CEN / TC 278

ROAD TRANSPORT AND TRAFFIC TELEMATICS

Working Group 14

After Theft Systems for Vehicle Recovery

Work Item 14.6

Messaging Interface

Document Reference WG14.6 messaging interface

Distribution Working Group 14

AMENDMENT RECORD

Issue	Amendment Detail	Author	Date
A	Preliminary Draft of Working Paper Distributed to WG14 co-ordinators		November 2001
B	Format and Grammatical Changes WG14 co-ordinators	WG14 Convenor	August 2003
C	Corrections to conform WG14.3	Tony Scorer	December 2003
D	Corrections	Convenor	January 2004

DOCUMENT PRODUCTION SOFTWARE

Software	Version
Word for Windows	Word 2000

1 Introduction

1.1 Foreword

This document was developed by CEN TC 278 Road Transport & Traffic Telematics Working Group 14 (WG14) on the subject of After Theft Systems for Vehicle Recovery (ATSVR).
WG14 comprised representatives and experts from police, insurance associations (CEA), car manufacturers, transport associations, vehicle rental associations and ATSVR system and product providers. The work was also in co-operation with Europol and the European Police Co-operation Working Group (EPCWG).
The standard was developed to define an architecture within guidelines from CEN TC 278 through which a level of interoperability can be achieved between Systems Operating Centres (SOC) and Law Enforcement Agencies (LEA), both nationally and internationally.
This will provide minimum standards of information and assurance to users as to the functionality of systems, thereby enabling the recovery of vehicles, detection of offenders and a reduction in crime.
This document should be read in conjunction with prENVXXX Reference Architecture and Terminology which provides the preliminary framework for ATSVR concepts.

1.2 Scope

This document specifies guidelines for co-operation and the procedures to be followed between the LEA and ATSVR System Operating Centers (SOC) in response to alarm signals by ATSVR systems. For purposes of optimum mutual communication, this paper also includes suggestions and a format for the electronic exchange of information.

ATSVR are electronic systems that enable a communication centre or other authorised facility, such as the LEA, to monitor the location and theft status of a vehicle. Other information may also be available including speed and direction. These systems may be automatically activated by a signal from an anti theft security device or on receipt of a signal from an authorised SOC following confirmation of theft.

Systems may be short range or long range and may use different technology to achieve the results. Systems may identify the vehicle from on-board data or via reference to data held external to the vehicle. Nevertheless the standards of data and speed of communication should be compliant with requirements in this set of standards. System reliability and good, consistent procedures are extremely important.

System operators and users must remain aware that the level and timing of any response ultimately remains the responsibility of the LEA where the vehicle is currently located by an ATSVR system. It is implicit that there should be a uniform way of dealing internationally with these systems when the stolen vehicle is in a country other than where the originating SOC is located.

2 References

2.1 WG14 Documents

BN9607028 Nov 96	Task Force Report “After Theft Systems for Vehicle Recovery Investigation into Standardisation requirements
14N903E2 Jun 99	14.2 "Summary of Users Requirements"
14N007E Feb 00	WG14 revised work program
14N009E Feb 00	14.6 "Messaging Interface"
14N008U Nov 00	Internal Technical Report WG14.1 "Conceptual Architecture & Terminology "

2.2 Normative References

See those listed in associated documents.

EU 95/54	Automotive type approval for Suppression of Radio Interference (i.e. EMC) for 4 wheeled vehicles

3 Definitions and Abbreviations

3.1 After Theft System for Vehicle Recovery

An After Theft System for Vehicle Recovery (ATSVR) is a system that comprises various elements that communicate and interact through various interfaces in accordance with standard procedures and transmission protocols in order to facilitate the recovery of a Registered Stolen Vehicle.
This Standard does not seek to define the requirements or actions of the various human elements of the ATSVR, but it does aim to identify the interactions and interfaces that exist amongst the equipment and human elements operating within the system.

3.2 Remote Engine Degradation

The ability for an ATSVR system, or another system linked to an ATSVR system, to remotely degrade the engine performance of a stolen vehicle so as to significantly reduce the speed or cause the thief to park and abandon the vehicle.

