Feasibility Assessment of EVI

with respect to Requirements, User Needs

and Economic Aspects

Work Package 4

Version 2.0

August 2004

Produced by EVI project consortium

EVI is co-financed by the European Commission DG TREN

Programme name:	GRANT by DG TREN
Project ID:	SUB-B27020B-E3-EVI-2002-S07.18393
Project acronym:	EVI
Project name:	Feasibility study on Electronic Vehicle Identification
Dissemination level[1]:	EVI consortium, EVI consultation group, DGTREN, can be widely circulated under the condition that no modifications are applied to the version as originally circulated by the project consortium

Title of document:	Feasibility assessment of EVI with respect to requirements, user needs and economic aspects
Work package:	WP 4
Author(s):	EVI project consortium
Project co-ordinator:	Oene Kerstjens (ERTICO) Tel: +32 2 400 07 39, fax: +32 2 400 07 01 E-mail: o.kerstjens@mail.ertico.com

Abstract: This report describes the third in a series of Work Packages (WP4) that together will form the feasibility study concerning the introduction of an EU-wide EVI system. Its aim is to assess the EVI system as described in the previous Work Packages.

In this report four functional levels have been distinguished. For each functional level a technological, security, economical, legal and social and political assessment is conducted. The result of this assessment is that each functional level is technical feasible. Moreover, all functional levels will improve correct vehicle identification (first order benefits). Besides, for all functional levels the benefits will outweigh the costs.

Keyword list: EVI, feasibility assessment

[1] This is either: Public, restricted to other programme participants, restricted to a group specified by the consortium, confidential

Document Control Sheet

Version history:

Version number	Date	Summary of changes
0.1	18-02-2004	Starting document WP4
0.2	20-02-2004	Parts of First draft WP4-document
0.3	24-03-2004	Parts of draft WP4-document
0.4	27-04-2004	Rough version first WP4-document
0.5	05-05-2004	First draft WP4-document
1.0	21-06-2004	Second draft conform the structure as discussed with the WP4-partners and Steering Committee
1.1	24-06-2004	Second draft including the comments from the consortium meeting
1.2	07-07-2004	Third draft including the comments from the consortium
1.3 and 2.0	15-07-2004	Fourth draft including the comments from the Steering Committee and review recommendations

Approval:

	Name	Date
Prepared	EVI project consortium	18-05-2004
1st approval	EVI Steering Committee	09-06-2004
Reviewed	EVI project consortium	22-06-2004
2nd approval	EVI Steering Committee	14-07-2004
Authorised	EVI Steering Committee	07-09-2004

Circulation:

Recipient	Date of submission
EVI consortium partners	22-06-2004
EVI Steering Committee	02-07-2004
EC for final report	07-09-2004

Table of Contents

EXECUTIVE SUMMARY

EVI (Electronic Vehicle Identification) is defined as a system that uniquely identifies a vehicle electronically. It can be further defined as an electronic device that allows the unique, remote and reliable communication of identifying parameters of a vehicle. It would typically comprise a secure in-vehicle data storage element, suitable and secure interfaces and a vehicle-to-infrastructure data communication element.

This EVI will be a telematics system in its own right, allowing the electronic identification of vehicles. In doing so, EVI can act as an enabler for a whole range of applications which need a vehicle identifier. EVI can enable these applications directly or via other in-vehicle systems.

EVI may also be used to provide certified vehicle parameters to other applications like electronic fee collection. The use of certified vehicle parameters may become an important (non-mandatory) enabling application. Such an application of EVI may or may not require any vehicle identification.

To conduct a feasibility assessment of EVI with respect to requirements, user needs and economic aspects, functional levels have been distinguished:

- Level 1: In-vehicle EVI components, that respond with a unique, reliable vehicle identity on request to another in-vehicle system or to a close-by (within 0 – 1 m[1]) EVI reader and/or writer.
- Level 2: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader over a longer distance, or respond to a request of this reader.
- Level 3: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader and/or writer over a longer distance, or interact with an EVI reader and /or writer via challenge response.
- Level 4: In-vehicle telematic platform, that provides a range of telecommunication capabilities to other in-vehicle systems and that can enable applications by sending a unique, reliable vehicle identity to an EVI reader and/or writer, or interacts with an EVI reader and /or writer via challenge response.

The main findings from the assessment are:

- Each functional level is technical feasible;
- A functional level (with a specific communication technology) can enable a set of public authority applications but not all applications can be enabled;

[1] Given the fact that the in-vehicle EVI components will be connected to other in-vehicle systems a communication range of 10 cm within the vehicle seems to be enough. The range of 1 m is necessary for hand-held EVI reader and/or writers.

- A weak spot in the security is the availability of the wireless I/O to the reader and/or writer which can be blocked. The minimum countermeasure to protect this weak-spot is to make the EVI reader and/or writer capable of notifying jamming of the communication between vehicles and/or writer;

- The VIN is a good candidate for the unique vehicle identifier, under the premise that the VIN will really be unique;

- In order to enable specific applications even in split seconds, a small set of vehicle data has to be stored in the vehicle, more then just a unique vehicle identifier;

- All functional levels will improve correct vehicle identification (first order benefit). Function level 2 – 3 are able to improve the efficiency of public authority applications aimed at fairness of road pricing and efficient use of available infrastructure using both moving and stationary vehicles (second order benefit). Functional level 1 is limited to stationary vehicles and therefore limited in benefits. All functional levels are EU-wide beneficial for road safety and reduction of vehicle crime; and

- In fact for all functional levels the benefits will outweigh the costs, although the payback time is long for functional level 1. Functional level 3 scores best in case of retrofit.

Given the results of the assessment it can be concluded that EVI is feasible and can contribute to the policy goals (improve road safety, efficient use of the road infrastructure, quality of environment, security and compliance with social rules) of the European Commission and Member States.

SUMMARY

OBJECT OF ASSESSMENT

EVI (Electronic Vehicle Identification) is defined as a system that uniquely identifies a vehicle electronically. It can be further defined as an electronic device that allows the unique, remote and reliable communication of identifying parameters of a vehicle. It would typically comprise a secure in-vehicle data storage element, suitable and secure interfaces and a vehicle-to-infrastructure data communication element.

This EVI will be a telematics system in its own right, allowing the electronic identification of vehicles. In doing so, EVI can act as an enabler for a whole range of applications which need a vehicle identifier. EVI can enable these applications directly or via other in-vehicle systems.

EVI may also be used to provide certified vehicle parameters to other applications like electronic fee collection. The use of certified vehicle parameters may become an important (non-mandatory) enabling application. Such an application of EVI may or may not require any vehicle identification.

In figure A the outline of the EVI-system is presented.

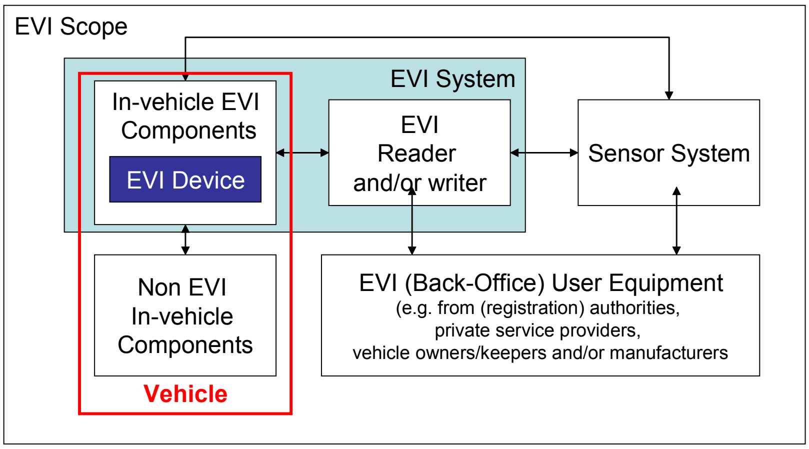


Figure A: EVI scope diagram (source: Work Package 2, EVI Feasibility Study)

The assessment of EVI is setup in 4 steps as presented in figure B that define the:

1. Functional levels of EVI;
2. Communication means for interaction between the EVI in-vehicle components and the EVI reader and / or writer;
3. Vehicle-related data distribution across the EVI device, the registration back office and the EVI reader and / or writer;
4. Deployment options for realising EVI pan-European.

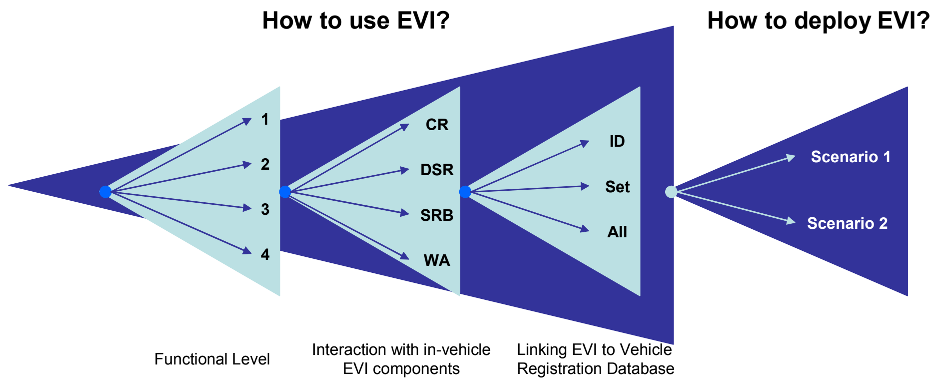


Figure B: Assemblage of the Objects of assessment.

Functional levels – step 1 -

The objects of assessment start with the functional levels which put the emphasis on the function of EVI: 'What is EVI and what can we use it for?'. Four functional levels have been distinguished:

Level 1: In-vehicle EVI components, that respond with a unique, reliable vehicle identity on request to another in-vehicle system or to a close-by (within 0 – 1 m[1]) EVI reader and/or writer.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components once and read many times;
- the in-vehicle EVI components form a passive device that responds to a request;
- the in-vehicle EVI components can only enable those application focusing on stationary vehicles directly;
- the in-vehicle EVI components can enable applications focusing on moving vehicles only indirectly via (an)other in-vehicle system(s)';
- vice versa, the in-vehicle EVI components can be used to provide certified vehicle parameters to other applications; and
- the in-vehicle EVI components does not need an human-machine interface (HMI), at most it needs an activity/diagnostic notification unit.

Level 2: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader over a longer distance, or respond to a request of this reader.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components once and read many times;
- the in-vehicle EVI components can enable applications that focus on stationary as well as moving vehicles directly;

[1] Given the fact that the in-vehicle EVI components will be connected to other in-vehicle systems a communication range of 10 cm within the vehicle seems to be enough. The range of 1 m is necessary for hand-held EVI reader and/or writers.

- the in-vehicle EVI components can be both active (send a vehicle identity) and passive (respond to a request of this reader and /or writer with a vehicle identity);
- since the distance between vehicle and reader and /or writer becomes bigger and vehicles might also be moving an activity/diagnostic notification unit may be needed; and
- since the in-vehicle EVI components enable application directly also in cases where the vehicle is moving, for some applications a human-machine interface is needed.

Level 3: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader and/or writer over a longer distance, or interact with an EVI reader and /or writer via challenge response.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components more than once and read many times;
- the in-vehicle EVI components can enable applications that focus on stationary as well as moving vehicles directly;
- the in-vehicle EVI components can be both active (sends a vehicle identity) and passive (responds to a request of this reader and /or writer with a vehicle identity);
- since the distance between vehicle and reader and /or writer becomes bigger and vehicles might also be moving an activity/diagnostic notification unit may be needed; and
- since the in-vehicle EVI components enables application directly also in cases where the vehicle is moving, for some applications a human-machine interface is needed.

Level 4: In-vehicle telematic platform, that provides a range of telecommunication capabilities to other in-vehicle systems and that can enable applications by sending a unique, reliable vehicle identity to an EVI reader and/or writer, or interacts with an EVI reader and /or writer via challenge response.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components more than once and read many times;
- the in-vehicle EVI components can enable applications that focus on stationary as well as moving vehicles directly;
- the in-vehicle EVI components can be both active (send a vehicle identity) and passive (respond to a request of this reader and /or writer with a vehicle identity);
- the in-vehicle EVI components are explicitly available to other in-vehicle components to offer telecommunication capabilities;
- since the distance between vehicle and reader and /or writer becomes bigger and vehicles might also be moving an activity/diagnostic notification unit may be needed; and
- since the in-vehicle EVI components enable applications directly also in cases where the vehicle is moving, for some applications a human-machine interface is needed.

The main findings from the assessment on the functional levels:

- Each functional level is technical feasible;
- The basics for security is to make the EVI device a secure device, in order to safeguard the integrity of the data send to the reader and/or writer. The security is increased even more in case of ‘Write once-Read many’;
- All functional levels will improve correct vehicle identification (first order benefit). Function level 2 – 3 are able to improve the efficiency of public authority applications aimed at fairness of road pricing and efficient use of available infrastructure using both moving and stationary vehicles (second order benefit). Functional level 1 is limited to stationary vehicles and therefore limited in benefits.

All functional levels are EU-wide beneficial for road safety and reduction of vehicle crime;

- In fact for all functional levels the benefits will outweigh the costs, although the payback time is long for functional level 1. Functional level 3 scores best in case of retrofit; and
- Public authorities will have to get used to EVI and have to upgrade their legacy systems to be enabled by EVI.

Interaction with in-vehicle EVI components – step 2 -

The functional characteristics of the external interface between the in-vehicle EVI components and the reader and/or writer have implications for EVI as a whole, for instance:

- The usability of EVI in terms of which applications can and cannot be enabled. This usability determines the benefits of EVI.
- The costs for EVI.

In order to understand the implications, we differentiate the characteristics of the external interface for each of the four basic functional levels. The following external interfaces are used:

- Close Range ('*close*' is between 0 - 1 m[1]);
- Dedicated Short Range ('*dedicated*' is the possibility to pin-point a vehicle, '*short range*' is in between 10- 30 and 100[2] m);
- Short Range Broadcast ('*broadcast*' is spread the information at certain moments in time, with a certain time interval in an area with a range of 0-at least 50 m); and
- Wide Area ('*wide area*' is connection-oriented over a wide area).

The main findings from the assessment on Interaction with in-vehicle EVI components are:

- A specific communication technology can enable a set of public authority applications but not all of them. By smart combining the communication technologies all applications can be enabled;

[1] Given the fact that the in-vehicle EVI components will be connected to other in-vehicle systems a communication range of 10 cm within the vehicle seems to be enough. The range of 1 m is necessary for hand-held EVI reader and/or writers.

[2] The factual limits for short range depend on the technology, for example 0-30m if microwave and 0-100m if infrared.

- A weak spot in the security is the availability of the wireless I/O to the reader and/or writer which can be blocked. The minimum countermeasure to protect this weak-spot is to make the EVI reader and/or writer capable of notifying jamming of the communication between vehicles and reader and/or writer.

Linking EVI to the Vehicle Registration Database – step 3 -

In fact there is a variety of possibilities available for the data distribution over the in-vehicle EVI components, reader and/or writer and Vehicle Registration Database in the back-office. The three basic options are:

1. Store all the data needed to support the applications in the in-vehicle EVI components;

2. Store a subset of the data in the in-vehicle EVI components and leave the rest of the data in the Vehicle Registration Database (in the back-office);

3. Keep all the data stored in the Vehicle Registration Database and store a basic, unique vehicle identifier in the in-vehicle EVI components only.

From an assessment point of view the capabilities of the external interface between the EVI reader and/or writer and the Vehicle Registration Database is of interest. After all, some applications need more data in the vehicle than just a unique vehicle identity. In case of moving vehicles this means a request-response operation within seconds or even split seconds. So the response times of the Vehicle Registration Databases determine more or less the best options for the distribution of the vehicle data. Vice versa, a choice for the distribution of the vehicle data determines (amongst others) the needed response times of the Vehicle Registration Databases.

The main findings from the assessment on linking EVI to the vehicle registration database are:

- By storing the set of vehicle (component) identifiers in the EVI device, a fast and simple cross-check of the vehicle status is possible.

- The VIN is a good candidate for the unique vehicle identifier, under the premise that the VIN really will be unique.

- In order to enable specific applications even in split seconds, a small set of vehicle data has to be stored in the vehicle, more then just a unique vehicle identifier.

- The major part of the data can be kept at the back-office, under the premise that an EVI reader and/or writer can receive the data in seconds after sending a request.

- Just as with the licence plate confidentiality should be guarded by the back-office.

Deployment of EVI – step 4 -

For the deployment of EVI, a large number of deployment scenarios are possible. For the assessment we have used two more or less likely scenarios, namely (figure C):

- Assessment deployment scenario 1: Starting with an EVI on basic functional level (2), mandatory for all, at once, using a common standard. Given this solid basis, EVI can grow further on a voluntary basis towards a complex version on functional level (4).
- Assessment deployment scenario 2: Starting with an EVI on basic functional level (2), mandatory for all, however this time in phases, using a common standard. The solid basis for further development has to grow over the years. Once there is a solid basis of equipped vehicles it will become mandatory to upgrade all at once the EVI system to a more complex version on functional level (4), using a common standard.

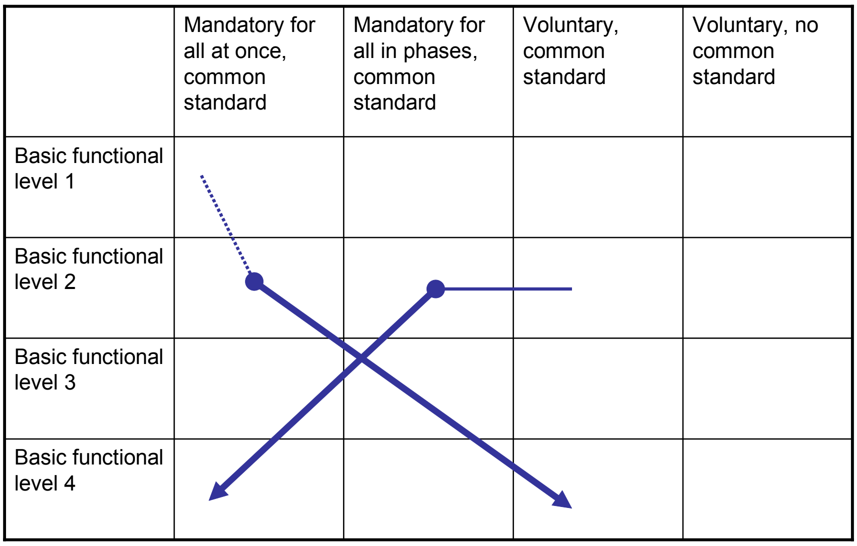


Figure C: Deployment scenarios which are part of the object of assessment.

Both scenarios do have a mandatory EVI as starting point. In fact this is the assumption used in the assessment in order to understand the full complexity of EVI. Later on (in Work Package 5) we should also consider starting on a voluntary basis. The advantage of starting on a voluntary basis is that it will give the public authority more time to upgrade the own organisation, gain support and acceptance of the vehicle (registration) owners, issue the in-vehicle EVI components, in other words it might be less complex.

The main findings from the assessment on the deployment issues are:

- The complexity of installing the in-vehicle EVI components increases from level 1 to level 4.
- The life cycle of EVI should be covered via secure environments, despite of the basic functional level.
- Functional level 2 might ask for an organisation to roll out gantries with EVI readers and/or writers.
- The deployment scenarios do have different timelines, and therefore will have different payback times.
- It is interesting to combine the rollout of EVI with starting to use EVI and therefore gaining the benefits from EVI from start on.
- By smart rollout of EVI immediate usage of EVI may be possible, which helps to reduce the payback time.

IS EVI FEASIBLE?

In the world of intelligent transport systems (ITS) new ideas and concepts come and go. In order to find out whether EVI is a realistic concept, and a concept that is worth implementing, the following questions need to be answered:

- What benefit(s) can EVI deliver above and beyond the existing mechanisms for identifying individual vehicles?
- What are the possibilities to actually improve the reliability of the unique vehicle identity and the vehicle identification?
- Do the identified benefits that can be derived from EVI outweigh the costs of implementation and operation (regarding the way(s) of deployment);
- What are the possibilities and barriers to realise EVI from a technological point of view?
- What are the possibilities and barriers to deploy EVI on a European and / or nation wide basis?
- What legal barriers are to be expected when deploying EVI?
- What social and political barriers are to be expected when deploying EVI?

What are the possibilities and barriers to realise EVI from a technological point of view?

EVI can fulfil its basic technological premises (as identified in Work Package 2), needed to enable (support) the public authorities applications. However, the actual capabilities (deficiencies besides the possibilities) of the available or planned wireless communication technologies used to realise the in-vehicle EVI components can form a barrier to enable all applications. Not every communication technology or even combination of communication technologies can enable all the applications. Therefore a careful selection of communication technologies is necessary when the final Realization Type of EVI is assembled.

Some public authority applications need a HMI to pass on information to the vehicle driver. The in-vehicle EVI components have to be linked to such a HMI in order to be able to enable (support) these applications.

Some public authority applications need precise pinpointing of the vehicle. In case a communication technology is used that does not support the exact pinpointing of a vehicle, a link to an external localisation unit should be provided.

'What are the possibilities to actually improve the reliability of the unique vehicle identity and the vehicle identification?'

By embedding security in the complete life cycle of EVI, the reliability of the unique vehicle identity and the vehicle identification can be improved. However, even with EVI it is realistic to expect impostors to fraud the EVI system or to misuse the EVI system and violate the privacy of the vehicle (registration) owners. On the other hand there are quite some possibilities to take countermeasures to protect EVI for such fraud and threat of privacy.

Issues left over after exploring those countermeasures are:

- Interrupting the availability of the in-vehicle EVI components by a vehicle (registration) owner (and/or driver). Surveillance teams are needed to discover these impostors.
- The protection of the integrity and confidentiality (in case all data is stored in the in-vehicle EVI components) will weaken during the lifetime of the in-vehicle EVI components. Regular (e.g. once in the four years) deinstallation and reinstallation of new in-vehicle EVI components is needed if we want to keep the protection on the same level.

The countermeasures for both issues will increase the costs for EVI and therefore will influence the 'business case' of EVI.

What are the possibilities and barriers to deploy EVI on a European and / or nation wide basis?

In principle EVI can be deployed on a nation or European wide basis. However it should be understood that EVI certainly has impact on the institutions needed for a properly operating (distribution of data), secure and environmental acceptable EVI. The seriousness of this impact depends to a large extent on the way the vehicle registration is organised in a country nowadays. This seriousness might be a barrier for the deployment of EVI nationally or Europe wide.

For example, the impact will be manageable in countries where the licence plate is under strict control. Many of the organisations already exist and only need to be upgraded to organisations that are able to deal with electronic devices and security key management. While in countries where the licence plate is not under a strict control yet, a more complex upgrade of the organisation will be necessary.

Another example; in countries where the vehicle registration database does already cover the items of Directive 1999/37/EC and does already posses of a real-time (seconds), external interface for challenge-respond with EVI reader and/or writer, the impact of EVI will be manageable again. On the other hand, in countries where the vehicle registration database does not cover al relevant data yet and/or does not posses of such a real-time (seconds), external interface, a more complex upgrade of the vehicle registration database will be needed.

So the severity of the institutional impact should be considered per country when starting the preparations for the introduction of EVI. In fact the differences between the Member States do form a barrier to deploy EVI on a European wide basis.

What benefit(s) can EVI deliver above and beyond the existing mechanisms for identifying individual vehicles?

Do the identified benefits that can be derived from EVI outweigh the costs of implementation and operation (regarding the way(s) of deployment)?

EVI is economically feasible dependent on the applications that are supported and the policy goals that are aspired. Dependent on these desires a final conclusion could be drawn whether EVI is economically feasible or not.

EVI comes with three kinds of benefits:

- First order of benefits: improvement of correct vehicle identification;
- Second order of benefits: improved efficiency in enabling applications, and
- Third level of benefits: these are the benefits of the applications which can be enabled (supported) by EVI directly (e.g. tracking of missing vehicles, road safety via enforcement)

The *first order benefits* are inherent to EVI. They are not only an economic factor but also an ethical factor ('all vehicle owners do have the same obligations towards the public authorities').

The second order of benefits consists of:

- Benefits due to reduction of system costs;
- Benefits due to efficiency of vehicle identification; and
- Benefits due to effectiveness of traffic management measures.

In all cases the benefits of EVI outweigh the cost, if EVI was deployed on a regional basis. To be precise in the region where massive vehicle identification is needed due to road pricing schemes, or where a more efficient use of the available infrastructure is needed. These types of benefits are not a justification for nation, or Europe wide deployment of EVI.

The third order of benefits reflects the benefits applicable for all the European Union Member States. These benefits concern road casualties and reduction of stolen vehicles. Again benefits of EVI outweigh the cost, be it that the payback time varies between 7 and more than 25 years, depending on the basic functional level of EVI.

Table A: Costs of functional levels over a period of 25 years.

	Manufacturing costs			Installation costs			Infrastructure costs	Commu-nication costs	Total
	Existing vehicles	New vehicles	Total	Existing vehicles	New vehicles	Total			
Functional level 1	1.655.970.822	2.237.306.806	3.893.277.628	0	0	0	555.018.207	0	4.448.295.834
Functional level 2	3.187.825.320	4.474.613.612	7.662.438.932	2.789.347.155	3.915.286.910	6.704.634.065	1.736.210.709	0	16.103.283.707
Functional level 3	7.969.563.301	11.186.534.029	19.156.097.330	5.578.694.310	7.830.573.821	13.409.268.131	1.736.210.709	0	34.301.576.170
Functional level 4	14.519.963.406	22.373.068.059	36.893.031.465	10.163.974.384	15.661.147.641	25.825.122.026	2.359.287.916	12.822.897.822	77.900.339.229

Table B: Benefits of functional levels over a period of 25 years.

	Road fatalities	Vehicle theft	Total
Functional level 1	1.146.580.122	1.144.841.228	2.291.421.350
Functional level 2	10.761.489.487	10.745.168.691	21.506.658.179
Functional level 3	53.807.447.435	21.490.337.383	75.297.784.818
Functional level 4	91.508.499.421	45.684.859.153	137.193.358.574

Table C: Overview of costs and benefits of functional levels over a period of 25 years.

	Manufacturing costs	Installation costs	Infrastructure costs	Communication costs	Total	Road fatalities	Stolen vehicles	Total	Cost-benefit ratio	Cost minus benefits	Payback
Functional level 1	3.893.277.628	0	555.018.207	0	4.448.295.834	1.146.580.122	1.144.841.228	2.291.421.350	1.94	2.156.874.485	> 25 years
Functional level 2	7.662.438.932	6.704.634.065	1.736.210.709	0	16.103.283.707	10.761.489.487	10.745.168.691	21.506.658.179	0.75	-5.403.374.472	14 years
Functional level 3	19.156.097.330	13.409.268.131	1.736.210.709	0	34.301.576.170	53.807.447.435	21.490.337.383	75.297.784.818	0.46	-40.996.208.648	7 years
Functional level 4	36.893.031.465	25.825.122.026	2.359.287.916	12.822.897.822	77.900.339.229	91.508.499.421	45.684.859.153	137.193.358.574	0.57	-59.293.019.345	11 years
	Copied from table A					Copied from table B			Newly calculated		

All in all, EVI is economically feasible depending on the political priorities for implementation of public authority applications.

With respect to the costs of introducing EVI in society, it should be stated that the costs do not only consist of implementing the EVI device in the vehicle. Realising the roadside infrastructure and improving back-office systems are additional costs for realising EVI in Europe. These costs will increase the pay back time for EVI.

What legal barriers are to be expected when deploying EVI?

In fact there are no real legal barriers for the introduction of EVI with respect to the existing legal framework. The reality however will be that while introducing EVI the legal framework will change due to test cases for court and new to be developed jurisprudence.

What social and political barriers are to be expected when deploying EVI?

From social point of view a lack of public support for and acceptance of the introduction of EVI can be foreseen, due to the following reasons:

- The cost for EVI are concrete for the individual vehicle (registration) owner, where the benefits are abstract (efficient, effective, policy goals); and
- The efficiency of EVI might give vehicle owners the impression public authorities will start to track them wherever they are ('big brother is watching you').

Furthermore there is the risk that the efficiency of EVI gives vehicle owners the impression that the level of enforcement and road pricing will increase.

From political point of view a lack of support for and acceptance of the introduction of EVI can be foreseen, due to the following reasons:

EVI implies that the vehicle registration should be improved in a specific country and therefore brings costs first; and

EVI implies that a set of secure environments (see security assessment) have to be installed and again brings costs first.

1 INTRODUCTION

1.1 THE ROOTS FOR EVI

All economic regions within Europe are dealing with a decreasing performance of their road network while the demand for transport has increased and is expected to increase even further. The match between road infrastructure and supply is getting more and more out of balance, resulting in increasing problems of congestion, delays, reliability, traffic safety and quality of the environment. The possibilities to construct additional infrastructure are limited and moreover expansion of the infrastructures more or less serves to meet latent demand for (auto)mobility. Hence, it is not a sustainable solution to congestion. Still there is increasing pressure for change (see Work Package 2). Within the European Commission and Member States action is being taken to:

- Improve traffic safety;
- Reduce the environmental impact of road traffic;
- Enhance an efficient use of the existing infrastructure; and
- Fair road pricing.

In addition the European Union and Member States are working to reduce crime and criminality including terrorism and vehicle crime.

In order to fulfil these policy goals public authorities have a whole range of measures at their disposal. For instance, enhancement of traffic safety requires *safer vehicles and safer driving* in order to prevent accidents and injuries in cases where accidents do occur. Inspections of both the safety of the vehicle and the safety of driving can contribute to road safety by raising awareness, standards and compliance to social rules. Where an incident occurs, efficient *incident management* saves lives and reduces the severity of injuries in the so called 'golden hours' and reduces congestion in the area and on diversion routes.

Enhancement of the environment requires *acceptable emissions from individual vehicles* as well as managing the overall emission levels of the traffic (see below). As for road safety, inspections of the state of the vehicle can raise standards and compliance with regulations. With respect to reducing risk for the surroundings of the road (and with respect to security) proper controls of hazardous goods transport bring significant benefits.

