed to be trusted
  - The internal structure of the ITS-S is not subject to analysis
  - Attacks are considered against the ITS-S over its open interfaces
    - In this instance over radio at 5.9GHz

What we’re trying to determine

- RISK value or RISK categorisation
  - Critical, Major, Minor
  - Critical risks have to be designed out of the system
  - Major risks should be designed out of the system
  - Minor risks should be mitigated
- Risk is calculated from both likelihood and impact of an attack
  - Threat agents are considered in isolation – in practice one attack may be a precursor of a later attack and where this is known the risk is also assessed

Key management issues #1

- Volume considerations
  - With (say) 6 billion stations worldwide and an annual change of (say) 6% it is absolutely infeasible to give every ITS-Station a unique key and to also give it the key required to communicate uniquely with every other vehicle.
- Symmetric versus asymmetric keying
  - A perennial debate in security circles is the use of symmetric versus asymmetric keying and cryptology. Both have value in ITS. In those instances where there is no predefined symmetric security association obviously asymmetric approaches hold sway.

Key management issues #2

- Rekeying or revocation
  - Symmetric keys are deleted when no longer required, whereas asymmetric keys have to be revoked.
- Geographic or domain keying
  - As many messages have a strict geographic domain of applicability a geographic or domain key should be used either as a key directly in transmission, or as a key modifier. On entering a geographic area each ITS station should be able to either receive on demand (pull) or be given (push) the domain key.

Key management issues #3

- Hybrid keying
  - For vehicle to vehicle scenarios each vehicle may be populated with a set of keys (most likely in the form of PKCs) that are owned and distributed by the controlling authority and which may be modified using the vehicle key. This associates the vehicle with an infrastructure without the requirement to maintain a roadside ITS Comms infrastructure (but there is a requirement to ensure key freshness).
  - Capabilities:
    - Confidentiality using shared infrastructure keys, authentication and integrity piggy back.
  - Concerns:
    - Session key creation may not be possible nor may verification of any vehicle key modifier.

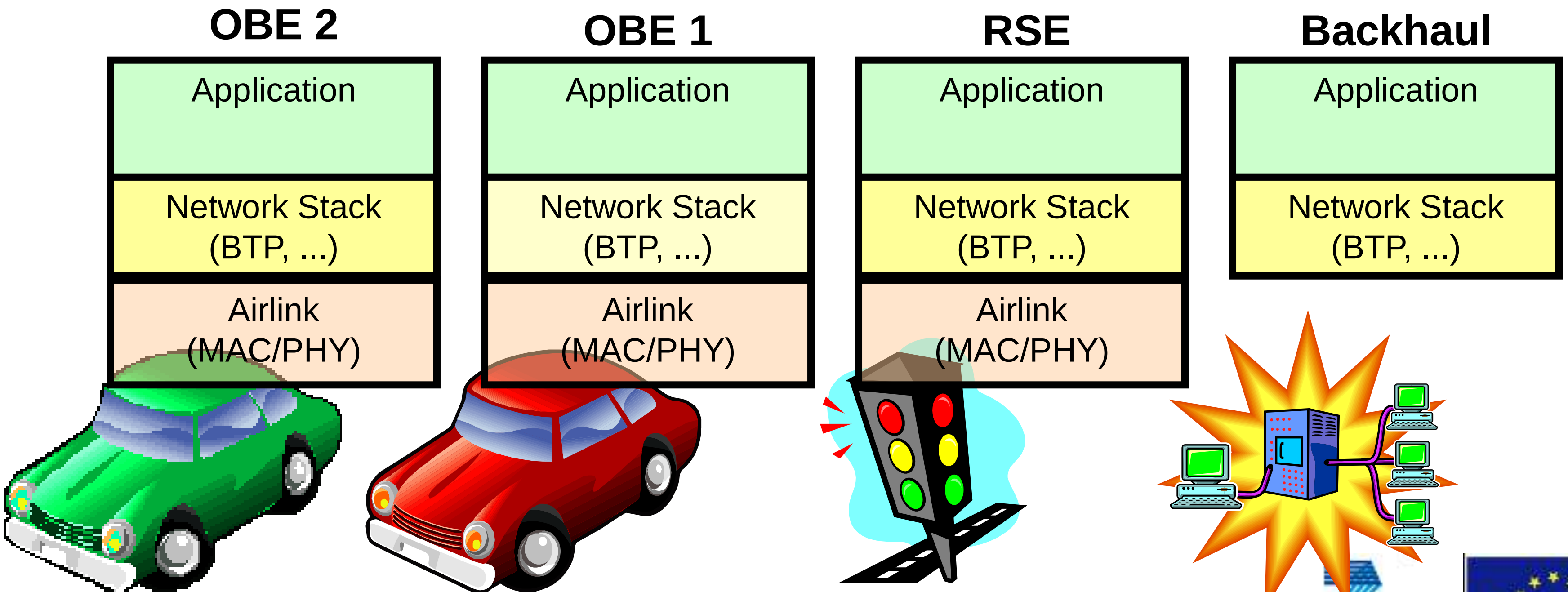
How is consent managed in ITS?

- ❑ Definition:
  - ❑ any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed
- Problem:
  - – Correspondents (data transmitters and receivers for CAM/DNM) are unknown to each other
  - – Consent cannot be given for general case (it has to be specific)
  - – How does the ITS-S user signify his agreement?

Personal data in ITS?

- ❑ Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- Direct:
  - Restrict transmission of any data that can directly identify a person (i.e. name, address)
    - Unless between known parties who have explicitly consented (with proof) of their willingness to restrict use of the data to explicit purposes
    - Unless such data is protected from eavesdropping and interception
- Indirect:
  - Restrict ability of a receiver of data to process data such that it can be linked to a real person

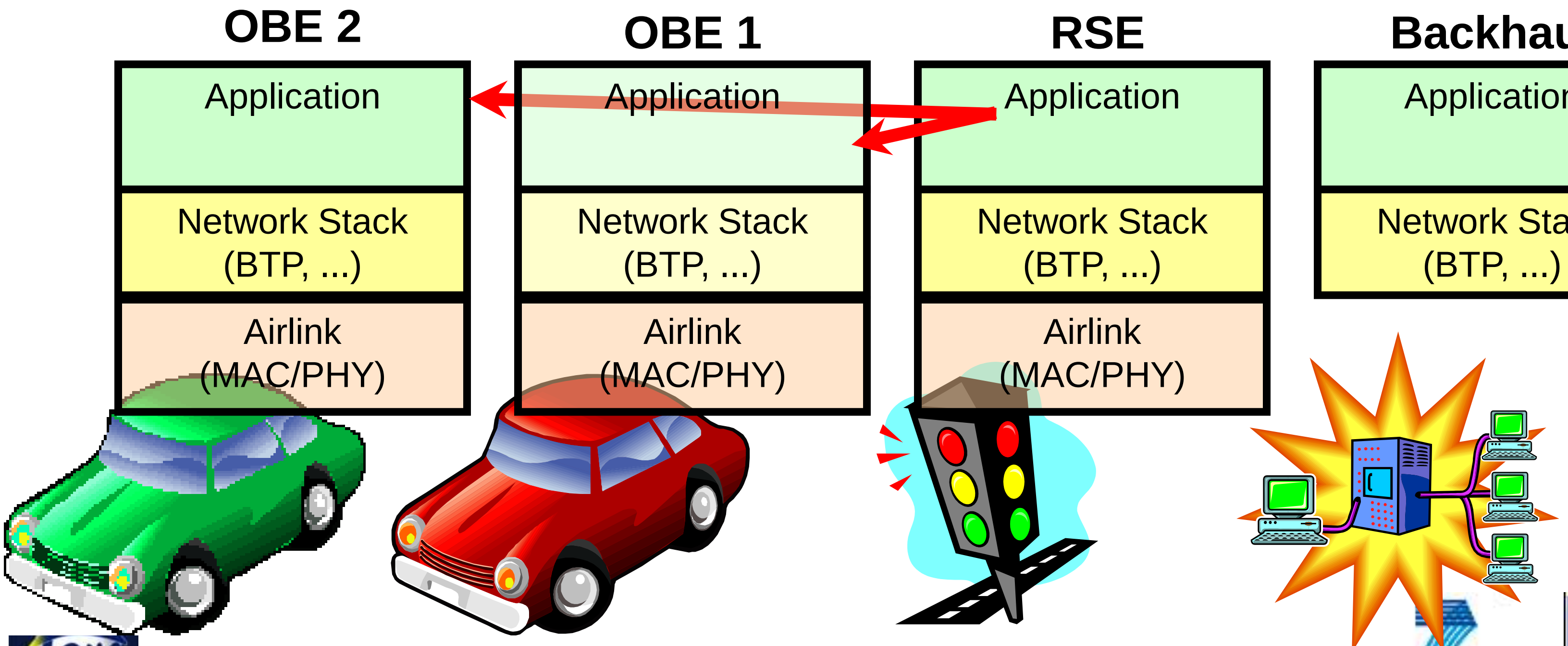
Application Communication Models



OBE 2	OBE 1	RSE	Backhaul
Application	Application	Application	Application
Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)
Airlink (MAC/PHY)	Airlink (MAC/PHY)	Airlink (MAC/PHY)	