3.3 Abbreviations

ATSVR	After Theft Systems for Vehicle Recovery
LEA	Law Enforcement Agency
SOC	System Operating Centre
OBE	On Board Equipment
DE	Detection Equipment
LR	Long Range (Communications Interface)
SR	Short Range (Communications Interface)
ETSI	European Telecommunications Standards Institute

4 Message requirements.

4.1 National & Local level messaging for ATSVR technology

This document was developed by CEN TC 278 Road Transport & Traffic Telematics Working Group 14 (WG14) on the subject of After Theft Systems for Vehicle Recovery (ATSVR). The potential for widespread adoption of ATSVR and the possibility of false or malicious calls requires an agreed process at local and national level.

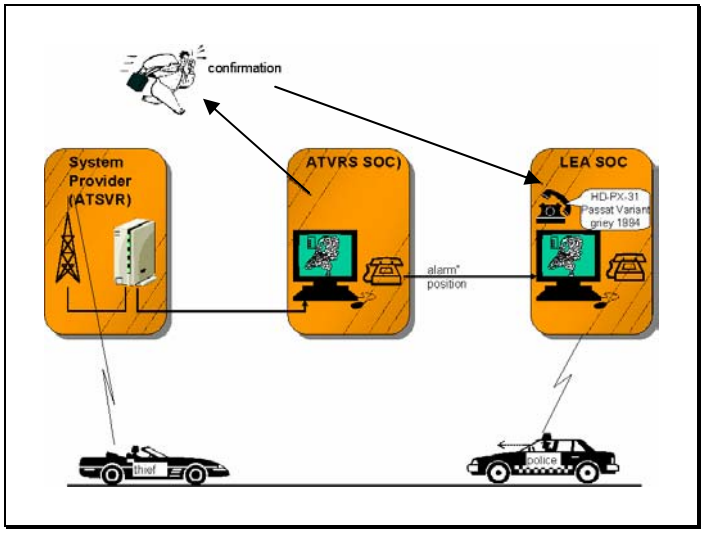

Figure1: National level: five-step process.

:

1. SOC notifies the Vehicle Owner or Authorised User of indication of unauthorised use of the Target Vehicle / OR, owner notifies SOC of theft to start process where the system is activated by the SOC,

2. Vehicle Owner or Authorised User confirms that the Target Vehicle has been stolen,

3. SOC and / or owner/authorised user report the vehicle, as a Confirmed Stolen Vehicle to LEA. When a case of car jacking is confirmed by other, possibly technical, means the SOC is not obliged to confirm the emergency call to the owner/authorised user who is with the vehicle.

4. SOC gives location, speed, direction, and other data to LEA and agrees continuous commentary or regular updates at defined intervals of time or distance. This data is system dependent.

5. LEA decides on level of response and advises SOC.

4.2 International Level messaging for ATSVR technology

The exchange of information between police forces across borders is a matter for those police forces, Interpol, Europol and Schengen to address and not for CEN.

These LEA organisations are responsible for the exchange of crime intelligence and operations against organised crime. Looking to the future when many vehicles will be fitted with After Theft

devices, some of which will also offer audit trials for debt collection or failure to return hire vehicles. These applications are not an area that will concern these international police organisations. Indeed, the tracking of a stolen car will be low on the list of their priorities when speed may be essential as the vehicle travels towards seaports or non-EU countries.

This scenario is based on the fact that a bureau in one country could easily monitor the theft and location of vehicles in several other countries. The police in the country where the vehicle was stolen may not agree to detain a vehicle and driver based on information from a non-police source outside their country.

The CEN/TC 278 preferred model is that if a company offers an ATSVR product that is capable of operating in other countries and some SOC facility is required to contact the police, then the responsibility for transmitting the information across borders remains with the SOC. It is not for the police to assist them with international communication to carry out their commercial obligations.

It should be the responsibility of the SOC to have links with an authorised SOC in each country where the system will operate. The location/tracking information will be passed to the SOC in the country where the vehicle was stolen and they will contact the local police and give details of location. This way the operators speak the local language, will know much of the local geography and will be known to the police who may then have more faith in the information being correct.

At the time of first publication of this standard the information exchange will be by telephone, but future systems will make it possible to exchange data information electronically.