These are just two examples of the tasks which might be executed by the public authorities when trying to realise the (European and national) policy goals. In a lot of these tasks the identity of the vehicle and/or owner is rather essential in order to stimulate compliance to the social rules coming with the tasks. Traditionally over the last hundred years the identification of motor vehicles is done through license plates and later with the registration of the vehicles. The technology allow us to explore more advanced systems to identify cars. Electronic Vehicle Identification (EVI) is meant to be such a system.

1.2 THE RATIONALE OF ELECTRONIC VEHICLE IDENTIFICATION

EVI (Electronic Vehicle Identification) is defined as a system that uniquely identifies a vehicle electronically. It can be further defined as an electronic device that allows the unique, remote and reliable communication of identifying parameters of a vehicle. It would typically comprise a secure in-vehicle data storage element, suitable and secure interfaces and a vehicle-to-infrastructure data communication element.

This EVI will be a telematics system in its own right, allowing the electronic identification of vehicles. In doing so, EVI can act as an enabler for a whole range of applications which need a vehicle identifier. EVI can enable these applications directly or via other in-vehicle systems.

EVI may also be used to provide certified vehicle parameters to other applications like electronic fee collection. The use of certified vehicle parameters may become an important (non-mandatory) enabling application. Such an application of EVI may or may not require any vehicle identification.

In figure 1.1 the outline of the EVI-system is presented.

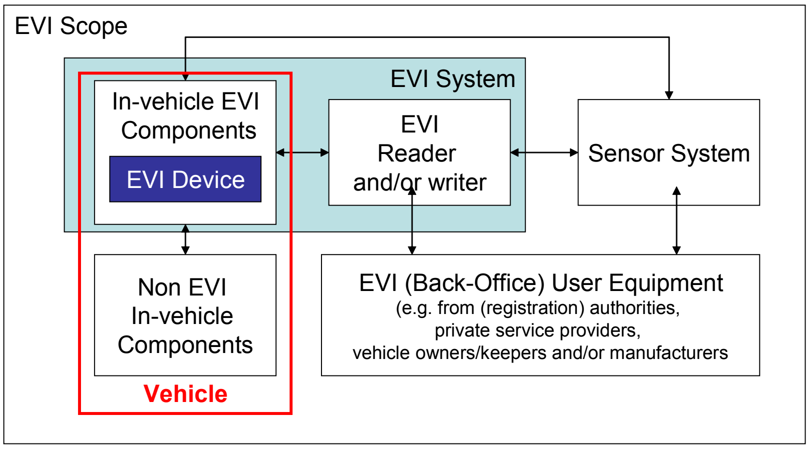


Figure 1.1: EVI scope diagram. (source: Work Package 2, EVI Feasibility Study)

The relevant public authority applications that can be enabled by EVI have been determined in Work Package 2. Annex A contains a set of relevant public authority applications. For each application a range of potential theoretical and realisable benefits are described. In addition, the necessary steps to implement the public authority application, the minimum dataset that should be stored in the vehicle and the added value of the application are specified.

In the world of intelligent transport systems (ITS) new ideas and concepts come and go. In order to find out whether EVI is a realistic concept, and a concept that is worth implementing, the following questions need to be answered:

- What benefit(s) can EVI deliver above and beyond the existing mechanisms for identifying individual vehicles?
- What are the possibilities to actually improve the reliability of the unique vehicle identity and the vehicle identification?
- Do the identified benefits that can be derived from EVI outweigh the costs of implementation and operation (regarding the way(s) of deployment);
- What are the possibilities and barriers to realise EVI from a technological point of view?
- What are the possibilities and barriers to deploy EVI on a European and / or nation wide basis?
- What legal barriers are to be expected when deploying EVI?
- What social and political barriers are to be expected when deploying EVI?

The assessment part of this study (part B) deals with each of these questions. Part A first deals with the definitions to determine the objectives that need to be assessed.

1.3 Structure of the Assessment of EVI

The assessment of EVI is executed in four phases, namely:

1. Definition of the Functional Types of EVI;
2. Definition of Deployment Scenarios for EVI;
3. Actual assessment of EVI; and
4. Indicating the realistic options for EVI.

The phases 1 and 2 are preparation steps for the actual assessment and are documented in part A. Part B of this document covers phases 3 and 4.

Part A. 'What are the Objects of Assessment?'

Functional Types of EVI for the Assessment

2 Functional types of EVI for the Assessment

2.1 Entry Point to define the Functional EVI Types

Functional types for EVI can be defined from more than one point of view. In Work Package 3 'High level architecture, technology options and realization options' functional types have been defined as a logical step towards possible realisation types of EVI (i.e. functional types filled out with the communication technologies as drawn up). In Work Package 4 we need functional levels which put the emphasis on the function of EVI: '*What is EVI and what can we use it for?'*

As entry point for the definition of the functional types three reflections have been used, namely:

- What is the 'raison d'être' of EVI?
- How to interact with the In-vehicle EVI components?
- How should EVI be linked to the Vehicle Registration Database?

These reflections are the subject of the next two sections.

2.2 Reflection 1: What is the 'raison d'être' of EVI?

From the results of Work Package 2 'EVI Requirements and user needs' the following basic premises (or basic reasons) for EVI have been identified:

1. EVI enables interaction with a uniquely identified vehicle in a number of applications, remotely, securely and efficiently;
2. EVI improves the vehicle registration process by improving the reliability of the unique vehicle identity[1]; and
3. Interaction with a uniquely identified vehicle brings possibilities to contribute to European and national policy goals (improve road safety, efficient use of the road infrastructure, quality of environment, security and compliance with social rules).

[1] The objective of the registration process is to come with a correct and complete registration of the vehicle in a certain region or state. Tampering the vehicle identity (allocated to the vehicle during the vehicle registration process) is a serious barrier for the registration process to realise its objective. Vice versa, improving the reliability of the vehicle identity helps the registration process.

Especially the first premise can be used as a starter to define the basic, functional levels of EVI for the assessment. For the sake of the assessment, we define a functional level as: 'the EVI system as it will be introduced and that can (at a certain moment in the future) enable a number of applications by identifying or addressing a specific vehicle'. In this functional level a whole series of choices are captured. We take the following choices in consideration (figure 2.1):

- Read – write capability (write once – read many , versus write many – read many);
- Communication range (close range, short range, wide area);
- Link to the vehicle driver (own human-machine interface (HMI) or linked to external HMI);
- Active (in-vehicle EVI components send the vehicle data by itself) or passive (responds to a request);
- Stationary of Moving vehicles.

All functional levels are based on the assumption that the application logics are fully at the road side, i.e. the in-vehicle EVI components does not run part of the application.

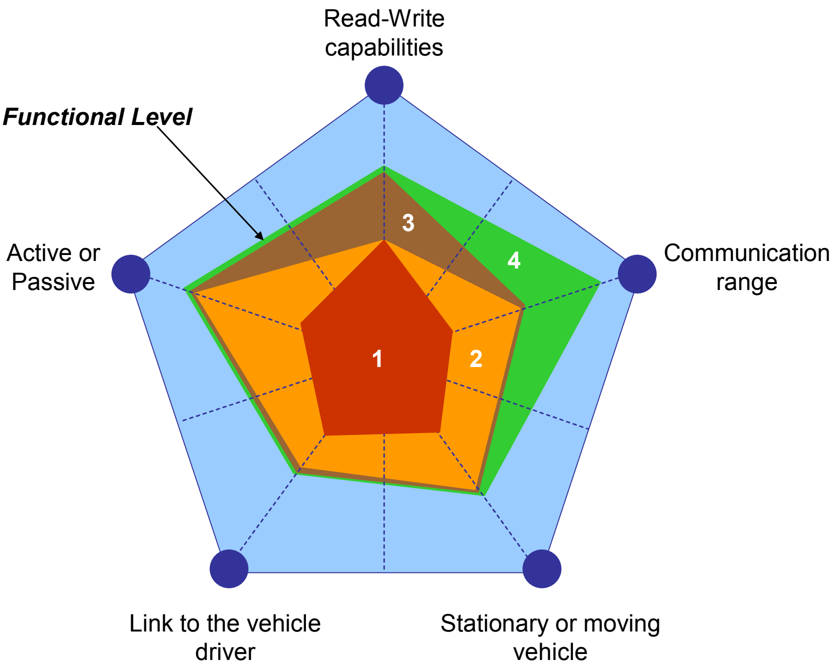


Figure 2.1: Pallet of possible functional levels for EVI.

To keep the complexity of the assessment manageable, the following four levels are in fact levels of increasing complexity:

Level 1: In-vehicle EVI components, that respond with a unique, reliable vehicle identity on request to another in-vehicle system or to a close-by (within 0 – 1 m[1]) EVI reader and/or writer.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components once and read many times;
- the in-vehicle EVI components form a passive device that responds to a request;
- the in-vehicle EVI components can only enable those application focusing on stationary vehicles directly;
- the in-vehicle EVI components can enable applications focusing on moving vehicles only indirectly via (an)other in-vehicle system(s)';
- vice versa, the in-vehicle EVI components can be used to provide certified vehicle parameters to other applications; and
- the in-vehicle EVI components does not need a human-machine interface (HMI), at most it needs an activity/diagnostic notification unit.

Level 2: In-vehicle EVI components, that send a unique, reliable vehicle identity to a EVI reader over a longer distance, or respond to a request of this reader.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components once and read many times;
- the in-vehicle EVI components can enable applications that focus on stationary as well as moving vehicles directly;
- the in-vehicle EVI components can be both active (send a vehicle identity) and passive (respond to a request of this reader and /or writer with a vehicle identity);
- since the distance between vehicle and reader and /or writer becomes bigger and vehicles might also be moving an activity/diagnostic notification unit may be needed; and
- since the in-vehicle EVI components enable application directly also in cases where the vehicle is moving, for some applications a human-machine interface is needed.

Level 3: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader and/or writer over a longer distance, or interact with an EVI reader and /or writer via challenge response.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components more than once and read many times;
- the in-vehicle EVI components can enable applications that focus on stationary as well as moving vehicles directly;
- the in-vehicle EVI components can be both active (sends a vehicle identity) and passive (responds to a request of this reader and /or writer with a vehicle identity);
- since the distance between vehicle and reader and /or writer becomes bigger and vehicles might also be moving an activity/diagnostic notification unit may be needed; and
- since the in-vehicle EVI components enables application directly also in cases where the vehicle is moving, for some applications a human-machine interface is needed.

[1] Given the fact that the in-vehicle EVI components will be connected to other in-vehicle systems a communication range of 10 cm within the vehicle seems to be enough. The range of 1 m is necessary for hand-held EVI reader and/or writers.

Level 4: In-vehicle telematic platform, that provides a range of telecommunication capabilities to other in-vehicle systems and that can enable applications by sending a unique, reliable vehicle identity to an EVI reader and/or writer, or interacts with an EVI reader and /or writer via challenge response.

Characteristics:

- the vehicle data can be written in the in-vehicle EVI components more than once and read many times;
- the in-vehicle EVI components can enable applications that focus on stationary as well as moving vehicles directly;
- the in-vehicle EVI components can be both active (send a vehicle identity) and passive (respond to a request of this reader and /or writer with a vehicle identity);
- the in-vehicle EVI components are explicitly available to other in-vehicle components to offer telecommunication capabilities;
- since the distance between vehicle and reader and /or writer becomes bigger and vehicles might also be moving an activity/diagnostic notification unit may be needed; and
- since the in-vehicle EVI components enable applications directly also in cases where the vehicle is moving, for some applications a human-machine interface is needed.

These four basic functional levels are used as the objective of assessment.

2.3 Reflection 2: How to interact with the in-vehicle EVI components?

From Work Package 3 we already know that a variety of possibilities is available to interact with the vehicle, or better with the in-vehicle EVI components. The functional characteristics of the external interface between the in-vehicle EVI components and the reader and/or writer have implications for EVI as a whole, for instance:

- The usability of EVI in terms of which applications can and cannot be enabled. This usability determines the benefits of EVI.

- The costs for EVI.

In order to understand these implications, we differentiate the characteristics of the external interface for each of the four basic functional levels. The following external interfaces are used:

- Close Range (*'close'* is between 0 - 1 m[1]);

- Dedicated Short Range (*'dedicated'* is the possibility to pin-point a vehicle, *'short range'* is in between 10- 30 and 100[1] m);

---

[1] Given the fact that the in-vehicle EVI components will be connected to other in-vehicle systems a communication range of 10 cm within the vehicle seems to be enough. The range of 1 m is necessary for hand-held EVI reader and/or writers.

- Short Range Broadcast (*'broadcast'* is spread the information at certain moments in time, with a certain time interval in an area with a range of 0-at least 50 m); and
- Wide Area ('*wide area*' is connection-oriented over a wide area).

Combined with the four basic functional levels this gives us the nine functional sub-levels as outlined in table 2.1

Table 2.1: Basic functional levels of EVI differentiated to external interface between the in-vehicle EVI components and the reader and/or writer.

characteristics external interface → Basic Functional Level↓	Close Range	Dedicated Short Range	Short Range Broadcast	Wide Area
Level 1	1 - CR	-	-	-
Level 2	-	2-DSR	2-SRB	-
Level 3	-	3-DSR	3-SRB	-
Level 4	4-CR	4-DSR	4-SRB	4-WA

Level 1: In-vehicle EVI components, that respond a unique, reliable vehicle identity on request to another in-vehicle system or to a close-by (within 0 - 1 m) EVI reader.

Level 2: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader over a longer distance, or respond to a request of this reader.

Level 3: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader and/or writer over a longer distance, or interact with an EVI reader and /or writer via challenge response

Level 4: In-vehicle telematic platform, that provides a range of telecommunication capabilities to other in-vehicle systems and that can enable applications by sending a unique, reliable vehicle identity to an EVI reader and/or writer, or interacts with an EVI reader and /or writer via challenge response.

2.4 Reflection 3: How should EVI be linked to the Vehicle Registration Database?

From Work Package 2 we already know that a variety of possibilities is available for the data distribution over the in-vehicle EVI components, reader and/or writer and Vehicle Registration Database in the back-office. The three basic options are:

1. Store all the data needed to support the applications in the in-vehicle EVI components;
2. Store a subset of the data in the in-vehicle EVI components and leave the rest of the data in the Vehicle Registration Database (in the back-office);

[1] The factual limits for short range depend on the technology, for example 0-30m if microwave and 0-100m if infrared.

3. Keep all the data stored the Vehicle Registration Database and store a basic, unique vehicle identifier in the in-vehicle EVI components only.

From an assessment point of view the capabilities of the external interface between the EVI reader/writer and the Vehicle Registration Database is of interest. After all, some applications need more data in the vehicle than just a unique vehicle identity. In case of moving vehicles this means a request-response operation within seconds or even split seconds. So the response times of the Vehicle Registration Databases determine more or less the best options for the distribution of the vehicle data. Vice versa, a choice for the distribution of the vehicle data determines (amongst others) the needed response times of the Vehicle Registration Databases. We will elaborate on this in chapter 7.

In order to understand the implications of data distribution, we differentiate the three options for data distribution, as described above, for each basic functional level. Combined with the basic functional levels this gives us the seven functional sub-levels as outlined in table 2.2.

Table 2.2: Basic functional levels of EVI differentiated to external interface between the in-vehicle EVI components and the reader and/or writer.

characteristics external interface → Basic Functional Level↓	Close Range			Dedicated Short Range			Short Range Broadcast			Wide Area		
	ID	Set	All	ID	Set	All	ID	Set	All	ID	Set	All
Level 1	1 – CR-ID	1 – CR-set	1 – CR-all	-	-	-	-	-	-	-	-	-
Level 2	-	-	-	2-DSR-ID	2-DSR-set	2-DSR-all	2-SRB-ID	2-SRB-set	2-SRB-all	-	-	-
Level 3	-	-	-	3-DSR-ID	3-DSR-set	3-DSR-all	3-SRB-ID	3-SRB-set	3-SRB-all	-	-	-
Level 4	4-CR-ID	4-CR-set	4-CR-all	4-DSR-ID	4-DSR-set	4-DSR-all	4-SRB-ID	4-SRB-set	4-SRB-all	4-WA-ID	4-WA-set	4-WA-all

Level 1: In-vehicle EVI components, that respond a unique, reliable vehicle identity on request to another in-vehicle system or to a close-by (within 0 - 1 m) EVI reader.

Level 2: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader over a longer distance, or respond to a request of this reader.

Level 3: In-vehicle EVI components, that send a unique, reliable vehicle identity to an EVI reader and/or writer over a longer distance, or interact with an EVI reader and /or writer via challenge response

Level 4: In-vehicle telematic platform, that provides a range of telecommunication capabilities to other in-vehicle systems and that can enable applications by sending a unique, reliable vehicle identity to an EVI reader and/or writer, or interacts with an EVI reader and /or writer via challenge response.

2.5 Object of Assessment – part 1

The objects of assessment that we use are the four basic functional levels, the four characteristics of the external interface, and the three options for data distribution.

In figure 2.2 the relevance of the differentiators of the functional levels for the several assessment issues is indicated. In fact, this is how we use the functional levels and their differentiators in the actual assessment in part B of this document.

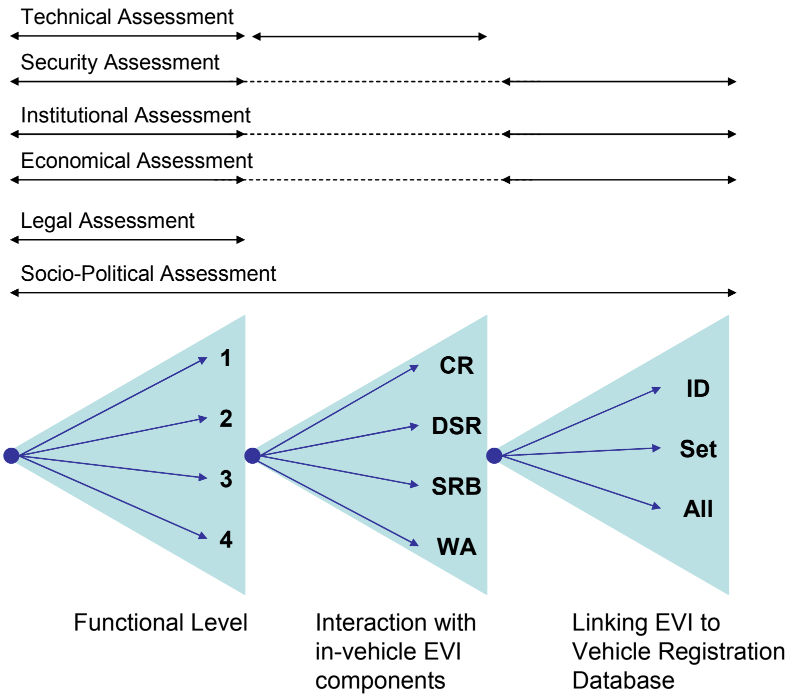


Figure 2.2: The way to take the object of assessment ('how to use EVI') forward.

The functional levels for the assessment differ slightly from the functional types as defined in work package 3. Annex B explains how the functions of the functional types, as distinguished in Work Package 3, are incorporated in the assessment functional levels or elsewhere in the assessment study.

3 DEPLOYMENT ISSUES

3.1 SCOPE FOR THE DEPLOYMENT

The EVI-system and its context are drawn in figure 1.1. For the deployment of EVI not only the components of the EVI-system itself (the in-vehicle EVI components and the reader and/or writer) need to be considered but also the vehicle registration database in the back-office (figure 3.1). Reason for including this specific back-office is that decisions on the data distribution (section 2.4) will affect the response time requirements of the vehicle registration database and the external interface of the reader and/or writer and this database.

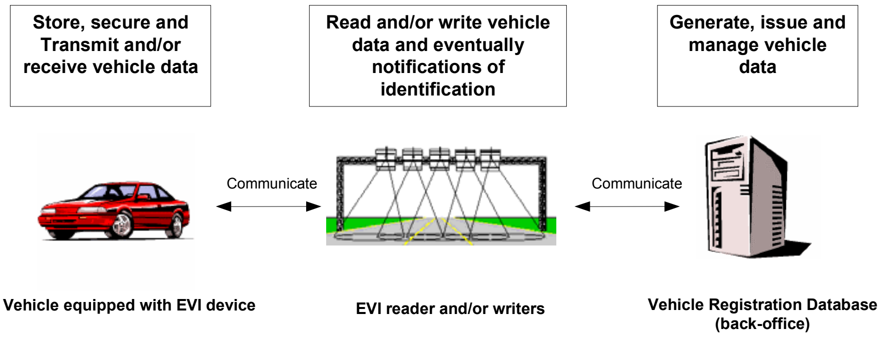


Figure 3.1: Scope for the deployment of EVI.

Given this scope, the deployment challenge is twofold, namely: (1) organising the life cycle of EVI and to make it operational, and (2) embed EVI in the applications that can use EVI. This feasibility study focuses on the first challenge.

3.2 GENERIC LIFE CYCLE OF EVI

The life cycle links the different phases in life of EVI, namely (source: Work Package 2):

- Specification and requirements

  During this stage the specifications for the EVI system are developed and published. Security should be an integral part of the specifications and requirements.

- Design

  This life-cycle stage considers the design of one or more specific implementations (parts) of EVI in-vehicle components and/or EVI reader/writers. The location of the in-vehicle EVI components and the external interfaces to other in-vehicle systems and external antennas should form a part of the design. Security should also be an integral part of the design.

- Manufacturing

During this stage the design is manufactured. The EVI devices should be manufactured in a secure environment. This environment should be certified by the public authorities, since they are responsible and therefore liable for EVI. A certified environment will result in a healthy balance between commercial competition (keeping the price per unit low), back up possibilities (limiting the risk of delay when one or more parties go out of business), and lead time to develop enough EVI devices and the security 'span of control' (keeping the number of possible fraud points for the EVI limited).

- Issuing

In this stage the in-vehicle EVI components are brought from the manufacturers into the vehicles. Besides distribution aspects, it is important to specify how to activate and/or update the configuration matching the characteristics of that specific vehicle and how to fit it in the vehicle:

  - Distribution;
  - Activation/configuring;
  - Installation;
  - Granting authority/Commissioning.

The In-vehicle EVI components should be issued in a secure environment.

Another important point in the issuing phase is to determine the authorities who are responsible for embedding the Unique Vehicle Identity in the EVI system. There are three choices:

1. Embedding by the automotive industry;
2. Embedding by the national registration authorities; and
3. Embedding by a network of certified dealers

The advantage of the third option is that it is possible to select a network of certified dealers. Therefore, it is possible to embed the Unique Vehicle Identity in retrofit. The drawback however is that it will possibly take a lot of time before a certified network of dealers is set up. Another possibility is the automotive industry that embeds the in-vehicle EVI components in the vehicle in-factory.

- Use

During this stage the EVI in-vehicle components and the EVI reader/writer have become operational and constitute an enabler for a range or applications.

- Management and updating of system

This part of the EVI life-cycle is about ensuring and maintaining operational conditions. In line with issuing, management and updating of the system should be done in a secure environment.

- End of life

This is the last part of the EVI life-cycle. In line with issuing and manufacturing of the in-vehicle EVI components, removing the device out of the vehicle should be done in a secure environment certified by public authorities.

- Certification

Orthogonal to the previous phases in the life cycle, there is the phase of certification. Certification is new and not mentioned in Work Package 2. In all phases except ‘Use’ either the environment where the activities take place or the product from a phase needs to be certified (from security point of view, see security assessment).

The way these phases in the life cycle of EVI will be shaped depends on:

- complexity of the EVI system ('simple versus complex EVI');
- level of obligation ('voluntary versus mandatory).

The implications of these choices are explored in the next paragraphs.

3.3 Impact of the complexity of the EVI system on the deployment

The basic functional levels of EVI as defined in chapter 2 in fact form increasing levels of complexity. The capabilities of the EVI increase per functional level. On the other hand we may expect that the increasing complexity is reflected in the deployment. In table 3.1 per phase in the life cycle specific characteristics of the deployment for the four basic functional levels of EVI are outlined.

Table 3.1: Characteristics for the basic functional levels.

Phase in life cycle of EVI	Basic Functional Level 1	Basic Functional Level 2	Basic Functional Level 3	Basic Functional Level 4
Specification and requirements	The requirements of the supported in-vehicle systems should be taken into consideration from the start.	-	-	The requirements of the supported in-vehicle systems should be taken into consideration from the start.
Design	From a technological point of a relatively simple design; examples do exist.The in-vehicle EVI components should be provided with an external interface to a commercial open telematics platforms. Functional levels (1) and (4) then fuse together.	From a technological point of a relatively simple design; examples do exist. The possibility to write more than once should be blocked in the design of the in-vehicle EVI components.	From a technological point of a relatively simple design; examples do exist. From a security point of view; a complex design.	From a technological point of a complex design; not state-of the art yet. From a security point of view; a complex design. The in-vehicle EVI components can be designed as a stand-alone telematics platform or can be embedded in the design of commercial open telematics platforms of the Automotive Telematics Industry. Another possibility is to link in-vehicle EVI components of

Phase in life cycle of EVI	Basic Functional Level 1	Basic Functional Level 2	Basic Functional Level 3	Basic Functional Level 4
				basic functional level 1 to commercial open telematics platforms. Functional levels (1) and (4) then fuse together.
Manufacturing	-	-	-	Manufacturing becomes more complex in case a set of communication channels will be used.
Issuing	Installation of the in-vehicle EVI components itself is rather straight forward. The device should be connected to the other in-vehicle systems directly or via the 'car area network' in case EVI should enable applications that aim at moving vehicles. In case more than just a unique vehicle identity is stored in the in-vehicle EVI components, this device should be deinstalled and replaced for a new device in case the vehicle data changes.	Installation of the in-vehicle EVI components itself is rather straight forward, however it will be slightly more complex than functional level 1, since both the EVI device and the antenna have to be placed correctly. In case more than just a unique vehicle identity is stored in the in-vehicle EVI components, this device should be deinstalled and replaced for a new device when the vehicle data changes.	Installation of the in-vehicle EVI components itself is rather straight forward, however it can be done slightly more robust than functional level 2 since deinstallation due to change in stored vehicle data is not necessary.	Installation of the in-vehicle EVI components itself is more complex since it has to be connected to the other in-vehicle systems directly or via the 'car area network', plus more than one antenna might need to be installed.
Use	Can only be used for those applications that focus on stationary vehicles. Usability for applications that focus on moving vehicles depends fully on other in-vehicle systems.	Can be used for applications that focus on stationary and moving vehicles.	Can be used for applications that focus on stationary and moving vehicles.	Can be used for applications that focus on stationary and moving vehicles.
Management and updating of system	Updating has to be done by de-installing the in-vehicle EVI	Updating has to be done by de-installing the in-vehicle EVI	In case wide area or wireless network communication channels are in	In case wide area or wireless network communication channels are in

Phase in life cycle of EVI	Basic Functional Level 1	Basic Functional Level 2	Basic Functional Level 3	Basic Functional Level 4
	components and replacing it with a new device.	components and replacing it with a new device.	use, maintenance of data can be done remotely.	use, maintenance of data can be done remotely.
End of life	Deinstalling the in-vehicle EVI components will have consequences for other in-vehicle systems which use the vehicle data.	-	-	Deinstalling the in-vehicle EVI components will not only have consequences for other in-vehicle systems which use the vehicle data. In case the in-vehicle EVI components functions as a stand-alone telematics platform, de-installing the in-vehicle EVI components will have consequences for other in-vehicle systems which use its telecommunication function.

3.4 IMPACT OF THE LEVEL OF OBLIGATION ON THE DEPLOYMENT

Despite the basic functional level of EVI (as defined in chapter 2) there are numerous options for the deployment of a European wide EVI

We take the following choices in consideration (figure 3.2):

- Level of obligation (voluntary versus mandatory) – We might consider a sliding scale from voluntary per member state to mandatory for all member state vehicles. The level of obligation will impact the complexity of the deployment. Think of the difference in the process of issuing EVI in case EVI is mandatory for all European vehicles versus EVI that is introduced on a strictly voluntary basis, or the difference in support and acceptance from/of the public;
- Period of introduction (at once versus in phases);
- Level of standardisation of EVI (common standard versus no common standards);
- Vehicle type (all at once or specific groups of vehicles) – the level of obligation can be linked to a specific group of vehicles, for instance mandatory for freight trucks and lorries and voluntary for the other vehicles. In our objects of assessment no distinction has been made.

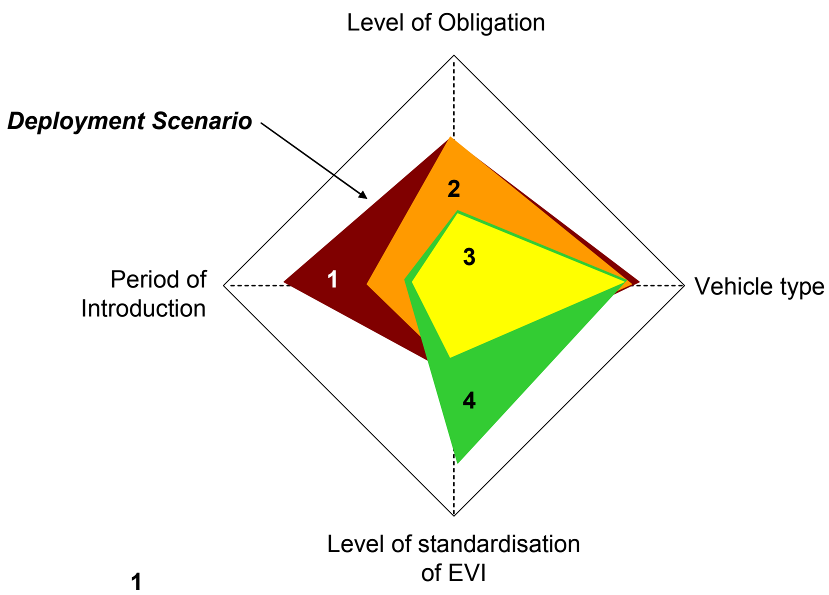


Figure 3.2: Pallet of possible deployment scenarios for EVI.