DEN – Curve Rollover Warning

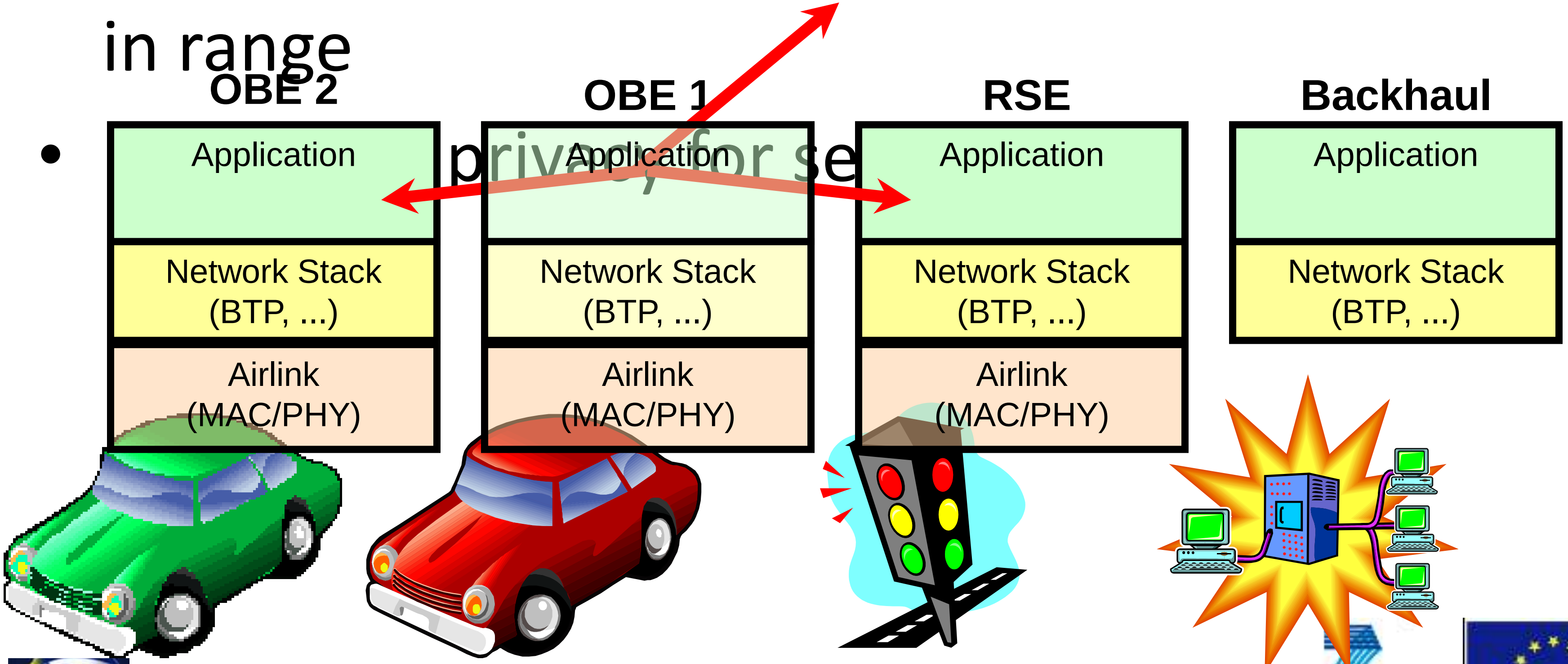
- Broadcast, RSE application to OBE application



OBE 2	OBE 1	RSE	Backhaul
Application	Application	Application	Application
Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)
Airlink (MAC/PHY)	Airlink (MAC/PHY)	Airlink (MAC/PHY)	

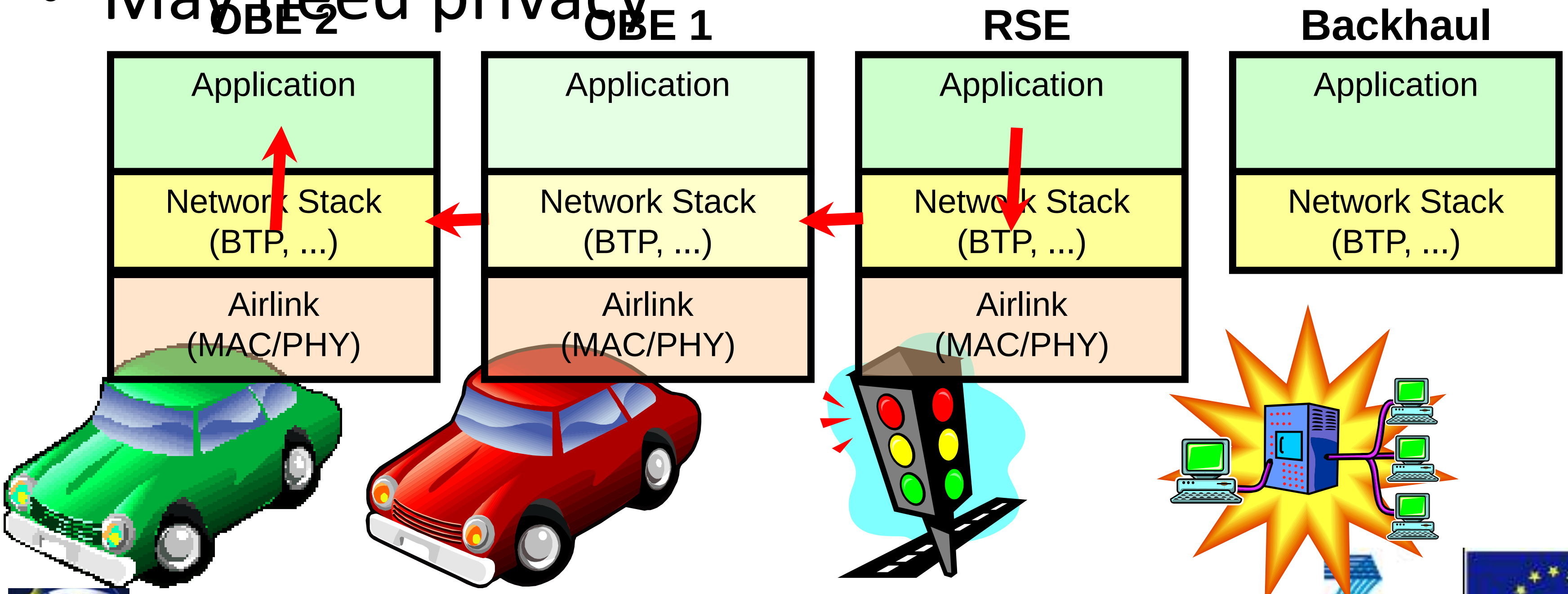
CAM – Basic Safety Message

- Broadcast, OBE application to all applications in range
- privacy, for se



CAM / DEN – Geonetworked Message

- Needs to be authenticated / authorized
- May need privacy



OBE 2
Application
Network Stack (BTP, ...)
Airlink (MAC/PHY)

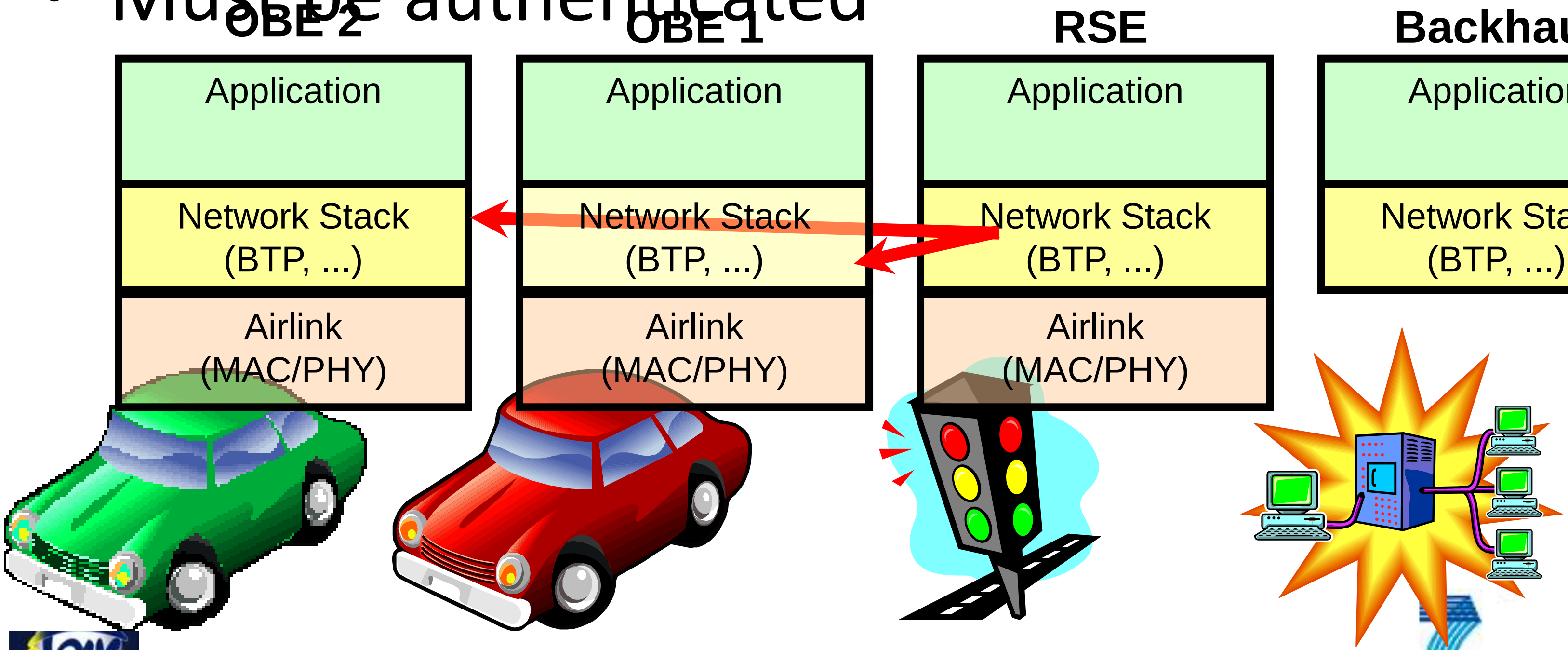
OBE 1
Application
Network Stack (BTP, ...)
Airlink (MAC/PHY)

RSE
Application
Network Stack (BTP, ...)
Airlink (MAC/PHY)

Backhaul
Application
Network Stack (BTP, ...)