5 SOC Approval by LEA.

5.1 Non-confirmed theft & Calls from non-certified SOC's

LEA's do not normally accept location/tracking data for a non-confirmed theft or from a non-approved SOC. There will be occasions where such information is accompanied by other important information that leads an LEA to believe that, in spite of the lack of conformity with these rules, there is a special case to accept that police response is desirable. Such occasions will be the rare exception than the rule and there must be no assumption by the ATSVR provider, the SOC or the owner of vehicles that such response will be given. The only reasonable means of gaining police response is compliance with this standard.

5.2 The minimum standard for an approved SOC

- Operates 24 hours a day, 365 days a year
- Provides full backup monitoring systems in the event of down time
- Has a recovery plan enabling continuity of service.
- Adheres to its own national data protection laws.

The following information should be available to the LEA from the ATSVR system or from the SOC data. The exact data will be that appropriate to the system technology.

1) Long Range

a. Dynamic:

- Incident, place of theft
- Dynamic data, direction
- Incident, time of theft
- Dynamic data, descriptive location
- Dynamic data, speed
- Dynamic data, geographic location
- Dynamic data, date and time

b. Static:

- Incident, URN
- Incident, vehicle load
- Incident, vehicle passengers
- Name and address of owner / keeper
- Incident report

c. Object:

- Vehicle manufacturer
- Vehicle, body type
- Vehicle colour
- Vehicle, licence plate / registration number
- Vehicle, country of registration
- Vehicle VIN number
- Vehicle, other descriptive information

When the vehicle with an ATSVR system is in another country and the information of the vehicle's position is received in the home country, the SOC sends this information to its partner in the relevant country.

The receiving partner SOC informs the local LEA in accordance with national regulations.

2) Short Range

a. Dynamic:

- Dynamic data, date and time
- Dynamic data, descriptive location
- Dynamic data, speed
- Dynamic data, geographic location
- Dynamic data, direction of travel

b. Object:

- Vehicle manufacturer
- Vehicle, body type
- Vehicle licence plate / registration number
- Vehicle, nationality
- Vehicle, colour
- Vehicle VIN
- Vehicle, other descriptive information

6 Procedures

6.1 Procedure for the System Operating Centre (ATSVR SOC)

Figure 3 shows a schematic representation of the procedure for a System Operating Center (SOC) upon receipt of a missing vehicle call.