By exploring the following four deployment scenarios, we might gain insight in the implications of the different parameters (choices) on the deployment of EVI:

- *Mandatory for all at once, common standard*: A Mandatory deployment of EVI across all Member States within a fixed and fairly short time period (e.g. 2-3 years), with all Member States beginning the process simultaneously.
- *Mandatory for all in phases, common standard*: A Mandatory deployment of EVI across all Member States within a fixed timed period, with Member States joining in a coordinated but phased process, e.g. by region, or readiness to start. Longer EU wide deployment period 3-5 years.
- *Voluntary, common standard*: A voluntary deployment of EVI by Member States, based on the business case in each Member State, but operating to a common standard across the EU to ensure interoperability. EU wide deployment period potentially never.
- *Voluntary, no common standard*: Member States would be allowed to introduce a Member State specific EVI based on their own requirements without the requirement for EU wide interoperability. EU wide deployment – potentially impossible .

In table 3.2 per phase in the life cycle specific characteristics of the deployment for the four levels of obligation of EVI are outlined.

Table 3.2: Characteristics for different levels of obligation.

	Mandatory for all at once, common standard	**Mandatory for all in phases, common standard**	**Voluntary, common standard**	**Voluntary, no common standard**
Specification and requirements	Build a specification for the EVI system which is accepted by all Member States, but preferably also on CEN and ISO level.	Build a specification for the EVI system which is accepted by all Member States, but preferably also on CEN and ISO level.	Build a specification for the EVI system which is accepted by all Member States, but preferably also on CEN and ISO level.	Learn form each others specification, see to what extent the specification can be brought in one line and accept differences in the specifications due to differences in requirements.
Design	Build a design for the EVI system which is accepted by all Member States, but preferably also on CEN and ISO level.	Build a design for the EVI system which is accepted by all Member States, but preferably also on CEN and ISO level.	Build a design for the EVI system which is accepted by all Member States, but preferably also on CEN and ISO level.	Learn form each others design, see to what extent the designs can be brought in one line and accept differences in the designs due to differences in specifications.
	Two designs are necessary, one for retro-fit and one for in-factory installation.			
Manufacturing	Manufacture the components of the EVI System on a European level for all countries at once.	Manufacture the components of the EVI System on a European level in phases starting with the countries at the forefront.	Manufacture the components of the EVI System on a European level in phases starting with the early adopters.	Manufacture the components of the EVI System on a (multi-)national level in phases starting with the early adopters.
Issuing	Install the in-vehicle devices in retrofit for the existing vehicle park. Install the in-vehicle devices in factory for the new vehicles.	Install the in-vehicle devices in retrofit for the existing vehicle park. Install the in-vehicle devices in factory for the new vehicles.	Install the in-vehicle devices in retrofit for the early adopters with an existing vehicle. Another possibility is to start with the new vehicles and install the device in factory.	Install the in-vehicle devices in retrofit for the early adopters with an existing vehicle. Another possibility is to start with the new vehicles and install the device in factory.
Use	After the whole vehicle park is equipped the device can be used European wide for all applications for which the available communication	After the whole vehicle park is equipped the device can be used European wide for all applications for which the available communication	The device can immediately be used in a certain (set of) country for all applications which do not need full coverage of vehicle park. When	The device can immediately be used in a certain (set of) country for all applications which do not need full coverage of vehicle park. When

	Mandatory for all at once, common standard	**Mandatory for all in phases, common standard**	**Voluntary, common standard**	**Voluntary, no common standard**
	capabilities will do. Applications which need more than close range communication can only be enabled by those vehicles which posses over the appropriate in-vehicles system enabled by the In-vehicle EVI components.	capabilities will do.	whole vehicle park is equipped the other applications can be used.	whole vehicle park is equipped the other applications can be used.
Management and updating of system	Since the system is mandatory, a quick response is necessary in case the in-vehicle EVI components do not operate properly. Updating the data stored in the in-vehicle EVI components or replacing the in-vehicle EVI components should also be possible within a short period of time. Both are institutional requirements.	Since the system is mandatory, a quick response is necessary in case the in-vehicle EVI components do not operate properly. Updating the data stored in the in-vehicle EVI components or replacing the in-vehicle EVI components should also be possible within a short period of time. Both are institutional requirements.	Since the system is voluntary, a commercial acceptable response is necessary in case the in-vehicle EVI components do not operate properly. Updating the data stored in the in-vehicle EVI components or replacing the in-vehicle EVI components should also be possible within a commercial acceptable period of time. Both are institutional requirements.	Since the system is voluntary, a commercial acceptable response is necessary in case the in-vehicle EVI components do not operate properly. Updating the data stored in the in-vehicle EVI components or replacing the in-vehicle EVI components should also be possible within a commercial acceptable period of time. Both are institutional requirements.
End of life	Large amount of in-vehicle EVI components to be deinstalled and destroyed.	Large amount of in-vehicle EVI components to be deinstalled and destroyed.	Amount of in-vehicle EVI components to be deinstalled and destroyed depends on the number of vehicle (registration) owners who have installed an in-vehicle EVI component.	Amount of in-vehicle EVI components to be deinstalled and destroyed depends on the number of vehicle (registration) owners who have installed an in-vehicle EVI component.

3.5 POSSIBLE VARIATIONS IN DEPLOYMENT SCENARIOS

When the basic functional levels are combined with the levels of obligations a series of possible deployment scenarios emerges. These variations are outlined in figure 3.3 and will be briefly clarified.

By starting with a basic functional level 1 EVI system on a mandatory for all at once basis using a common standard, a solid foundation will be laid for further deployment. On this basis the EVI system can evolve both on a mandatory and voluntary basis towards a more complex EVI-system. The usability of EVI after the first step however is still limited, although all vehicles will be equipped in a relatively short period.

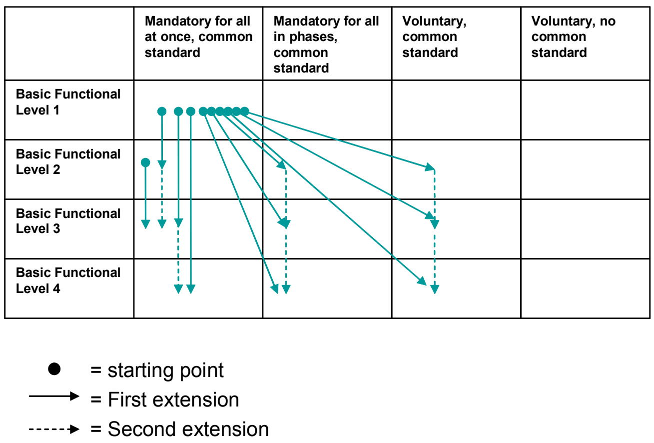


Figure 3.3: Illustrations of possible variations in deployment scenarios starting with a basic functional level 1 EVI system on a mandatory introduction all at once basis using a common standard.

By starting with a basic functional level 1 EVI system on a mandatory for all basis, but introduced in phases, using a common standard, a similar solid foundation is laid for further deployment. This time the public authorities can use the lessons learned by another authority and/or in a previous phase.

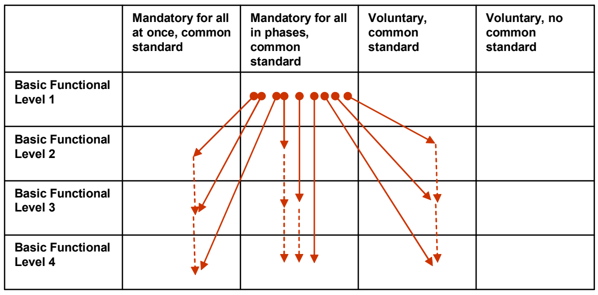


Figure 3.4: Illustrations of possible variations in deployment scenarios starting with a basic functional level 1 EVI system on a mandatory introduction in phases using a common standard.

By starting with a basic functional level 1 or 2 EVI system on a voluntary basis using a common standard, a rather thin foundation will be laid for further deployment. The 'foundation has to grow in strength' (i.e. the number of vehicles equipped with an in-vehicle EVI component has to increase) before EVI becomes really usable for most public authority applications.

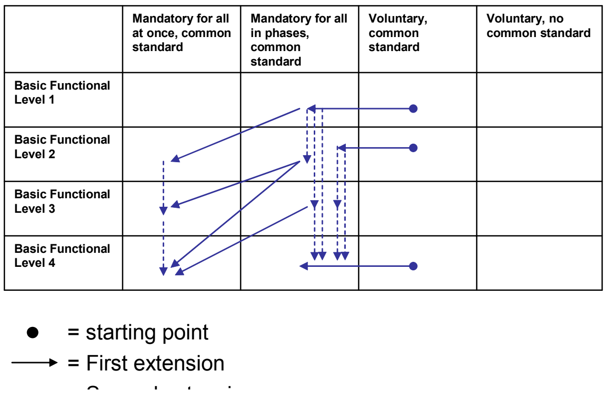


Figure 3.5: Illustrations of possible variations in deployment scenarios starting with a basic functional level 1 or 2 EVI system on a voluntary basis using a common standard.

By starting on a voluntary basis not using a common standard, a rather 'crumbled' foundation will be laid, which will form a barrier for further European wide deployment.

3.6 Object of Assessment - Part Two

As we have seen a large number of deployment scenarios are possible. For this assessment we will use two more or less likely scenarios, namely (figure 3.6):

- Assessment deployment scenario 1: Starting with an EVI on basic functional level (2), mandatory for all, at once, using a common standard. Given this solid basis, EVI can grow further on a voluntary basis towards a complex version on functional level (4).

- Assessment deployment scenario 2: Starting with an EVI on basic functional level (2), mandatory for all, however this time in phases, using a common standard. The solid basis for further development has to grow over the years. Once there is a solid basis of equipped vehicles it will become mandatory to upgrade all at once the EVI system to a more complex version on functional level (4), using a common standard.

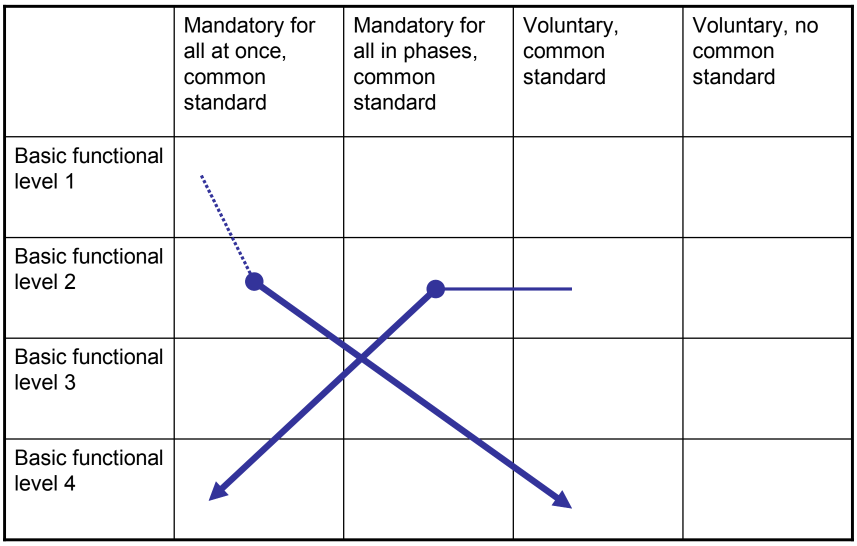


Figure 3.6: Deployment scenarios which are part of the object of assessment.

Both scenarios do have a mandatory EVI as starting point. In fact this is the assumption used in the assessment in order to understand the full complexity of EVI. Later on (in Work Package 5) we should also consider starting on a voluntary basis. The advantage of starting on a voluntary basis is that it will give the public authorities more time to upgrade the own organisation, gain support and acceptance of the vehicle (registration) owners, issue the in-vehicle EVI components, in other words it might be less complex.

The deployment scenarios will be used in the economical and socio-political assessment.

In figure 3.7 the objects of assessment as will be used in part B of this document are assembled.

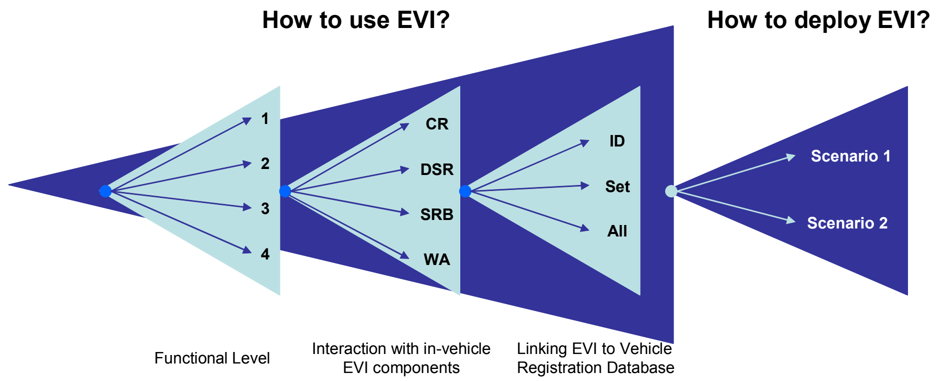


Figure 3.7: Assemblage of the Objects of assessment.

Part B. 'Assessment of EVI'

4 Introduction to the Assessment Issues

So far we have defined the object of assessment using the understanding of EVI as has grown during the Work Packages 2 and 3. Now, this object will be assessed in the next chapters from six perspectives, namely:

- *Technological*: 'What are the possibilities and barriers to realise EVI from a technological point of view?'
- *Security*: 'What are the possibilities to actually improve the reliability of the unique vehicle identity and the vehicle identification?'
- *Institutional*: 'What are the possibilities and barriers to deploy EVI on a European and / or nation wide basis?'
- *Economical*: 'What benefit(s) can EVI deliver above and beyond the existing mechanisms for identifying individual vehicles?' and 'Do the identified benefits that can be derived from EVI outweigh the costs of implementation and operation (regarding the way(s) of deployment)'
- *Legal*: 'What legal barriers are to be expected when deploying EVI?'
- *Social and Political*: 'What social and political barriers are to be expected when deploying EVI?'

For every perspective the main question is rephrased from the introduction (chapter 1). The environmental assessment has been incorporated in the institutional assessment.

5 TECHNOLOGICAL ASSESSMENT

The technological assessment focuses on the basic functional levels plus the differentiation on the external interface between in-vehicle EVI components and the reader and/or writer, as well as the deployment scenarios. As was stated in Work Package 3 the amount of data to be stored in the EVI device is not critical from a technological point of view.

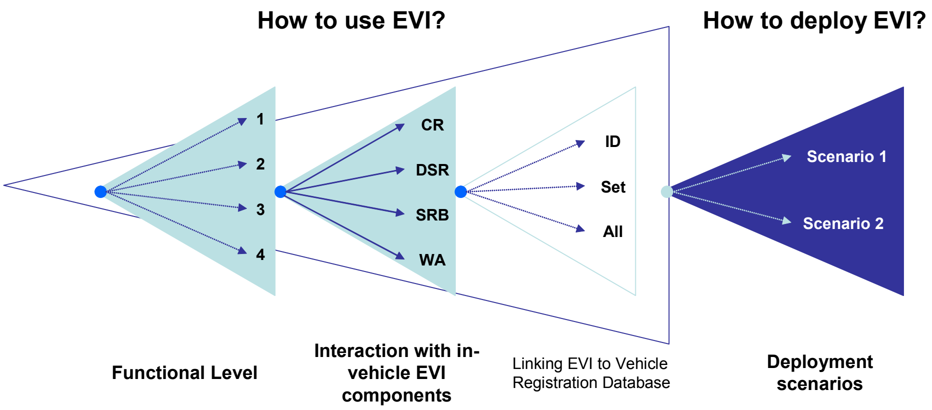


Figure 5.1: Objects of technological assessment.

5.1 EVI AS AN ENABLER FOR THE PUBLIC AUTHORITY APPLICATIONS

EVI consist of the following components (see figure 5.2):

- In-vehicle EVI components;
- External interface in-vehicle EVI components versus reader/writer;
- External interface reader/writer versus back-office;

To understand the possibilities of the EVI-realisation types as derived in work package 3, it is necessary to assess at least both external interfaces on a technological level. The following figure focuses on the in-vehicle EVI components versus reader/writer interface.

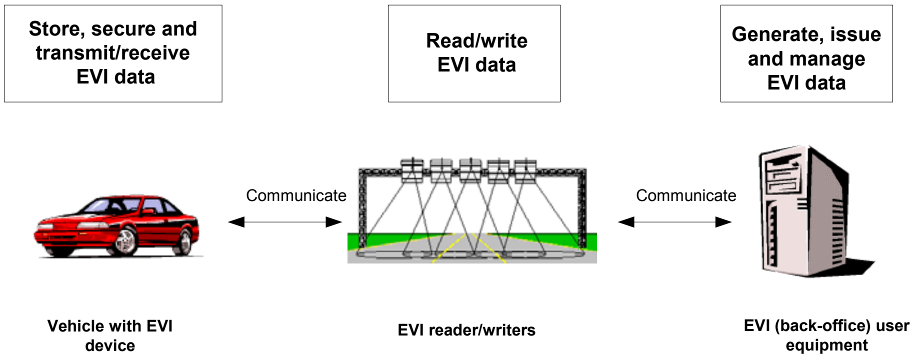


Figure 5.2: Functional architecture (source: work package 3)**.**

5.2 CRITERIA FOR THE TECHNOLOGICAL ASSESSMENT

The capabilities of the realisation types as described in chapter 2 (result from work package 3) are defined using a set of 20 criteria. The criteria have been derived from those user requirements that put the focus on the technological requirements for the reader-writer – vehicle link as established in work package 2. In order to assess whether a specific realisation type of EVI can enable a public authority application, the minimum claims of the applications on these criteria have been derived from their description and the examples of use cases.

An overview of the technological assessment criteria is presented in annex C, together with the scales on which the criteria are measured. The definition of the scale on which the criteria are measured is described in annex D.

5.3 POSSIBILITIES TO ENABLE APPLICATIONS PER COMMUNICATION TECHNOLOGY

The first step in the assessment in whether a public authority application can be enabled by an EVI-realisation type is to assess which basic communication technologies can support which applications.

To select the public authority applications that can be enabled by the identified communication technologies in work package 3, radar plots will be used. A radar plot is the visualisation of the assessment on the evaluation criteria. The essence of the plot is that supporting a public authority application will be more difficult if the score on a criterion is situated further from the centre of the radar plot.

In work package three a technical assessment has been conducted for each of the eight described communication technologies. The accompanying radar plots can be pasted on the radar plots of the public authority applications (as shown in figure 5.3). This assessment of the public authority applications is described in annex E.

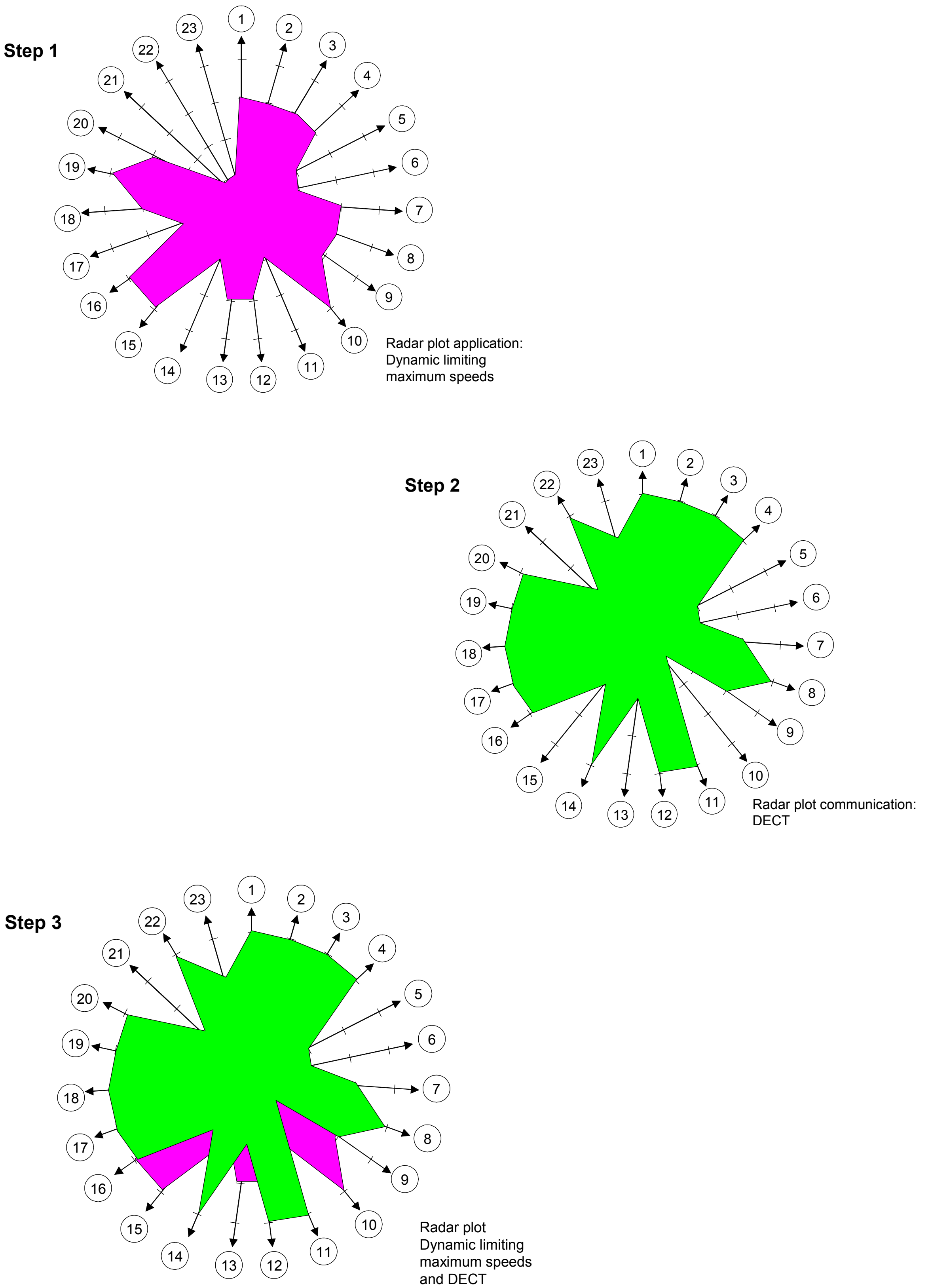


Figure 5.3: Steps to be taken in the assessment of public authority applications.

In this example one can see that the technology DECT cannot support the public authority application “dynamic limiting maximum speeds”, on all criteria. If this application is necessary, additional features should be added to the EVI-realisation type using DECT or another communication technology should be chosen.

Radar plots can be made for each application in relation to each technology. The interpreted results of all these plots are presented in table 5.1. It matches the 32 applications with the eight communication technologies. As can be seen in the table, all communication technologies are able to support several applications on all criteria for evaluation. Cellular telephone fulfils all criteria if the UMTS technology is chosen. UMTS has specified so called nanocells that will enable pinpointing of a specific vehicle.

Annex F describes which evaluation criteria cannot be supported by a specific communication technology. On the basis of this annex it can be concluded that some applications can be enabled if the deficiencies of a communication technology are by-passed.

Table 5.1: Support of Public Authority Applications by Communication Technologies.

	Crime Prevention				Access control			Vehicle tolling				Traffic management and driver information											Enforce-ment		Vehicle Life Cycle			Traffic and transport regulation				
	Prevention of vehicle theft	Tracking and tracing of stolen vehicles and assets	Remote stopping of tracked stolen vehicles	Terrorism	Overview of cross border traffic	Border control	Access control of vehicles	Charging according to use	Charging according to use to include all social costs	Value pricing	Tolling	Dynamic limiting maximum speeds	Dynamic advice maximum speed on individual basis	Intelligent speed adaptation	Incident management	Misfit of the vehicle on the infrastructure	Informing road users	Anonymous guidance of road users	Taylor-made guidance of vehicles	Dynamically regulating of the road traffic	Offering additional capacity	Tracking and tracing of vulnerable people	Reduce damage to road	Enforcement	End of life	Identification of vehicle and components	Control vehicle life cycle	Safe vehicles - annual vehicle inspection	Safe vehicles - Inspection and recall information	Checking and controlling emissions	Controlling emissions	Monitoring/controlling hazardous goods
RFID[1]																																
RFID[2]																																
DSRC																																
WLAN, HIPER-LAN																																
CALM M5																																
Infrared																																

[1] For magnetic field powered device with crypto-controller, typically 125 kHz or 13.56 MHz

[2] for electric field powered device without crypto-controller, typically UHF (e.g. 869 MHz)

	Crime Prevention				**Access control**			**Vehicle tolling**				**Traffic management and driver information**											**Enforce-ment**		**Vehicle Life Cycle**			**Traffic and transport regulation**				
	Prevention of vehicle theft	Tracking and tracing of stolen vehicles and assets	Remote stopping of tracked stolen vehicles	Terrorism	Overview of cross border traffic	Border control	Access control of vehicles	Charging according to use	Charging according to use to include all social costs	Value pricing	Tolling	Dynamic limiting maximum speeds	Dynamic advice maximum speed on individual basis	Intelligent speed adaptation	Incident management	Misfit of the vehicle on the infrastructure	Informing road users	Anonymous guidance of road users	Taylor-made guidance of vehicles	Dynamically regulating of the road traffic	Offering additional capacity	Tracking and tracing of vulnerable people	Reduce damage to road	Enforcement	End of life	Identification of vehicle and components	Control vehicle life cycle	Safe vehicles - annual vehicle inspection	Safe vehicles - Inspection and recall information	Checking and controlling emissions	Controlling emissions	Monitoring/controlling hazardous goods
tag	■				■		■	■	■	■	■	■	■	■		■	■	■		■	■					■		■	■	■	■	
CALM IR	■				■		■	■	■	■	■	■	■	■		■	■	■		■	■		■			■		■	■	■	■	
DECT																																
Mobile[1]	■	■	■		■			■	■	■	■					■								■		■		■	■	■	■	

■ = Application to be enabled by regarded communication system

[1] Only valid for the UMTS technology, if GSM DATA, SMS or GPRS is used non of the applications is possible because pinpointing a specific vehicle is not possible

5.4 POSSIBILITIES TO ENABLE APPLICATIONS PER FUNCTIONAL LEVEL OF EVI

To identify the applications that can be enabled by each basic functional level of EVI it is necessary to link communication technologies to functional types. In this assessment we assume that the realisation examples as identified in WP3 could be linked to the functional types as drawn in figure 5.4.

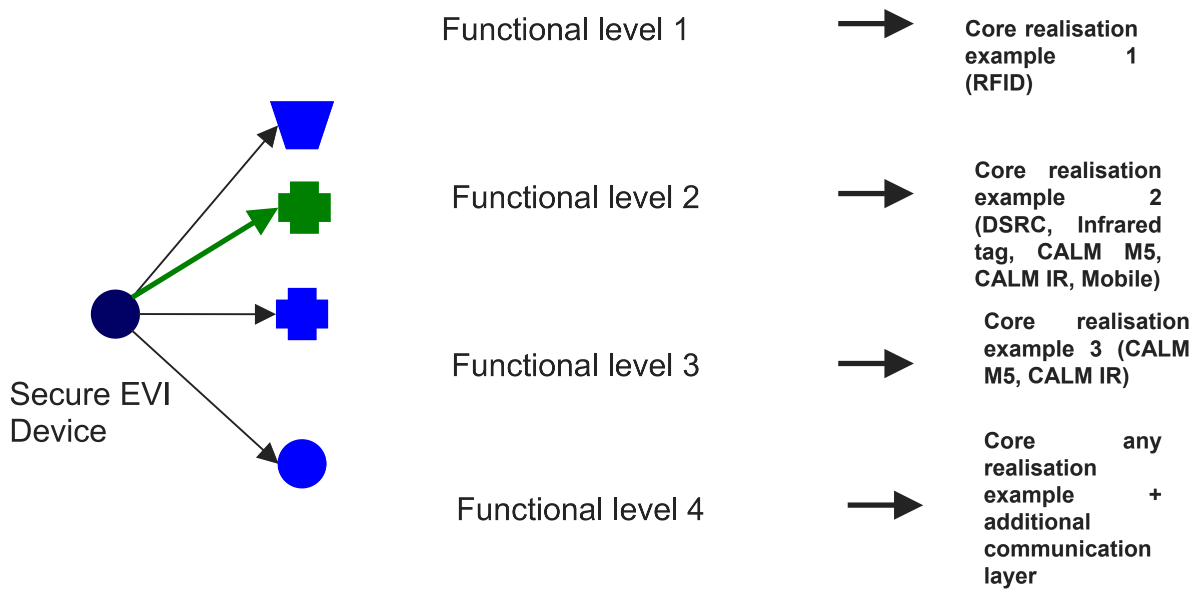


Figure 5.4: Linking the basic functional levels for EVI with the realisation types of Work Package 3.

The applications that could be enabled by functional level 1 to 3 could be identified from table 5.1 and are dependent on the chosen communication technology. The enabled applications by functional type four are dependent on the chosen core. In table 5.2 examples of possible cores are identified (as identified in Work Package 3). The applications that each core enables are represented by capital C. Adding another communication technology will result in more enabled applications (green shaded).

The basic conclusion from table 5.2 is that each basic functional level can enable a specific set of public authority applications. Which applications precisely could be enabled is dependent on the choice of the communication technology, since some deficiencies in a communication technology might prohibit EVI to enable an application properly.

The criterion "supports broadcast" should be evaluated differently to the methodology used here. The purpose of broadcasted one-way communication is to be able to hide the reading device and still obtain information (The content of the broadcast and its data properties are discussed elsewhere). This is similar to current procedures where license plates can be read without interrogating the vehicle. The broadcast mode is therefore more an operational mode of the technologies discussed under here and is available for CALM M5, CALM IR, DECT and GSM. DSRC according to CEN TC 278 and RFID require interrogation as the communication is powered by the reader, or can be combined with any of the technologies named before.

Table 5.2: Enabling of Public Authority Applications by EVI-Realisation Types.