Service Advertisements

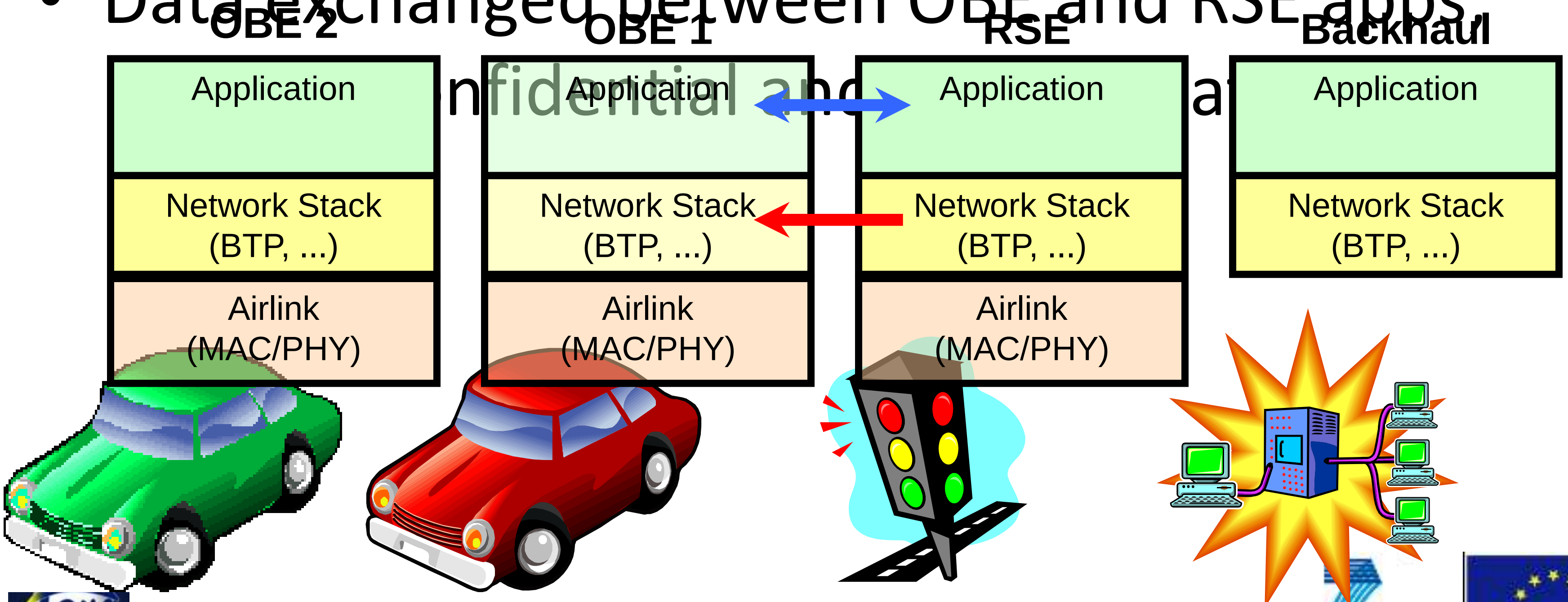
- Broadcast, RSE stack to OBE stack
- Must be authenticated



OBE 2	OBE 1	RSE	Backhaul
Application	Application	Application	Application
Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)
Airlink (MAC/PHY)	Airlink (MAC/PHY)	Airlink (MAC/PHY)	

High-speed payment

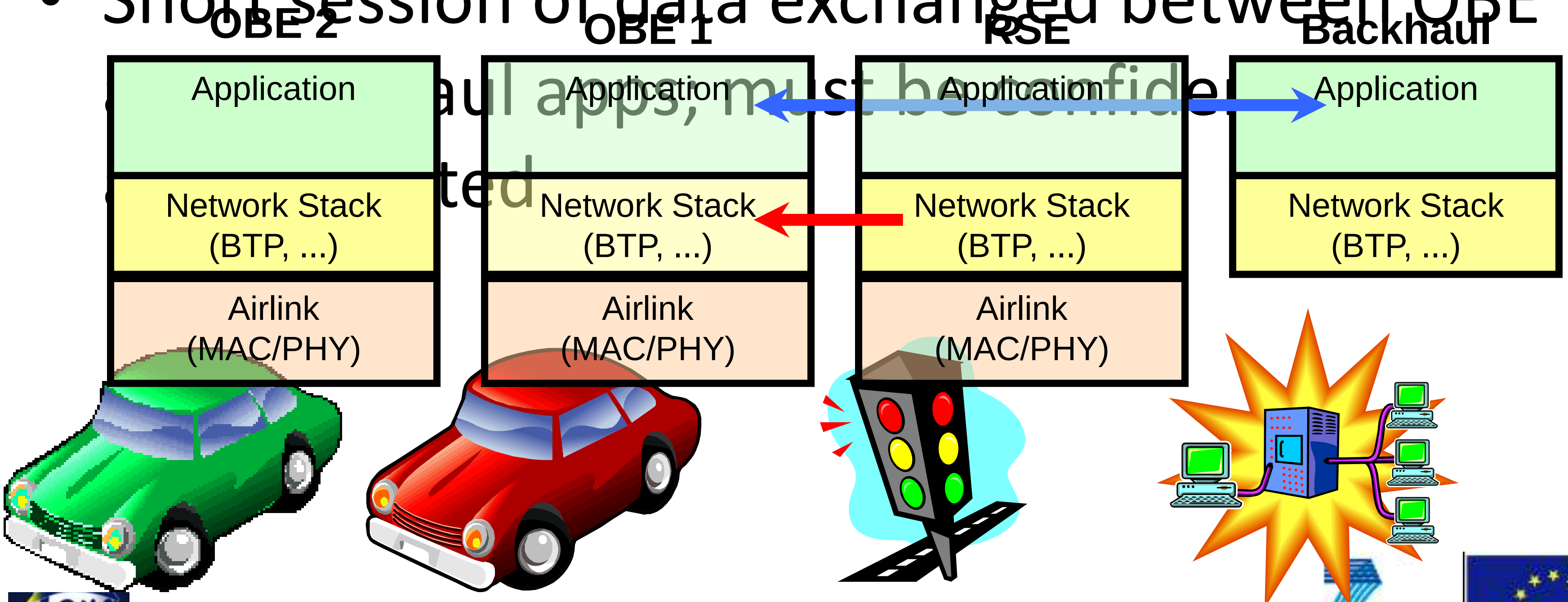
- Established via advertisement
- Data exchanged between OBE and RSE apps; nfidential anc a



OBE 2	OBE 1	RSE	Backhaul
Application	Application	Application	Application
Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)	Network Stack (BTP, ...)
Airlink (MAC/PHY)	Airlink (MAC/PHY)	Airlink (MAC/PHY)	

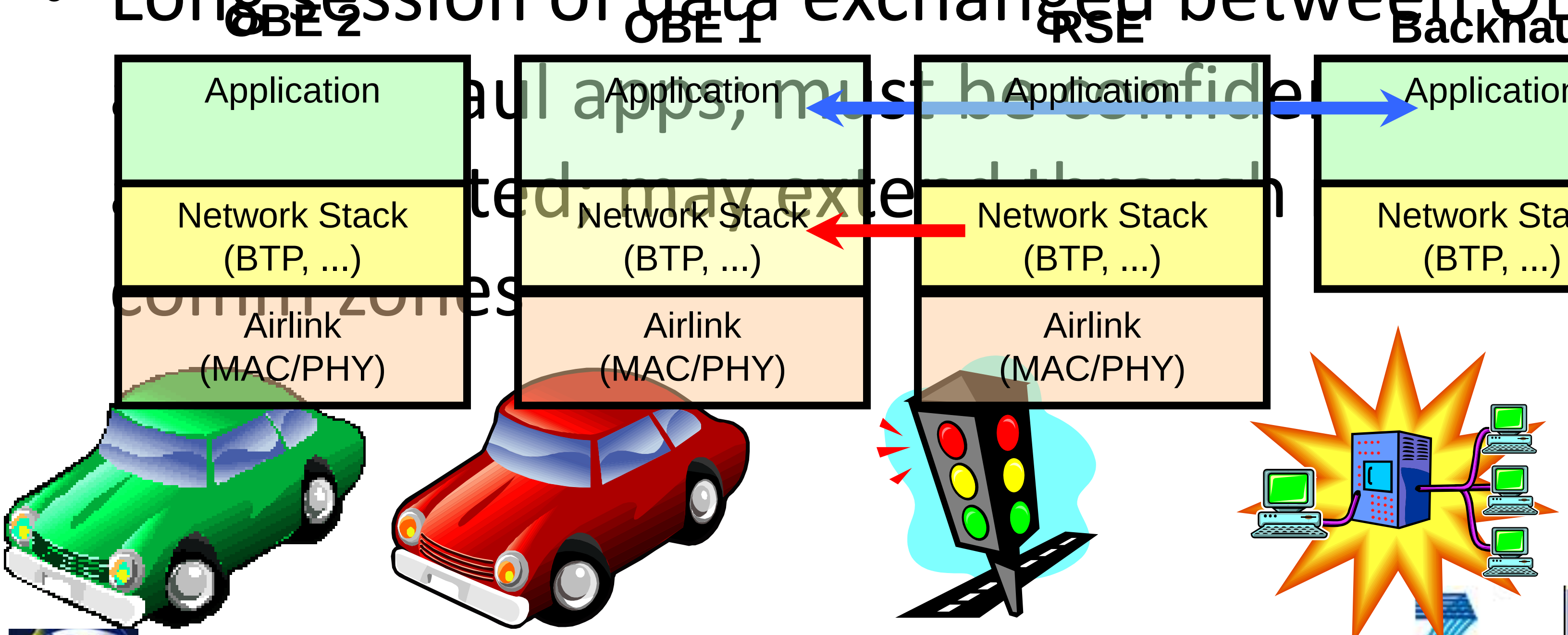
Low-speed payment

- WSIE advertises gateway to e-Payment
- Short session of data exchanged between OBE aul apps, must be confide ted



Media Download (scenario 1)

- WSIE advertises gateway to Media Download
- Long session of data exchanged between OBE aul apps, must be confide ted; may extend through comm zones



OBE 2

Application

Network Stack (BTP, ...)

Airlink (MAC/PHY)

OBE 1

Application

Network Stack (BTP, ...)

Airlink (MAC/PHY)

RSE

Application

Network Stack (BTP, ...)

Airlink (MAC/PHY)