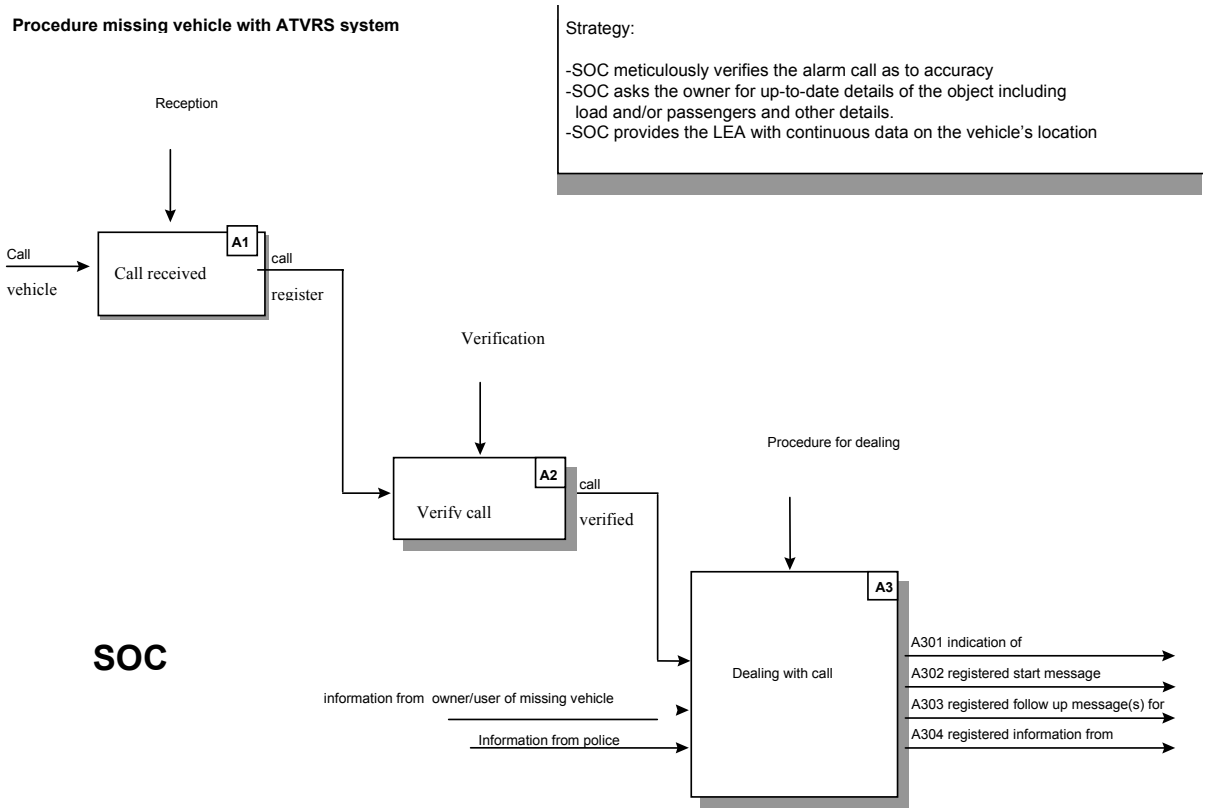

Figure 3:

A SOC (System Operating Center) is notified that the vehicle has gone missing, by the owner or the vehicle itself generating the call. This SOC verifies the facts with the owner and records the contents of the vehicle and any other (external) particulars.
Only when it is quite certain that the owner has confirmed that the vehicle is missing, is a message sent to the regional incident room of a LEA. The choice of the LEA depends upon the location of the vehicle and the national procedures. The selection should be done on the basis of a so-called 'relation chart' in which the relation is made between the name of every town and the LEA region within which the town is situated. The owner is instructed to report the theft to the LEA. This formal report depends on the requirements of the law in each country.
If the vehicle in question is moving, the SOC should provide information about the position, direction in which it is being driven and speed to the LEA. The frequency of new information or the use of continuous commentary will be determined by the LEA according to the level of LEA response and the type of ATSVR system. The LEA then take over the co-ordination of any (inter) regional deployment.

Specific systems
The certified SOC's will have various automated systems at their disposal. It is desirable for them to have the same system for facilitating electronic exchange of information with the LEA.
This LEA procedure should contain the following elements (Registered advice or information means that this advice or information is officially logged and recorded):

- A301: Indication of follow-up care

- A302: Registered start message for the LEA
- A303: Registered follow-up message(s) for the LEA
- A304: Registered information for the party making the call/owner

6.2 Co-operation procedure to the Law Enforcement Agency (LEA SOC's)

Fig. 4 shows a schematic representation of the procedure for the police upon receipt of a missing vehicle call.