■ = application to be enabled by regarded communication system C = Core enabled

	Crime Prevention				Access control			Vehicle tolling				Traffic management and driver information											Enforce-ment		Vehicle Life Cycle			Traffic and transport regulation				
	Prevention of vehicle theft	Tracking and tracing of stolen vehicles and assets	Remote stopping of tracked stolen vehicles	Terrorism	Overview of cross border traffic	Border control	Access control of vehicles	Charging according to use	Charging according to use to include all social costs	Value pricing	Tolling	Dynamic limiting maximum speeds	Dynamic advice maximum speed on individual basis	Intelligent speed adaptation	Incident management	Misfit of the vehicle on the infrastructure	Informing road users	Anonymous guidance of road users	Taylor-made guidance of vehicles	Dynamically regulating of the road traffic	Offering additional capacity	Tracking and tracing of vulnerable people	Reduce damage to road	Enforcement	End of life	Identification of vehicle and components	Control vehicle life cycle	Safe vehicles - annual vehicle inspection	Safe vehicles - Inspection and recall information	Checking and controlling emissions	Controlling emissions	Monitoring/controlling hazardous goods
Core RFID → implementation of basic functional level 1																																
																									C	C	C	C	C	C		
Core RFID → implementation of basic functional level 1 , this time connected to other in-vehicle systems																																
CALM M5	■				■		■	■	■	■	■	■	■	■		■	■	■		■	■		■		C	C	C	C	C	C	■	■
Infrared tag	■				■		■	■	■	■	■	■	■	■		■	■	■		■	■				C	C	C	C	C	C	■	
CALM IR	■				■		■	■	■	■	■	■	■	■		■	■	■		■	■		■		C	C	C	C	C	C	■	■
Mobile	■	■	■		■			■	■	■	■					■								■	C	C	C	C	C	C	■	
Core DSRC or Infrared Tag → implementation of basic functional level 2																																
RFID	C				C		C	C	C	C	C	C	C	C		C	C	C		C	C				■	C	■	C	C	C	C	
CALM M5	C				C		C	C	C	C	C	C	C	C		C	C	C		C	C		■									■
CALM IR	C				C		C	C	C	C	C	C	C	C		C	C	C		C	C		■									■
Mobile	C	■	■		C		C	C	C	C	C	C	C	C		C	C	C		C	C			■		C		C	C	C	C	
Core CALM IR or CALM M5 → implementation of basic functional level 2																																
RFID	C				C		C	C	C	C	C	C	C	C		C	C	C		C	C		C		■	C	■	C	C	C	C	C
Mobile	C	■	■		C		C	C	C	C	C	C	C	C		C	C	C		C	C		C	C		C		C	C	C	C	C

5.5 SOME CONSIDERATIONS OF THE IN-VEHICLE INTERFACES OF THE IN-VEHICLE EVI COMPONENTS

Before stepping further into the assessment we would like to consider the in-vehicle interfaces of the EVI in-vehicle components, which might be needed in order to be able to support public authority applications properly. The in-vehicle interfaces to take into consideration are the interfaces to a:

- Human-Machine Interface (HMI); and
- Localisation device.

Let us start with the HMI.

Human-Machine Interface

Regardless of the application to be enabled (supported) by EVI, it is necessary to inform the vehicle driver, respectively owner that the in-vehicle EVI components are functioning properly. In addition, some public authority applications might require passing on information directly to the vehicle owner and/or driver. This asks for a human-machine interface (HMI). In this assessment study we distinguish three functional levels for the HMI device, namely:

- Basic – enabling the vehicle driver/owner to read what data is stored on the in-vehicle EVI components and to check whether the device is working;
- Simple – enabling applications to pass on basic information to the driver while driving in a simple way; and
- Advanced - enabling applications to pass on more complex information to the driver while driving in a sophisticated way. The most realistic option is that such a HMI is provided by another in-vehicle system to which the in-vehicle EVI components are linked.

In table 5.3 an indication is given of the functional level of the human-machine interface which might be necessary to enable the specific application. It should be stressed that a HMI is necessary to enable applications and is not part of EVI per se. However, if Member States prefer to enable applications in the way as described in annex A, it is also necessary to have an in-vehicle interface with a HMI. In case a HMI is needed this will increase the costs, necessary to gain the benefits.

Table 5.3: Indication of the public authority applications which need a HMI.

Generic application	**Public authority application**	**Implicit choice for HMI**
Crime	Prevention of vehicle theft	Basic
	Tracking and tracing of stolen vehicles and assets	basic
	Remote stopping of tracked stolen vehicles	basic
	Terrorism	basic
Access control	Overview of cross border traffic	basic
	Border control	basic
	Access control of vehicles	basic
Vehicle tolling	Charging according to use	simple
	Charging according to use to include all of the social costs for road traffic	simple
	Value pricing	simple
	Tolling	simple
Vehicle (registration) ownership Obligation	No public authority applications identified in WP2	simple
Excise duty	No public authority applications identified in WP2	advanced
Traffic management and driver information	Dynamically limiting maximum speeds, generically	advanced
	Dynamic advice on maximum speeds, on an individual basis	advanced
	Intelligent speed adaptation	simple
	Incident management	advanced
	Misfit of the vehicle on the infrastructure	simple
	Informing road users	advanced
	Anonymous guidance of road users	advanced
	Taylor-made guidance of vehicle drivers	advanced
	Dynamically regulating of the road traffic	basic
	Offering additional capacity (for target groups)	basic
	Tracking and tracing of vulnerable people	basic
Enforcement	Reduce the damage to the road due to traffic	advanced
	Enforcement of established regulations on excises duties, vehicle inspections (including driver license and insurance checks), freight transport, traffic regulations (e.g. speed checks, red light control, banned turns and tail gating), road pricing and vehicle fraud	advanced
Vehicle Life Cycle	Accurate identifying vehicles and their components, assists with end of life directive preventing illegal dumping of vehicles	basic
	Identification of the vehicle and the combination of vehicle components	basic
	Control the vehicle life cycle	basic
Traffic and transport regulation	Safe vehicles – Annual vehicle inspection	basic
	Safe vehicles – Inspection and recall information	basic
	Checking and controlling the emissions from the individual vehicles	basic
	Controlling emissions from the individual vehicle	
	Monitoring/controlling the transport of hazardous goods	

Localisation Device

For some public authority applications it is necessary to be able to pinpoint a specific vehicle rather precisely. As can be derived from the technical assessment so far, not every communication technology supports this precise pinpointing (e.g. cellular telephone like GSM or GPRS). In case the in-vehicle EVI components will be realised using such a communication technology, an in-vehicle interface to a separate localisation device will be needed (as was already stated in Work Package 3). An example of such a device is a GNSS (GPS or Galileo) receiver.

Again it should be stressed that a separate localisation device is necessary to enable applications and is not part of EVI per se. However, if Member States prefer to enable applications in the way as described in chapter 4, it is also necessary to have an in-vehicle interface with a localisation device for some communication technologies. In case an external localisation device is needed this will increase the costs, necessary to gain the benefits

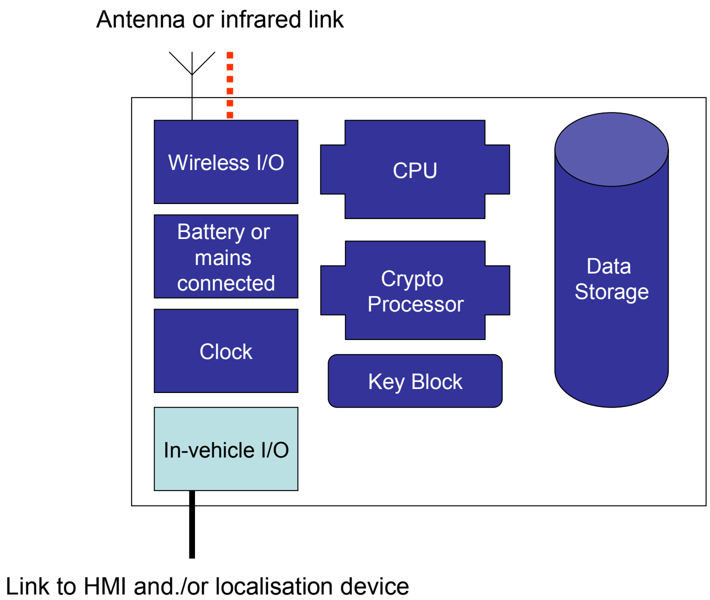


Figure 5.5 Illustration of the in-vehicle EVI-components derived from Work Package 3 plus separate in-vehicle I/O added to it.

5.6 Reflection of the Technical Assessment

EVI can fulfil its basic technological premises (as identified in WP2), needed to enable (support) the public authorities applications. However, the actual capabilities (deficiencies besides the possibilities) of the available or planned wireless communication technologies used to realise the In-vehicle EVI components can form a barrier to enable all applications. Not every communication technology or even combination of communication technologies can enable all the applications. Therefore a careful selection of communication technologies is necessary when the final Realization Type of EVI is assembled.

The in-vehicle EVI components from Work package 3 have to be extended with an in-vehicle interface to an HMI and, depending on the communication technology chosen, a localisation unit. The interface to the HMI might be necessary for some public authority applications to pass on information to the vehicle driver. The interface to a localisation device might be necessary to retrieve the vehicle location in case the chosen communication technology does support pinpointing a vehicle precisely.

The complexity of installing the in-vehicle EVI components increases from level 1 to level 4.

The technological assessment results are summarized in figure 5.6.

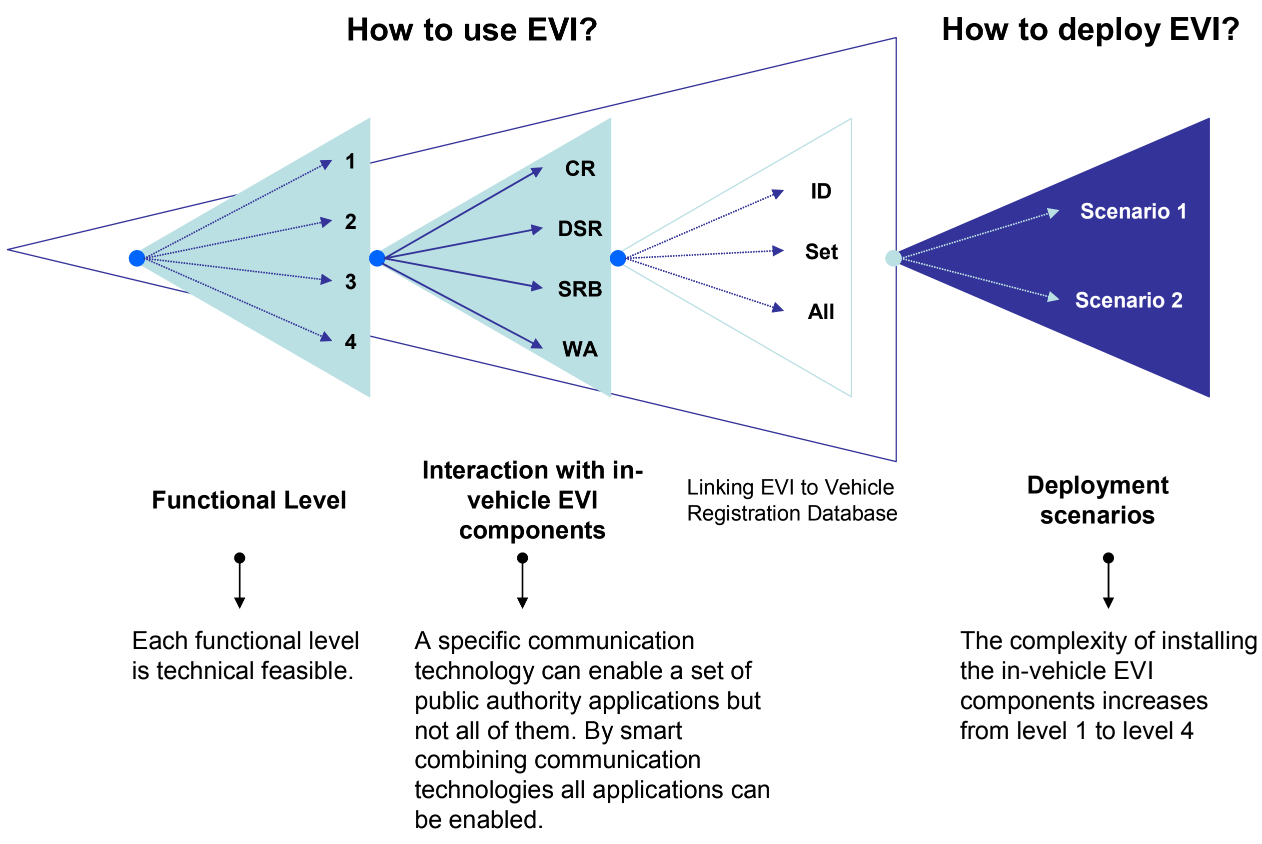


Figure 5.6: Summary of the technological assessment results.

6 Security Assessment

The security assessment focuses on the basic functional levels plus the distribution of the data over the EVI-system and the back-office. On the level of abstraction of this assessment study there is no real difference in the security of the different communication systems. So we will not take the differentiation to communication system into consideration. Since in both deployment scenarios EVI will be mandatory, it is in both scenarios realistic to expect fraud to occur.

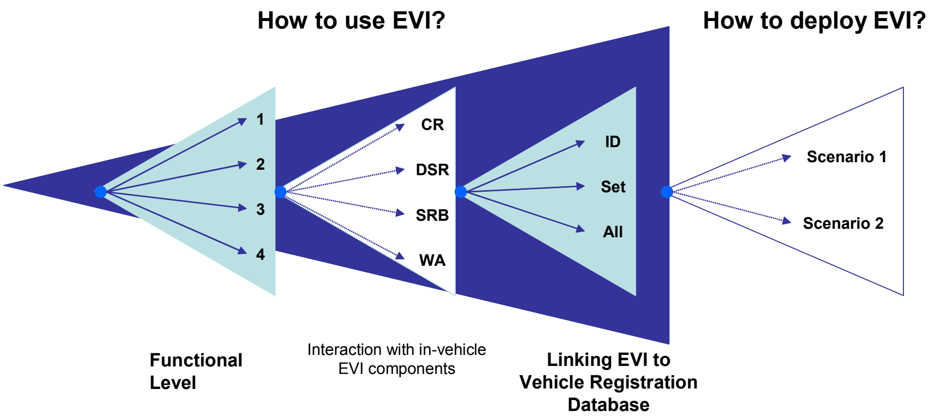


Figure 6.1: Objects of security assessment.

6.1 Introduction

Since EVI should improve the reliability of the unique vehicle identity and thereby improve the registration process of the vehicles, security is an important issue.

From an economic point of view, it makes sense to take fraud measures when the total costs of the measures (design, manufacturing, deployment, control) are lower than the expectation of the total of loss (tax) income over the life time of the fraud measures.

EVI is an initiative of public authorities and should enable public services. Thus, besides the economic point of view there is the requirement of 'equality of law for all taxpayers'. There should not be a separate group of people that can have more benefits from fraud than other groups.

However security is not only related to fraud, it is also related to protecting the privacy of the vehicle (registration) owner. Since EVI comes with an efficient way of reading the vehicle identity, misusing this identity (and other data if stored in the in-vehicle EVI components) might also be done in a more efficient way than in the present situation.

The security of EVI will be assessed by exploring the possibilities to take countermeasures against fraud and privacy threats. First we will define fraud and privacy threats a bit more in detail.

6.2 Definitions

Privacy Aspects

From security perspective, safeguarding the privacy of the vehicle owner, c.q. driver includes the communication between the in-vehicle EVI components and the reader and/or writer, as well as the tracking of the vehicle.

A communication definition of privacy in the EVI context is related to eavesdropping:

Privacy is protection of the communication from all but intended recipients.
The communication should be confidential.

Privacy can also be intruded by building user patterns using available, unique and therefore distinguishable data. From this perspective a second definition of privacy is:

> *Privacy is protection of the vehicle owner from building user patterns using the possibility to track vehicles, which send their identity to a reader and/or writer.*

Integrity of the Communication

Starting point of this privacy threat is that unlawful eavesdropping should not lead to the disclosure of any personal data. This requires solid encryption of the communicated vehicle data as the first step. Where the vehicle data communicated only refers to vehicle characteristics which are visible for the human eye (e.g. registration number or colour) eavesdropping is not a new threat, although it might be done more efficiently using EVI.

Integrity of the Use of Vehicle Identification

Starting point for this privacy threat is that the received vehicle identity and other vehicle data should not be used to build user patterns of the vehicle (registration) owner.

Fraud Aspects

Before discussing the security of EVI, we will elaborate the definition of fraud and some considerations concerning the countermeasures for fraud.

The premise on security is that the public acceptability of EVI is for a significant part dependent on the issue of fraud. But what is fraud? Fraud can be defined technically and from a user's point of view.

A technical definition of fraud in the EVI context is:

Fraud is the evasion or disturbance of a correct identification of the vehicle

Fraud can be initiated by a vehicle owner, c.q. vehicle driver. In this case, fraud can be defined as follows.

Fraud is to willingly and knowingly manipulate the EVI System
in such a way that the send data do not
commensurate with the correct vehicle identity in order to gain a benefit.

Fraud can also be initiated by a third party. In this case, fraud can be defined as follows:

Fraud is to willingly and knowingly manipulate the EVI System
in such a way that the received data is not
commensurate with the correct vehicle identity in order to gain a benefit.

Benefit in this sense can be taken in its widest meaning, it includes financial gains or losses, an advantage or other benefit.

There are two basic principle ways to manipulate the EVI System. The first principle focuses on the integrity of the EVI System, the second on the availability of the EVI System.

Integrity of the In-vehicle EVI components

The starting point for fraud is the possibility that the in-vehicle EVI components do not indicate:

- the correct vehicle identity (e.g. another EVI identity is spoofed); and
- the correct vehicle data (other than the vehicle identity) in case this data is stored in the in-vehicle EVI components.

The information processed in the EVI System should not be violated. The manipulation of the correctness of the EVI System aims at deliberate modification or destruction of data. Correctness is also known as integrity.

> **Example:** The software in the In-vehicle EVI components is modified (e.g. by means of a Trojan horse or virus) resulting in a non-correct vehicle identity or other vehicle data.

Availability of the In-vehicle EVI components

Starting point for this fraud possibility is that a vehicle can not be identified since its in-vehicle EVI components are not available or the signal is jammed. All elements of the In-vehicle EVI components should be readily available to be able to identify the vehicle correctly. Manipulation of the availability of the In-vehicle EVI components aims at deliberate creations of defects.

> **Example:** Disconnecting the external power supply from the in-vehicle EVI components.

Privacy Threats and Fraud from the Perspective of an Impostor

In case of EVI, it is realistic to expect privacy threats and fraud to occur. We will demonstrate this via a set of scenarios, not having the intention to be complete. In the next section the possibilities to embed countermeasures in the EVI-system will be explored, given the definition of privacy threat and fraud and the illustrative scenarios.

Scenario 1: threatening the privacy via non-authorized use

A garage owner challenges with an EVI reader and/or writer the in-vehicle EVI components of passing or stationary vehicles and checks the latest date of the MOT (annual vehicle control). He sends vehicle (registration) owners whose MOT is overtime an offer to take care of the MOT for a reduced price.

> **Motive & Benefit:** more efficient and concentrated acquisition and therefore more trade for the garage owner.

Scenario 2: threatening the privacy via unlawful eavesdropping and tracking vehicles

A fleet owner eavesdrops unlawfully using EVI reader and/or writers along the road side. In this way he can build user patterns of the trucks of his competitors. The user patterns might give him information about the clients of his competitors. This might result in increased trade for the fleet owner and an opportunity to unfairly compete.

> **Motivation & Benefit:** more efficient and concentrated acquisition.

Scenario 3: fraud via incorrect vehicle data

The vehicle (registration) owner changes or spoofs the vehicle identity and eventually other vehicle data as stored in the in-vehicle EVI components. The vehicle identity is not reliable anymore.

> **Motivation & Benefit:** the costs to fraud are lower or equal to the revenues. For example, in case of enforcement of traffic rules: costs: cost for an EVI reader and writer, revenues: missed fines, no tax payment.

Scenario 4: fraud via non-availability of the communication between in-vehicle EVI components and reader and/or writer

The vehicle driver winds a piece of foil around the antenna of the in-vehicle EVI components and thereby prohibits the in-vehicle EVI components to broadcast the vehicle identity or to be challenged by the reader and/or writer to request the vehicle identity.

> **Motivation & Benefit:** the costs to fraud are lower or equal to the revenues. For example, in case of enforcement of traffic rules: costs, 2 cent; revenue, missed fine of 40 Euros.

Scenario 5: malicious attack on EVI

An impostor jams the communication between in-vehicle EVI components and reader and/or writer and thereby prohibits identification of the passing vehicles.

> **Motivation & Benefit:** civil disobedience.

6.3 Possibilities for Countermeasures

As said, for the EVI System there are two reasons to define countermeasures. The first reason is to provide protection against the fraud possibilities. The second reason is to provide protection against threats of privacy of the vehicle owner / user.

Possibilities for countermeasures

The type of security measures can differ. The following types can be distinguished:

- *Legal*: A law or a set of laws provide the do's and don'ts of using the EVI System (i.e. an overall security policy) including the sanctions;
- *Operational*: Threats such as Denial of Service by tampering or covering the EVI device can be countered by operational means such as close range reading, spot checking, matching with automatic licence plate recognition and setting the EVI device in a broadcast mode. As such mobile enforcement might be necessary;
- *Organisational*: Principle, according to which information security issues are organised (e.g. separation of duties, i.e. someone cannot perform a certain task and control that same task). These measures relate to the organisations responsible for certain parts of the EVI System (topic for the institutional assessment);
- *Physical*: Reduces the vulnerability of, or threat to an asset by the application of physical barriers and control procedures (e.g. secure environment for issuing the in-vehicle EVI components);

- *Procedural*: A regular order of performing activities compliant with security guidelines (e.g. obligatory responsibility for the vehicle (registration) owner and regular inspection of the in-vehicle EVI components by the vehicle owner and by the public authority).
- *Technical*: Reduces the vulnerability of, or threat to an asset by using software features, firmware and/or hardware (e.g. a hardware card that implements a cryptographic algorithm).

In order to be able to define the reliability of the vehicle identity and identification, the possibilities to come to a secure EVI will be explored bottom up for every type of countermeasure.

Possible Technical Countermeasures

For the EVI-system as a whole six elements are important, namely: confidentiality, integrity (data), availability, controllability, authenticity and non-repudiation. In table 6.1 the definition of these elements is given plus the part in the EVI-system where a certain element has to be covered.

Table 6.1: Security elements for the EVI system.

Security elements	Definition	To be covered in part of the EVI-system
Confidentiality	Property that information on the vehicle itself and the vehicle (registration) owner is not made available or disclosed to unauthorised individuals, entities or processes;	ID Only: Access to the Vehicle Registration database
		Data Set: Access to the Vehicle Registration database
		All Data: EVI Device + Access to the Vehicle Registration database
Integrity (data)	Feature ensuring that data have not been changed or destroyed. Property that data has not been altered or destroyed in an unauthorised manner;	EVI device Reader and/or Writer (Out of the scope of EVI: Vehicle Registration database)
Availability	Property of being accessible and useable upon demand by an authorised authority	EVI device (Out of the scope of EVI: Vehicle Registration database)
Controllability	Property of being controllable that the data stored in the in-vehicle EVI components belongs to the vehicle and vice versa	EVI device
Authenticity	Feature that information is guaranteed to be of the stated vehicle and to be send to an authorised authority and vice versa.	EVI device Reader and/or Writer (Out of the scope of EVI: Vehicle Registration database)
Non-repudiation	The originator or recipient of information cannot successfully deny having sent or receiving the information.	EVI device (link to reader and./or writer) Reader and/or Writer (link to Vehicle Registration database)

In the exploration of the technical countermeasures we assume that the in-vehicle EVI components are designed, manufactured, issued and maintained correctly.

Confidentiality (via mutual identification and authentication), ***Integrity*** of data (via authorized access to the data and via mutual control of the exchanged data) and ***Authenticity*** (via mutual authentication) can be covered for a restricted period by transferring the in-vehicle EVI components into a so-called secure device. ‘Restricted period’ since ‘methods to attack will improve while the chip will stay the same for at least 10-20 years’ (Work Package 3). An option is to deinstall the in-vehicle EVI components after a fixed period and reinstall a new, improved type of in-vehicle EVI components. A way of working rather common in the banking world with credit cards, debit cards and inter-sector electronic purses.

In case of a Write-Once-Read-Many (WORM) EVI device the possibility to manipulate the vehicle data stored in the device becomes even more difficult, if not impossible. On the other hand, someone knowing the security algorithms can rather easily copy such a WORM.

In work package 3 it was stated that the most important components of an in-vehicle EVI components will be: CPU, Data Storage, Crypto Processor, Key Block, Wireless I/O, Clock and Internal battery or connection to vehicle mains (figure 5.5).

With respect to transferring these in-vehicle EVI components into a secure device (at least) four options can be distinguished, namely:

- *Option 1: a monolithic whole with internal power supply* (figure 6.2): All components (including the internal power supply) are embedded in one so-called secure device. The fraud and security related requirements can be defined for this whole, plus the external interface between secure device and EVI environment.

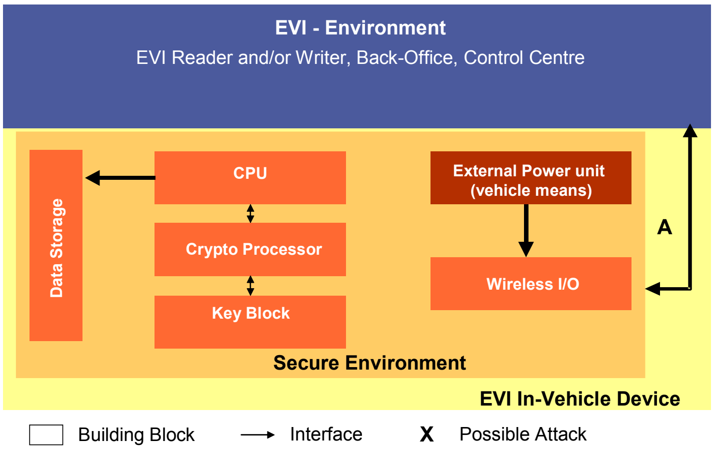


Figure 6.2: Option 1: In-vehicle EVI components as a monolithic whole with internal power supply.

- *Option 2: a semi-monolithic whole with external power supply* (figure 6.3): All components are embedded in one so-called secure device except for the external power supply. The fraud and security related requirements can be defined for the secure device plus the external interfaces between secure device and power supply and EVI environment.

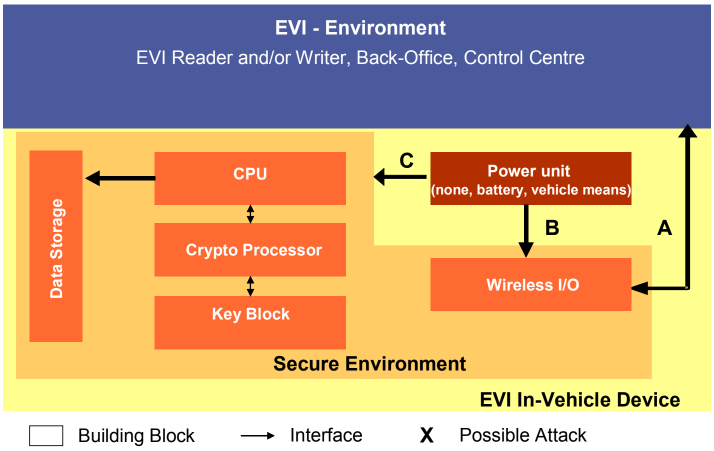


Figure 6.3: Option 2: In-vehicle EVI components as a semi-monolithic whole with external power supply.

- *Option 3: a semi-monolithic whole with external power supply and antenna* (figure 6.4). All components are embedded in one so-called secure device except for the external power supply and the antenna for the communication with the reader and/or writer. The fraud and security related requirements can be defined for the secure device plus the external interfaces between secure device and power supply, in-vehicle antenna and EVI environment.

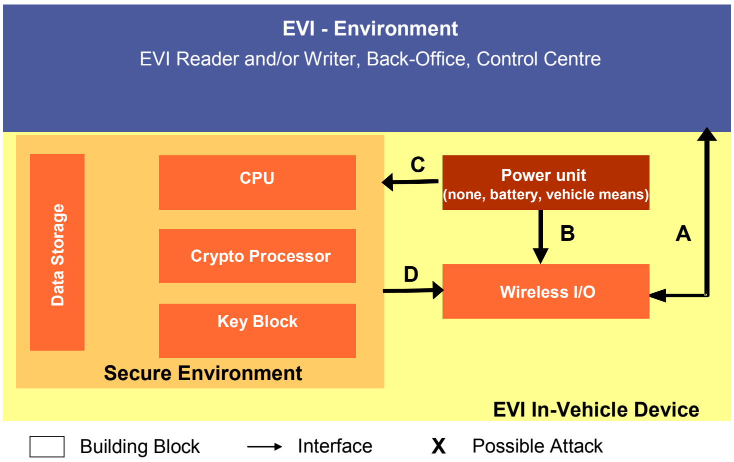


Figure 6.4: Option 3: In-vehicle EVI components as a semi-monolithic whole with external power supply and antenna.

- *Option 4: built up out of a series of components*: Each component has its own functionality for which fraud and security related requirements need to be defined.

The (semi-)monolithic options help us to safeguard the confidentiality and the integrity (of data) with a very limited set of points to be attacked by an intruder.

The ***availability*** of the interface between the in-vehicle EVI components and the reader and/or writer can be jammed or spoofed by a third party, not being the vehicle (registration) owner of the passing vehicles. This attack can be detected by the reader and/or writer and notified to the competent authority. This authority can remove the jammer[1].

From inside the vehicle, the availability of the in-vehicle EVI components can be undone by forcefully removing the tag from the car. The reader and/or writer has to fall back on a video shot of the license plate, or has to pass a signal on to a surveillance team who has to retrieve the specific vehicle.

More subtle, the availability of the in-vehicle EVI components can be interrupted via the power supply and the antenna for wireless communication with the reader and/or writer.

The need for internal power supply (option 1 versus options 2 and 3) depends on the chosen communication technology, as was already illustrated in the realisation types of Work Package 3. In fact only functional level 1 can be realised in a batteryless form by using RFID. The rest of the functional levels will need an internal or external

[1] In case of an infrared communication, the jammer will be visible since the only place where the jammer can be is within the line of sight.

(vehicle) power supply. So this is a serious entrance point for fraud. A possible countermeasure is to put a time stamp (data + time) in the 'data storage' inside the in-vehicle EVI components at the moment the power supply is switched on and off. An authorised authority can always control whether the in-vehicle EVI components have not been out of order improperly (see box below). Depending on the way functional level 2 (write once, ready many) will be realised this time-stamping is whether or not possible.

