3GPP TSG-SA ***Tdoc SP-050130***
Meeting #27, Tokyo, Japan, March 2005

Source: **MCC**
mailto:john.meredith@etsi.org

Title: **eCall initiative**

Document for: **information**

As part of the European eSafety project, eCall is investigating ways in which data can be included in (voice) emergency call setups initiated automatically in the event of a road traffic accident. The objective would be to transfer appropriate information (see annex D) to the emergency call answering point in order to direct the most appropriate form of emergency service to the scene.

The participants in the eCall project have hit upon the existence of the User-User Service as being the ideal mechanism for accomplishing this, without apparently being aware that UUS has been rarely if ever implemented on any mobile network (or indeed, fixed network). Within ETSI, work is being coordinated by Special Committee EMTEL (http://portal.etsi.org and click on EMTEL), and liaison is already established amongst EMTEL and SA1 and CN3 (now CT3). In addition, ETSI Technical Committee MSG (same URL, click on MSG) will coordinate the production of any necessary regulatory standards based on 3GPP base specifications, and has already started work on an initial Technical Report.

The purpose of the present document is to make the wider 3GPP community aware that the European Commission is putting heavy emphasis on establishing the eCall service, and to warn equipment suppliers and network operators that legislation is likely to enforce the obligatory provision of the service within the medium term.

Operators are naturally concerned that they will be required to support a large number of mobile terminals – including international and national roaming – which with luck will never make a call, and thus generate no revenue other than the monthly subscription (which may in fact be supplied by a supplement to the annual vehicle tax rather than directly by the vehicle owner). They are also concerned that they will have to implement UUS unless a better solution can be found.

On the other hand, equipping every vehicle with a cellular phone could, with imagination, give rise to using it for providing the driver with road traffic information (fog warnings, speed restrictions, diversions, queues, etc); and for providing passengers with entertainment services, announcements of tourist attractions ahead, etc. Such services could potentially be revenue-producing.

Incidentally, it is thought that the eCall initiative is quite unrelated to the emergency information conveyed over SMS which has been investigated by 3GPP T2.

The purpose of the present document is to make the wider 3GPP community aware that the European Commission is putting heavy emphasis on establishing the eCall service, and to warn equipment suppliers and network operators that legislation is likely to enforce the obligatory provision of the service within the medium term.

Annexed to the present document is an exciting collection of documents from several sources:

Annex A – Letter to ETSI from European Commission (DG Information Society)

Annex B – Safety Forum: eCall Memorandum of Understanding

Annex C – List of signatories to the eCall Memorandum of Understanding

Annex D – In-Vehicle E112 eCall based on UUS [Contribution to EMTEL from the eCall project]

Annex E – LS from EMTEL to SA1#27 and CN1#36: Support of eCall on UUS type 1 Supplementary Service

Annex F – Reply to EMTEL LS from SA1 (S1-050230)

Annex G – Emerge: Specifications of the European in-vehicle emergency call

Annex H – GST RESCUE newsletter

EUROPEAN COMMISSION
Directorate-General Information Society

The Director-General

Brussels, 05 I 2005
INFSO-C5/ AV /JJ/es D(2004) 550885

Mr. Karl Heinz Rosenbrock
ETSI Director-General
650, route des Lucioles
FR – 06921 Sophia-Antipolis
Cedex

Subject: The implementation of the pan-European in-vehicle emergency call (eCall): Need for standards

Dear Sir,

The European Commission, ACEA (Association of European Automotive manufacturers) and ERTICO ITS Europe established in 2002 the eSafety initiative. The eSafety initiative promotes the use of advanced Information and Communications Technologies for improving road safety, thus contributing to our goal of halving the number of road fatalities in Europe by 2010.

In 2003, the Commission adopted a Communication on eSafety[1]. It introduces a number of important actions for all road safety holders, including the establishment of the eSafety Forum as a common platform for all stakeholders, and actions for implementing a harmonised, pan-European in-vehicle emergency call (eCall) service that builds on the location-enhanced single emergency number E-112. On a related development, and building on the provisions of the Universal Service Directive 2002/22/EC, the Commission adopted a Recommendation on the caller processing of location-enhanced emergency calls[2].

Realising the importance of parallel commitment in the implementation of eCall, we established together with other stakeholders the so called eCall Driving Group that is co-chaired by Mr. M. Nielsen (ERTICO) and Mr. W. Reinhardt (ACEA). The eCall Driving Group has produced so far the following results:

[1] Communication from the Commission to the Council and the European Parliament: Information and Communications Technologies for Safe and Intelligent Vehicles, COM(2003) 542 Final, 15.9.2003

[2] Commission Recommendation on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services, 2003/558/EC, 25.7.2003.

- The eCall architecture that is based on a simultaneous voice-data link from the in-vehicle terminal to the PSAP. This architecture was introduced by a research project E-MERGE.

- A technical proposal for using UUS as the data over voice technology for eCall

- An eCall MoU, signed by the DG Information Society, ACEA and ERTICO on 27 August this year, and now with 21 signatures (attached).

Role of standardisation is emphasised both in the Communication and the Recommendation, and is seen by the eCall Driving Group as one of the prerequisites for a successful introduction of interoperable, pan-European eCall. This is why we have participated already in the meetings of EMTEL and TG37, explaining the eCall concept.

Mr. Bob Williams, chair of the ERMTG37, proposed as a practical vehicle inside ETSI the establishment of a Project Team, consisting of EMTEL, TG37, 3GPP and possibly other groups. We very much support this idea, based on the huge potential socio-economic benefits of eCall and the general support by the industry and the Member States, and we would like to urge you to:

(1) Initiate in ETSI the necessary work for standardisation of the necessary interfaces, protocols and data messages for transmitting data over voice from the in-vehicle eCall terminal to the Public Service Answering Point over GSM and ISDN networks

(2) To establish, if deemed necessary, a Project Team inside ETSI, and consider signing the eCall MoU on behalf of ETSI

(3) To liaise in this issue with the European Commission and the eCall Working Group.