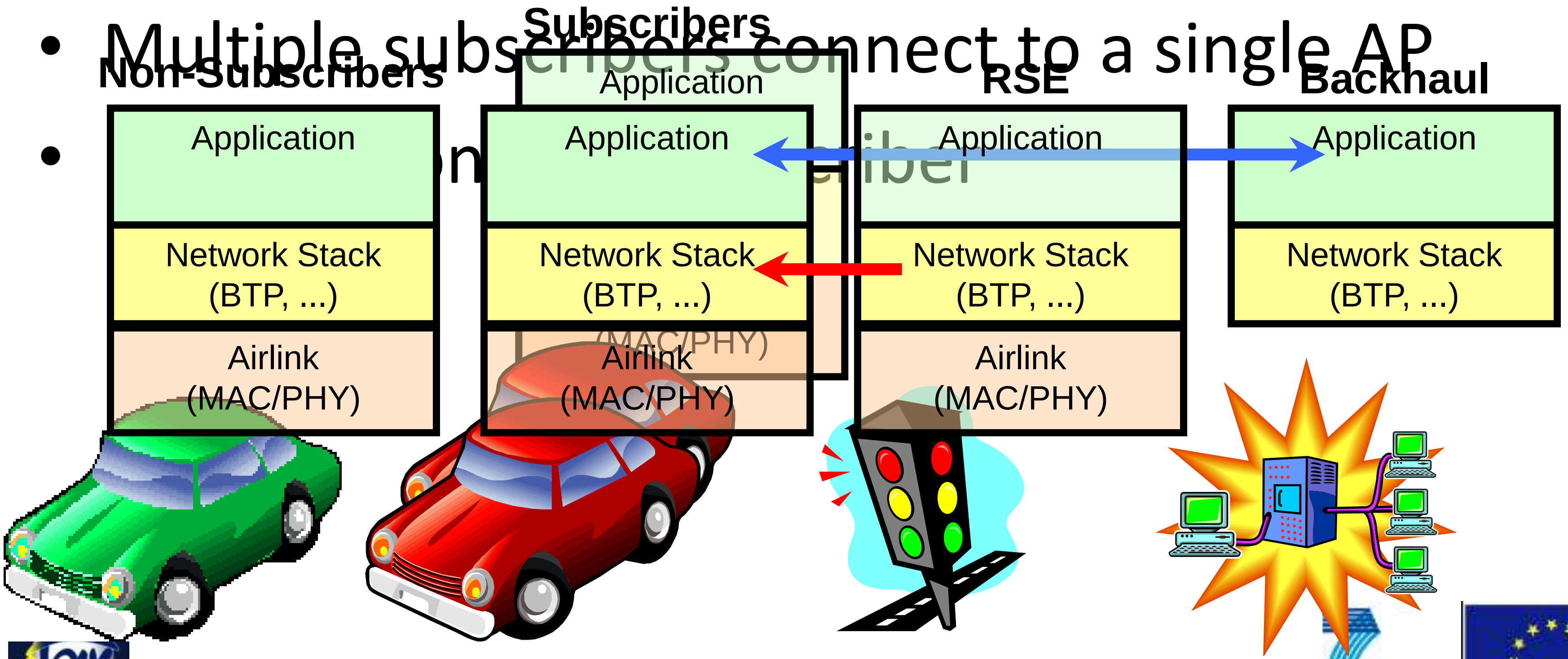
Backhaul

Application

Network Stack (BTP, ...)

Media Download (scenario 2)

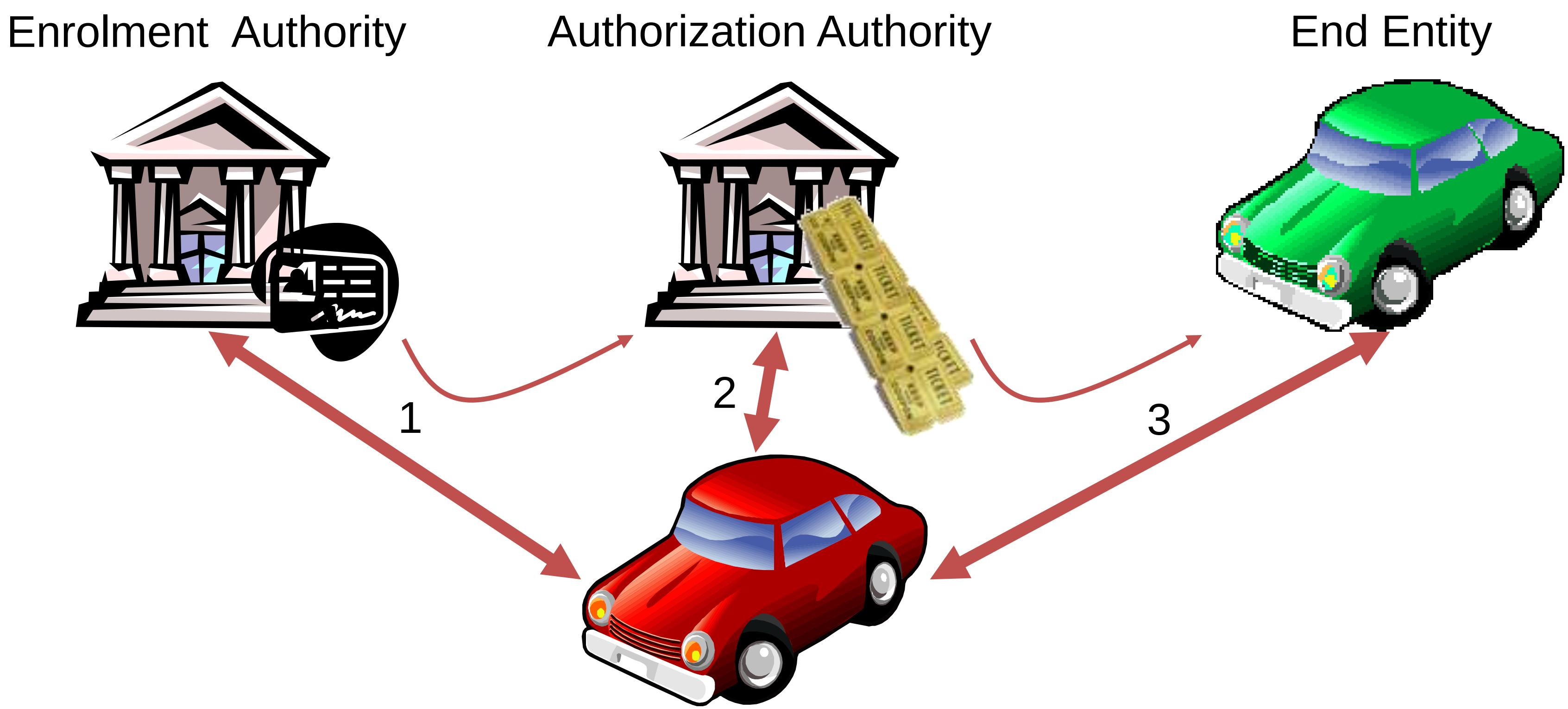
- WSIE advertises gateway to Media Download
- Multiple subscribers connect to a single AP
- n criber



Stage 2 Services (1)

- Enrolment – establish identity
  - Obtain, update, remove enrolment credentials
- Authorization – establish permissions
  - Obtain, update authorization ticket
  - Add / verify authorization on single message
- Security Associations
  - Establish, update, remove security association

Stage 2 Services: Enrolment and Authorization



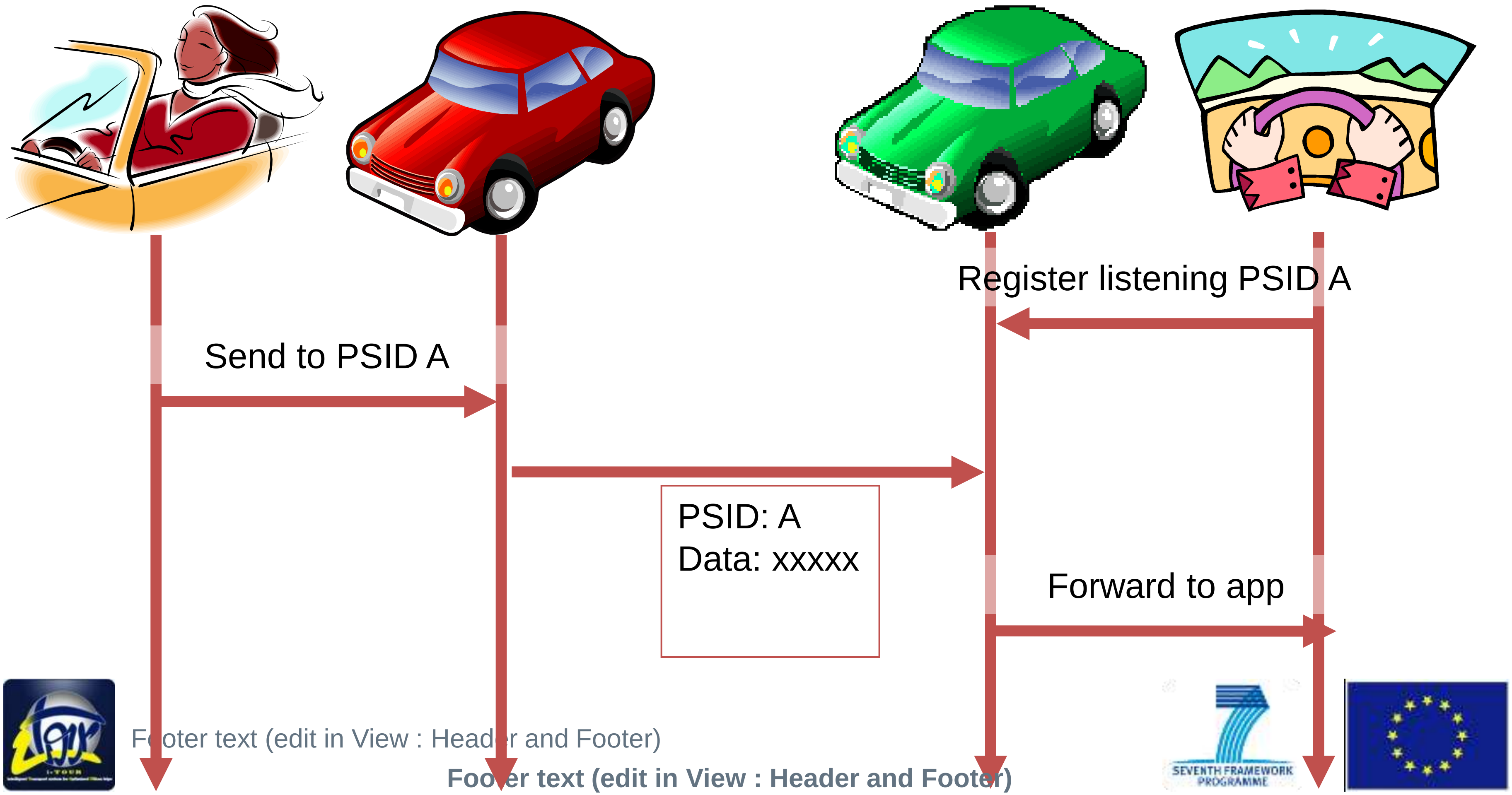
1609.2 Mapping: Services

ITS Stage 2	1609.2
Enrolment	Supported via CSR certificates
Authorization	Supported via messaging certificates
Security Association Management	Not supported
Authentication	Supported via messaging certificates
Confidentiality	Supported for single messages
	No support for secure sessions
Integrity	Supported via signing
Replay Protection	Supported via timestamping only
Accountability	Higher Level
Plausibility	Basic support / Higher Level
Remote Management	Higher Level
Report Misbehavior	Higher Level

1609.2 Security for broadcast messages

- Broadcast messages may be signed by the sender
- 1609.2 defines a custom, bandwidth-optimized signed message format including:
  - Application Identifier – Provider Service ID
  - (Optional) Generation time to prevent replay attacks / enable plausibility tests
  - (Optional) Expiry time to prevent replay attacks / enable plausibility tests
  - (Optional) Location to prevent translation attacks
  - Cert to attest that signing key has appropriate permissions.
- The options used by a specific sender and receiver are specified in the 1609.2 “Security Profile”
  - Profiles exist for SAE J2735 Basic Safety Message, Signal Phase and Timing, …

1609 system without security: WSMP and PSID



Privacy: identifiers

- Nothing in broadcast messages from private vehicles that identifies the specific vehicle
- No static, unique identifiers visible in RF transmissions
  - MAC address
  - IP or other network addresses
  - Certificates
- In practice we can’t have unlinkability between any pair of transmissions as transactions would be impossible
  - Clearly need rules to change reply-to addresses over time
  - Addressing information must be made available to layers that need it; additional information must be hidden unless the sender chooses to reveal it

Privacy v safety

- Safety: The LDM processing constructs the trajectories of other vehicles
  - These are constructed from vehicle speed / location
  - “Join the dots”
- Privacy: Don’t want an eavesdropper to reconstruct my path over a long distance
- Are there ways to improve privacy without impacting safety?