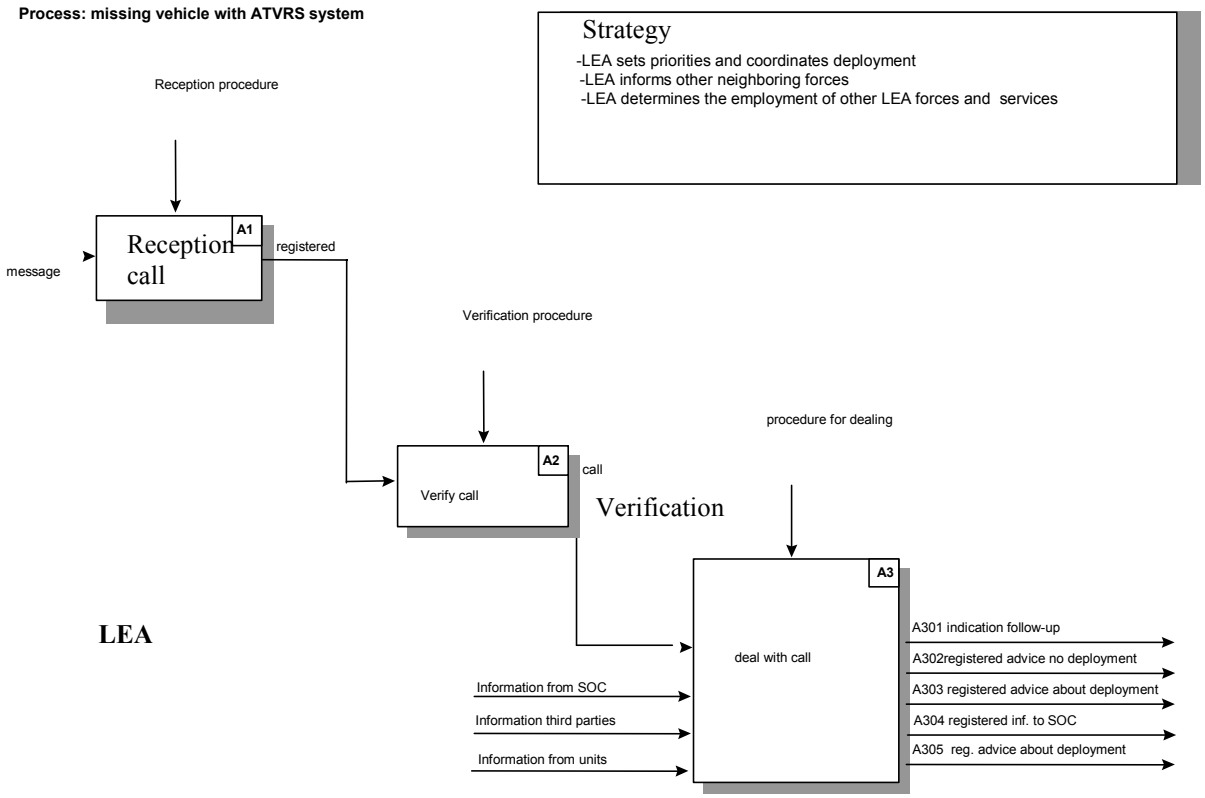

Figure 4:

A SOC (System Operating Center) advises the LEA by sending a 'starting message' to commence the process. If the vehicle is moving, the SOC sends frequent information about the position, direction in which it is driving and speed to this incident room by sending so-called 'follow-up messages.' (In case of homing systems initial information from the SOC is sufficient) In this manner, the LEA officers that are involved in the deployment have adequate information at their disposal for determining the tactics to be followed. The regional incident room of the LEA is responsible for the deployment of the LEA.
Accurate data and prompt response creates a good chance that suspects can still be found in or in the vicinity of the vehicle.

Specific systems

The message sent by the ATSVR SOC is checked for authenticity by the LEA that receives it. After it has been authenticated, the message is prioritized according to quality of data, resources available and the nature of other messages being handled (no uniform systems) to determine the LEA response. By using a GIS (Geographical Information System), the characteristics for determining location can be projected on the 'map'. After each follow-up message this data can be brought up-to-date in the GIS.
This procedure should contain the following elements:

- A301: indication of follow-up action

- A302: Registered advice about no deployment/action
- A303: Registered advice about deployment by/via regional incident room
- A304: Registered information to the SOC
- A305: Registered advice about deployment of an auxiliary service (non LEA unit)

7 Remote Engine Degradation Function

This function provides the possibility to degrade remotely the vehicle's performance using either long or short-range transmission techniques. Short-range communication may be preferable as some countries require the vehicle to be in direct line of sight of authorised personnel to trigger this function.

Regulations for these devices will be developed according to the laws in each country. However, this standard seeks to establish main principles as currently requested by the LEA's. These are:

- Use of the system and the resulting engine degradation must not lead to the contravention of vehicle or road transport legislation in the country where it is to be operated. Differences in legislation in different countries must be taken into account.

- The system must not compromise the safety of the vehicle, or any other vehicle. It must only influence the intended vehicle and no other, irrespective of system or system operator (anti-collision protection).

- For safety reasons the device must not switch off the engine or have any influence on the braking, steering or safety of the vehicle. Subject to these requirements a slow degradation of power that the engine can generate is permissible. The degradation time may be as long as 30 to 60 minutes until a steady low power state is reached. This would permit the driver to park the vehicle safely without endangering passing traffic.

- There must be a positive identification of the vehicle and a confirmation that it is actually stolen.