Illustration of a countermeasure for fraud (disconnecting the in-vehicle EVI components from the external power supply)

1. Valid in-vehicle EVI components are installed correctly in the correct accompanying vehicle;
2. The driver disconnects in-vehicle EVI components from the external power supply;
3. The in-vehicle EVI components detects that it is disconnected from the external power supply and writes a time stamp in the data store;
4. The vehicle (registration) owner's Obligatory Responsibility starts, and thus the driver makes an appointment with the correct repair-organisation to repair the in-vehicle EVI components.
5. The date of the repair is four days later (e.g. the last day that is allowed by law).
6. On the date of repair the vehicle (registration) owner connects the in-vehicle EVI components to the external power supply again.
7. The in-vehicle EVI components detects that it is connected to the external power supply (again) and writes a time stamp in the data store;
8. The vehicle (registration) owner cancels the repair appointment.
9. A couple of day's later the vehicle (registration) owner starts with point 2.
10. A couple of months later an authorised authority inspects the in-vehicle EVI components. He derives from the time-stamps that the in-vehicle EVI components has been connected and disconnected from the external power supply more and longer than reasonable.

The choice to embed the antenna in the secure device depends to a certain extent on the way the in-vehicle EVI components are build. In Work Package 3 three locations in the vehicle for the in-vehicle EVI components have been distinguished, namely: on the dash-board, against the front-window and on the vehicle body (the bulkhead). The location on dashboard will (according to Work Package 3) often depend on specific car designs and won't be always available. The location behind the windscreen has as disadvantage that the windscreen itself is rather vulnerable. Many vehicles have to change their windscreen, sometimes even more than once, during their life time due to cracks. This implies that with changing the windscreen, the in-vehicle EVI components should be changed too, or at least be disconnected and connected again. The location on the vehicle body implies in case of functional levels 2, 3 and 4 that the in-vehicle EVI components will have an external interface to an antenna more on the outside of the vehicle for wireless communication short range or wide area.

Within or outside the secure device, an antenna is an obvious point of attack. 'Shielding the antenna with a special metal foil' prohibits the in-vehicle EVI components to receive or send any information. This type of impostor is difficult to catch. Just as with forcefully removing the tag from the car, the reader and/or writer has to fall back on a video shot of the license plate, or has to pass a signal on to a surveillance team who has to retrieve the specific vehicle. Shielding the antenna however is not permanently and can be done on a trip basis.

In case of an extra external interface between the secure device and the antenna an extra point of attack is introduced.

So availability is a security element of concern for EVI.

This brings us tot the question: ‘how will the system differentiate between a vehicle from a non-participating country and one that has had its EVI device blocked or removed?’. One method is to combine the EVI reader and/or writer with a ‘traditional’ camera and take a snapshot of the licence plate in case the EVI reader and/or writer can not communicate with the in-vehicle EVI device. This means that EVI will not replace the licence plate and the camera, but is a more efficient addition to the traditional way of vehicle identification.

The ***controllability*** can be improved by cross-linking the data used to identify a vehicle. In the current situation, the act of identifying a vehicle always involves the vehicle, vehicle documents and a registration authority. The features of the vehicle have to comply with both the vehicle documents and the information in the vehicle registration database. Information that should be found in all sources is:

- The Vehicle Identification Number (VIN), which would need some improvement to make it unique;
- The vehicle characteristics (weight, height, class as mentioned in directive 99/37); and
- The vehicle registration number.

Every passenger car registered after 1994 should be equipped with a vehicle identification numbers (VIN) according to the directive 76/114/EC. This directive prescribes among others that a vehicle must be uniquely identifiable - without assistance of the manufacture - for at least 30 years after introduction. The VIN is often 'punched into metal' or stored in for instance the motor management system by the OEM and on behalf of the OEM. The VIN-number is checked during the periodical inspection (96/96/EC) with the vehicle documents. An investigation carried out in 2004 among 8 million vehicles in the Netherlands and among 6 million vehicles in Norway - not older than 10 years - pointed out that only about 10 vehicles used a double VIN number. These duplications were due to processing errors and are recovered by now.

No study has been carried out to compare the uniqueness of VIN in two or more countries; for instance can the same VIN be found in the Netherlands and in another Member state? Practice shows that this is not a real issue. Cross border registration, for instance by import and export never gave any problem due to a duplicate VIN.

Therefore it can be concluded that in practice the present VIN is a probably 100% identifier for passenger cars not manufactured before 1994.

With EVI all the conventional identifiers can be stored in the EVI device (see figure 6.5). In this way an impostor has to falsify both the physical numbers and the digital numbers in the in-vehicle EVI components. This is still not a guarantee that the vehicle identifier(s) is/are one hundred percent reliable, but we can come one step closer again compared to the current situation.

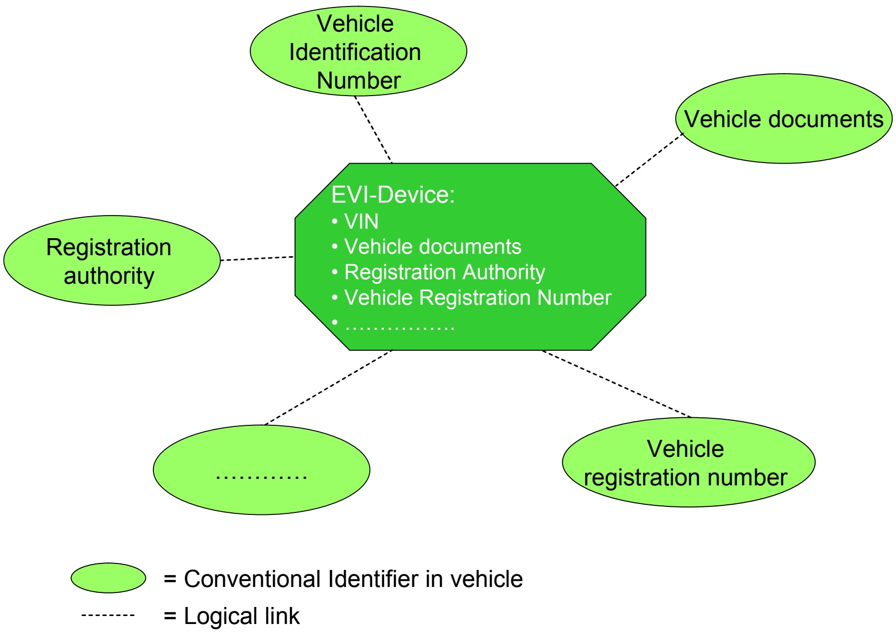


Figure 6.5: Cross-linking of vehicle identifiers to improve the controllability and thereby the reliability.

This leaves us with the **non-repudiation**. To cover the non-repudiation, in-vehicle EVI components should be able to send a (merged) combination of data elements (e.g. vehicle identities as drawn in figure 6.5) to a reader and/or writer (in case of broadcasting and challenge response) or signs the identification transaction (in case of challenge-response).

Possible for Procedural, Physical, Organisational and Legal Countermeasures

Taking stock of the possibilities to introduce technical countermeasures, we are left with the correctness of designing, manufacturing, issuing and maintaining the in-vehicle EVI components, the availability of the in-vehicle EVI components and the protection of the integrity and confidentiality (in case all data is stored in the in-vehicle EVI components; not over the short period but over the longer period). It should be possible to cover all three aspects with other types of countermeasures.

On the level of *procedural countermeasures* the ***availability*** of the in-vehicle EVI components can be placed under the Obligatory Responsibility for the vehicle (registration) owner. We still need surveillance teams to discover the impostors, however once an impostor is caught it is not a question anymore of who is responsible for the availability of the in-vehicle EVI components. In fact, the same counts for integrity of data.

Besides surveillance, the operations of the in-vehicle EVI components can be inspected during the MOT or any other regular inspection by a public authority.

As said in the previous section, the ***integrity*** and ***confidentiality*** (in case all data is stored in the in-vehicle EVI components) in fact ask for deinstallation of the in-vehicle

EVI components and reinstallation of a new device after several years. This means that the deployment scenarios as described in chapter 3 will be repeated with a cycle time of a couple of years. This will increase both the complexity of the deployment and the costs for EVI. The alternative is to accept an increasing risk that the integrity and confidentiality (in case all data is stored in the in-vehicle EVI components) are tampered with. No choice has been made in this feasibility study so far.

In the exploration of the technical countermeasures we assumed that the in-vehicle EVI components are designed, manufactured, issued and maintained correctly. This assumption is based on the possibility to take *organisational countermeasures* to create so-called secure environments, where the different steps in the life cycle of EVI are organised and executed. In a secure environment the steps taken are verified and if necessary certified by a competent authority. In case of manufacturing the manufacturer can produce a limited set of devices by giving the devices a hardware key and thereby a unique number.

The following environments can be distinguished:

- *ENV_GCTRL*: Environment under public authority ('government') controlled circumstances. An environment suitable for manufacturing, installing, issuing and maintaining the in-vehicle EVI components, c.q. devices. It is also an environment where EVI is used by public authorities to enable their services;
- *ENV_PCTRL*: Environment under trusted market controlled circumstances. An environment suitable for manufacturing, issuing and maintaining the in-vehicle EVI components, c.q. devices; and
- *ENV_PUB*: Public environment. An environment where the EVI is used to enable private services out of the control of a public authority.

In the institutional assessment these environment are used to identify the institutional consequences of EVI.

A *physical countermeasure* is to really protect a secure environment not only by verification and certification of the 'input' and 'output', but also by physically protecting the building or the area where the activities take place.

A *legal countermeasure* is to put the Obligatory Responsibility for the vehicle (registration) owner and the rule on the proper use and what is seen as misuse in a legal framework for EVI. This is in fact the last step in a series of countermeasures.

6.4 Reflection on the Security assessment

By embedding security in the complete life cycle of EVI, the reliability of the unique vehicle identity and the vehicle identification can be improved. However, even with EVI it is realistic to expect impostors to fraud the EVI system or to misuse the EVI system and violate the privacy of the vehicle (registration) owners. On the other hand there are quite some possibilities to take countermeasures to protect EVI for such fraud and threat of privacy.

At any rate, the EVI device should be implemented as a secure device. In case of a Write-Once-Read-Many (WORM) EVI device the possibility to manipulate the vehicle data stored in the device becomes even more difficult, if not impossible. In case of an external power supply, the EVI device should be able to notify and for instance time-stamp both connection and disconnection to the power supply.

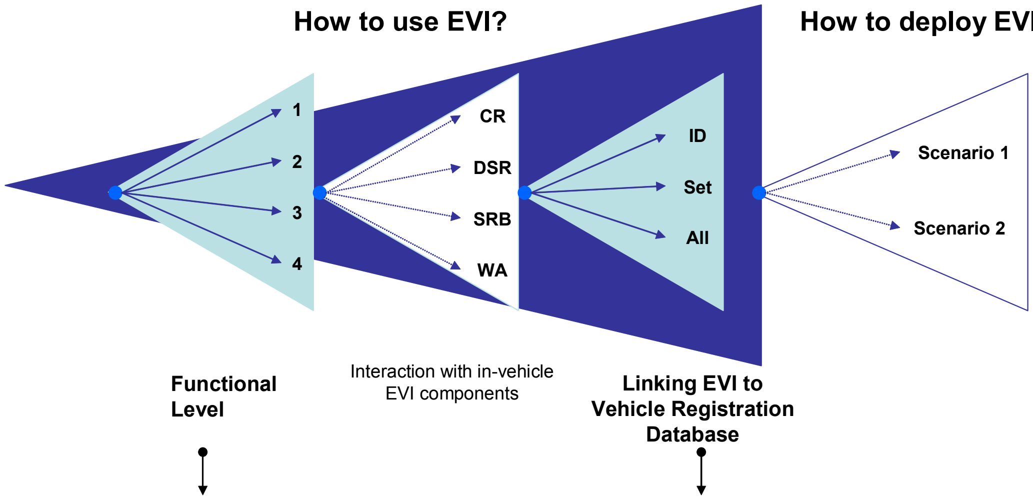
The EVI reader and/or writer should be able to notify jamming of the communication between the in-vehicle EVI components and the reader and/or writer. More difficult is spoofing of the EVI-data send by the in-vehicle EVI device. Jamming can be detected externally, spoofing not. If spoofed, the EVI reader and/or writer will receive a false reading. Spoofing has to be solved in the security of the communication between the two secure devices.

Issues left over after exploring those countermeasures are:

- Interrupting the ***availability*** of the in-vehicle EVI components by a vehicle (registration) owner (and/or driver). Surveillance teams are needed to discover these impostors.
- The protection of the ***integrity*** and ***confidentiality*** (in case all data is stored in the in-vehicle EVI components will weaken during the life time of the in-vehicle EVI components since. Regular (e.g. once in the four years) deinstallation and reinstallation of new in-vehicle EVI components is needed if we want to keep the protection on the same level.

The countermeasures for both issues will increase the costs for EVI and therefore will influence the ‘business case’ of EVI.

The security assessment results are summarized in figure 6.6.



The basics for security is to make the EVI device a secure device, in order to safeguard the integrity of the data send to the reader and/or writer. The security is increased even more in case of 'Write once-Read many'.

A weak spot is the availability of the wireless I/O to the reader and/or writer which can be blocked.

A reader and/or writer should be capable to notify jamming of the communication between vehicles and reader and/or writer.

The life cycle of EVI should be covered via secure environments

By storing the set of vehicle (component) identifiers in the EVI device, a fast and simple cross check of the vehicle status is possible.

Just as with the licence plate confidentiality should be guarder by the back-office.

Figure 6.6: Summary of the security assessment results.

7 INSTITUTIONAL ASSESSMENT

In this chapter the institutional assessment is described. From an institutional point of view basic functional levels and scenarios are linked together.

The institutional assessment focuses (figure 7.1) on the basic functional levels plus the differentiation both on the external interface between in-vehicle EVI components and the reader and/or writer and the distribution of the vehicle data over the EVI-system and the back-office. Furthermore, the deployment scenarios are taken into consideration.

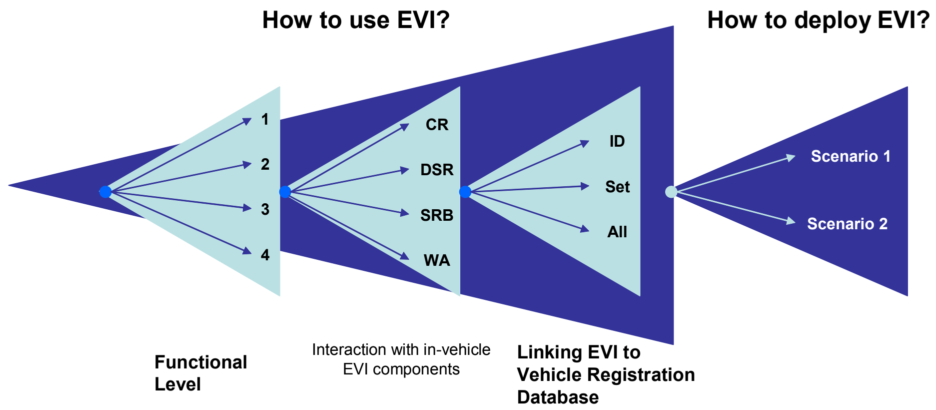


Figure 7.1: Objects of institutional assessment.

7.1 INSTITUTIONAL CONSEQUENCES OF THE EVI SYSTEM

So far the focus has been on the technical assessment of the EVI system. However the EVI system is only a part of EVI (figure 7.2). Also the systems that surround the EVI system should be assessed since EVI is not only a technical device inside the vehicle. The device has also close relationships with 'the world around us'. This chapter focuses on the institutional assessment, where we will consider the following issues:

- Impact of the distribution of the vehicle data over the in-vehicle EVI components and the vehicle registration database;
- Impact of security on the organisation of the vehicle registration and identification; and
- Impact of environment on the organisation of EVI.

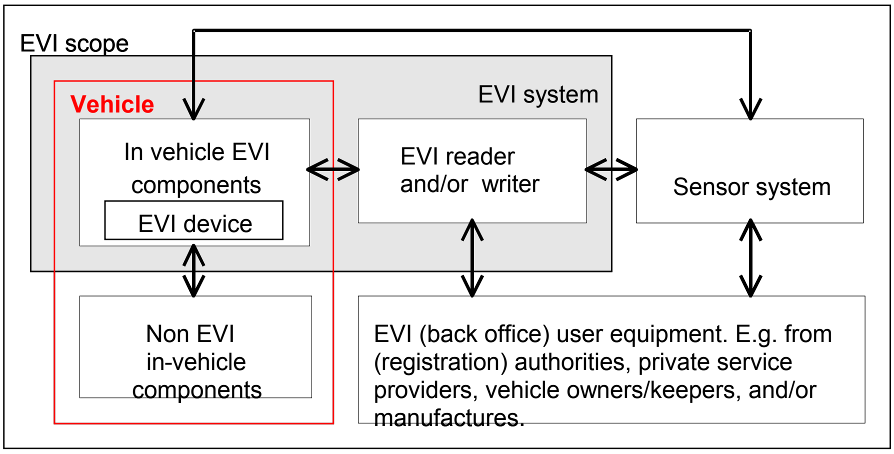


Figure 7.2: EVI scope diagram. (source Work Package 2)

7.2 Institutional consequences of the chosen communication technology

As shown in figure 5.2 the explored communication systems are the realisations of the external interface between the in-vehicle EVI device and the reader and/or writer. As an alternative for wired connection, the communication systems can also be (or have to be) the result of the external interface between the EVI reader and/or writer and back-office operational.

The construction of this reader and/or writer depends on the communication system it belongs to.

For close range communication hand-held reader and/or writers will do. The communication between hand-held reader and/or writer and back-office can be done via one of the commercial wireless communication systems, like for instance cellular telephone or WIFI.

Short Range Communication requires gantries on which the reader and/or writer can be attached. For some road stretches gantries are already available for traffic management purposes or for road and city lights, which might be used for EVI. For other roads no gantries are available, which requires an additional investment in order to deploy EVI readers and/or writers. Furthermore the reader and/or writers need to be connected to the back-offices. In some regions the available wired communication systems can be used while in other regions the available wireless communication systems, such as mobile phones, can be used. Installing the gantries plus reader and/or writers and connecting them to the back-office asks for a specific organisation of public authorities or commercial organisations servicing the public authorities.

Wide area communication is available in large parts of Europe. It requires base stations which function as a reader and/or writer. Telecommunication operators have to be paid for the use of their wireless network. For specific regions or locations with a poor coverage by the wireless, wide area communication system, one or more extra base stations might be necessary for EVI. These base stations will be installed in negotiation with the telecommunication operator. No specific organisation will be needed.

7.3 INSTITUTIONAL CONSEQUENCES OF THE DISTRIBUTION OF THE VEHICLE DATA

With respect to the distribution of the vehicle related data over the EVI system, roughly there are three extreme options, namely:

1. Store all the data needed in the in-vehicle EVI components;
2. Download regularly and store all the data in the EVI reader and/or writer and store a basic, unique vehicle identifier in the in-vehicle EVI components only; and
3. Keep all the data stored in the back-office and store a basic, unique vehicle identifier in the in-vehicle EVI components only.

Every option has its own advantages and disadvantages. If all vehicle-related data needed to enable applications are stored in the vehicle (option one), a real-time interrogation with the vehicle is possible in free flow conditions. Moreover, it will be possible to check cross-links in vehicle data for stationary vehicles within a reasonable time frame. The main disadvantage of this option is that it is complex to update data stored in the vehicle. When only a unique vehicle identifier is stored (option three), the reader and/ or writer has to request all additional data needed to enable a certain application from the back-office 'real-time'. This makes severe claims on the real-time response-request capabilities of the back-offices. On the other hand it is easier to update data stored in the back-office. Option two also has a unique identifier in the vehicle, but all data is stored in the reader and/or writer as well as the back-office. This limits the demands on the real-time response-request capabilities and provides an easier update procedure through the back-offices.

Option two and three could be realised by means of introducing a Unique Vehicle Identifier. The VIN-number could be used, under the restriction that the VIN is unique. Every passenger car registered after 1994 should be equipped with a vehicle identification numbers (VIN) according to the directive 76/114/EC. This directive prescribes among others that a vehicle must be uniquely identifiable - without assistance of the manufacture - for at least 30 years after introduction. The VIN is often 'punched into metal' or stored in for instance the motor management system by the OEM and on behalf of the OEM. The VIN-number is checked during the periodical inspection (96/96/EC) with the vehicle documents. An investigation carried out in 2004 among 8 million vehicles in the Netherlands and among 6 million vehicles in Norway - not older than 10 years - pointed out that only about 10 vehicles used a double VIN number. These duplications were due to processing errors and are recovered by now.

No study has been carried out to compare the uniqueness of VIN in two or more countries; for instance can the same VIN be found in the Netherlands and in another

Member state? Practice shows that this is not a real issue. Cross border registration, for instance by import and export never gave any problem due to a duplicate VIN.

Therefore it might be that in practice the present VIN will be quite near to 100% identifier for passenger cars not manufactured before 1994. However before coming with conclusions further study and testing is necessary.

Using the VIN as the unique vehicle identity is highly favoured by some Member States and the automotive industry. An open question is what the opinion is of the imported vehicles in Europe, especially in those countries where the VIN is not a requirement and/or for low volume vehicles that still operate on a chassis number.

All options contain some bottlenecks, while this assessment does not choose an option; we do feel it is necessary to identify these bottlenecks.

- The reliability of the vehicle identity;
- The real-time capabilities of the wireless interface between the EVI reader and/or writer and the EVI back office at the registration agencies, and
- The efficiency of EVI in enabling applications.

The *reliability* of the vehicle identity has been discussed in the security assessment. Given this discussion the set of conventional vehicle identifiers should be stored in the in-vehicle EVI components. In order to retrieve additional vehicle data, the vehicle identity and the identity of the specific vehicle registration office should be known. The latter asks for an additional identifier in the in-vehicle EVI components.

The *interface capabilities* together with the registration agencies determine whether it is possible to retrieve vehicle related data dynamically (e.g. during interaction with a passing vehicle in free flow traffic conditions). Therefore it is important to know how European back-offices are organised and how they communicate. Two studies of the Dutch registration authority, RDW, were used; *the vehicle chain in Europe* and a survey carried out among 19 registration authorities in Europe. The aim of the survey was to roughly map the way registration authorities communicate with the enforcing authorities and what keys where used to consult the databases. Due to the size of the response (9), the way the questions were posed, and the way the respondents were selected conclusions about the validity and reliability of the survey findings cannot be considered representative but indicative for the European registration authorities. From that point of view the most important conclusions are:

- A majority of the questioned authorities (seven out of nine) provide access to vehicle and ownership data via an on line real time system. Both national and international authorities can get access. The size of the response times is in seconds. Many less sophisticated applications can perform with a response time of seconds or even with batch processing. More sophisticated applications like weighing in motion demand a shorter response time;
- Although not every country has a centrally operating licensing organisation or population register, interfaces for opening up the data for different users (national and international enforcement, statistics etc) are already operating;

- A concern remains cross border traffic. Based on the same RDW survey 5 out of 9 countries provide foreign enforcing authorities access to their national vehicle data via an on line, real time connection. The system used is EUCARIS. At this moment twelve countries are connected via EUCARIS. Countries who are not connected and non-EU countries (e.g. former Yugoslavia, Albania or Switzerland) remain an issue.

From the study "The Vehicle Chain in Europe", we can draw three conclusions (see text box below):

1. Not every country has a centrally operating licensing organisation, but the interface for opening up the data for different users (national and international enforcement, statistics, etc) is already operating. There is a big difference in data access. In for instance Sweden information about the vehicle and the owner is given to the public based on a licence plate. In the Netherlands this is only supplied if the owners gives permission;
2. Not every country has a central population register, but the interface for opening up this information for national purposes is already in operation.
3. Licensing organisations show great differences in the extent of their involvement in other links in the vehicle and driving licence chains.

Interfaces provide connections between licensing organisation

In Germany there are sixteen federal states that carry out the licensing activities. The state government department Kraftfahrt-Bundesamt (KBA) only manages and operates activities involved in the central registrations. In France there are approximately one hundred departments involved in carrying out licensing activities. Although the Ministry of Transport is responsible for policy, supervision, and legislation, it has no implementation tasks. In Switzerland, licensing activities are conducted by the twenty-six cantons. The Federal Road Office (ASTRA), that forms part of the Ministry of the Environment, Transport, Energy and Communication, is responsible for policy, legislation and central registrations.

Interfaces provide connections between population registers

An important aspect in regard to licensing is the presence of a central population register in the individual countries. After all, this kind of register can be very helpful in updating personal details (names and addresses) in the central vehicle and driving licence registers. This is the case in Belgium, Sweden and Finland. The larger countries such as Germany, the United Kingdom and France, however, have no central population register. Here, people holding registered vehicles update their own personal details (names and addresses) in the vehicle registration and are legally obliged to submit changes to the various agencies. Within the vehicle licensing systems used in the various countries, the presence or absence of the role played by a central population register is notable. In countries where the register is updated by a central population register, the vehicle register often plays a major role in implementing various vehicle-related legal requirements. In countries without a central population register, however, the implementing of vehicle-related requirements such as tax payment is used to update personal details (names and addresses).

Licensing organisations show great differences in the extent of their involvement in other links in the vehicle and driving licence chains

Every country has its own opinions on how licensing and other administrative and technical tasks surrounding the vehicle chain should be organised; for this reason, there is no single standard licensing organisation.

Understanding the differences in the vehicle registration in Europe, the question whether the back-offices are able to meet with the strict real-time constraints becomes more serious. It is doubtful whether there are back-offices that can respond to a request within one hundred milliseconds (see text box below). On the other hand many less sophisticated applications can perform with a response time of seconds or even with batch processing. Think for instance about red light, tolling and speed enforcement. Based on the RDW survey it is expected that several back-offices in Europe can already perform with sufficient response time. Additional research is needed to investigate the feasibility of split second real-time response.

In order to gain the full efficiency benefits of EVI it should be possible to replace the existing systems for classification and identification along the road. Especially when the classification asks for more data than just a unique vehicle identifier, for instance the vehicle type. After all there are offences such as speed enforcement where for example trucks have lower speed limits than the maximum for the road, also think of bus lane enforcement priority lanes.

Sophisticated applications demand limited time for interrogation with the vehicle

Weighing in motion

Work Package two identified weighing-in-motion as one of the public authority applications. As the communication between the vehicle and the reader and/or writer take place with, for example, DSRC (with a reading range of approximately 30 meters if microwave and 100 meters if infrared), the time for interrogation is, in case of Heavy Duty Trucks which are limited to 90 km/hour, 1.2 seconds. During this short time it might be necessary to consult back-offices, placing a large constraint on the system. If data such as axle weights limits and total weight limits are already in the EVI, a simple cross- check can be performed afterwards.

Speed enforcement

EVI can be used for a more human way of speed enforcement when supported by an infrared communication technology. According to WP3 the communication range of infrared is 100 meter. When speed offences up to 250 km/hour should be registered, the time for interrogation with the vehicle is limited to 1.4 seconds. For a normal offense (e.g. 100 km / hour instead of 80 km / hour) the interrogation time is larger; 3.6 seconds. In case of a contravention the processing (connecting the vehicle to the owner) does not have to take place in a split second. It can be done for instance in a batch run.

Given the preference of some stakeholders for only a basic vehicle identifier stored in the in-vehicle EVI components, several issues need to be dealt with. First, the limitations of the back-offices to respond in real time on a request by the EVI reader and/or writer, second the claim for additional data to improve the reliability of the vehicle registration, and third the claim for additional data to replace conventional road side systems for classification and identification. A compromise can be found in storing a minimum set of vehicle related data in the in-vehicle EVI components and bring into operation (or keep operational) a real-time (seconds) interface between the EVI reader and/or writer and the EVI back-office. This minimum data set could consist of the conventional vehicle identifier plus the visual characteristics of a vehicle. We can use a subset from Directive 1999/37/EC, which is not likely to change often during the lifetime of the vehicle, such as:

- Vehicle identification number;
- Registration number;
- Vehicle make;
- Vehicle type;
- Vehicle category;
- Number of axles;
- Wheelbase; and
- Maximum and permissible laden mass of the whole vehicle in service.

None of this data is specifically privacy sensitive, since this data can already be read visually in every vehicle nowadays.

Of course, the subset to be used is dependent on the public authority application that should be supported. Table 7.1 illustrates how the public authority applications use vehicle related data (*green cells*). The table clarifies that not all applications can be supported by means of the identified subset. In some applications the subset is only a first starting point for enabling the application. More information should be available in the back-office to support the application (*orange cells*). An example is the application "Safe vehicle - annual vehicle inspection". In annex A it is described that the date of the last MOT inspection should be stored in the EVI device. However, through a Vehicle Identification Number (VIN) it is possible to enable this application in another way; namely, to track the necessary information from an appropriate database system. It should be stressed that the back-office has to be very well organised to enable a specific application. A one-to-one correspondence between the vehicle particulars appearing in the registration and the actual vehicle itself is critical. If the Unique Vehicle Identifier does not correspond with the data in the back-office none of the applications can be supported.

How to deal with cross border traffic is a second concern. As stated above not every country has an all-included central back-office system. Therefore solutions are needed how to deal with receiving data from foreign databases on time. A solution for finding the appropriate database quicker could be to include the country of residence of the specific vehicle. Moreover, as the European continent consists of several countries, it could be expected that not all countries are participating in an EU-wide EVI system (for example the new accession countries or countries like the former Yugoslavia, Albania and Switzerland). However cross-border traffic between these countries and countries using an EVI system is very likely. Hence, there is a chance that some public authority applications are not supported because e.g.

challenge-response between the vehicle and the reader/writer is not possible due to the absence of the necessary in-vehicle EVI components. Standard procedures followed today can be used to ensure support to the public authority applications.

Table 7.1: Illustration of how applications make use of data.