Privacy: Multi-application

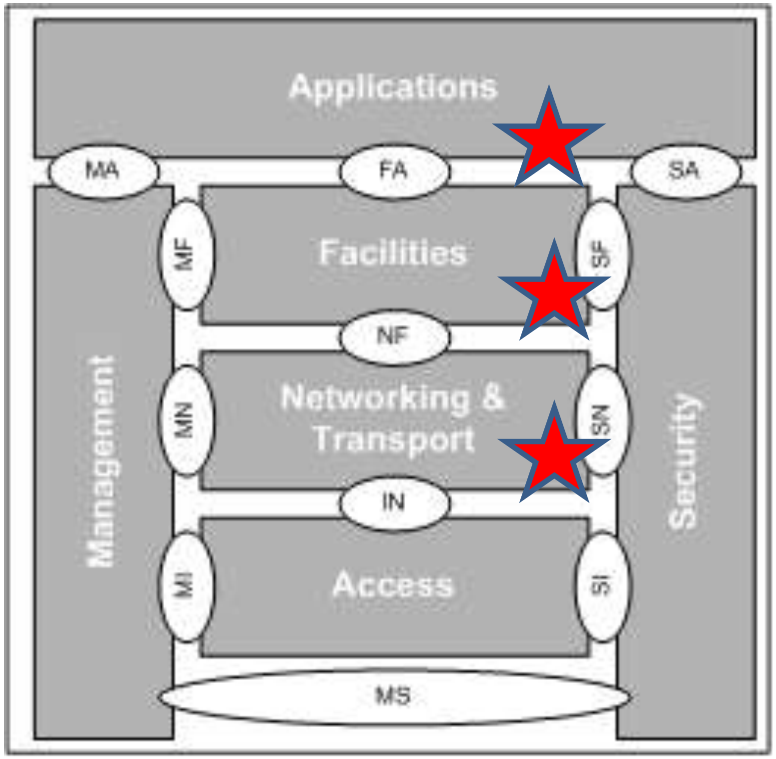
- If a private user interacts with separate services A and B, services A and B should not be able to tell it was the same user.
- A transaction with a user should not be linkable with the user’s vehicle
- An eavesdropper should not be able to use an ITS-S’s collection of applications to identify it

- Possible solution:
  - The user has a different cert for each service they use
    - Single PSID per service (or per group of services so long as all vehicles have that group)
  - Different networking identifiers for each service?
  - For further investigation

Privacy in 1609

- 1609.2
  - has a “hook” for an anonymous certificate format
    - VSC-3 / CAMP will provide anonymous certificate and CRL formats
  - does not address synchronized identifier changes
- 1609.4, Multi-Channel Operation
  - has a primitive to change MAC address
- 1609.0
  - Architecture document
  - Planned to integrate 1609.2 privacy mechanisms with identifier change and other station-level privacy services
  - Under development but proceeding slowly

Where to sign/verify in the stack?

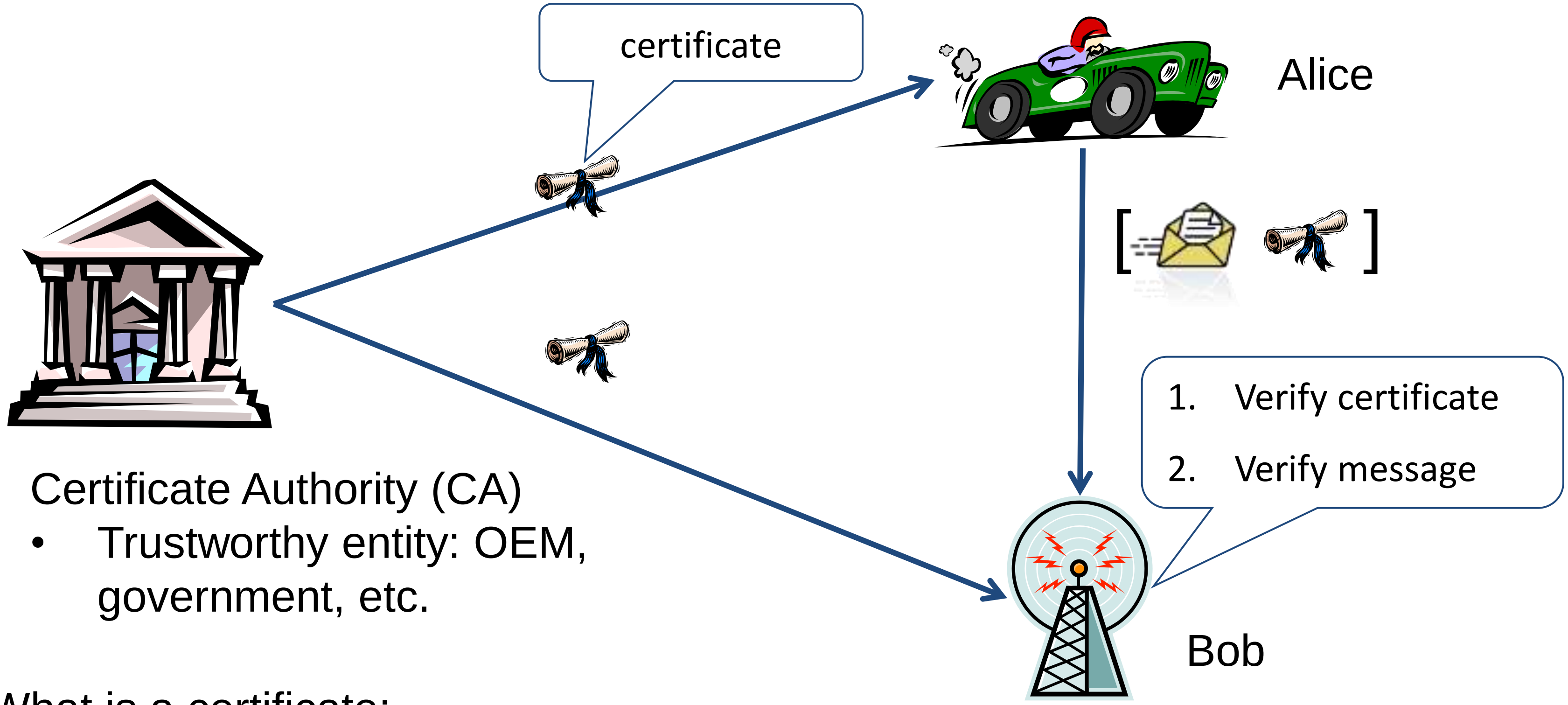


- Consider a strictly layered system
  - Sending application data comes only from application
  - Only one receiving application per receiving unit
  - Natural place to sign / verify is the application layer
    - Supports applications on remote processors
    - Improves privacy by allowing different applications to be distinct over the air
    - Allows applications to choose whether or not to verify based on payload
- ITS station architecture is not strictly layered in this sense
  - Geonetworking information is used by CAM
  - Multiple applications sit on facilities layer
  - Geonetworking may need to be secured – don’t want to sign a message twice
- For further investigation with WG2 / 3

Introduction and Open Issues

PUBLIC KEY INFRASTRUCTURE

PKI and Certificates



certificate

Alice

[✉ 📜]

1. Verify certificate
2. Verify message

Bob

Certificate Authority (CA)

- Trustworthy entity: OEM, government, etc.

What is a certificate:

- A signed (by the CA) public key (of Alice or Bob)
- A certificate binds an identity (Alice) and/or a role (e.g. emergency vehicle) to a public key
- Certificate(Alice) 📜 = [Alice, 🔑, Sig$_{CA}$(Alice, 🔑)

Certificate Authority

- CAs are the basis of PKIs
- There might be several CAs
  - Vehicle enrolment CA
  - Application specific CA (ticket authorization)
- All nodes must trust a CA
- CAs can be public and/or private
  - OEM CA
  - Verisign CA
  - European Union CA
  - National CAs
  - ...
- CAs can be designed hierarchically
  - EU root CA
  - National sub CAs

Problems and Opportunities

- The introduction of certificates
  - Provides protection against message tampering ✓
  - Offers removal of individual bad actors

☒

  - Introduces privacy problems
    - Nodes can potentially be tracked based on the certificate
  - Requires processes to determine identity of nodes before issuing a certificate