- The systems may only be activated by a person authorised by the LEA or a relevant government department. Some countries may require the vehicle to be in direct line of sight of such an authorised person to trigger this function.

- ATSVR companies will indemnify, in writing, each LEA where it is intended that the system will operate. The indemnity shall cover the LEA, and their officers and servants, against any claim under any course of action made by any person in respect of:

  (a) personal injury (including death) directly caused as a result of the use of the tracking/ remote engine degradation system,

  (b) any loss, damage, expense, personal injury (including death), wrongful arrest, prosecution or charge caused by the negligent operation of the system by the SOC, or by any malfunction of the system which results in a vehicle being wrongly identified as stolen.

- The ATSVR companies and SOC's must have international public liability insurance.

This section does not inhibit the use of Prohibit Engine Start function when the vehicle is in Engine Off mode.

8 Data Protection

8.1 General requirements

All data shall be accurate, up to date and secure, particularly where this relates to personal data. All data shall be kept in accordance with the data protection principles set out by the Council of Europe Convention on 28th January 1981 and shall take account of Recommendation R(87)15 of the Committee of Ministers of the Council of Europe 17th September 1987 concerning the use of personal data in the police sector.

There are some variations in requirements across EU member states. Therefore the data shall also be kept in accordance with the national data protection requirements of the country where the data originates and the country where the data is stored.

Appendix A Form for vehicle registration for use by ATSVR SOC's:

The initial registration of vehicles provided with a vehicle tracking system requires some what more detailed registration by the SOC's than has hitherto been used. In order to avoid each SOC developing its own version, WG14.6 recommends using a standard format for this registration. This document contains a proposal for this format form for vehicle registration for use by SOC's. The exact content, layout and language of the form is for the SOC and LEA to agree. Some of the installation data may be "commercial confidential", therefore the exact data will depend on the contract.

Contracting Party					
Name (of firm /owner)					
Contact person					
Address					
Postal code		Town		Country	
Telephone no.		Fax no./ e-mail address			

Vehicle			
Registration no.		Category (chart)	
VIN no.		Country of Registration	
Make		Type/Model	
Colour (chart)		Other	

Installation Data			
Installed by		Town	
Recognition no.		Class	
Make of equipment		Type	
Code		GSM no	
Burglary		Robbery	

(Insert Data Protection statement in accordance with Section 8.1.)

Alert			
1	title	Telephone no.	
		Radio/mobile no.	
2	Mr/Mrs/Ms	Telephone no.	
		Radio/car phone no.	
3	Mr/Mrs/Ms.	Telephone no.	
		Radio/car phone no.	
4	Mr/Mrs/Ms	Telephone no.	
		Radio/car phone no.	

System Operating Centre		
	Name and address Telephone no.	Fax :

Colour Chart				Category Chart	
0	White	5	Blue	01	Passenger car
1	Yellow	6	Green	02	Lorry
2	Orange	7	Grey	03	Trailer
3	Red	8	Brown	04	Semi-trailer
4	Purple	9	Black	05	Other

Free Text Page					

*** Colour code and category code like EU standard for the registration authorities.**

Appendix B Message specification

B.1 Scenario

Figure B1 shows a scenario for co-operation between SOC's and the police forces in response to the alarm call of an ATSVR system. It does not indicate whether and how many times each messages that can appear within a transaction.