	Crime				Access control			Vehicle tolling				Traffic management and driver information											Enforce-ment		Vehicle Life Cycle			Traffic and transport regulation				
	Prevention of vehicle theft	Tracking and tracing of stolen vehicles and assets	Remote stopping of tracked stolen vehicles	Terrorism	Overview of cross border traffic	Border control	Access control of vehicles	Charging according to use	Charging according to use to include all social costs	Value pricing	Tolling	Dynamic limiting maximum speeds	Dynamic advice maximum speed on individual basis	Intelligent speed adaptation	Incident management	Misfit of the vehicle on the infrastructure	Informing road users	Anonymous guidance of road users	Taylor-made guidance of vehicles	Dynamically regulating of the road traffic	Offering additional capacity	Tracking and tracing of vulnerable people	Reduce damage to road	Enforcement	End of life	Identification of vehicle and components	Control vehicle life cycle	Safe vehicles - annual vehicle inspection	Safe vehicles - Inspection and recall information	Checking and controlling emissions	Controlling emissions	Monitoring/controlling hazardous goods
Vehicle Identification Number	green	green	green	green	green	green	green	green	orange	green	green	green	orange	orange	orange	orange	green	green	green	green	green	orange	orange	orange	green	green	green	orange	green	green	green	orange
Registration number	green	green	green	green	green	green	green	green	orange	green	green	green	orange	orange	orange	orange	green	green	green	green	green	orange		orange	green	green	green	orange	green	green	green	orange
Vehicle make	green	green	green	green											orange								orange		green	green	green					
Vehicle type	green	green	green	green											orange								orange		green	green	green					
Vehicle category	green	green	green	green			green	green	orange	green	green	green	orange	orange	orange	orange		green	green	green	green		orange	orange								orange
Number of axles											green	green	orange	orange	orange	orange							orange	orange								orange
Wheelbase															orange																	
Maximum permissible laden mass of the whole vehicle in service																orange							orange	orange								orange

(*green cells*) Illustration of how the public authority applications use vehicle related data
(*orange cells*) Illustration that not all applications can be supported by means of the identified subset of data in paragraph 7.3

7.4 Institutional Consequences of Security

As said in the security assessment, secure environments are needed to assure the security of the in-vehicle EVI components. To cover the complete life cycle of EVI the following secure environments are needed.

ENV_GCTRL

High trust

Specifying and Designing the in-vehicle EVI components in an environment under public authority controlled circumstances (ENV_GCTRL)

A consortium of public and private companies will design the in-vehicle EVI components, c.q. EVI device. The public authorities select and certify trusted companies. The public authorities control the environment.

Possible level of trust:	High
External perspective:	Everything that happens in this environment or that comes out of this environment can be fully relied on.

ENV_PCTRL

High trust

Manufacturing the in-vehicle EVI components in an environment under trusted market controlled circumstances (ENV_PCTRL)

Private companies build the in-vehicle EVI components, c.q. EVI device. Therefore the public authorities select and certify trusted companies. These companies control the environment.

Possible level of trust:	High
External perspective:	Everything that happens in this environment or that comes out of this environment can be fully relied on.

ENV_GCTRL

High trust

Manufacturing the in-vehicle EVI components in an environment under public authority controlled circumstances (ENV_GCTRL)

The administration on the issuing, maintenance and en-of-life of the in-vehicle EVI components, c.q. EVI devices will be done by the public authority. The public authority or one of her agencies controls the environment.

Organisation involved:

1. *Administrative organisation* (public authority or public agency):
    - *Initiation*: Organisation involved in the administrative processes with respect to central initialisation and configuration of in-vehicle device;
    - *Maintenance*: Organisation involved in the administrative processes with respect to changes of vehicle (registration) owner and changes in vehicle features;
    - *End-of-life*: Organisation involved in the administrative processes with respect to the end of life of a vehicle.

Possible level of trust:	High
External perspective:	Everything that happens in this environment or that comes out of this environment can be fully relied on.

ENV_GCTRL

Moderate trust

Issuing, Maintaining and End-of-Life of the in-vehicle EVI components in an environment under government controlled circumstances (ENV_GCTRL)

The EVI devices will be issued (distributed, installed, initialized), maintained and taken out of the vehicle again (end-of-life) in an environment that is under control of the public authorities. A public authority (or agency) is responsible for defining the fraud and security regulations that apply as a minimum in this environment. Furthermore, this agency is responsible to determine and enforce that the procedures are implemented and used in this environment. For retrofit this environment is distributed over a rather large number of locations, since a couple of million in-vehicle EVI components have to be issued. Therefore this environment is regarded to have a moderate level of trust.

Organisations involved:

1. *Physical-issuing (distribution) organisation* (public-authority-certified distributor): Organisation involved in the distribution of the manufactured EVI device to the organizations that will install and initialize the device.
2. *Physical-issuing (installation and initializing) organisation* (OEM for in-factory and public authority-certified garage for retrofit): Organisation involved in the issuing the EVI device
3. *Physical-maintenance organisation* (public authority-certified garage): Organisation involved in the physical

processes with respect to changes of the vehicle (registration) owner and changes in vehicle features;

4. *Physical-end-of-life organisation* (public authority-certified destruction company): Organisation involved in the physical processes with respect to the end of life of a vehicle.
5. *Security maintenance body*: Organisation involved in the processes of keeping the EVI System secure (tests, key management)

Physical location:	Private area
Security regulations:	Specific requirements of the public authorities (e.g. current requirements for MOT-garage plus some additional)
Level of trust:	Moderate
External perspective:	Everything that happens in this environment can be relied on. Everything that comes out of this environment needs to be verified on correctness.

ENV_PCTRL

Low trust

Using the in-vehicle EVI components in an environment under government controlled circumstances (ENV_GCTRL)

The EVI devices will be used in an environment that is under control of the public authorities. A public authority (or agency) is responsible for defining the fraud and security regulations that apply as a minimum in this environment. Furthermore, this agency is responsible to determine and enforce that the procedures are implemented and used in this environment. Usage of EVI takes place in the open field. Therefore this environment is regarded to have a low level of trust.

Example:	Enforcement of compliance to social rules.
Physical location:	Open field
Security regulations:	Specific requirements of the public authority with respect to detection of jamming and spoofing and taking countermeasures against both jamming and spoofing and against impostors who have blocked the availability of their in-vehicle EVI components.
Level of trust:	Low. The low level of trust contrasts with the essence of

	enforcement. Enforcement is about strict rules and procedures and strict regulations on type approval and certification. So in fact, the level of trust here can never be low. The open environment however makes the level of trust low. This contrast has to be solved in the security of the communication between the two secure devices (which can be trusted after all).
External perspective:	Everything that happens in this environment can be relied on. Everything that comes out of this environment needs to be verified on correctness

7.5 Institutional consequences of Environmental Rules

During the complete life cycle of the EVI System waste material will be produced, especially in the phases manufacturing, issuing and end-of-life. Given the fact that EVI concerns millions of vehicles, even small portions of waste material should be collected and recycled as much as possible. The environmental issue becomes even more important in a situation where from security perspective in-vehicle EVI components, c.q. EVI devices will be deinstalled and replaced regularly (every couple of years).

So in addition to the security related organisations (see previous section), a sanitation and recycle organisation is needed. Given the fact that EVI is a public authorities initiative this organisation should be under control of the same public authorities.

7.6 Organisation of the deployment

Organisations needed for the deployment

The different phases are organised in different environments. In table 7.2 these environments are outlined. Per environment the relevant phases in the life cycle of EVI are summed up.

As where it a fractal, within these environments secure environment might be necessary given the security assessment so far. The distinguished environment is adopted in table 7.2.

Table 7.2: Environments needed to realise the life cycle of EVI.

Environment	Character of the environment	Relevant phases
Specification	The environments in which the stakeholders participate that are responsible for setting a standard specification of EVI on a European level. A reference implementation will be build to evaluate the usability of the specifications. Secure environment: Specifying and Designing the In-vehicle EVI components in an environment under public authority controlled circumstances (ENV_GCTRL)	Specification Requirements
Realisation	The environment in which the stakeholders participate that will actually produce the components of the EVI system. This is also the environment in which the competent authorities certify these components. Secure environment: Specifying and Designing the in-vehicle EVI components in an environment under public authority controlled circumstances (ENV_GCTRL); and Manufacturing the in-vehicle EVI components in an environment under trusted market controlled circumstances (ENV_PCTRL)	Design Manufacturing

Implementation	The environments in which the stakeholders participate that are responsible for bringing EVI to an operational level.
	
	Secure environment:
	Issuing, Maintaining and End-of-Life of the in-vehicle EVI components in an environment under government controlled circumstances (ENV_GCTRL)
		Issuing:
		• Distribution;
		• Activation/configuring;
		• Installation.
		• Granting authority/Commissioning
		    ○ Self commissioning;
		    ○ Commissioning of other authorities

Operations	The environments in which the stakeholders participate that actually use EVI or operate applications that use EVI. Secure environment: Using the in-vehicle EVI components in an environment under government controlled circumstances (ENV_GCTRL); and Maintaining of the in-vehicle EVI	Use Management and updating of system

	components in an environment under government controlled circumstances (ENV_GCTRL)	
Recycling	The environment in which the stakeholders participate to disable the EVI components and recycle those components. Secure environment: End-of-Life of the in-vehicle EVI components in an environment under government controlled circumstances (ENV_GCTRL)	End-of-life

Deployment scenario 1

Specification

During the realisation not only the EVI components will be specified, but also the organisation for realisation will have to be organised and certified. We assume that the total time to pass through these activities is 2 years.

Realisation

During the realisation not only the EVI components will be designed, manufactured and certified, but also the organisation for issuing will have to be organised and certified. We assume that the total time to pass through these activities is 3 years.

Implementation

Deployment scenario 1 might start with a mandatory EVI of basic functional level 1 at once. Equipping the full car fleet at once in a region (country) is a large but still comprehensible logistical operation. Suppose:

- In a region of about 8 million vehicles circa 10,000 installation points are available;
- At each installation point net one qualified engineer is working on the installation of the in-vehicle EVI components;
- He can install the EVI device of basic functional type 1 in 10 minutes;
- An engineer can effectively produce 800 man-hours per year;
- No installation of gantries for EVI readers and/or writers is needed;
- Under these assumptions, the roll out of the mandatory EVI of functional level 1 will take about 2 months net

We assume that the gross total time to pass through these activities is 3 years, which seems reasonable given the net time of 2 months.

However it is most likely for scenario 1 to start with a mandatory EVI of basic functional level 2 at once. Even now equipping the full car fleet at once in a region (country) is a large, but comprehensible logistical operation. Suppose:

- The installation time of the EVI device of basic functional type 2 is 30 minutes;

- Under the same assumptions, the roll out of the mandatory EVI of functional level 2 will take about 6 months net.

We assume that the gross total time to pass through these activities is 4 years, which seems reasonable given the net time of 6 months.

Optional is to roll out a network of EVI readers and/or writers of gantries. This can be done on a step-by step basis starting with the available gantries and then adding new gantries.

The next phase is to grow further on a voluntary base to an EVI of functional level 2. Suppose:

- The installation time of the EVI device of basic functional type 4 is 2 hours (120 minutes);
- Under the same assumptions, every year about 4 million vehicles can be equipped with in-vehicle EVI components.
- Assuming that an engineer can only effectively produce 400 man-hours per year, since EVI level 4 is on a voluntary basis, every year about 2 million vehicles can be equipped, which brings us to 4 years for the total of 8 million vehicles.

We assume that the gross total time to pass through these activities is even more than 10 years, which seems reasonable given the net time of 4 years.

The timelines for scenario 1 are drawn in figure 7.3.

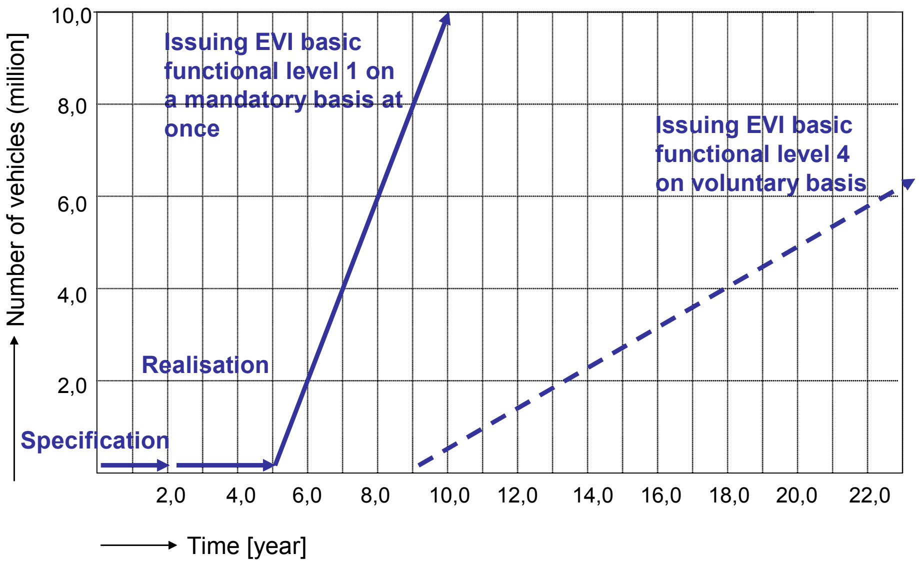


Figure 7.3: Timelines for deployment scenario 1.

Operations

Culturally public authorities are used to use the licence plate to identify the vehicle. In fact most or even all legacy systems are built up around this licence plate. It will take time to change this habit. Combining the actual rollout of EVI with the voluntary introduction of EVI can speed up this change. An example is given in the box below.

Illustration of combining mandatory implementation of EVI and learning to use EVI at the same time.

For instance, the public authority starts the rollout of EVI in those regions where road pricing or tolling is already used. Public authorities can upgrade their systems in order to use the capabilities of EVI. As will be quantified in the following chapter, EVI will bring efficiency benefits in back-office systems as scanning and verifying license plates are automated. So using EVI in such an early stage will teach the public authorities how to use EVI and will provide efficiency benefits.

The next areas that can be targeted are those with severe traffic problems or low safety. In this way, EVI is introduced bit by bit, which reduces and spreads out the complexity of implementation.

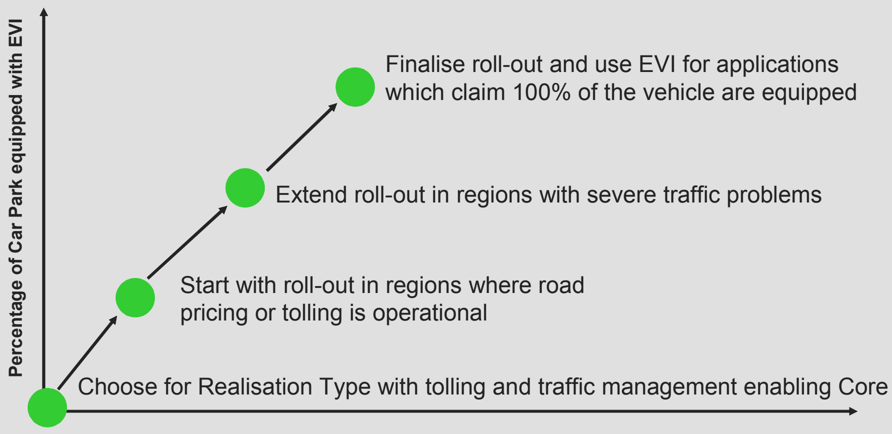


Figure 7.4: Bring applications and technology together in the implementation strategy.

Deployment scenario 2

Specification – Realisation

For both specification (2 years) and Realisation (3 years) we will use the same total times to pass through the activities.

Implementation

Deployment scenario 2 will start with a mandatory EVI of basic functional level 2 in phases. Under the same assumptions we take the gross total time to pass through these activities to be 10 years.

The next phase is to grow further to an EVI of functional level 4, this time on a mandatory basis at once. Under the same assumptions we take the gross total time to pass through these activities to be 10 years at maximum.

The timelines for scenario 2 are drawn in figure 7.5.

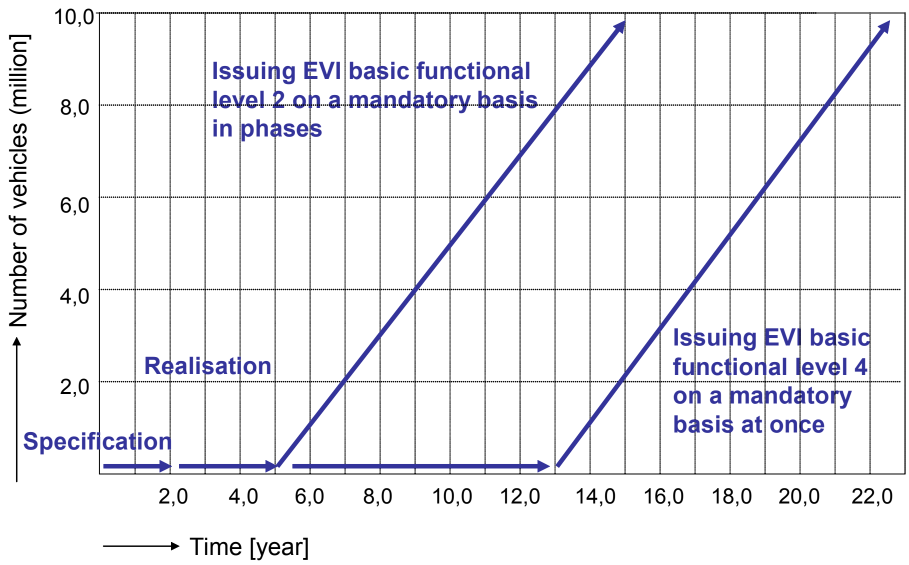


Figure 7.5: Timelines for deployment scenario 2.

7.7 REFLECTION ON THE INSTITUTIONAL ASSESSMENT

In principle EVI can be deployed on a national or European wide basis. However it should be understood that EVI certainly has impact on the institutions needed for a properly operating (distribution of data), secure and environmental acceptable EVI. The seriousness of this impact depends to a large extent on the way the vehicle registration is organised in a country nowadays. This seriousness might be a barrier for the deployment of EVI national or European wide.

For example, the impact will be manageable in countries where the licence plate is under strict control. Many of the organisations are already there and should be upgraded to organisations that are able to deal with electronic devices and security key management. On the other hand, in countries where the licence plate is not under a strict control yet, a more complex upgrade of the organisation will be needed.

Another example; In countries where the vehicle registration database does already cover the items of Directive 1999/37/EC and does already posses of a real-time (seconds) external interface for challenge-respond with EVI reader and/or writer, the impact of EVI will be manageable again. While in countries, where the vehicle registration database does not cover all relevant data yet and/or does not posses of such a real-time (seconds) external interface, a more complex upgrade of the vehicle registration database will be needed.

So the severity of the institutional impact should be considered per country when starting the preparations for the introduction of EVI. In fact the differences between the Member States do form a barrier to deploy EVI on a European wide basis.

The institutional assessment results are summarized in figure 7.6.

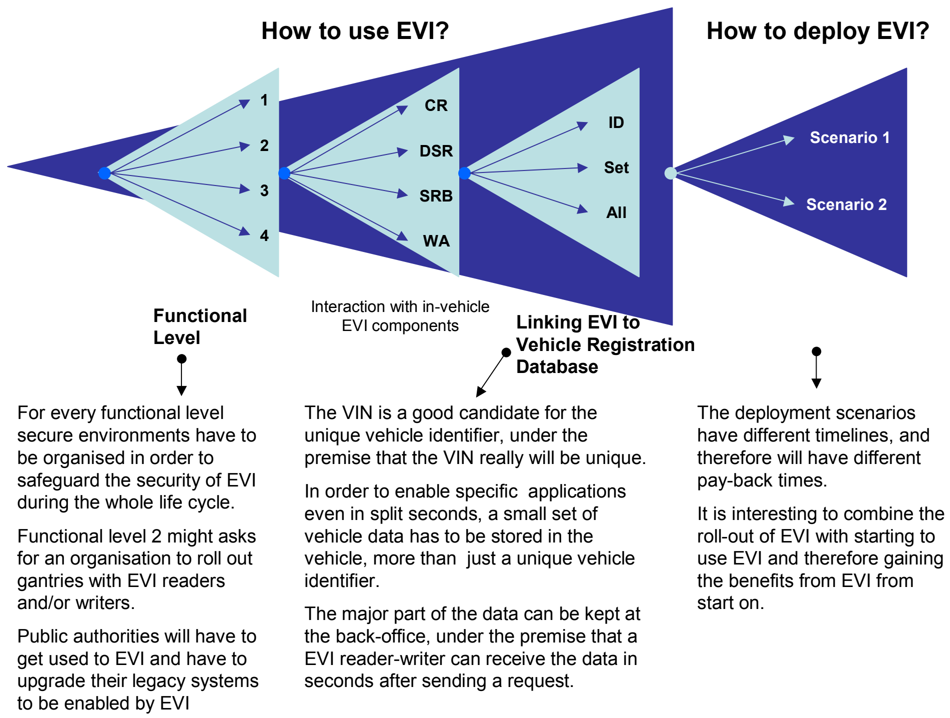


Figure 7.6: Summary of the institutional assessment results.

8 Economical Assessment

The next step is the economical assessment. The aim of this assessment is to determine if the introduction of EVI is feasible from the perspective of costs and benefits. In fact in the economical assessment all differentiations on the basic functional levels are of interest, as well as the deployment scenarios. To prevent ourselves to 'drown' in the details, we will limit ourselves to the four basic functional types and the deployment scenarios (figure 8.1).

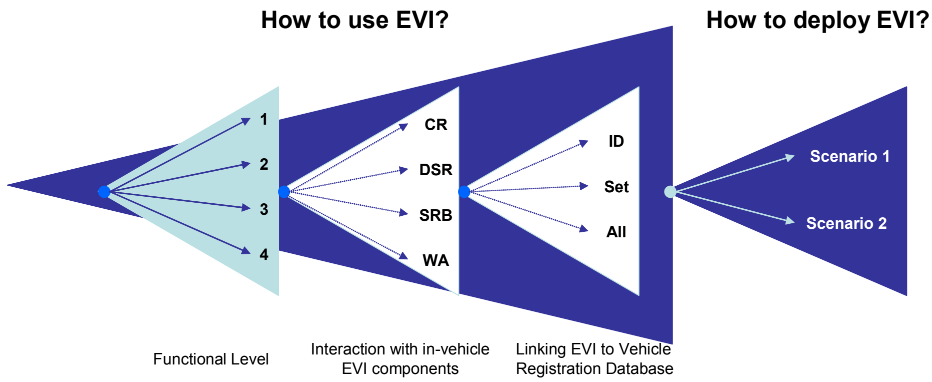


Figure 8.1: Objects of economical assessment.

All costs and benefits are calculated for a 25-year period using the Net Present Value methodology. The method as used for the costs and benefits estimation is detailed in annex G.

8.1 Overview of benefit factors

Three types of benefits

From a public authority point of view, we can distinguish three types of benefits for EVI, namely:

- First order of benefits: improvement of correct vehicle identification;
- Second order of Benefits: improved efficiency in enabling applications; and
- Third level of benefits: these are the benefits of the applications which can be enabled (supported) by EVI directly (e.g. tracking of missing vehicles, road safety via enforcement)

All three types of benefits are explained in the following sections.

First order benefits – improvement of correct vehicle identification

Increase in revenues due to improved registration process

This is a first order of benefits, which is more of an objective then a clear benefit. The objective is to improve the reliability of the vehicle identity. By doing so, the vehicle registration process can be improved and the number of impostors will decrease. In economic terms the missed incomes (taxes, fees) will decrease. However, since this is an objective or better an assumption which has to be proved in practice, we will not take these benefits into consideration.

Increase in revenues due to correct vehicle identification

As indicated before, EVI can be the enabler for automatic enforcement of established speed regulations, but it can also be a first start for reducing vehicle criminality. Both applications may result in more revenues.

Speed enforcement

At the moment speed checks are carried out manually (e.g. radar detection or following vehicles) or by means of speed cameras. The main disadvantage of the latter method is that the proof may be lost due to the poor quality of photos, the escape from pursuits or the faltering of radar equipment. Dutch literature (RDW, 2003) shows that 35% of all offences could not be collected as the proof (mainly photos) is of poor quality (shadows, weather circumstances, quality of the speed cameras) and therefore the license plate could not accurately be recognised. An electronic vehicle identifier reduces this loss. This type of identifier can be an aid for identifying the license place and tracing the vehicle owner.

Table 8.1 shows the number of speed offences in some countries. As the average value of a fine is estimated at € 41,06 (source: CJIB, 2003), the revenues of an EVI device that enables better identification of the vehicles can be calculated.

Table 8.1: Number of speed offences in studies countries.

	France	Netherlands	Norway	United Kingdom
Speed offences	1.263.000	6.738.724	621.133	1.391.000

Table 8.2 presents an overview of the revenues in case a percentage of the 35% not identifiable pictures could be collected.

Table 8.2: Revenues of collecting currently not identifiable offences.

	France	Netherlands	Norway	United Kingdom
10%	1.815.057	9.684.220	892.630	1.999.006
25%	4.537.643	24.210.551	2.231.576	4.997.515
50%	9.075.287	48.421.101	4.463.151	9.995.031
75%	13.612.930	72.631.652	6.694.727	14.992.546

It should be noted that the revenues as calculated above change over time. When EVI is introduced the revenues will be higher than after several years. Better enforcement will result in catching more speed offenders in the start-up phase of EVI. When drivers are used to this improved enforcement they will adopt their behaviour (less inclined to drive too fast) and therefore the number of speed offences will be reduced.

Second order benefits – Improved efficiency

The second order benefits can be split into:

- Benefits due to reduction of system costs;
- Benefits due to efficiency of vehicle identification
- Benefits due to effectiveness of traffic management measures.

Benefits due to reduction of system costs

Depending on the set of vehicle data stored in the in-vehicle EVI components, EVI can enable (support) some applications by itself, that at present need more than one system. For example, in case the unique vehicle identity, the vehicle class and the maximum weight are stored in the in-vehicle EVI components the application Weighing-in-Motion can be supported. Currently, Weighing-in-Motion needs two systems, one for vehicle classification and one for vehicle identification. This kind of benefit relies on a specific type of public authority application.

Benefits due to efficiency of vehicle identification

EVI can improve the efficiency in scanning pictures, as produced in public authority applications like the London Congestion Charge Scheme.

Let us use the example of a Road Pricing Scheme in a densely populated region. Suppose almost every day (300 days a year) about 400.000 images of vehicles and their licence plates are produced which have to be verified manually. If this procedure could be automated by means of EVI, labour forces could be reduced drastically. If the costs of back-end labour are 36 euro per hour, the efficiency benefits could be realised as outlined in table 8.3.

Table 8.3: Efficiency benefits in back-office.

State of image	Assumption	Time for review (seconds)	Benefits per year (million euro)
Perfectly legible and OCR-able images	75%	3	2,70
Requires manual post-processing	20%	18	4,32
Illegible under all circumstances	5%	10	0,60
Revenues recovered turnover vehicles	7,50 euro per vehicle in “illegible under all circumstances” class		4,50
	Total benefits		**12,12**

This basic example demonstrates that EVI is efficient by nature and will bring us significant benefits in case of large applications like road pricing schemes. However, it should be mentioned that a part of these benefits could also be realised through the introduction of OCR-friendly license plates.

Benefits due to effectiveness of traffic management measures

Basically, traffic management follows the control cycle of observation (‘what is the actual traffic situation like?’), evaluation (‘what are the bottlenecks, where is free space in the road network?’), decision (which information, recommendations and/or directives should be passed on to the traffic) and activation (‘activation of the actuators’). As an additional benefit EVI might enable this control cycle.

Observation

Traditionally observation is done using road-bound sensors like induction loops, radar, video or infrared cameras. A draw back of induction loops is their vulnerability, since they are embedded in the road surface, which makes the loops rather expensive. Another drawback of road bound sensors are the limited set of traffic processes they can measure. In most cases these processes are limited to traffic intensity and driving speed. Other processes like density or travel times over longer trajectories have to be calculated afterwards. Building dynamic origin-destinations matrices is even more difficult.

With the market penetration of mobile telecommunication and satellite localisation the possibilities to use vehicles as mobile probes came to the front; the so-called floating car data (FCD). FCD can be used to measure processes like density, travel times and even dynamic origin-destinations matrices directly. A drawback of FCD, however, are the communication costs, since FCD makes use of commercial cellular telephone systems, like GSM or

GPRS. However, initiators found the past decade that there it is very difficult to realise a real business case for traffic information build on FCD sec.

An installed base of EVI can be used as alternative for road-bound sensors. Similar to FCD the range of traffic processes from intensities and driving speeds to density, travel times and even dynamic origin-destinations matrices can be measured directly. The multi-functionality of EVI implies that the investment for EVI is not only limited to traffic management. Moreover, traffic management might be seen as a spin-off of EVI. In case EVI makes use of commercial cellular telephone for the communication between the EVI in-vehicle component and the EVI reader and/or writer, the issue of communication cost will remain.

Evaluation and Decision

The results of the effectiveness of traffic management studies, based on the Dutch evaluation studies, are portrayed in figure 8.2. The effectiveness of traffic management measures is indicated using the results of evaluating studies in The Netherlands. By using EVI to build dynamic origin-destination matrices the effectiveness of traditional traffic management measures like dedicated traffic information, ramp metering, route information using VMSs[1] and motorway traffic management systems (signalling) can be improved. Moreover, EVI can be used to allocate a lane to a specific target group, perhaps without severe investments in the geometry of the cross section of the road.

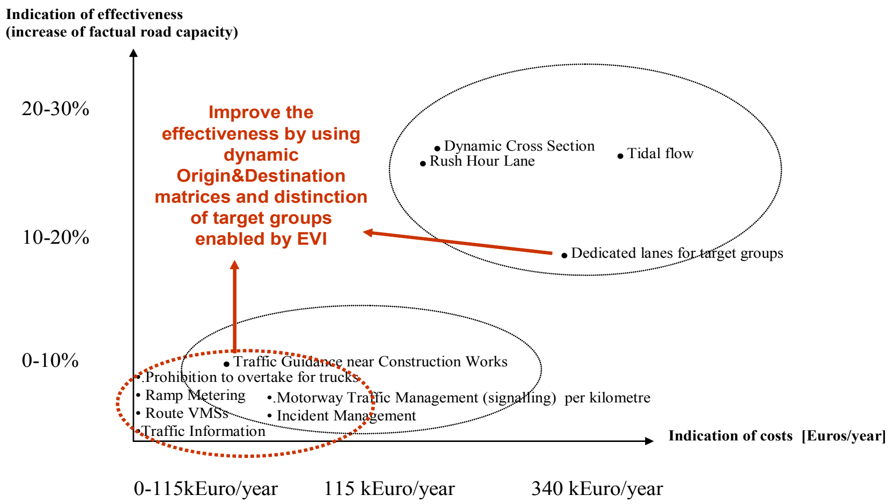


Figure 8.2: EVI can improve the effectiveness of traffic management measures.