Privacy: Overview

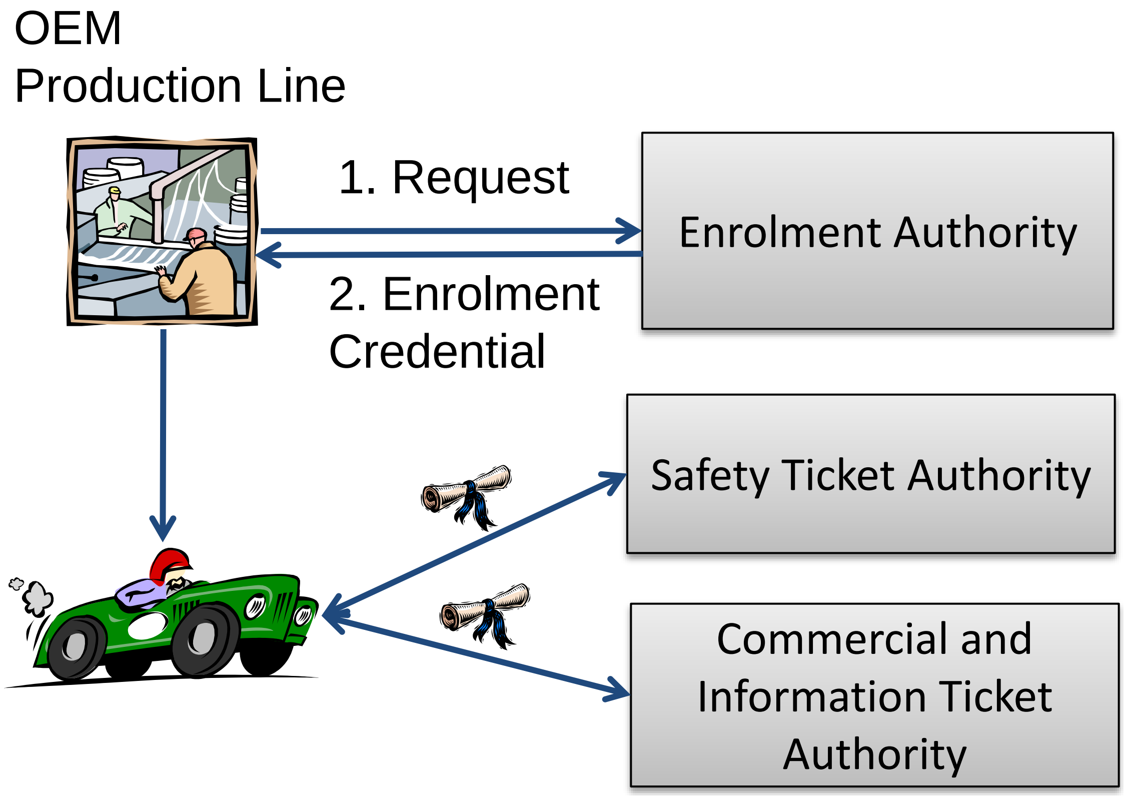
- There is tension between privacy and misbehavior detection & revocation
  - Revocation requires identification of misbehaving vehicles, thus discarding privacy of potentially misbehaving vehicles
  - A high level of privacy complicates identification of individual vehicles and eventually prohibits revocation
- Privacy can be split into 3 objectives:
  - Anonymity: no identifier in credentials
  - Short-term linkability: required by safety applications!
  - Long-term unlinkability: provided by changing credentials regularly
- The scope of privacy must be distinguished
  - Privacy against the authorities
  - Privacy against 3rd parties: is ensured by design (changing certificates)

Privacy: Overview (continued)

- Designing a solution that provides privacy against authorities is risky
  - National legislation might require access
  - Revocation of vehicles is prone to errors (false vehicles are revoked), slow (a vehicle can misbehave over a long time) or even impossible.
- *Big brother*: legislation might always overrule the design and require a change of design and/or organization, and force the CA to disclose secret keys.

- Suggestion
  - Provide a technical design that allows flexibility
  - Limit power on organizational level
  - Proposal: split the ability of the CA to disclose private data. For instance, the OEM‘s CA and national CA must collude to disclose private data and revoke a vehicle

CA Hierarchy: Example



OEM
Production Line

1. Request

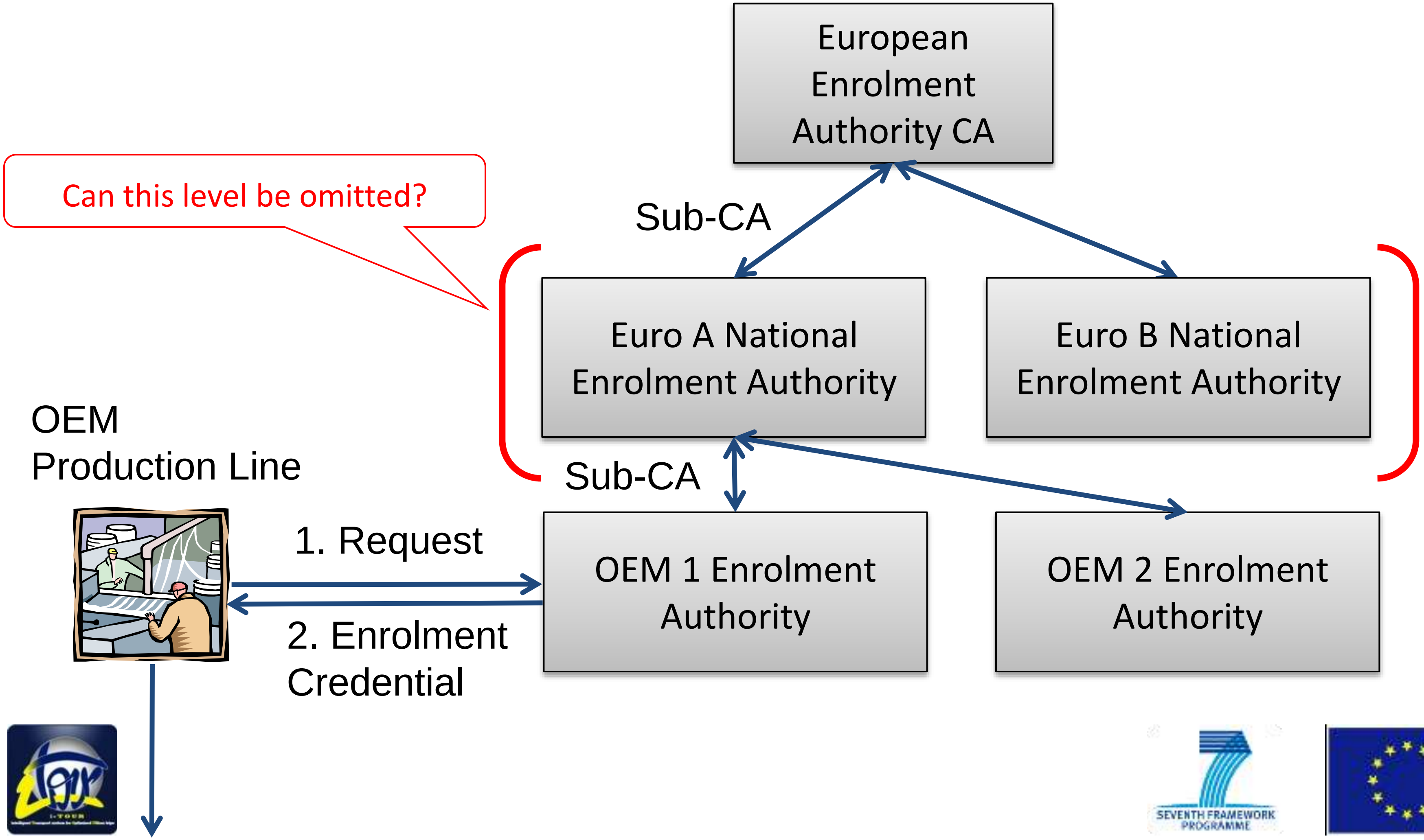
2. Enrolment
Credential

Enrolment Authority

Safety Ticket Authority

Commercial and
Information Ticket
Authority

Enrolment Authority: Example 2



European Enrolment Authority CA

Can this level be omitted?