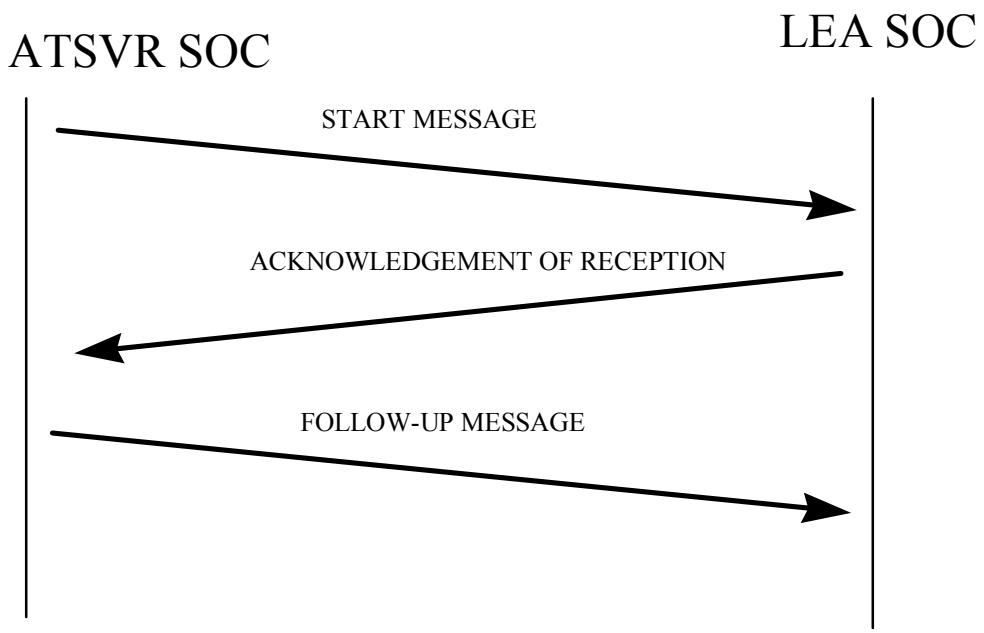

Figure B1: Scenario for co-operation between ATSVR SOC's and the LEA SOC.

B.2 Form and content of the message

The message elements are defined in prENV XXX. These elements are grouped together to form messages that pass between the SOC and LEA. If the information is not available then the code FF (hex) will be used.

B.3 Primary information (Fixed content)

Object
• Make (Vehicle, Manufacturer) • Type (Vehicle, Model) • Colour (Vehicle, Colour) • Registration number (Vehicle, Nationality & Licence Plate) • Country • Particularities (Vehicle, other Descriptive Information)

Dynamics
• Position: Dynamic Data, Descriptive Location or Dynamic Data, Geographic Location. Incident, Theft Update, Location • Time: Date and Time, Incident, Time of Theft, • Route see also Dynamic Data Descriptive Location • Direction Dynamic Data, Direction • Speed Dynamic Data, Speed

Static
• Confirmation • Motor on/off

B.4 Secondary information

Dynamics
• Place of theft

Static
• The Owner • Load • Passengers • Circumstances of theft

Object
• VIN

Appendix C Internet Communication

Suggestion for a model to be used in Internet-communication.

XML representation

<ELEMENT (starting message, receipt message, follow-up message*).>

<!--The ID of the starting message consists of a combination of the identification of the SOC in question with another unique characteristic. For example, in combination with the date and time when the message was drawn up. In this way, the unique character of each starting message is guaranteed.

The ID of the addressee can consist of part of the so-called 'PL-code', at least the first two positions of this.

The type indicates that it is a starting message.

These attributes can be left out if a choice is made for the message ID for including the date and time when the message was drawn up.-- >

<ELEMENT starting message (missing object, determining location)>

<!--Formats:
ID an..35

ID addressee an..35

type of message n2 chart: see list with attribute

date sent n8

time sent n4

- - >

<!ATTLIST starting message ID object CDATA #REQUIRED

ID addressee CDATA #REQUIRED

Type CDATA # REQUIRED

Date sent CDATA #REQUIRED

Time sent CDATA #REQUIRED>

<!--The significance of the receipt message is to acknowledge that the starting message has been properly received and processed. The ID of the receipt message consists of the ID of the starting message. The combination with the indication of the type of message as 'receipt message' makes it significant as such to the original sender of the starting message.

Date when sent and time when sent represent the time when the message was drawn up.

-->

<!ELEMENT receipt message (#PCDATA)>

<!--Formats:

(see starting message)- - >

<!ATTLIST receipt message ID object CDATA #REQUIRED

ID addressee CDATA #REQUIRED

TYPE CDATA #REQUIRED

Date sent CDATA #REQUIRED

Time sent CDATA #REQUIRED>

<!--The follow-up message is intended to send the up-to-date data of the location of the vehicle being tracked to the police. The ID of this message is composed of the ID of the original starting message. The indication of the type 'follow-up message' and the combination of date and time make it a uniquely identifiable message, provided that the time includes seconds as well.-- >

<!ELEMENT follow-up message (determination of location)>

<!--Formats:

(see starting message)-- >

<!ATTLIST follow-up message ID object CDATA #REQUIRED

ID addressee CDATA #REQUIRED

Type CDATA #REQUIRED

Date sent CDATA #REQUIRED

Time sent CDATA #REQUIRED>

<!--This element contains a collection of characteristics which can serve, in the first place, to make it possible to identify the vehicle for purposes of investigation and, in the second place, actually establish the identity of the vehicle.