My services are naturally available should you need additional information or support in meetings on eSafety and eCall, please contact Mr. Juhani Jaaskelainen, tel. +32-2-2965459, fax. +32-2-2969548, email juhani.jaaskelainen@cec.eu.int

Fabio Colasanti

Encl: eCall Memorandum of Understanding (MoU)
List of signatures eCall MoU

cc: B. Williams - Chair of ETSI/ERMTG37, M. Nielsen - ERTICO, W. Reinhardt – ACEA

EUROPEAN COMMISSION
Directorate-General Information Society

The Director-General

Brussels, 05 I 2005
INFSO-C5/ AV /JJ/es D(2004) 550885

Mr. Karl Heinz Rosenbrock
ETSI Director-General
650, route des Lucioles
FR – 06921 Sophia-Antipolis
Cedex

Subject: The implementation of the pan-European in-vehicle emergency call (eCall): Need for standards

Dear Sir,

The European Commission, ACEA (Association of European Automotive manufacturers) and ERTICO ITS Europe established in 2002 the eSafety initiative. The eSafety initiative promotes the use of advanced Information and Communications Technologies for improving road safety, thus contributing to our goal of halving the number of road fatalities in Europe by 2010.

In 2003, the Commission adopted a Communication on eSafety[1]. It introduces a number of important actions for all road safety holders, including the establishment of the eSafety Forum as a common platform for all stakeholders, and actions for implementing a harmonised, pan-European in-vehicle emergency call (eCall) service that builds on the location-enhanced single emergency number E-112. On a related development, and building on the provisions of the Universal Service Directive 2002/22/EC, the Commission adopted a Recommendation on the caller processing of location-enhanced emergency calls[2].

Realising the importance of parallel commitment in the implementation of eCall, we established together with other stakeholders the so called eCall Driving Group that is co-chaired by Mr. M. Nielsen (ERTICO) and Mr. W. Reinhardt (ACEA). The eCall Driving Group has produced so far the following results:

[1] Communication from the Commission to the Council and the European Parliament: Information and Communications Technologies for Safe and Intelligent Vehicles, COM(2003) 542 Final, 15.9.2003

[2] Commission Recommendation on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services, 2003/558/EC, 25.7.2003.

- The eCall architecture that is based on a simultaneous voice-data link from the in-vehicle terminal to the PSAP. This architecture was introduced by a research project E-MERGE.

- A technical proposal for using UUS as the data over voice technology for eCall

- An eCall MoU, signed by the DG Information Society, ACEA and ERTICO on 27 August this year, and now with 21 signatures (attached).

Role of standardisation is emphasised both in the Communication and the Recommendation, and is seen by the eCall Driving Group as one of the prerequisites for a successful introduction of interoperable, pan-European eCall. This is why we have participated already in the meetings of EMTEL and TG37, explaining the eCall concept.

Mr. Bob Williams, chair of the ERMTG37, proposed as a practical vehicle inside ETSI the establishment of a Project Team, consisting of EMTEL, TG37, 3GPP and possibly other groups. We very much support this idea, based on the huge potential socio-economic benefits of eCall and the general support by the industry and the Member States, and we would like to urge you to:

(1) Initiate in ETSI the necessary work for standardisation of the necessary interfaces, protocols and data messages for transmitting data over voice from the in-vehicle eCall terminal to the Public Service Answering Point over GSM and ISDN networks

(2) To establish, if deemed necessary, a Project Team inside ETSI, and consider signing the eCall MoU on behalf of ETSI

(3) To liaise in this issue with the European Commission and the eCall Working Group.

My services are naturally available should you need additional information or support in meetings on eSafety and eCall, please contact Mr. Juhani Jaaskelainen, tel. +32-2-2965459, fax. +32-2-2969548, email juhani.jaaskelainen@cec.eu.int

Fabio Colasanti

Encl: eCall Memorandum of Understanding (MoU)
List of signatures eCall MoU

cc: B. Williams - Chair of ETSI/ERMTG37, M. Nielsen - ERTICO, W. Reinhardt – ACEA eSafety Forum

eCall Driving Group

Memorandum of Understanding

for

Realisation of Interoperable In-Vehicle eCall

Table of Contents

European Memorandum of Understanding for Realisation of Interoperable In-Vehicle eCall

The purpose of this European Memorandum of Understanding (MoU) is to secure the realisation of an interoperable in-vehicle emergency call service (eCall) supplied, introduced and operated across Europe. This MoU does not represent a legally binding agreement; rather, it is an expression of the individual and collective commitment of the signatories to work in partnership in order to realise a shared objective to the benefit of everyone.

1. Preamble

1.1 Rationale

The introduction and use of in-vehicle eCall for deployment of emergency assistance will save lives and reduce social burden by improving the notification of road accidents and speeding up emergency service response. There is an urgent need for a European solution in order to contribute to a reduction of the 39,200[1] people killed, 3.3 million casualties and annual costs in relation to traffic accidents of more than 180 billion Euro. This is why the European Commission-led eSafety Forum adopted eCall as the highest priority amongst the eSafety measures contained in the recent eSafety Communication[2].

1.2 Definition of In-vehicle eCall

The in-vehicle eCall is an emergency call generated either manually by vehicle occupants or automatically via activation of in-vehicle sensors. When activated, the in-vehicle eCall system will establish a voice connection directly with the relevant PSAP (Public Safety Answering Point), this being either a public or a private eCall centre operating under the regulation and/or authorisation of a public body. At the same time, a minimum set of incident data (MDS)[3] will be sent to the eCall operator receiving the voice call.

1.3 Framework

This MoU creates a framework for the introduction of in-vehicle emergency call at all levels in the emergency call chain – including the public sector, the private sector and/or through public-private partnerships. The aim of this MoU is to encourage co-operation between the vehicle makers, Telecom Operators, the EC and the Member States (in particular the emergency agencies, the public PSAPs and the private PSAPs operating under the regulation of a public body) together with other relevant parties such as the insurance industry, automobile clubs and other relevant industrial partners.