Activation

[1] Variable Message Sign

In case EVII is linked to a HMI, EVI can help the traffic manager to address (a) specific (group of) vehicles. Addressing individuals might help in influencing the choices of the individual drivers. In this way EVI in combination with an in-vehicle HMI might help to shift from the external control as the paradigm for traffic management (where the traffic manager is supposed to have his hands on all the taps and valves needed to steer and guide traffic) to more internal control (where vehicle drivers, with all the natural intelligence at their disposal, look for their own solutions and new directions, supported by the traffic manager.

It should be stated that traffic management can be supported in a similar way with commercial floating-car data systems.

Third order benefits - social benefits

The second order benefits focus on regional implementations, at least in the present situation. The third order benefits, that are the social benefits, are defined in this assessment study to be the benefits for all the European Union Member States. These benefits concern road casualties and reduction of stolen vehicles.

Benefits road casualties

The benefits due to a reduction of road casualties are mainly dependent on the realizable average speed reduction through the introduction of EVI. Also the assumed costs per fatality and injury influence these benefits. The benefits for road casualties cover the following variables:

R = Benefits due to a reduction of road fatalities

AS_r = Average speed reduction due to the introduction of EVI

N_{RI} = Number of annual road injuries in EU-15

V_{RI} = Costs per injury

N_{RF} = Number of annual road fatalities in EU-15

V_{RF} = Costs per fatality

Mp = Period to realize maximum benefits

R = Interest rate

Benefits due to a reduction of stolen vehicles

The benefits due to a reduction of stolen vehicles are dependent on the total losses due to stolen vehicles in the EU-15 and the contribution EVI will have on the reduction of vehicle crime. The benefits for reduction of stolen vehicle cover the following variables:

S = Benefits due to a reduction of stolen vehicles

L_{SV} = Total annual losses due to stolen vehicle in EU-15

$\%_{Red}$ = Reduction percentage of stolen vehicles in EU-15

Mp =Period to realize maximum benefits

R = Interest rate

8.2 OVERVIEW OF COST FACTORS

The costs of the identified functional levels could be split up in four major quantifiable components: manufacturing, installation, infrastructure and communication costs.

Manufacturing costs

The manufacturing costs are the costs of producing the EVI device. These costs are dependent on the number of currently registered vehicles and new registered vehicles. Also the price of the EVI device will influence the manufacturing costs. The manufacturing costs cover the following variables:

M = Manufacturing costs

Vc = Number of currently registered vehicles

Vn = Number of annually new registered vehicles

P = Price of the EVI-device

Ip = Introduction period of EVI device

R = Interest rate

Installation costs

The installation costs are the costs for installing the EVI device inside the vehicle. The costs are dependent on the number of currently registered vehicles and new registered vehicles. Moreover, installation time and installation price will influence the installation costs. The installation costs cover the following variables:

Is = Installation costs

Vc = Number of currently registered vehicles

Vn = Number of annually new registered vehicles

It = Installation time

ISp = Installation price

Ip = Introduction period of EVI device

R = Interest rate

Infrastructure costs

The infrastructure costs are the costs of the reader and/or writer equipment. These costs are dependent on the chosen reader and/or writer equipment. Three possible reader and/or writer equipment types are identified: hand-held readers and/or writers, road-side readers and/or writers (excluding the necessary network to connect road-side readers and/or writers with control centres) or back-offices and road-side beacons to complete the geographical gaps in the communication coverage. It is assumed that each reader and/or writer equipment type has its own costs. The infrastructure costs cover the following variables:

I_F *= Infrastructure costs*

$\%_H$ *= Percentage of hand-held reader and/or writer equipment*

$N_{R/W}$ *= Amount of reader and/or writer equipment in EU-15*

P_H *= Price of hand-held reader and/or writer equipment*

%R/W = Percentage of road-side reader and/or writer equipment

$P_{R/W}$ *= Price of road-side reader and/or writer equipment*

P_{NET} *= Price of network to connect road-side reader and/or writer to control centre or back-office*

$\%_B$ *= Percentage of beacons to complete the geographical gaps in the communication coverage*

P_B *= Price of beacon to complete the geographical gaps in the communication coverage*

Ip = Introduction period of EVI device

R = Interest rate

Communication costs

The communication costs are the costs of the communication between the reader and/or writer and the control centre or back-office. The communication costs are dependent on the transaction costs and the amount of beacons to complete the geographical gaps in the communication coverage. The communication costs cover the following variables:

C = Communication costs

Tc=Transaction costs

$\%_B$ *= Percentage of beacons to complete the geographical gaps in the communication coverage*

$N_{R/W}$ *= Amount of reader and/or writer equipment in EU-15*

N_{TC} *= Amount of transactions per reader and/or writer*

Ip = Introduction period of EVI device

R = Interest rate

8.3 ASSUMPTIONS FOR SOCIAL ECONOMICAL ASSESSMENT (THIRD ORDER)

To identify the costs and benefits of each functional level some assumptions have to be made. Using these assumptions it is possible to fill out the equations as described in Annex G. The assumptions are summarized in the table 8.4.

Table 8.4: Overview of assumptions for economical assessment.

	Functional level 1	**Functional level 2**	**Functional level 3**	**Functional level 4**
Number of currently registered vehicles	179.018.000 (Source; EUROSTAT (2000)	179.018.000 (Source; EUROSTAT (2000)	179.018.000 (Source; EUROSTAT (2000)	179.018.000 (Source; EUROSTAT (2000)
Number of annually new registered vehicles	14.321.440 (based on Dutch figures it is assumed that the number of new registered vehicles is in average 8%)	14.321.440 (based on Dutch figures it is assumed that the number of new registered vehicles is in average 8%)	14.321.440 (based on Dutch figures it is assumed that the number of new registered vehicles is in average 8%)	14.321.440 (based on Dutch figures it is assumed that the number of new registered vehicles is in average 8%)
Price of the EVI-device	EUR 10	EUR 20	EUR 50	EUR 100
Installation time	0 hours	0.5 hours	1 hour	2 hours
Installation price	35 euro per hour	35 euro per hour	35 euro per hour	35 euro per hour
Percentage of hand-held reader and/or writer equipment	100%	50%	50%	50%
Amount of reader and/or writer equipment in EU-15	15.000 (1.000 in average per country)	15.000 (1.000 in average per country)	15.000 (1.000 in average per country)	15.000 (1.000 in average per country)
Price of hand-held reader and/or writer equipment	EUR 40.000	EUR 40.000	EUR 40.000	EUR 40.000

	Functional level 1	**Functional level 2**	**Functional level 3**	**Functional level 4**
Percentage of road-side reader and/or writer equipment	0%	50%	50%	0%
Price of road-side reader and/or writer equipment	EUR 200.000	EUR 200.000	EUR 200.000	EUR 200.000
Price of network to connect road-side reader and/or writer to control centre or back-office	EUR 20.000	EUR 20.000	EUR 20.000	EUR 20.000
Percentage of beacons to complete the geographical gaps in the communication coverage	0%	0%	0%	50%
Price of beacon to complete the geographical gaps in the communication coverage	EUR 400.000	EUR 400.000	EUR 400.000	EUR 400.000
Transaction costs	EUR 0,02 per transaction	EUR 0,02 per transaction	EUR 0,02 per transaction	EUR 0,02 per transaction
Amount of transactions per reader and/or writer	20.000	20.000	20.000	20.000
Average speed reduction due to the introduction of EVI	0,01 km per hour	0.1 km per hour	0.5 km per hour	1 km per hour
Number of annual road injuries in EU-15	1.295.400 (source: ICF consultants (2003))	1.295.400 (source: ICF consultants (2003))	1.295.400 (source: ICF consultants (2003))	1.295.400 (source: ICF consultants (2003))
Costs per injury	EUR 152.087 (source: ICF consultants (2003))	EUR 152.087 (source: ICF consultants (2003))	EUR 152.087 (source: ICF consultants (2003))	EUR 152.087 (source: ICF consultants (2003))

	Functional level 1	Functional level 2	Functional level 3	Functional level 4
	consultants (2003))	consultants (2003))	consultants (2003))	consultants (2003))
Number of annual road fatalities in EU-15	40.812 (source: ICF consultants (2003))	40.812 (source: ICF consultants (2003))	40.812 (source: ICF consultants (2003))	40.812 (source: ICF consultants (2003))
Costs per fatality	EUR 1.555.002 (source: ICF consultants (2003))	EUR 1.555.002 (source: ICF consultants (2003))	EUR 1.555.002 (source: ICF consultants (2003))	EUR 1.555.002 (source: ICF consultants (2003))
Total annual losses due to stolen vehicles in EU-15[1]	EUR 7.802.436.152	EUR 7.802.436.152	EUR 7.802.436.152	EUR 7.802.436.152
Reduction percentage of stolen vehicles in EU-15	1%	10%	20%	50%
Introduction period of EVI device	3 years	5 years	5 years	10 years
Period to achieve maximum deployment and therefore realize maximum benefits	3 years	5 years	5 years	10 years
Interest rate	4%	4%	4%	4%

8.4 Results of the social cost-benefit analysis (third order)

Based on the assumptions as identified in the previous section, the costs as described in table 8.6 are calculated for each functional level over a period of 25 years. The benefits of each functional level are described in table 8.7 over the same period of 25 years.

A summary of costs and benefits is presented in table 8.8. In this table the estimated payback time within a period of 25 years has been estimated.

[1] The RDW study (RDW (2003)) estimates that financial losses due to vehicle theft are approximately 285 million euro per year in the Netherlands. As the Dutch registered vehicle park is 6.539.000 (source: EUROSTAT (2000)), the financial losses per vehicle are 43,58 euro. This means that the financial losses due to vehicle theft for EU-15 are 43,58 euro * 179.018.000 (vehicle park EU-15; source Eurostat (2000)) = 7.802.436.152 euro per year.

Under the assumptions of table 8.4, the EVI of functional level 3 has the shortest payback time.

Table 8.8 presents the most optimistic scenario; the benefits of EVI are assumed to be high. A sensitivity analysis, in which the average speed reduction due to the introduction of EVI and the reduction percentage of stolen vehicles in the EU-15 are lowered (table 8.5), results in a reduction of the total benefits of EVI. These benefits, for each functional level, are described in table 8.9. A summary of costs and benefits is presented in table 8.10. In this table the estimated payback time within a period of 25 years has been estimated. Under the assumptions of table 8.5, only the EVI of functional level 3 is economical feasible within the period of 25 years.

Table 8.5: Overview of assumptions sensitivity analysis.

	Functional level 1	**Functional level 2**	**Functional level 3**	**Functional level 4**
Average speed reduction due to the introduction of EVI	0,01 km per hour	0.05 km per hour	0.1 km per hour	0.5 km per hour
Reduction percentage of stolen vehicles in EU-15	1%	5%	10%	20%

Table 8.6: Costs of functional levels over a period of 25 years.

	Manufacturing costs			Installation costs			Infrastructure costs	Commu-nication costs	Total
	Existing vehicles	New vehicles	Total	Existing vehicles	New vehicles	Total			
Functional level 1	1.655.970.822	2.237.306.806	3.893.277.628	0	0	0	555.018.207	0	4.448.295.834
Functional level 2	3.187.825.320	4.474.613.612	7.662.438.932	2.789.347.155	3.915.286.910	6.704.634.065	1.736.210.709	0	16.103.283.707
Functional level 3	7.969.563.301	11.186.534.029	19.156.097.330	5.578.694.310	7.830.573.821	13.409.268.131	1.736.210.709	0	34.301.576.170
Functional level 4	14.519.963.406	22.373.068.059	36.893.031.465	10.163.974.384	15.661.147.641	25.825.122.026	2.359.287.916	12.822.897.822	77.900.339.229

Table 8.7: Benefits of functional levels over a period of 25 years.

	Road fatalities	Vehicle theft	Total
Functional level 1	1.146.580.122	1.144.841.228	2.291.421.350
Functional level 2	10.761.489.487	10.745.168.691	21.506.658.179
Functional level 3	53.807.447.435	21.490.337.383	75.297.784.818
Functional level 4	91.508.499.421	45.684.859.153	137.193.358.574

Table 8.8: Overview of costs and benefits of functional levels over a period of 25 years.

	Manufacturing costs	Installation costs	Infrastructure costs	Communication costs	Total	Road fatalities	Stolen vehicles	Total	Cost-benefit ratio	Cost minus benefits	Payback
Functional level 1	3.893.277.628	0	555.018.207	0	4.448.295.834	1.146.580.122	1.144.841.228	2.291.421.350	1.94	2.156.874.485	> 25 years
Functional level 2	7.662.438.932	6.704.634.065	1.736.210.709	0	16.103.283.707	10.761.489.487	10.745.168.691	21.506.658.179	0.75	-5.403.374.472	14 years
Functional level 3	19.156.097.330	13.409.268.131	1.736.210.709	0	34.301.576.170	53.807.447.435	21.490.337.383	75.297.784.818	0.46	-40.996.208.648	7 years
Functional level 4	36.893.031.465	25.825.122.026	2.359.287.916	12.822.897.822	77.900.339.229	91.508.499.421	45.684.859.153	137.193.358.574	0.57	-59.293.019.345	11 years
	Copied from table 8.6					Copied from table 8.7			Newly calculated		

Table 8.9: New benefits of functional levels over a period of 25 years due to sensitivity analysis.

	Road fatalities	Vehicle theft	Total
Functional level 1	1.146.580.122	1.144.841.228	2.291.421.350
Functional level 2	10.761.489.487	5.372.584.346	16.134.073.833
Functional level 3	21.522.978.974	10.745.168.691	32.268.147.666
Functional level 4	45.754.249.711	18.273.943.661	64.028.193.372

Table 8.10: New overview of costs and benefits of functional levels over a period of 25 years due to sensitivity analysis.

	Manufacturing costs	Installation costs	Infrastructure costs	Communication costs	Total	Road fatalities	Stolen vehicles	Total	Cost-benefit ratio	Cost minus benefits	Payback
Functional level 1	3.893.277.628	0	555.018.207	0	4.448.295.834	1.146.580.122	1.144.841.228	2.291.421.350	1.94	2.156.874.485	> 25 years
Functional level 2	7.662.438.932	6.704.634.065	1.736.210.709	0	16.103.283.707	10.761.489.487	5.372.584.346	16.134.073.833	1.00	-30.790.126	25 years
Functional level 3	19.156.097.330	13.409.268.131	1.736.210.709	0	34.301.576.170	21.522.978.974	10.745.168.691	32.268.147.666	1.06	2.033.428.504	> 25 years
Functional level 4	36.893.031.465	25.825.122.026	2.359.287.916	12.822.897.822	77.900.339.229	45.754.249.711	18.273.943.661	64.028.193.372	1.22	13.872.145.857	> 25 years
	Copied from table 8.6					Copied from table 8.9			Newly calculated		

8.5 INFLUENCE OF DEPLOYMENT SCENARIOS ON COSTS AND SOCIAL BENEFITS (THIRD ORDER)

Figure 8.3 shows the influence of the deployment scenarios on costs and benefits. The figure shows that if all countries decide to install functional level 2 (in stead of functional level 1) in new registered vehicles the total costs will increase, but also the benefits will increase. When some countries decide to migrate from a functional level 2 to a functional level 4, the costs for these countries will extremely increase, whereas the benefits will increase, but this growth is lower as no synergy between countries could be expected (not all foreign vehicles will be detected in this scenario).

In the case the EC decides to introduce EVI in a phased way, after some countries already have introduced EVI in their country, the costs will increase, but the benefits will increase more. This is due to expected synergy between countries (after some time it is possible to detect for example all foreign vehicles). When all countries decide to migrate to a functional level 4 (from a functional level 2), the costs will increase extremely, but also the benefits will increase. Besides, we expect that the vehicle industry, which is also developing an in-vehicle platform, decides to integrate EVI in their platform. The consequence would be a cost decrease in manufacturing and installation (maybe these costs approach zero), making this functional level economically feasible from the start.

	All	Phased	Voluntary	None
Functional level 1				
Functional level 2	Costs + Benefits +	Costs + Benefits ++		
Functional level 3				
Functional level 4	Costs ++ Benefits ++		Costs ++ Benefits + (only national)	

Figure 8.3: Influence of deployment scenarios on costs and benefits.

8.6 OBSERVATIONS ON THE COSTS AND BENEFITS

General observations

It should be noted that European and national governments do have a public responsibility and therefore the decision to implement EVI should not only be based on the economic feasibility.

Moreover, in this cost-benefit analysis no attention has been paid to the time for developing a specific functional level. As the complexity increases when migrating between the functional levels, the development time will also increase. Figure 8.4 presents a likely scenario for these development times. Moreover the period of increasing costs and benefits and the period of maximum benefits is also included in this figure.

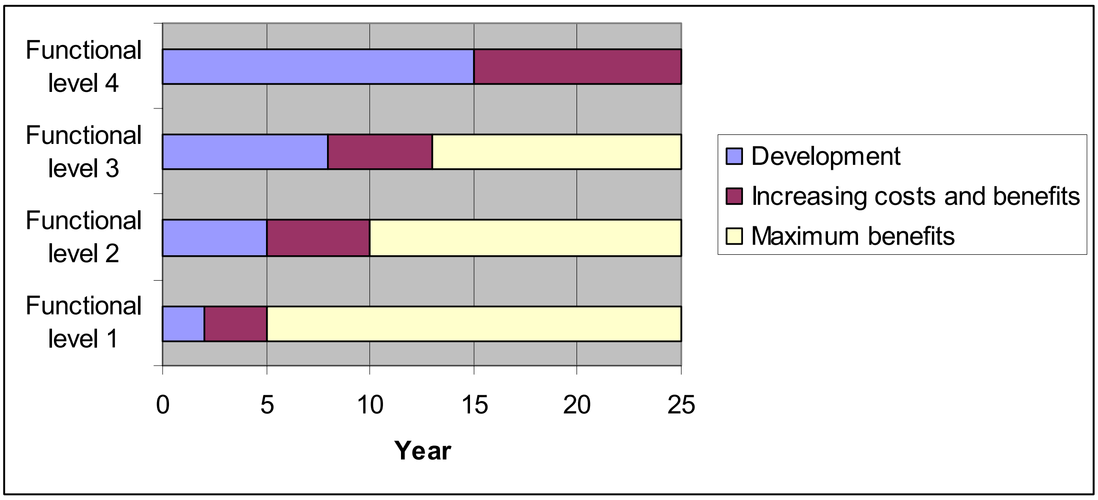


Figure 8.4: Overview of development and cost-benefit scenario of functional levels.

Observations on costs

In the cost analysis only manufacturing, installation, infrastructure and communication costs are included.

In fact also costs should be included for:

- updating the data stored in the in-vehicle EVI components;
- deinstalling and replacing the in-vehicle EVI components, depending on the security strategy.

The costs for de-installation and replacement are quite similar to the cost for installation. More difficult are the costs for updating the data. Perhaps the main part of these costs is the lost time needed for visiting a, for instance, certified garage (secure environment for issuing, see security assessment). These costs are secondary and express more the inconvenience for the vehicle (registration) owners.

Observations on benefits – 1

EVI needs more than a single link between the EVI reader and/or writer and the back-office of the registration agency. Since one of the main functions of EVI is to enable public authority applications there should be an interface between the EVI reader and/or writer and the control centre of the public authority running an application. Figure 8.5 gives an example of both interfaces to and from the EVI reader and/or writer for the application 'traffic management - dynamically dedicated lanes'. The external interface between EVI reader and/or writer and control centre should be capable to meet with the same strict real-time constraints as the external interface between EVI reader and/or writer and the back-office of the vehicle registration agency.

When exploring the benefits of EVI it is important to take into consideration the whole chain, since the use of EVI might be restricted due to bottleneck(s) in the 'pipeline'.

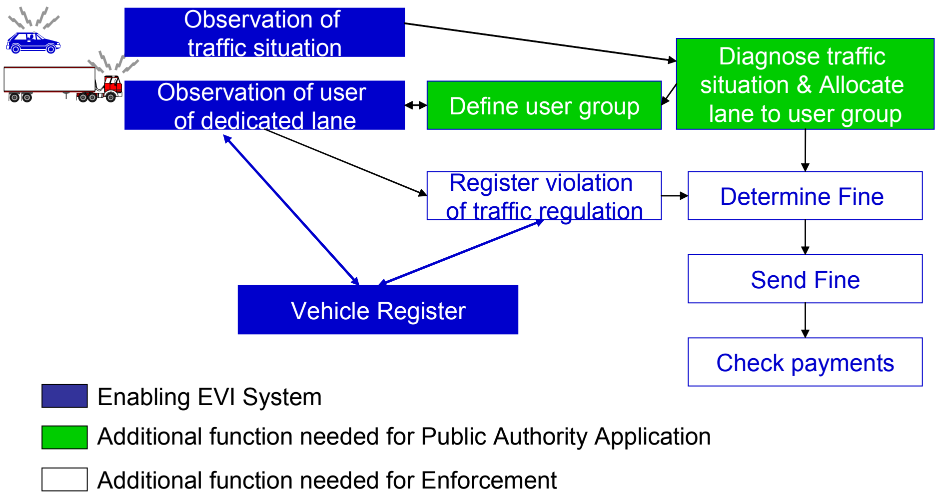


Figure 8.5: Limitations due to bottlenecks in the 'pipeline'.

Notifications about benefits - 2

It should be mentioned that EVI is one of the enablers of automatic enforcement and contributor to the reduction of road casualties. However, other successful alternatives are available. For example, a study conducted by the Parliamentary Advisory Council for Transport Safety (PACTS) showed that speed cameras are a successful medium for reducing speed locally. Therefore, the number of road fatalities decreases at dangerous crossings or curves. The study showed that speed cameras can result in 35% fewer road fatalities.

Another alternative for reducing road fatalities is better enforcement on using safety belts and drunk driving. Together with better enforcement on speed limits this can result in a reduction of 25% (source: ESCAPE project) of the number of road casualties. At last trajectory control systems could be introduced at lower costs and moreover these systems have a higher accuracy. Hence, trajectory control systems could also be an effective deterrent for driving too fast.

It is outside the scope of this cost-benefit analysis to compare the benefits of EVI with the benefits of alternative solutions.

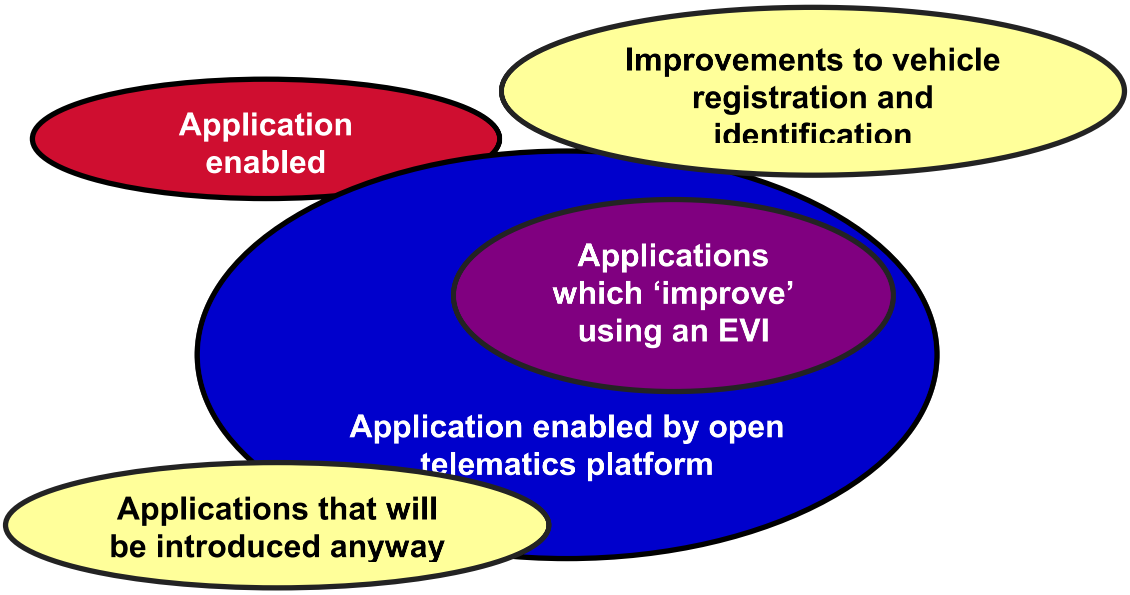


Figure 8.6: Benefits for EVI could also be benefits for 'duplicators' of EVI.

Finally, it always should be kept in mind that EVI is an enabler, so new applications (both public authority as private applications) may be developed, increasing the benefits for EVI. One can think of mobile phones. The aim of text messaging was to provide additional information from provider to phone owner. Now the text messaging is nearly as profitable as the calls themselves. It should be noted that EVI is not a replacement of the current license plate. Eyewitnesses should always have the possibility to identify a vehicle by means of the license plate. Furthermore, it should be kept in mind that legislation might form barriers that prevent gaining full benefits. For example, it could be possible that it is not allowed to replace speed cameras for only an electronic unique vehicle identifier; a photo could always be necessary as proof of the offence.

8.7 Reflection on the Economic Assessment

EVI is economically feasible dependent on the applications that are supported and the policy goals that are aspired. Dependent on these desires a final conclusion can be drawn whether EVI is economically feasible yes or no.

EVI has three kinds of benefits:

- First order of benefits: improvement of correct vehicle identification;
- Second order of Benefits: improved efficiency in enabling applications; and
- Third level of Benefits: these are the benefits of the applications which can be enabled (supported) by EVI directly (e.g. tracking of missing vehicles, road safety via enforcement)

The *first order benefits* are inherent to EVI. They are not only an economic factor but also an ethical factor ('all vehicle owners do have the same obligations towards the public authorities').

The *second order of benefits* consists of:

- Benefits due to reduction of system costs;
- Benefits due to efficiency of vehicle identification; and
- Benefits due to effectiveness of traffic management measures.

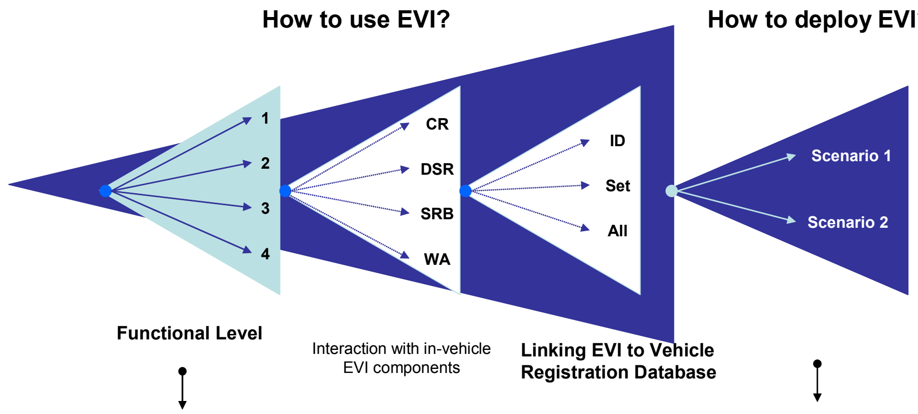
In all cases the benefits of EVI outweigh the cost, if EVI was deployed on a regional basis. To be precise in the region where massive vehicle identification is needed due to road pricing schemes, or where a more efficient use of the available infrastructure is needed. These types of benefits are not a justification for national, or European wide deployment of EVI.

The third order of benefits reflects the benefits applicable for all the European Union Member States. These benefits concern road casualties and reduction of stolen vehicles. Again benefits of EVI outweigh the cost, be it that the payback time varies between 7 and more than 25 years, depending on the basic functional level of EVI

All in all, EVI is economically feasible depending on the political priorities for implementation of public authority applications.

With respect to the costs of introducing EVI in society, it should be stated that the costs do not only consist of implementing the EVI device in the vehicle. Realising the road side infrastructure and improving back-office systems are additional costs for realising EVI in Europe. These costs will increase the pay back time for EVI.

The economical assessment results are summarized in figure 8.7.



All functional levels will improve correct vehicle identification (first order benefit).

Function level 2 – 3 are able to improve the efficiency of public authority applications aimed at fairness of road pricing and efficient use of available infrastructure using both moving and stationary vehicles (second order benefit). Functional level 1 is limited to stationary vehicles and therefore limited in benefits.

All functional levels are EU-wide beneficial for road safety and reduction of vehicle crime.

In fact for all functional levels the benefits will outweigh the costs, although the pay-back time is long for functional level 1. Functional level 3 scores best in case of retrofit.

By smart roll-out of EVI immediate usage of EVI must be possible, which helps to reduce the pay-back time.

Figure 8.7: Summary of the economical assessment results.

9 LEGAL ASSESSMENT

9.1 LEGAL REQUIREMENTS

Work Package 2 identified various legal requirements that are relevant to a feasibility assessment of EVI. These requirements were broken down in Work Package 2 into two types: vertical and horizontal. Each is explained and expanded below in the context of the feasibility assessment of EVI.

Vertical Legal Requirements

Vertical legal requirements are separate but potentially overlapping existing areas of legislation and regulation that reside at national and EU levels and require consideration in relation to any EVI system or type. It is outside the scope of Work Package 4 to set out the actual current laws, regulations, codes of practice and other legal instruments at local, national and European levels that populate these vertical categories, not least, because these are likely to change over the life of the project. Detailed assessment of Member States' road traffic rules has already been undertaken in a recent European Commission Report[1] and Work Package 5 will explore and consider Member State feedback and opinions in relation to EVI.

The broad categories and a breakdown of what is encompassed in each of these vertical legal requirements identified in Work Package 2 are attached at annex H.

The fact that these areas of existing law need to be considered does not mean that they are necessarily barriers to the development or implementation of EVI. Rather, they are laws and issues that may affect the way in which an EVI system and the data that it generates are used, operated and managed. It should also be noted that they are requirements that are likely to apply to the development of most types of telematic systems.