The ID of the object in this context is usually the registration number, and if possible, combined with the vehicle identification number, as far as motor vehicles are concerned.

In the case of a trailer, this is often a registration sign which is different to the one on the vehicle.

The vehicle identification number makes a more reliable identification of the vehicle possible, compared with the registration number. Yet this VIN has a clearly lesser significance when police is in pursuit. As the exact position of the vehicle is known, in theory, for purposes of localizing it, law enforcement officers will be able to identify the vehicle from the description of the vehicle. Make, type and colour must be able to provide sufficient information for this purpose. After stopping the vehicle the VIN can be of great value for the final identification.

- - >

<!ELEMENT missing object (permanent features, up-to-date features*)>

<!-- By ID object is meant here the registration number or registration sign.

Format

ID an..35-- >

<!ATTLIST missing object ID object CDATA #REQUIRED>

<!--The data relating to determining the location are intended for establishing the position of the vehicle which has to be tracked. A collection of attributes has been selected which enables the police to be informed about the location of the vehicle, irrespective of whether they have a GIS at their disposal. Preference is given, however, to application of the coordinates. If that is the case (after the transfer of the x-y coordinates, the deployment by the police is given considerably better support, provided that they have a GIS at their disposal. If they do not have a GIS, then the other attributes must provide the necessary information about the position of the vehicle. In the indication of roads, this could be an indication of national and provincial roads.

The direction in which the vehicle is travelling is indicated with the directions of compass

The speed is given in kilometres per hour.-- >

<!ELEMENT determining of location(#PCDATA)>

<!--Formats:

name of town an..24 chart:PTT list of names of towns

x-coordinate an..30

y-coordinate.an..30

indication of road an..35

street name an..35

Direction in which vehicle is travelling n2 chart:???

Speed n..3 (in km/hour)

- - >

<!ATTLIST determination of location x-coordinate CDATA #IMPLIED

y-coordinate CDATA #IMPLIED

name of town CDATA #IMPLIED

street name CDATA #IMPLIED

direction of travelling CDATA #IMPLIED

speed CDATA #IMPLIED>

<!-- Permanent features in this connection are properties which are more or less invariable. It is not possible, for example, to convert a passenger car into an estate car in a trice.

The option for permanent features is partly based upon the impossibilities and possibilities connected with the initial registration of objects with the SOCs.-- >

<!ELEMENT permanent features (#PCDATA)>

<!-- Formats:

colour n2 chart: Colour of motor vehicle established by the RDW (TOO11)

type an..35

make an..35

category n2 chart: see list with attribute

other an..35-- >

<!ATTLIST permanent features colour CDATA #REQUIRED

type CDATA #IMPLIED

make CDATA #REQUIRED

other CDATA #IMPLIED

kind (passenger car /lorry/trailer/other/semi-trailer)

#REQUIRED>

<!-- This collection of data offers the police the possibility of attuning the deployment to the actual situation of the vehicle and the load and/or passengers, if any.

Up-to-date features will not part of the registration of the object with the SOCs.

Features of this kind will not usually be known until there is a dialogue between the owner of a stolen vehicle and a SOC. The staff of the SOCs must, therefore, expressly ask for these.

Passengers:

The present situation as regards the passengers of a missing vehicle is important for the police in determining how they are to be deployed. Passengers means other persons then the thieve(s).

Load:

In the section on load an indication can be given of whether, and if there is one, what load there is in the vehicle. In the case of a lorry or trailer, this can also influence the manner in which the police organize the manner in which they are to be deployed. That could be the case where there is a dangerous load or something similar.-- >

<!ELEMENT up-to-date features (#PCDATA)>

<!--FORMATS:

passengers an..70

load an..70-- >

<!ATTLIST up-to-date features passengers CDATA #IMPLIED

Load CDATA #IMPLIED>