Sub-CA

Euro A National Enrolment Authority

Euro B National Enrolment Authority

OEM
Production Line

Sub-CA

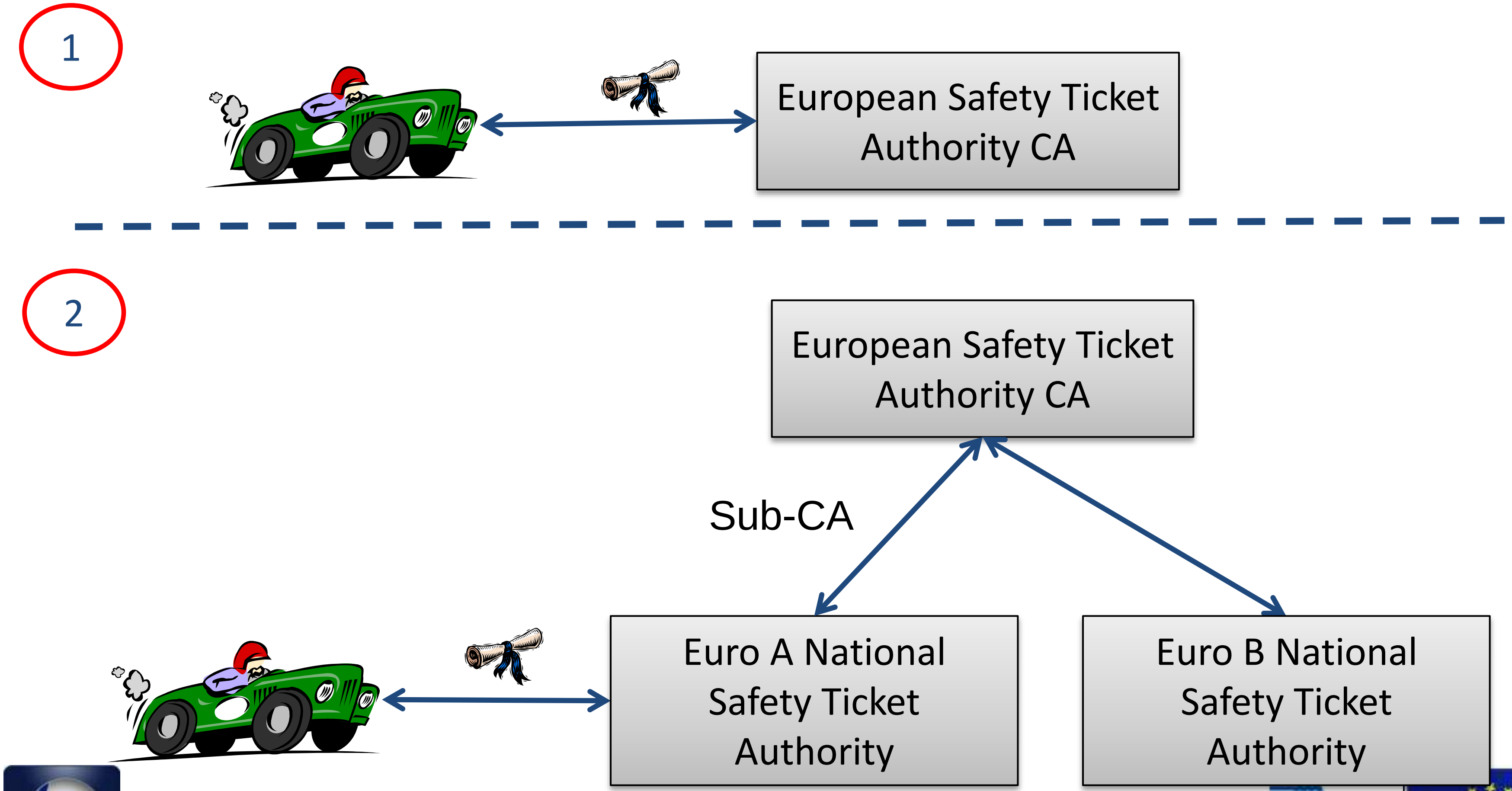
1. Request

OEM 1 Enrolment Authority

OEM 2 Enrolment Authority

2. Enrolment
Credential

Safety Ticket Authority: Example 1 & 2



1

European Safety Ticket Authority CA

2

European Safety Ticket Authority CA

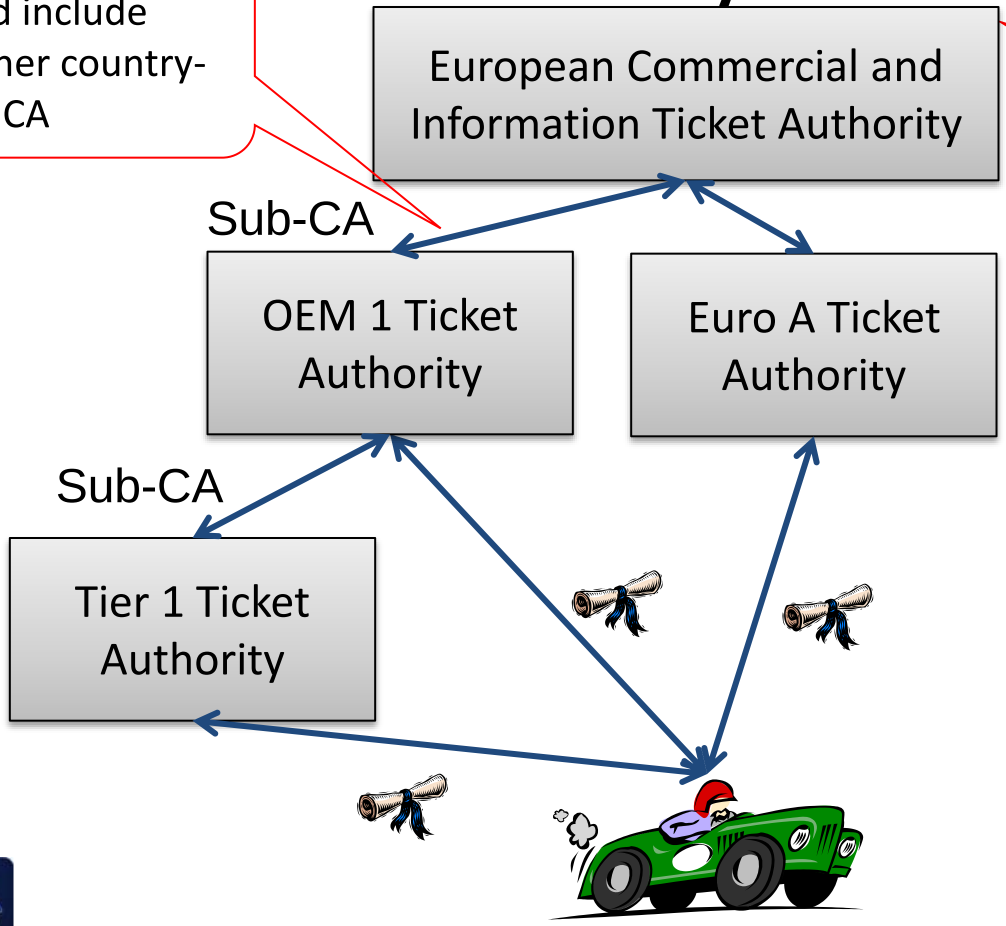
Sub-CA

Euro A National Safety Ticket Authority

Euro B National Safety Ticket Authority

Commercial and Information Ticket Authority: Example

Could include another country-level CA



Root authority certifies provider authorities (need to satisfy minimum requirements).

Then basically any structure is allowed

- OEMs offering services
- 3rd party service providers
- Government agencies
- etc.

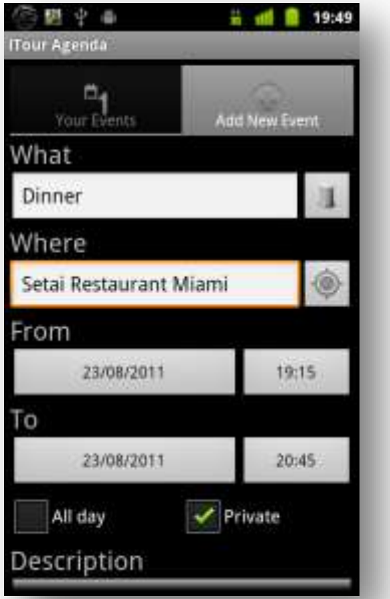
Challenges

- The accepted level of privacy must be defined
  - Involves (at least) national legislation and OEMs
- What happens with revoked vehicles?
  - Need a process to re-instantiate revoked vehicles or execute prosecution
- What happens with junked vehicles?
  - Need a process to deactivate radio or put vehicles on CRL
- Who organizes CA on European and national level?
  - Responsibility and power of European and national CAs must be defined.
  - Responsibility and power of commercial CAs must be included.
- Is a standard for misbehavior reporting required?
  - Message format from vehicles to CA

Integrating ITS to everyday living

- Google Calendar Integration
- Allows Custom Data (e.g. Rating)
- Stored on i-Tour DataBase to allow spatial queries
- Geolocalised Events shown and connected on the map

AM
Meeting with John and Anna



iTour Agenda

What
Dinner

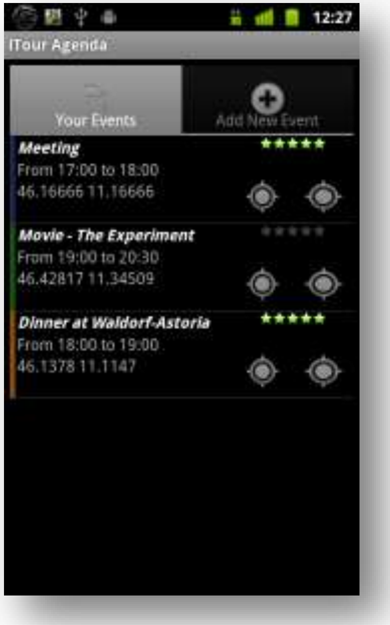
Where
Setai Restaurant Miami

From
23/08/2011 19:15

To
23/08/2011 20:45

□ All day ☑ Private

Description

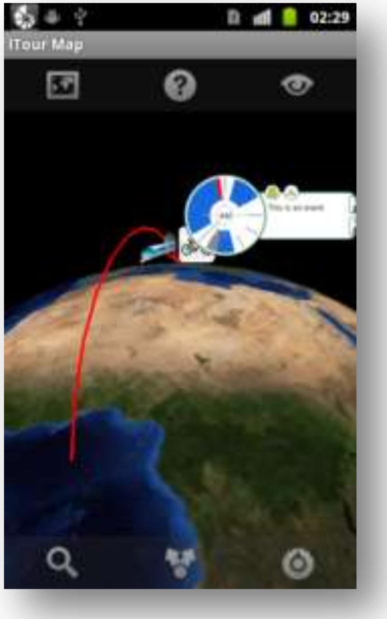


iTour Agenda

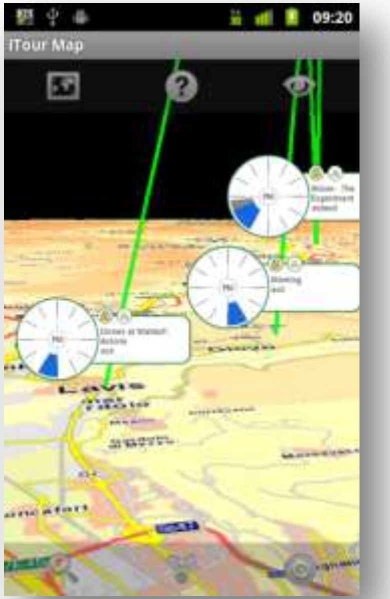
Meeting ★★★★★
From 17:00 to 18:00
46.16666 11.16666

Movie - The Experiment ★★★★★
From 19:00 to 20:30
46.42817 11.34509

Dinner at Waldorf-Astoria ★★★★★
From 18:00 to 19:00
46.1378 11.1147

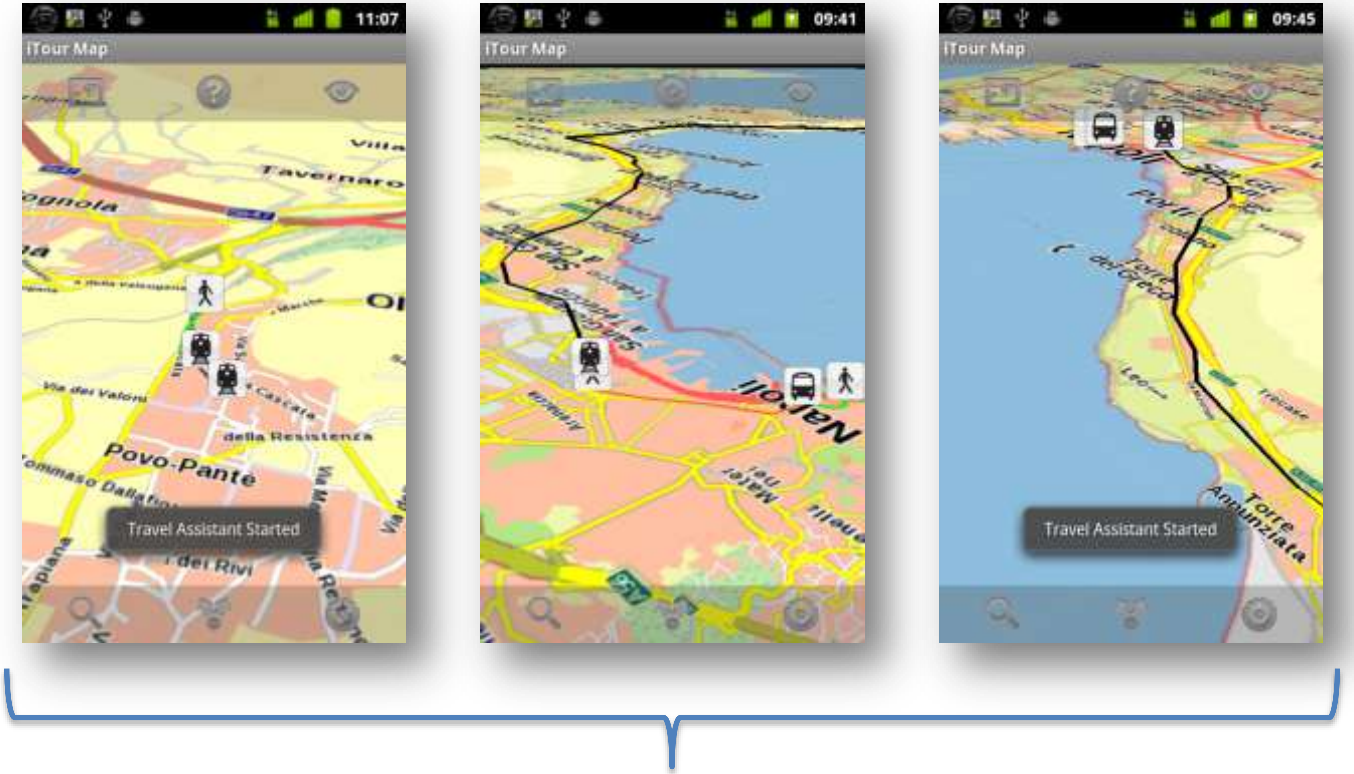


iTour Map



iTour Map

Routing function



3D view
(WMS Navteq Imagery)