[1] *ETSC report on Transport Safety Performance in the EU – A statistical overview 2003 (2001 statistics)*

[2] *COM(2003) 542 final: COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT "Information and Communications Technologies for Safe and Intelligent Vehicles"*

[3] *See Annex B*

2. Involved Parties

Moving forward with implementation of in-vehicle eCall requires parallel commitment and joint effort to work on common, co-ordinated implementation and supporting business plans from all Parties constituting the basic eCall service and value chain.

Such co-ordinated roll-out and business plans need to include optimised technical solutions, quality standards, co-ordinated target dates when emergency calls from in-vehicle systems can be handled by the infrastructure, the incremental investments needed to develop, produce and operate such systems and infrastructure adaptations, a financial model how investments and service costs could be financed and by whom, the possibility of fiscal and financial incentives, the benefits and savings by stakeholder group, etc.

The relevant stakeholder groups with the highest impact on the realisation of a European solution can be divided into two major groups: The Parties directly forming the eCall service chain (2.1 – 2.4) and the other Parties (2.5 – 2.8), which are essential contributors and accelerators of the process. Both groups need to work together to achieve the overall objectives and should be represented in the European Coordination Platform.

2.1 Member States

Member States signing this MoU and in particular those authorities in charge of emergency call services and related finance - e.g. civil protection authorities, Ministry of Interior and Ministry of Finance - agree to contribute to the development and agreement of country specific implementation plans conforming to the principles for pan-European eCall as defined in 1.2 and Annex B. For Member States having one or more Service Providers acting as PSAPs for the 112 services, this MoU requires a special handling. The Member State should, after signing this MoU, ensure that the Service Providers who are operating as PSAPs under their regulation gets a commission to handle in-vehicle eCall services. The agreement between the Member State and the Service Provider should include specification, financing and time plan of the in-vehicle eCall service implementation and operations.

2.3 Telecom operators

Telecom Operators signing this MoU agree to contribute to the development and agreement of feasible implementation and business plans conforming to the principles for pan-European eCall as defined in 1.2 and Annex B.

2.4 Vehicle Manufacturers

Vehicle Manufacturers signing this MoU agree to contribute to the development and agreement of feasible implementation and business plans conforming to the principles for pan-European eCall as defined in 1.2 and Annex B.

2.4 Service Providers operating as PSAPs under the regulation of a public body

Private Service Providers who are operating as PSAPs under the regulation of a public body signing this MoU agree to contribute to the development and agreement of implementation and business plans conforming to the principles for pan-European eCall as defined in Para 1.2 and Annex B.

In addition to the essential Parties constituting the eCall service chain, other players are an important part of the value chain and have an important role in supporting and accelerating market take up e.g. through specific support in the business and implementation planning phase and/or contributing to the overall business and outreach plan. These players have been identified as follows:

2.5 Insurance companies
2.6 Automobile clubs, service providers and other end user focused entities
2.7 European Commission DG Information Society, DG Transport, DG Environment
2.8 Related Industrial partners (equipment manufactures, location technology providers, repair industry etc.)

3. Act

The Parties signing this MoU will actively contribute to the development and agreement of feasible implementation and business plans conforming to the principles for pan-European eCall as defined in 1.2 and Annex B.

The Parties signing this MoU will – within the first 12 months following the signature of this MoU, which is targeted to take place within the first half of 2004 - define an overall European work plan and present their recommendation for decision.

To achieve the objectives each party signing the MoU will delegate minimum one expert as a member to the Driving Group on eCall. The representative should be empowered to take necessary decisions.

4. Process

4.1 European Co-ordination

The Parties signing this MoU will interact through a European Co-ordination Platform to co-ordinate their activities by bringing together all relevant stakeholders. Provided sufficient funds can be made available, the co-ordination platform will include studies on the economics underlying the introduction and the drafting of a road map at European level.

The European Commission is the appropriate body to determine the platform to be used for this European Co-ordination. Currently the Driving Group on eCall within the eSafety Forum is the appropriate platform, but the co-ordination may take another form in subsequent years to support implementers and monitor progress of implementation across Europe. However, such co-ordination should continue to be under the auspices of the eSafety Forum.

4.2 Status of the Memorandum of Understanding

This MoU summarises the current intentions of the different Parties signing this MoU. It will form the basis for action by each of the Parties according to their respective roles. However, nothing in this MoU legally obliges any Party to any other Party. Also, this MoU does not affect the rights (including intellectual property rights) of any Party to material or services supplied by them as part of the in-vehicle eCall chain. This MoU recognises that all Parties carry their own risks and costs in providing, carrying and handling the in-vehicle eCall initiative.

4.3 Review of this MoU

For this MoU to provide an effective framework for co-operation active participation of all sectors concerned is required. Progress on implementation and business planning by all Parties concerned will be reviewed when appropriate. However, first review should take place not later than after 12 months following the signature of the MoU. When appropriate the Parties, will consider the need for improvements in their co-operation and make and introduce suitable proposals for modification or termination to this MoU.

European Memorandum of Understanding
for in-vehicle e-call
SIGNATURE PAGES

Representative from *(Please tick)*	□ Member State	□ Telecom Operator	□ Vehicle manufacturer	□ Service Provider operating as PSAP under the regulation of a public body
	□ Insurance Company/ Organisation	□ Automobile Club	□ Service Provider	□ Related Industrial Party
	□ Other			

Name ______________________________

Status ______________________________

Organisation ______________________________

Contact Address ______________________________

Signature ______________________________

Date ______________

Annex A - Relevant European Resolutions, Conclusions and Decisions

C(2003) 2657 final
COMMISSION RECOMMENDATION of 25/07/2003 on the processing of caller location information in electronic communication networks for the purpose of location-enhanced emergency call services

COM(2003) 542 final:
COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT "Information and Communications Technologies for Safe and Intelligent Vehicles"

Universal Service Directive
(http://europa.eu.int/eur-lex/en/archive/2002/l_10820020424en.html)

Final CGALIES report
(http://europa.eu.int/comm/environment/civil/index.htm)

ETSC report
Transport Safety Performance in the EU – A statistical overview 2003 (2001 statistics)
ISBN: 90-76024-154

Annex B - The in-vehicle e-call minimum data set

Minimum Data Set

The parties agree to the following minimum data set that have to be sent directly from the vehicle to the public PSAPs or the private service providers operating as PSAPs under the regulation of a public body, in case of a manual or automatic emergency call initiated from the in-vehicle system.