The extent to which these legal issues will affect the feasibility of an EVI system or present potential barriers will be affected by the following considerations:

- *Who uses the EVI system*

  Work Package 2 has focused on the potential use of EVI by public authorities without precluding the fact that it may be possible for further use to be made by commercial/private entities (although outside the scope of this assessment). Decisions as to who has responsibility for and access to the system and its data

[1] 'Comparative Study of road traffic rules and corresponding enforcement actions in the Member States of the European States of the European Union', Final Report prepared by TiS.PT undertaken pursuant to the EU road safety programme "Promoting Road Safety in the EU".

will shape the legal considerations and structure that will be required. Such decisions have not yet been made, but legal considerations do not preclude options at this stage.

- *The use of the EVI system*

  Work Package 2 has focused on public authority applications for EVI although again noting that an EVI system may be open to further value added applications.

- *The structure for deployment and use of the EVI system*

  The framework developed for the development and deployment of an EVI system will affect the legal relationships between the different parties involved in such structure and the impact that it may have externally. Choices made in relation to architecture, access, standards and any external infrastructure may affect many of the vertical legal requirements to a greater or lesser degree. Work on standards and possible structures is ongoing and further legal analysis will be possible once the results of this work are made available.

- *Whether the EVI system is mandatory or voluntary*

  A mandatory system is more likely to require more scrutiny in order to satisfy public, Member State and industry player concerns. Where consent has been obtained from individuals for the installation and use of an EVI system and the purposes of its use are accepted, then many issues including, for example data protection and human rights considerations, are likely to be less onerous than if a system is mandatory. These are issues that the Commission and Member States will need to analyse and to obtain feedback from interested parties within such Member States in order to assess the feasibility issues further.

Decisions within these categories will affect the analysis of the legal issues that will be relevant. At present however, any decisions within these considerations are not precluded as a consequence of legal issues per se. Further analysis can usefully be undertaken once more robust and detailed scenarios and models have been developed.

Table 9.1 below indicates which of certain legal requirements are relevant to the use of any EVI system for each of the public authority applications.

An "X" indicates that existing laws in this area will need to be considered and may affect and regulate the use of EVI for that public application. Again, it should be emphasised that these are not identified as barriers as such, but are rules into which such system will need to fit.

An "S" indicates that existing laws in this area are significant to the use of EVI for that public application and will require particular attention and feedback from individual Member States in terms of social acceptance and policy considerations. The chart at table 9.1 shows that existing legal issues surrounding the use of personal data and human rights issues are significant in this way. This does not mean that they have been identified as barriers to use of public authority applications identified. However, it is recognised that these are likely to be significant from a public policy and acceptance perspective where EVI is introduced as a mandatory system.

Table 9.1: Mapping of Vertical Legal Issues on Public Authority Applications.

	Crime	Access Control	Vehicle Tolling	Vehicle (registration) ownership[1]	Excise Duty	Traffic Management/Driver	Enforcement	Vehicle Life Cycle	Traffic and Transport Regulation
Data protection (where and depending on whether personal data is processed)	S	S	S	-	-	S	S	S	S
Human Rights	S	S	S	-	-	S	S		S
Anti-Terrorism (significance increased where human rights and data protection are involved)	X	X		-	-	X	X		
Crime investigation and detection	X	X	X	-	-	X	X	X	X
Vehicle specific				-	-	X	X	X	X
Road use/traffic specific			X			X	X		X
Health & Safety	X			-	-	X		X	X
Environment	X			-	-			X	X
Tax and Insurance	X	X	X	-	-	X	X	X	X
Digital Signatures	Depending on the devices and architecture, potentially all								
Electronic communications	Depending on the devices and architecture and form of communications with and in relation to the system, potentially all								
Intellectual property rights				-	-				

[1] No public authority applications are identified in WP2 and therefore these cells are not filled in.

Employment				-	-	X			

The vertical legal requirements will affect any EVI system in different ways during the various deployment stages for such system. Table 9.2 below indicates which of the existing vertical legal issues will be relevant at each of the relevant deployment stages. Again "S" indicates those matches that are more significant and will require further assessment following the obtaining of feedback from Member States and interested parties.

Table 9.2: Indication of relevance of the vertical legal requirements to each of the Deployment Scenario Stages.

	Manufacture	Issue	Use (will vary according to application)	Management and Maintenance	End of Life
Data Protection		X	S	X	X
Human rights			S	X	
Anti-Terrorism		X	S	X	
Crime investigation/ detection		X	S	X	
Vehicle specific	S	S	X	X	S
Road use/traffic specific			S		X
Health and Safety	X	X	X	S	X
Environment			X	X	X
Tax and Insurance	X	X	X	X	X
Digital signatures (depending on architecture used)	S	S	S	X	X
Electronic communications			X	X	

Intellectual property rights	X	X			
Employment			X		

Horizontal Legal Requirements

Horizontal legal requirements are legal considerations and principles relating to implementation that lie across each of the vertical legal requirements, public authority applications and EVI system types as identified in Work Package three. They represent new legislation or legal mechanisms that will be required to give effect to EVI.

The horizontal requirements apply to the adoption, operation and use of any new large-scale system across Europe and require consideration (albeit to a lesser or greater degree) regardless of the EVI type or the application(s) for which such EVI system is used. The two areas into which horizontal legal requirements can be broken down are:

(a) Legislative Framework

This requires a consideration of the legal basis on which Community and national institutions can put in place relevant harmonised legislation to implement an EVI system and appreciation of the various legal instruments and mechanisms to establish legal vires for implementation of the appropriate legislative and regulatory framework (for example primary and secondary legislation, the need for standards, codes and guidelines or self-regulatory mechanisms). These issues will largely be dependent on whether a decision is made that EVI be a mandatory or a voluntary system.

At present and as identified in a recent report for the European Commission[1], as a general rule, core or framework road traffic and safety legislation is approved by National Parliaments and the responsibility for proposing and approving laws and rules is given to national governments. Although European Directives or Regulations may be implemented (for example as in relation to the equipping of all new manufactured buses and heavy trucks with a digital tachograph and Council Directives on general maximum speeds), transport continues to be an area in which national legislation predominantly shapes the development and structure of new traffic rules and enforcement and implementation of European initiatives is often very varied given the differences in local and national control of such issues.

At a European Community level, there are various legal bases for a European framework for adoption of an EVI system under the specific Treaty of the

[1] 'Comparative Study of road traffic rules and corresponding enforcement actions in the Member States of the European States of the European Union', Final Report prepared by TiS.PT undertaken pursuant to the EU road safety programme "Promoting Road Safety in the EU".

European Union provisions. These have different implications for adoption and therefore the length of time in which such policy could be implemented:

(i) Provisions on transport policy[1]

The Council operates under the co-decision procedure with the European parliament to lay down provisions for the purpose of implementing the framework of a common transport policy. Any provisions that could have a serious effect on, inter alia, the operation of transport facilities must be laid down by the Council operating unanimously.

(ii) Provisions on trans-European networks[2]

These provisions set out the objective and potential action by the Community for promoting the interconnection and interoperability of national networks as well as access to such networks. The Community may: implement any measures that may prove necessary to ensure interoperability of trans-European networks, particularly in the field of standardisation (to be adopted by the Council in accordance with the co-decision procedure subject to approval by any Member State to whose territory the measure relates); and financially support projects of common interest. Member States shall co-ordinate among themselves and with the Commission policies pursued at a national level with the Commission to pursue the overall objective.

(iii) Provisions on the harmonisation/approximation of laws[3]

Directives for the approximation laws, regulations or administrative provisions of Member States may be made where they directly affect the establishment or functioning of the common market. This requires the Council to act unanimously.

Measures that have as their object the establishment of functioning of the internal market require the Council to act on a qualified majority under the co-decision procedure with the European Parliament.

(iv) Provisions on home and justice affairs[4]

This basis has a focus on provisions in relation to external border controls and measures with respect to the prevention and combating of crime rather than transport per se. Generally concerned with promotion

[1] Treaty Title V, article 71 et seq (ex article 75).

[2] Treaty Title XV, article 154 ex seq (ex article 129b).

[3] Articles 94 and 95.

[4] Third pillar of the European Union on home and justice, Title VI.

of co-operation between relevant authorities through Europol or other relevant bodies, legislation may be brought forward where it is necessary in the progressive adoption of measures establishing minimum rules in the constituent elements of criminal acts and penalties in the fields of organised crime, terrorism and illicit drug trafficking.

The Council may also adopt framework decisions for the purpose of the approximation of the laws and regulations in Member States in pursuit of the objectives of the European Union including police and judicial co-operation in criminal matters.

There are therefore various bases for European decision and legislative decision making. It is outside the scope of this WP4 to draw any conclusions as to which base may be appropriate or the nature of any European legislation for implementation of promotion of EVI may be suitable. No realistic assessment of the timeframe in which any such option could be taken is possible or useful at this stage in the assessment since such matters will depend to a greater extent on political and socio-economic factors than on legal considerations.

(b) Life-cycle/implementation and operational requirements

These include legal considerations regarding the implementation, contractual structure, allocation of responsibility and liability and ongoing support of an EVI system. It is clear that these will vary depending on the given life cycle stages of the system. At present, work has only been undertaken to identify the possible EVI system types and applications and no particular models for implementation and deployment have been proposed. It is therefore not possible at this stage to identify the specific legal mechanisms, and structures that would be involved. It should be noted that, whilst there may be legal advantages and disadvantages of working with one structure as opposed to another, legal requirements do not constitute barriers and the legal issues can facilitate, shape and be led by the structure rather than determining it at this stage. Further analysis will be possible once options for the wider system of operation have been developed.

The next section draws out some of the differences that may result from the adoption of one EVI system type as opposed to another at this stage.

9.2 Legal Assessment of EVI deployment scenarios

This section identifies the potential legal considerations for each of the most important Deployment Scenario stages.

Manufacture

Considerations as to whether there will be full and open competition as to who will manufacture the EVI systems and whether and how this will be limited to a number of certified and authorised organisations will need to be considered. Schemes may need to be put in place for certification and accreditation. It will be particularly important from a legal perspective to ensure traceability of the system from manufacturer to end-user. Interoperability will also be a consideration.

Issue

Consideration of the role of Registration Authorities and their ambit of authority and various powers will need to be reviewed and set out by way of legal authorisation at a national level. The use of electronic signatures may be relevant depending on the system used. Establishment of and checks on the operations of approved organisations, certification etc will need to be considered.

Use

In terms of use of the system most of the vertical legal requirements will be relevant and, to this extent, whether new legislation or amendments to existing legislation are required will depend on the scope and nature of such. Consideration of rights of use and access, back-office regulations, codes of practice, commercial and contractual arrangements, monitoring and enforcement arrangements will be relevant.

Management and Maintenance

Ownership and liability issues will be significant including appropriate legal allocation of responsibility. Guarantees and warranty claim matters as well as enforcement and authorisation will also need to be taken into account.

End of Life

Consideration of allocation of responsibility and authorisation of relevant persons will be required.

9.3 Reflection on the Legal Assessment

In fact there are no real legal barriers for the introduction of EVI with respect to the existing legal framework. The reality however will be that while introducing EVI the legal framework will change due to test cases for court and new to be developed jurisprudence.

10 SOCIAL AND POLITICAL ASSESSMENT

10.1 EVI IN A POLITICAL CONTEXT

With the risk of mixing the premise with the assessment, we might say that EVI fits in the way the European Commission is taking the topic traffic and transport forward. By 'building' the Trans-European Networks (TENs) the EC is heading for a borderless Europe. Such a Europe asks for European wide interoperability of ITS-systems, in order to prevent that along the information- and communication technology used new borders will arise. The evolving directive on Electronic Fee Collection is an example of a serious step towards such interoperability. EVI fits within this development in two ways. First, EVI will help a whole pallet of applications to use certified vehicle parameters instead of measured estimated vehicle parameters. Second, EVI will help public authorities to identify vehicles in a borderless Europe; vehicles that might be registered in another country than the country where it is in. EVI will not bring back the borders; EVI will help to overcome the borders.

By enabling a pallet of public authority applications EVI will help to realise the policy goals: improvement of road safety, reduction of environmental impact of road traffic, a more efficient use of the existing road infrastructure, a fairer road pricing and a reduction of vehicle crime. More recently there is the objective of a securer Europe. EVI is not the solution for these policy objectives, but it is a vital slice in the stack of systems and applications needed to make traffic and transport measurements more efficient and effective.

So on a European level EVI is a rather logical system to explore on its feasibility. This premise is rather in line with the conclusion of the council of leaders the eEurope conference in 2000 (June, Feira, Portugal). In the eEurope declaration a rather high level of ambition was set to deploy information and communication technology (ICT) better and throughout the whole of Europe. This declaration also reflects to ITS (Intelligent Transport Systems). In the declaration (chapter 5) it was mentioned that member states should work together to find and establish ways to do so. More concrete it was advised to cooperate to establish standards for ITS in general. In particular the theme of Electronic Car ID was mentioned as an example where electronic and telematic information handling systems should be deployed. This feasibility study is a straight result of that intention and fits therefore in the eEurope ambition.

10.2 Questions, whose answers will influence the public and political opinion on EVI

The first question with respect to social and political acceptance is: ‘What changes in public’s perception might occur with the introduction of EVI in the current situation (for the distinguished deployment scenarios)?’.

The second question is: ‘is it realistic for the countries to implement EVI?’.

The third question is: ‘Who is going to pay for EVI and who will gain the benefits?’

All three questions will be explored.

10.3 Changes introduced by EVI

From an objective point of view EVI will not bring major changes to the public. After all EVI will enable (support) public authority applications that are already there. It can do this more efficient, secure (threat for privacy) and with less fraud. This is the objective observation. The perception of the vehicle (registration) owners, however, can be that the public authorities will use EVI to control them. Embedding a high level of security in the EVI system cannot change this perception. Altering the possible perception asks for support and acceptance of the vehicle (registration) owners. To gain this support and acceptance asks for clear and honest communications from the public authorities.

On the other hand EVI brings some advantages to the vehicle owners. If EVI really helps to improve the vehicle registration process, less impostors will occur who will evade all kinds of obligations, like taxes and paying fees.

EVI will also improve the efficiency of public authority applications which need a vehicle identity, like road pricing and enforcement. From the point of view of the tax payer this is an advantage of EVI. From the point of view of the vehicle (registration) owner, respectively vehicle driver this might also trigger the fear for even more enforcement and road pricing. Advantages of EVI turn into disadvantages instantaneously, which bring us back to the public support and acceptance.

Perhaps, the support for and acceptance of EVI can be gained by showing the benefits to the public. Recovery of stolen cars could be a key entry to increasing public support and acceptance levels. Moreover, the security of EVI can be demonstrated.

When public support and acceptance for EVI is really low, deployment scenarios on a voluntary basis might be in favour. Another option is the mandatory deployment in phases. In both cases it will be possible to show the benefits to the public and to learn lessons from practice.

10.4 Is it realistic to implement EVI?

The countries in Europe have a different background on the outlined public authority applications and have different levels of appropriate vehicle registration. They also have different experiences with implementing ITS[1]-services.

Given the state of development or the socio-political preferences in a country it will be more or less realistic to implement EVI. In case the differences prove to be too large, starting to deploy EVI on a voluntary basis or in phases might be more successful.

10.5 Who is going to pay for EVI and who will gain the benefits

As stated in the economic assessment EVI will be cost beneficial for the public. However the question is, will EVI be cost beneficial for the individual? The benefits of EVI are in generic terms like efficiency and effectiveness, or road safety, efficient use of available infrastructure and fair road pricing. Do these benefits appeal to the vehicle (registration) owner who will have to pay for the installation of EVI in his or her vehicle? With the risk of being negative, we might say that the benefits are to abstract to tickle the individual vehicle (registration) owner at once. This asks again for gaining a solid public support and acceptance.

10.6 Reflection on social and political assessment

From social point of view a lack of public support for and acceptance of the introduction of EVI can be foreseen, dues to the following reasons:

- The cost for EVI are concrete for the individual vehicle (registration) owner, where the benefits are abstract (efficient, effective, policy goals); and
- The efficiency of EVI might give vehicle owners the impression public authorities will start to track them wherever they are (‘big brother is watching you’).

Furthermore there is the risk that the efficiency of EVI gives vehicle owners the impression that the level of enforcement and road pricing will increase.

From political point of view a lack of support for and acceptance of the introduction of EVI can be foreseen, due to the following reasons:

[1] ITS = Intelligent Transport System

- EVI implies that the vehicle registration should be improved in a specific country and therefore brings costs first; and

- EVI implies that a set of secure environments (see security assessment) have to be installed and again brings costs first.

11 Assemblage and reflection on EVI

11.1 Assemblage of the Assessment Results

What are the possibilities and barriers to realise EVI from a technological point of view?

EVI can fulfil its basic technological premises (as identified in Work Package 2), needed to enable (support) the public authorities applications. However, the actual capabilities (deficiencies besides the possibilities) of the available or planned wireless communication technologies used to realise the in-vehicle EVI components can form a barrier to enable all applications. Not every communication technology or even combination of communication technologies can enable all the applications. Therefore a careful selection of communication technologies is necessary when the final Realization Type of EVI is assembled.

Some public authority applications need a HMI to pass on information to the vehicle driver. The in-vehicle EVI components have to be linked to such a HMI in order to be able to enable (support) these applications.

Some public authority applications need precise pinpointing of the vehicle. In case a communication technology is used that does not support the exact pinpointing of a vehicle, a link to an external localisation unit should be provided.

'What are the possibilities to actually improve the reliability of the unique vehicle identity and the vehicle identification?'

By embedding security in the complete life cycle of EVI, the reliability of the unique vehicle identity and the vehicle identification can be improved. However, even with EVI it is realistic to expect impostors to fraud the EVI system or to misuse the EVI system and violate the privacy of the vehicle (registration) owners. On the other hand there are quite some possibilities to take countermeasures to protect EVI for such fraud and threat of privacy.

Issues left over after exploring those countermeasures are:

- Interrupting the availability of the in-vehicle EVI components by a vehicle (registration) owner (and/or driver). Surveillance teams are needed to discover these impostors.
- The protection of the integrity and confidentiality (in case all data is stored in the in-vehicle EVI components will weaken during the lifetime of the in-vehicle EVI components since. Regular (e.g. once in the four years) deinstallation and reinstallation of new in-vehicle EVI components is needed if we want to keep the protection on the same level.

The countermeasures for both issues will increase the costs for EVI and therefore will influence the 'business case' of EVI.

What are the possibilities and barriers to deploy EVI on a European and / or nation wide basis?

In principle EVI can be deployed on a nation or Europe wide basis. However it should be understood that EVI certainly has impact on the institutions needed for a properly operating (distribution of data), secure and environmental acceptable EVI. The seriousness of this impact depends to a large extent on the way the vehicle registration is organised in a country nowadays. This seriousness might be a barrier for the deployment of EVI nation or Europe wide.

For example, the impact will be manageable in countries where the licence plate is under strict control. Many of the organisations already exist and only need to be upgraded to organisations that are able to deal with electronic devices and security key management. While in countries where the licence plate is not under a strict control yet, a more complex upgrade of the organisation will be necessary.

Another example; In countries where the vehicle registration database does already cover the items of Directive 1999/37/EC and does already posses of a real-time (seconds) external interface for challenge-respond with EVI reader and/or writer, the impact of EVI will be manageable again. On the other hand, in countries where the vehicle registration database does not cover al relevant data yet and/or does not posses of such a real-time (seconds) external interface, a more complex upgrade of the vehicle registration database will be needed.

So the severity of the institutional impact should be considered per country when starting the preparations for the introduction of EVI. In fact the differences between the Member States do form a barrier to deploy EVI on a European wide basis.

What benefit(s) can EVI deliver above and beyond the existing mechanisms for identifying individual vehicles?

Do the identified benefits that can be derived from EVI outweigh the costs of implementation and operation (regarding the way(s) of deployment)?

EVI is economically feasible dependent on the applications that are supported and the policy goals that are aspired. Dependent on these desires a final conclusion could be drawn whether EVI is economically feasible or not.

EVI comes with three kinds of benefits:

- First order of benefits: improvement of correct vehicle identification;
- Second order of Benefits: improved efficiency in enabling applications; and
- Third level of Benefits: these are the benefits of the applications which can be enabled (supported) by EVI directly (e.g. tracking of missing vehicles, road safety via enforcement)

The *first order benefits* are inherent to EVI. They are not only an economic factor but also an ethical factor (‘all vehicle owners do have the same obligations towards the public authorities’).

The *second order of benefits* consists of:

- Benefits due to reduction of system costs;
- Benefits due to efficiency of vehicle identification; and
- Benefits due to effectiveness of traffic management measures.

In all cases the benefits of EVI outweigh the cost, if EVI was deployed on a regional basis. To be precise in the region where massive vehicle identification is needed due to road pricing schemes, or where a more efficient use of the available infrastructure is needed. These types of benefits are not a justification for nation, or Europe wide deployment of EVI.

The third order of benefits reflects the benefits applicable for all the European Union Member States. These benefits concern road casualties and reduction of stolen vehicles. Again benefits of EVI outweigh the cost, be it that the payback time varies between 7 and more than 25 years, depending on the basic functional level of EVI

All in all, EVI is economically feasible depending on the political priorities for implementation of public authority applications.

With respect to the costs of introducing EVI in society, it should be stated that the costs do not only consist of implementing the EVI device in the vehicle. Realising the roadside infrastructure and improving back-office systems are additional costs for realising EVI in Europe. These costs will increase the pay back time for EVI.

What legal barriers are to be expected when deploying EVI?

In fact there are no real legal barriers for the introduction of EVI with respect to the existing legal framework. The reality however will be that while introducing EVI the legal framework will change due to test cases for court and new to be developed jurisprudence.

What social and political barriers are to be expected when deploying EVI?

From social point of view a lack of public support for and acceptance of the introduction of EVI can be foreseen, due to the following reasons:

- The cost for EVI are concrete for the individual vehicle (registration) owner, where the benefits are abstract (efficient, effective, policy goals); and

- The efficiency of EVI might give vehicle owners the impression public authorities will start to track them wherever they are (‘big brother is watching you’).

Furthermore there is the risk that the efficiency of EVI gives vehicle owners the impression that the level of enforcement and road pricing will increase.

From political point of view a lack of support for and acceptance of the introduction of EVI can be foreseen, due to the following reasons:

- EVI implies that the vehicle registration should be improved in a specific country and therefore brings costs first;

- EVI implies that a set of secure environments (see security assessment) have to be installed and again brings costs first.

11.2 REFLECTION ON EVI

As was stated in part A of this document, EVI can be designed in numerous ways. We can choose for a specific functional level ('how to use EVI'), also specifying the level to communicate between the in-vehicle EVI device and the EVI reader and/or writer, and a way to distribute the vehicle data over the EVI system and the back-office (vehicle registration database). We can also chose for a specific deployment scenario taking into account the functional level of EVI and the way of introducing EVI (mandatory versus voluntary, at once, versus in phases, common standard versus no common standard). What are the considerations that help us to make our choices on EVI? In this paragraph the consideration stemming from the assessment are summarized.

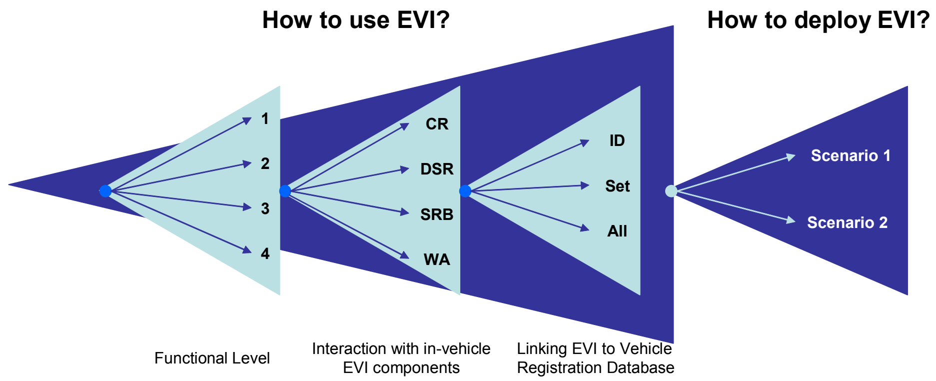


Figure 11.1: Assemblage of the Objects of assessment.

'How to use EVI' – Basic Functional Level

- Each functional level is technical feasible.
- The basics for security is to make the EVI device a secure device, in order to safeguard the integrity of the data send to the reader and/or writer. The security is increased even more in case of 'Write once-Read many'.
- All functional levels will improve correct vehicle identification (first order benefit). Functional level 2 – 3 are able to improve the efficiency of public authority applications aimed at fairness of road pricing and efficient use of available infrastructure using both moving and stationary vehicles (second order benefit). Functional level 1 is limited to stationary vehicles and therefore limited in benefits. All functional levels are EU-wide beneficial for road safety and reduction of vehicle crime.
- In fact for all functional levels the benefits will outweigh the costs, although the payback time is long for functional level 1. Functional level 3 scores best in case of retrofit.
- Public authorities will have to get used to EVI and have to upgrade their legacy systems to be enabled by EVI.

'How to use EVI' – External interface between in-vehicle EVI device and reader and/or writer

- A specific communication technology can enable a set of public authority applications but not all of them. By smart combining the communication technologies all applications can be enabled.
- A weak spot in the security is the availability of the wireless I/O to the reader and/or writer which can be blocked. The minimum countermeasure to protect this weak-spot is to make the EVI reader and/or writer capable of notifying jamming of the communication between vehicles and reader and/or writer.

'How to use EVI' – Linking EVI to the Vehicle Registration Database

- By storing the set of vehicle (component) identifiers in the EVI device, a fast and simple cross-check of the vehicle status is possible.
- The VIN is a good candidate for the unique vehicle identifier, under the premise that the VIN really will be unique.
- In order to enable specific applications even in split seconds, a small set of vehicle data has to be stored in the vehicle, more then just a unique vehicle identifier.

- The major part of the data can be kept at the back-office, under the premise that an EVI reader-writer can receive the data in seconds after sending a request.
- Just as with the licence plate confidentiality should be guarded by the back-office.

'How to deploy EVI'

- The complexity of installing the in-vehicle EVI components increases from level 1 to level 4
- The life cycle of EVI should be covered via secure environments, despite of the basic functional level.
- Functional level 2 might asks for an organisation to roll out gantries with EVI readers and/or writers.
- The deployment scenarios do have different timelines, and therefore will have different payback times.
- It is interesting to combine the rollout of EVI with starting to use EVI and therefore gaining the benefits from EVI from start on.
- By smart rollout of EVI immediate usage of EVI may be possible, which helps to reduce the payback time.

GLOSSARY OF TERMS AND ABBREVIATIONS

Authority

A user identifying vehicles under public law

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities or processes. [ISO7498-2]

EVI

The action or act of identifying a vehicle with electronic means for purposes as mentioned in this study.

EVI device

A trusted part of the OBE in which the EVI data is securely stored.

EVI reader

A device, e.g. fixed, mobile or hand-held, used to read EVI related data to the OBE of a vehicle.

EVI writer

A device, e.g. fixed, mobile or hand-held, used to write EVI related data to the OBE of a vehicle.

Privacy

The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. [ISO7498-2]

Reliability

The ability of a *functional unit* perform a required function under given conditions for a give time interval. [ISO2384-14]

Security

The protection of information and data so that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them. [ISO 12207]

NOTE Security vs safety (informal)

Security: protection of the system against its environment

Safety: protection of the environment against the system

Vehicle identification

The action or act of establishing the identity of a vehicle. [draft prENV ISO 24534]

User

A legal or natural person identifying vehicles.

ABBREVIATED TERMS

CALM	Continuous Air Interface for Long and Medium distance
DECT	Digital Enhanced Cordless Telecommunications
DSRC	Dedicated Short Range Communication
EC	European Commission
EU	European Union
EVI	Electronic Vehicle Identification
GNSS	Global Navigation Satellite System
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
HiperLAN	High Performance Local Area Network
HMI	Human Machine Interface
ISO	International Standards Organisation
OBE	On Board Equipment
OCR	Optical Character Recognition

OEM	Original Equipment Manufacturer
RFID	Radio Frequency Identification
UMTS	Universal Mobile Telecommunication System
VIN	Vehicle Identification Number
WLAN	Wireless Local Area Network
WORM	Write Once Read Many
WP	Work Package

BIBLIOGRAPHY

Centraal Justitieel Incasso Bureau, *“Jaarverslag 2003”*. Leeuwarden, Centraal Justitieel Incasso Bureau, 2003.

ESCAPE, *“Traffic enforcement in Europe: effects, measures, needs and future”*, Final report of the ESCAPE project. ESCAPE project, April 2003.

European Automobile Manufacturers Association, *“Electronic Vehicle Identification (EVI) – An ACEA Position Paper”*. Brussels, European Automobile Manufacturers Association, April 2004.

EVI, *“EVI requirements and user needs”*, WP2 report of the EVI project. EVI project, July 2003.

EVI, *“High level architectures, technology options and realization options”*, WP3 report of the EVI project. EVI project, March 2004.

Fildes, B, J. Scully and D. Logan, *“Discussion paper – Vehicle Identification number”*. Monash University, September 2003.

ICF Consulting, *“Cost-Benefit Analysis of Road Safety Improvements”*. London, ICF Consulting, June 2003.

KLPD, *“Motor vehicle identification – Why EVI is so important”*. March 2004.

Parliamentary Advisory Council for Transport Safety, *“Road Traffic Police Enforcement and New Technologies”*, Inception Report. London, Parliamentary Advisory Council for Transport Safety, October 2003.

Pelgrim, N., *“Dynamische verkeersmanagement; Een betaalbare oplossing voor het fileprobleem?”*. Amsterdam, University of Amsterdam, 29 June 1999.

RDW Centre for Vehicle Technology and Information, *“Businesscase-analyse Elektronisch Kenteken”*. Zoetermeer, RDW Centre for Vehicle Technology and Information, April 2003.

RDW Centre for Vehicle Technology and Information, *“Completeness and availability of the European back offices for EVI”*. Zoetermeer, RDW Centre for Vehicle Technology and Information, November 2003.

TNO, *“Overwegingen bij een kilometerteller ten behoeve van variabiliseren van autokosten”*. Delft, TNO, January 2001.

Tuuk, J. van, “*Vehicle chain of Europe”*. Veendam, RDW Centre for Vehicle Technology and Information, February 2003.

Reinhardt, W., *“EVI comments by automotive industry”*. Brussels, European Automobile Manufacturers Association, April 2004.