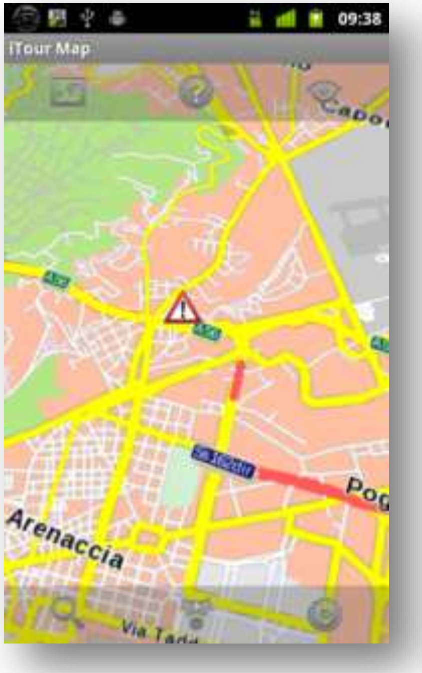
Augmented reality view

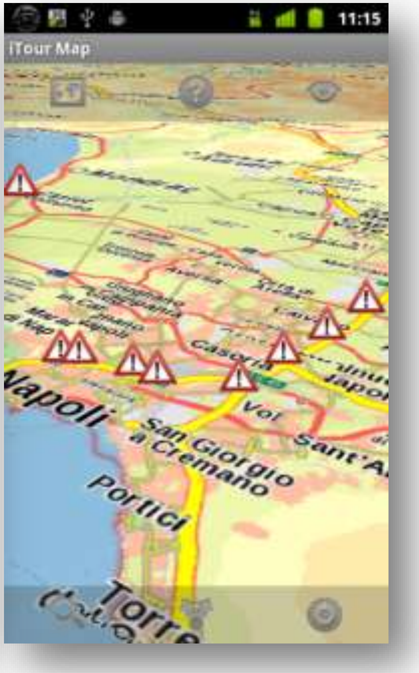
Localised real-time data

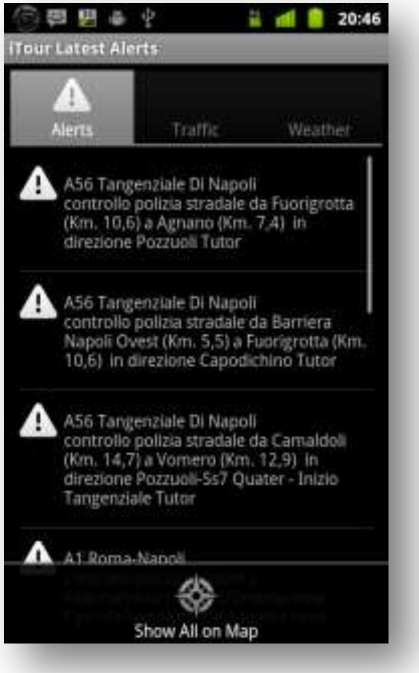
Alert visualisation from

MuoversiInCampania.it

This could use data from CAM and DENM too – an LDM?





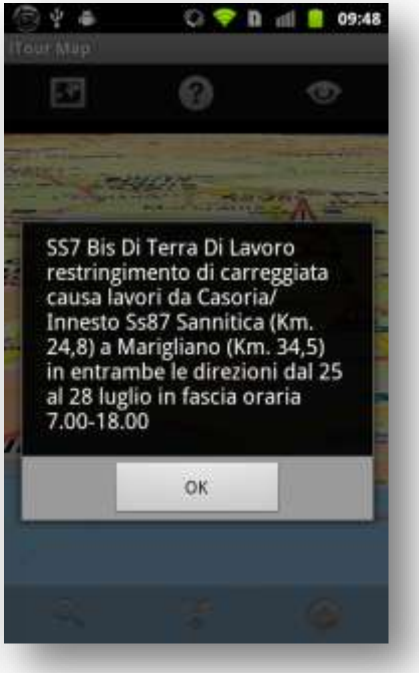


A56 Tangenziale Di Napoli
controllo polizia stradale da Fuorigrotta (Km. 10,6) a Agnano (Km. 7,4) in direzione Pozzuoli Tutor

A56 Tangenziale Di Napoli
controllo polizia stradale da Barriera Napoli Ovest (Km. 5,5) a Fuorigrotta (Km. 10,6) in direzione Capodichino Tutor

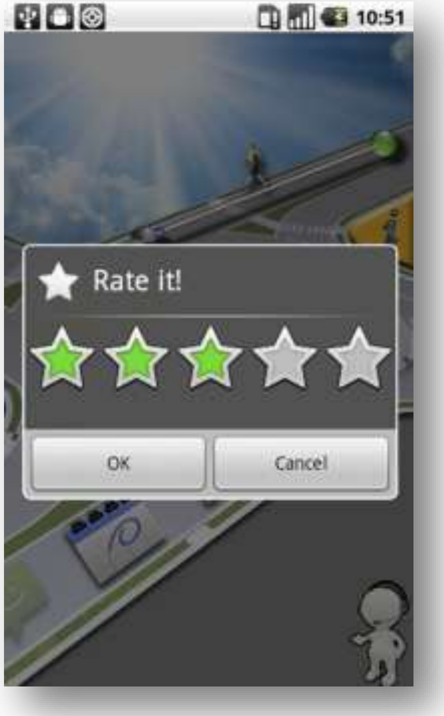
A56 Tangenziale Di Napoli
controllo polizia stradale da Camaldoli (Km. 14,7) a Vomero (Km. 12,9) in direzione Pozzuoli-Ss7 Quater - Inizio Tangenziale Tutor

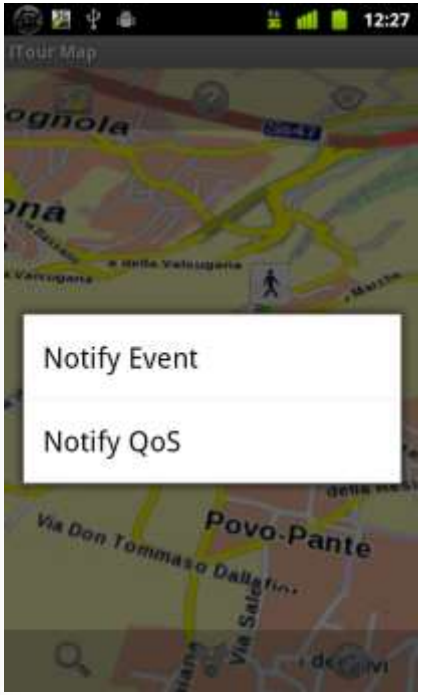
A1 Roma-Napoli



SS7 Bis Di Terra Di Lavoro restringimento di carreggiata causa lavori da Casoria/ Innesto Ss87 Sannitica (Km. 24,8) a Marigliano (Km. 34,5) in entrambe le direzioni dal 25 al 28 luglio in fascia oraria 7.00-18.00

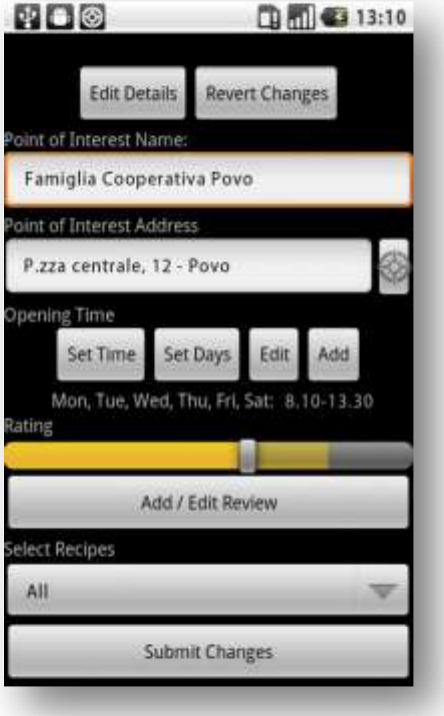
Crowdsourcing localised data





Notify Event

Notify QoS



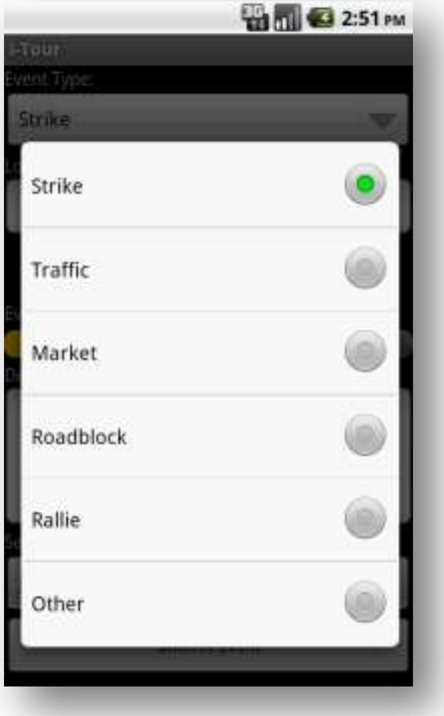
Point of Interest Name: Famiglia Cooperativa Povo

Point of Interest Address: P.zza centrale, 12 - Povo

Opening Time: Mon, Tue, Wed, Thu, Fri, Sat: 8.10-13.30

Rating

Select Recipes: All



i-Tour

Event Type: Strike

- ● Strike
- ○ Traffic
- ○ Market
- ○ Roadblock
- ○ Rallie
- ○ Other

A centralised (L)DM function may be seen as a crowdsourcing application

Conclusions

- Transport is societal and societies work through sharing knowledge and building from that shared base
- Trust is centred on learning from relationships
- Processing for complex systems needs to exist across the system
  - In ITS-Ss and in the core
  - Compliance is measured in the core

Acknowledgements

- The partners of the i-Tour consortium (see template)
- The work and analysis incorporated in this presentation has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under the Grant Agreement number 234239. The authors are solely responsible for it, it does not represent the opinion of the Commission, and the Commission is not responsible for any use that might be made of information contained therein

Thank you for your attention