Mandatory to be included:

- **Time stamp**
- **Precise Location**
- **Vehicle identification**
- **Service Provider Identifier**
- **E-call qualifier** *(as a minimum a indication stating if the eCall has been manually or automatically initiated)*

*e*Call Memorandum of Understanding

Status of signatures

	Organisation	Address	Name	Position/Title	Date of signature
1	ACEA	Rue du Noyer 211, BE-1000 Brussels	Mr Ivan HODAC	Secretary General	27/08/2004
2	ADAC e.V.	Am Westpark 8, DE-81373 Munich (contact person Bernhard Labudek)	Peter MEYER	President	30/11/2004
3	ARC Transistance S.A,	Av. des Pléiades, BE-1200 Brussels	Mr Andrew JOHNSON	Chief Executive	6/10/2004
4	CapGemini Finland OY	Niittymäentie 9, FIN02200 Espoo	Ms Anne-Maria HAUTALA	Chief Financial Officer	20/09/2004
5	City of Oulu Finland	PO Box 1, FIN-90015 Oulun Kapunki	Mr Kari NENONEN	Mayor	21/09/2004
6	Ellas SA TIC/PSAP				
7	ERTICO - ITS	Av Louise 326, BE-1050 Brussels	Mr Olivier MOSSE	Chief Executive Officer	27/08/2004
8	European Emergency Number Association - EENA 112	Chaussée de Saint-Job, BE-1180 Brussels	Mr Olivier PAUL-MORANDINI	Founder	31/08/2004
9	Finnish Road Administration	PO Box 33, FIN-00521 Helsinki	Mr Aulis NIRONEN	Director	22/09/2004
10	Hellenic Institute of Transport	6th Km Thessaloniki-Thermi Rd, GR-57001 Thessaloniki	Mr George GIANNOPOULOS	Director	30/08/2004
11	Indagon OY	Neijamiestentie 5A, FIN-00400 Helsinki	Mr Nikko WECKSTRÖM	Vice President/CTO	21/06/2004
12	Information Society Directorate-General - DG INFSO	BU24 3/43, BE-1049 Brussels	Mr Fabio COLASANTI	Director-General	27/08/2004
13	KLPD - The Netherlands' National Police Organisation	PO Box 100, NL-3970 AC Driebergen	Mr Pim MILTENBURG	Director of Police, Police Commissionar	30/09/2004
14	LSP Hungary	Debrecen Erzsébet u. 48 Hungary	Dr Graeme P SMITH	Managing Director	23/11/2004
15	Ministry of Transport and Communications Finland	PO Box 31, FIN-00023 Government Finland	Mr Harri KAVÉN	Director-General	22/09/2004
16	Mobisoft OY	Hatanpäävaltatie 26, FIN-33100 Tampere	Mr Heikki KARINTAUS	Managing Director	23/09/2004
17	Navteq B.V.	De Run 1115, NL-5503 LB Veldhoven	Mr Chris PETERS	VP Finance Europe	17/09/2004
18	Swiss Federal Roads Authority				23/11/2004
19	TeleAtlas NV	Montstraat 132, BE-9000 Gent	Mr Ad BASTIAANSEN	SR VP Business Development	2/09/2004
20	TISPOL, The European Traffic Police Network	PO Box 201, Hoddesdon, UK-EN11 8WX	Mr Ad HELLEMONS	President of the Tispol Organisation, Police Commissionar	30/09/2004
21	VTT Building and Transport	PO Box 1800 FIN-02044 VTT	Mr Juho SAARIMAA	Executive Director	20/09/2004
22	WirelessCar	Kajskjul 107, SE-41707 Göteborg	Mr Torbjörn SUNDSTRÖM	Director Marketing & Sales	14/09/2004

11/01/2005 12:35

*e*Call Memorandum of Understanding

Status of signatures

	Organisation	Address	Name	Position/Title	Date of signature
1	ACEA	Rue du Noyer 211, BE-1000 Brussels	Mr Ivan HODAC	Secretary General	27/08/2004
2	ADAC e.V.	Am Westpark 8, DE-81373 Munich (contact person Bernhard Labudek)	Peter MEYER	President	30/11/2004
3	ARC Transistance S.A,	Av. des Pléiades, BE-1200 Brussels	Mr Andrew JOHNSON	Chief Executive	6/10/2004
4	CapGemini Finland OY	Niittymäentie 9, FIN02200 Espoo	Ms Anne-Maria HAUTALA	Chief Financial Officer	20/09/2004
5	City of Oulu Finland	PO Box 1, FIN-90015 Oulun Kapunki	Mr Kari NENONEN	Mayor	21/09/2004
6	Ellas SA TIC/PSAP				
7	ERTICO - ITS	Av Louise 326, BE-1050 Brussels	Mr Olivier MOSSE	Chief Executive Officer	27/08/2004
8	European Emergency Number Association - EENA 112	Chaussée de Saint-Job, BE-1180 Brussels	Mr Olivier PAUL-MORANDINI	Founder	31/08/2004
9	Finnish Road Administration	PO Box 33, FIN-00521 Helsinki	Mr Aulis NIRONEN	Director	22/09/2004
10	Hellenic Institute of Transport	6th Km Thessaloniki-Thermi Rd, GR-57001 Thessaloniki	Mr George GIANNOPOULOS	Director	30/08/2004
11	Indagon OY	Neijamiestentie 5A, FIN-00400 Helsinki	Mr Nikko WECKSTRÖM	Vice President/CTO	21/06/2004
12	Information Society Directorate-General - DG INFSO	BU24 3/43, BE-1049 Brussels	Mr Fabio COLASANTI	Director-General	27/08/2004
13	KLPD - The Netherlands' National Police Organisation	PO Box 100, NL-3970 AC Driebergen	Mr Pim MILTENBURG	Director of Police, Police Commissionar	30/09/2004
14	LSP Hungary	Debrecen Erzsébet u. 48 Hungary	Dr Graeme P SMITH	Managing Director	23/11/2004
15	Ministry of Transport and Communications Finland	PO Box 31, FIN-00023 Government Finland	Mr Harri KAVÉN	Director-General	22/09/2004
16	Mobisoft OY	Hatanpäävaltatie 26, FIN-33100 Tampere	Mr Heikki KARINTAUS	Managing Director	23/09/2004
17	Navteq B.V.	De Run 1115, NL-5503 LB Veldhoven	Mr Chris PETERS	VP Finance Europe	17/09/2004
18	Swiss Federal Roads Authority				23/11/2004
19	TeleAtlas NV	Montstraat 132, BE-9000 Gent	Mr Ad BASTIAANSEN	SR VP Business Development	2/09/2004
20	TISPOL, The European Traffic Police Network	PO Box 201, Hoddesdon, UK-EN11 8WX	Mr Ad HELLEMONS	President of the Tispol Organisation, Police Commissionar	30/09/2004
21	VTT Building and Transport	PO Box 1800 FIN-02044 VTT	Mr Juho SAARIMAA	Executive Director	20/09/2004
22	WirelessCar	Kajskjul 107, SE-41707 Göteborg	Mr Torbjörn SUNDSTRÖM	Director Marketing & Sales	14/09/2004

11/01/2005 12:35

European Telecommunications Standards Institute
OCG EMTEL #9

Source: **eSafety DG eCall (Motorola GmbH / telmacon GmbH)**

Title:

In-Vehicle E112 eCall based on UUS data-over-voice technology,

message content and requirements for UUS-transmission

Date: **27.10.2004**

Document for:

Decision:	X
Discussion:	X
Liaison:	
Information:	X

Agenda item:

1. Used standards for In-Vehicle E112 eCall based on UUS data-over-voice technology

Transmitting UUS data from GSM to ISDN networks requires a number of specifications and standards.

These are:

- **E-Merge**

  E-MERGE, D3.0 Specifications of the European In-Vehicle E112 eCall. WP3,
  Version 1.5, 17.06.2003.

- **GSM**

  - 3GPP TS 24.087 - User-to-User Signalling (UUS) Supplementary Service; Service description - Stage 3

  - 3GPP TS 22.004 - Technical Specification Group Services and System Aspects; General on supplementary services

  - ETS 300 642 - Digital cellular telecommunications system (Phase 2); AT command set for GSM Mobile Equipment (ME)

  - 3GPP TS 24.008 / ETSI 124 008 - Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Mobile radio interface Layer 3 specification; Core network protocols; Stage 3

- **ISDN**

  - ETS 300 102-1 - Integrated Services Digital Network (ISDN); User-network interface layer 3 Specifications for basic call control

  - EN 300 403-1ntegrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification

2. UUS and its services

UUS is based on ITU-T Recommendations I.257.1 and Q.957.1.

The user-user signalling (UUS) supplementary service allows an ISDN- and mobile user to send/receive a limited amount of information to/from another ISDN user over the signalling channel in association with a call to the other ISDN user.

The UUS supplementary services provide a means of communication between two users by using as a basis the layer 3 protocol. Three UUS services associated with circuit-switched calls that may be provided by the network to users are:

- service 1 – User-to-User information exchanged during the setup and clearing phases of a call, by transporting User-user information element within Q.931 call control messages.
- service 2 – User-to-User information exchanged from the caller’s point of view during call establishment, between the ALERTING and CONNECT messages, within USER INFORMATION messages.
- service 3 – User-to-User information exchanged while a call is in the active state, within USER INFORMATION messages.

Currently Telecom supports service 1 with implicit invocation only.

Following figure shows communication and transmission way for UUS service 1 during the call set-up:

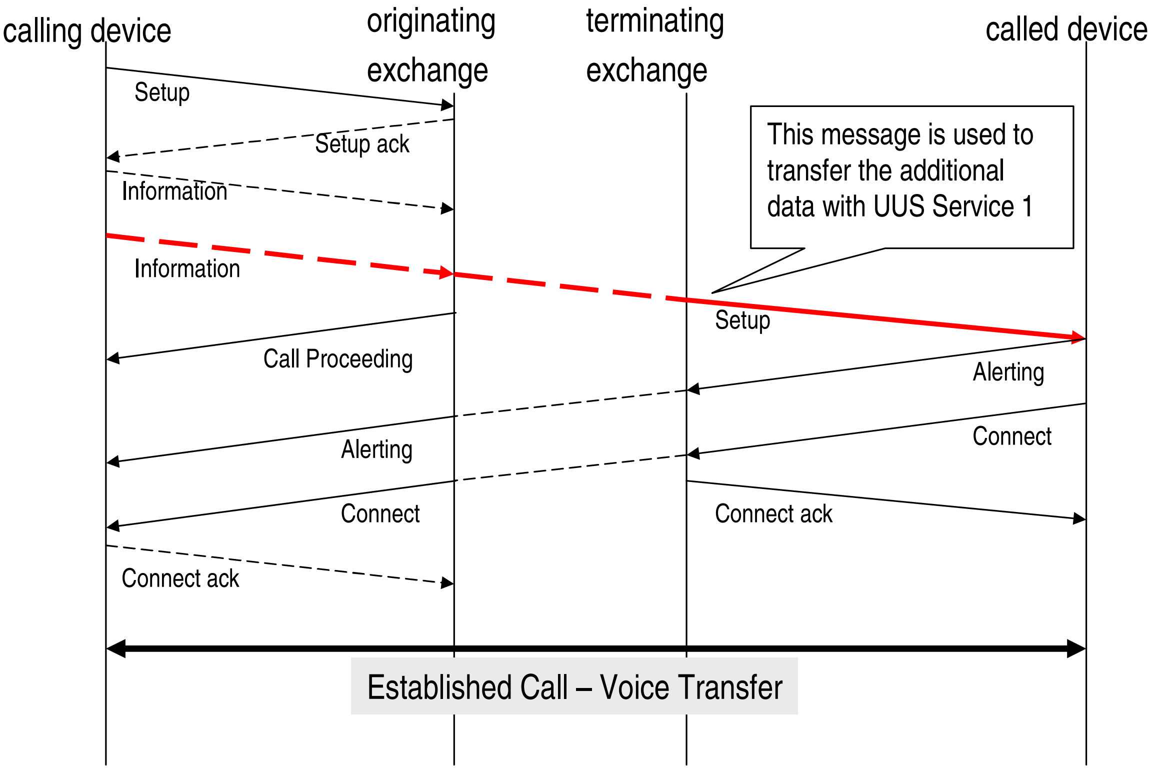


Figure 1: UUS information within call set up

3. Data to be transmitted within In-Vehicle E112 eCall data-string

The following information has been agreed within the eSafety Driving Group on eCall and endorsed by the Member States to be transmitted from the vehicle in case of a manual or automatically generated in-vehicle 112 call:

- Header
- Time stamp
- Precise location
- eCall qualifier
- Vehicle identification
- Service provider identifier

UUS supports 32 Byte of Data, but these "Bytes" are not really bytes but 7-bit characters.

32 7-Bit characters are equal to 224 Bit and 224 Bit are equal to 28 (real) "Bytes" (8-bit coded).

To code the information that are requested for an In-Vehicle E112 eCall we have 28 Bytes free. This must be formatted as 7-bit coded character string (32 characters) before sending the data in a UUS datagram. At the PSAP-site it must be decoded in the same way to get out the real information.

This set of fields is not a must. It is an example of how the relevant information could be coded in the 28 Bytes. At this setup 4 Bytes are free for extra use.

These 4 Bytes will be used to set the identifier (message header) at the beginning of the message.

The following figure shows the agreed optimized data set and how it fits with the E-merge data-string in comparison with In-Vehicle E112 eCall data-string:

		E-merge		**In-Vehicle E112 eCall**		
	Field	m/o	Length/Byte	m/o	Length/Bit	Length/Byte
Message Header	Message Header (for Telco)	m	24	m	14	4
	Message Header (for PSAP)	-	-	m	18	
Timestamp	Timestamp	m	4	m	16	2
Precise location	GPS current Pos	m	10	m	64	8
	GPS prior best	m	10	m	24	3
	GPS dead reck.	m	10	m	24	3
eCall qualifier	Sensors	m	2	m	8	1
	breakdown Source	m	2	-	-	-
Vehicle identification	Vehicle Data	m	40	m	40	5
	CLI	m	10	-	-	-
Service provider identifier	SP-IP	O	4	m	48	6
	SP Phone	O	12	-	-	-
	Satellite ID'S	m	3	-	-	-
	No of Sat	m	3	-	-	-

Length in total: **134 Bytes** **32 Bytes**

Legend:

GPS:	Global Positioning System
SP-IP:	Service provider IP-address
Satellite ID's:	Satellite identifier
No of Satellite:	number of satellites
CLI:	Call-Line-Identification-Number
m:	mandatory
o:	optional

Figure 2: Comparison E-merge data-string to In-Vehicle E112 eCall

Note: These 32 Bytes have to be reduced to 28 Byte; we're just looking for a solution!

3.1. Which data are relevant for In-Vehicle E112 eCall

3.1.1. Message Header

Message header is devided into 2 parts and values are estimations or proposals:

a) Message header for Telcos:
This header contains 14 Bit (2 characters in 7-Bit-format, which have to be developed) as a header for the Telco with content that an emergency call with UUS information is following. This header is fixed and will be always the same.
Regarding explanation in chapter 3 above, Telcos can interpret this 14 Bit message header without unpacking data.

b) Message header for PSAPs:
This part of the header contains 18 Bit (to fill message header up to 4 Byte) as a header for the PSAP. Content of the message is message type (emergency-call; 16 Bit) and information about emergency-type (automatic e-call, manual e-call, Good Samaritan call; 2 Bit).

In total this message header needs 4 Bytes instead of 24 Bytes in E-merge.

3.1.2. Timestamp

This timestamp is mandatory. However, it is not guaranteed that the device has the real time and by using UUS for additional data-transmission this transmission is real-time. If devices support GPS-time, it's possible to transmit this in a reduced format. So we only have to store the number of seconds in a part of the day, e.g the number of seconds in a quarter of the day. Result is use of 2 Bytes instead of 4 Bytes in E-merge. It is not possible that a UUS data-string will reach after the call is established and so this timestamp is only for synchronizing mechanisms.

3.1.3. Precise location

a) The first position is the actual position of the device/IVS. This is relative to a regional grid. It is not necessary to map the whole world for this kind of In-Vehicle E112 eCall as we only deal with pan-European eCalls.
In addition it is not necessary to store the position with a precision of millimetres. A range of 10 meters should be enough for each positioning system. This is more than ever valid because the precision of the GPS-satellites is not good enough to use a range smaller like this.
b) The 2nd and 3rd positions are relatively coded to the 1st one. So we don't need so much Byte to store the distance from the 1st position to the 2nd and the 3rd position.

Result is reducing location data from 30 Bytes to 14 Bytes.

3.1.4. E-Call qualifier

a) Sensors:
The sensors are reduced from 2 Byte to 1 Byte. Within this 1 Byte we can transmit how many sensors (max. 8) have been activated and if sequence is defined, which ones. If necessary than an extension to more Bytes is possible if there are some Bytes left.
b) Breakdown source:
This qualifier is left out because we're only talking about In-vehicle E112 e-Calls and not about breakdowns caused by e.g. damaged tires.

3.1.5. Vehicle identification

a) Vehicle data:
Currently 5 Bytes are needed for vehicle data.
Motorola and Telmacon on behalf of the eSafety Driving Group on eCall is currently looking to reduce these Bytes because maximum length of available data-string is 28/32 Bytes in total.

b) CLI:
Within In-vehicle E112 eCall it's not necessary to transmit CLI, because the system itself requires SIM-cards for used devices (for activation, user-registration, etc.). By using SIM-cards telcos automatically add CLI to emergency calls.

At this point of time the result of reducing vehicle identification data is from 50 Bytes to 5 Bytes.

3.1.6. Service provider identifier

a) Service provider IP-address:
To be future proved we should use IPv6 instead of IPv4; therefore we need 6 Bytes for service provider IP-address.

b) Service provider phone number:
Service provider phone-number is not necessary for In-vehicle E112 eCall.

This causes a data reduction from 16 Bytes to 6 Bytes.

3.1.7. Satellite ID's, NO of Sat

These data are not so important to identify the place and the ID of the satellites used for the GPS position.

Result is reducing data from 6 Bytes to 0 Bytes.

3.1.8. Total message size

The result of using this data-string structure as described is 32 Bytes. In comparison to the total space in the message there are 4 Bytes overload.

Note:
These 32 Bytes have to be reduced to 28 Byte; Motorola and Telmacon on behalf of the eSafety Driving Group on eCall are looking for a solution, based on some ideas, which have to be verified by the driving group. However, reaching the reduction seems realistic.

4. UUS-data filtering on PSAP-side

Below is seen an example of a PSAP architecture after introducing in-vehicle eCall over UUS. It is clear that individual Member States and suppliers of PSAP systems will introduce various ways to ensure that the date is decoded and visualised at the PSAP operators working stations.

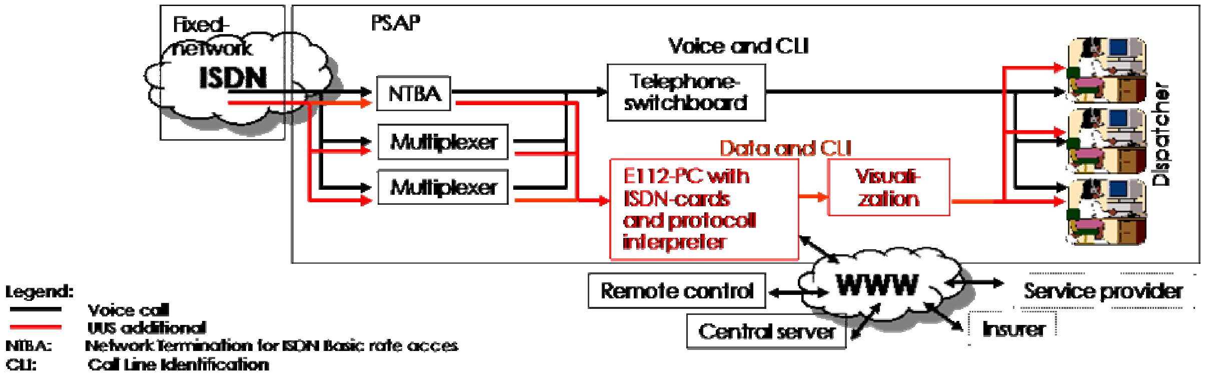


Figure 3: PSAP-diagram

In the above example the E112-PC is always sniffing the data stream for incoming calls and UUS-messages arriving from ISDN-network via NTBA or multiplexers.

PC separates emergency-data-strings into their different data fields and visualizes them with associated CLI on dispatcher screens.

5. Emergency set up with UUS

5.1. Description

Emergency set up is based on Technical Specification TS 24.008 V3.1.0 (1999-10) from 3rd Generation Partnership Project, which deals with UMTS, mobile radio interface layer 3 specification and core network protocol.

This setup message is sent from mobile station to the network to initiate emergency call establishment.

Current mobiles don`t support to add additional UUS-data to emergency call setup message and have to be modified. This however, is not crucial for the introduction of eCall as the eCall compliant system is targeted first at in-vehicle OEM fitted systems.
By developing and standardizing such a system we have to take care also for the after-market systems.
In case that nomad systems will be supplied then these have to comply to the agreed standard.

The User information message is sent by the mobile station to the network to transfer information to the remote user.

5.2. User information within UUS

This message is used if the User-to-User transfer is part of an allowed information transfer as defined in TS 24.010.

5.3. To do

It has to be verified, how much space for additional data transmission is available within the emergency call set-up.

If there's not enough space for the whole emergency data-string it's necessary to check the possibility to use the space to implement and transmit a special Bit, which is given in normal call set ups, as information for the networks that a second succeeding UUS data-string with the emergency data-string itself will be transmitted.

6. Requirements for the use of UUS

- In-vehicle GSM-devices have to support UUS 1 (and UUS 3); firmware changes on IVS-side.
- GSM-networks have to support UUS 1 (and UUS 3), because service is mostly blocked. To open the networks a subscription with all network providers is required (roaming)
- UUS-handover between GSM- and ISDN-networks has to be supported.
- ISDN-networks have to support UUS 1 (and UUS 3)
- ISDN multiplexers have to support UUS 1 (and UUS 3)
- ISDN-telephones have to support UUS 1 (and UUS 3); required AT-command is implemented in most of available ISDN-telephones because of some use cases within the telephone switchboards.
- Definition of AT- commands for UUS 3 is necessary (ETSI/EMTEL).

OCG EMTEL #8
Menthon St-Bernard, France
23-24 September 2004

EM08td035

LIAISON STATEMENT

Title: **Support of eCall on UUS type 1 Supplementary Service**

From:

Organisation: OCG EMTEL
Approval Date: 24 September 2004
Technical Contact: Ray Forbes (raymond.forbes@marconi.com)
Reply to: Ray Forbes (raymond.forbes@marconi.com)
Reply by (if required):

To:

Organisation: ETSI TISPAN, 3GPP TSG SA (SA1) & 3GPP TSG CN (CN1)
Contact Person: Steve Norreys/Michele Zarri/Hannu Hietalahti
e-mail: steve.norreys@bt.com / michele.zarri@t-mobile.co.uk

Attachements:

eCall MoU
eCall/eSafety-driving group letter from the CEC
eCall Detailed Statement of Requirement

For:

Action: ☒
Information: □

Action/Decision Requested:

ETSI OCG EMTEL has discussed the requirements for the support of pan-European in-vehicle eCall (Automatic & Manual), and the MoU for the support of eCall in the European Union. Resulting from the discussion ETSI EMTEL understands that it is required to support the conveyance of the minimal eCall data in the call-associated communication to the PSAP (Public Service Answering Point).

It was discussed that the ISDN Supplementary Service UUS type 1 may be sufficient to transport the required information. However, it was noted that an analysis of the detailed requirement, clear study of service description and the validation of the protocol capabilities have not yet been carried out. ETSI TISPAN being responsible for the ISDN Supplementary Services in the fixed network, and 3GPP being responsible for their support on the existing GSM networks.

The eCall/eSafety-driving group will provide, attached to this Liaison, the requirement definition. Based on this, the description and the validation of the protocol capabilities are required to be carried out.

This work is urgent and required to be completed by the end of January 2005; in line with the CEC MoU Agreement, attached. ETSI EMTEL requests confirmation of the starting and completion of this work.

Alternative solutions to fulfil this requirement may be feasible, and should be notified to the eCall/eSafety-driving group as the work progresses.

TSG-SA WG1 #27 **S1-050230**
Cape Town, South Africa, 17th to 21st January **Agenda Item:**

Title: Response to OCG EMTEL for Support of eCall on UUS type 1 Supplementary Service
Response to: LS S1-050019 (EM08td035) on "Support of eCall on UUS type 1 Supplementary Service"

Source: SA1
To: OCG EMTEL
Cc:

Contact Person:
Name: Holger Butscheidt
E-mail Address: **holger.butscheidt@regtp.de**

Attachments: None

1. Overall Description:

SA1 thanks OCG EMTEL for their LS in S1-050019 (EM08td035) and would like to inform EMTEL that SA1 have discussed the issue of using the ISDN supplementary service UUS type 1 to convey the user eCall data to the PSAP. Although SA1 believe that it may be possible to use the UUS in this case, SA1 would like to point out that there may be possible fraud implication with using the UUS. SA1 is also working with CN1 to investigate the use of UUS for the purpose of this use case.

Also, SA1 have the clarification questions regarding the eCall data:

- What would be the amount of data?
- Is this information static?
- Where would this data be stored (e.g., SIM/USIM/ISIM)?

2. Actions:

SA1 kindly requests EMTEL to provide the above requested information on the eCall data requirements.

3. Date of Next TSG-SA1 Meetings:

SA1#28 4 – 8 April 2005 Beijing, China

E-MERGE

D3.0
Specifications of the European in-vehicle emergency call

WP3

Version 1.5

17.06.2003

Produced by:
telmacon GmbH

E-MERGE is co-financed by the
European Commission DG Information Society

Programme name:	Information Society Technologies (IST)
Project ID:	IST-2001-34061
Project acronym:	E-MERGE
Project name:	Pan-European Harmonisation of Vehicle Emergency call Service Chain
Dissemination level[1]:	Public

Deliverable number:	D 3.0
Contractual date of delivery:	**25 December 2002**
Actual date of delivery:	**17 June 2003**
Title of deliverable:	**Specification of the European in-vehicle emergency call**
Work package:	WP 3
Nature of the deliverable:	Public
Author(s):	Gerhard Wolfien –telmacon Stefan Derolf - SOS Alarm Mats Orblom - Volvo Technological Development Alessandro Murro - MIZAR Automazione SpA Andy Rooke & Jim Hammond - ACPO ITS Dr. Wolfgang Reinhardt - OnStar Europe
Project co-ordinator:	Michael Nielsen (ERTICO) Tel: +32 2 400 07 49, fax: +32 2 400 07 01 E-mail: m.nielsen@mail.ertico.com

Abstract: This document “Specification of the European in-vehicle emergency call” describes all processes, minimum requirements, data and their transmission, protocols for all involved parties within an in-vehicle emergency call. This document ist the basic for all further activities in the project E-MERGE and shows a recommendation for an European wide realisation regarding to the present available technology as well as knowing laws and regulations.

[1] This is either: Public, restricted to other programme participants, restricted to a group specified by the consortium, confidential – Information about dissemination level can be obtained in 9.5 of the Technical Annex.

Document Control Sheet

Electronic reference: Specifications of the European In Vehicle Emergency Call Vers1.3.doc

Main author(s) or editor(s): Gerhard Wolfien - telmacon
Stefan Derolf - SOS Alarm
Mats Orblom - Volvo Technological Development
Alessandro Murro - MIZAR Automazione SpA
Andy Rooke & Jim Hammond - ACPO ITS
Dr. Wolfgang Reinhardt - OnStar Europe

Version history:

Version number	Date	Main author	Summary of changes
1.0	11/02/03	Gerhard Wolfien	First (based on the meeting in Utrecht)
1.1	25/02/03	Gerhard Wolfien	Second draft version based on input from partners
1.2	29/04/03	Gerhard Wolfien	Final draft version based on elaboration on comments
1.3	01/05/03	Gerhard Wolfien	Final version
1.4	12/06/03	Gerhard Wolfien	Final version after discussions with ETSI
1.5	17/06/03	Gerhard Wolfien	Final edited version

Approval:

	Name	Date
Prepared	Gerhard Wolfien	*25/02/03*
Reviewed	Stefan Derolf Mats Orblöm Alessandro Murro Andy Rooky & Jim Hammond Dr. Wolfgang Reinhardt	*11.2.03 – June 03*
Authorised	Michael Nielsen	*18.06.03*

Circulation:

Recipient	Date of submission
WP 3 participants	Final draft version 11.2.03
Consortium	Final draft version 11.2.03
Co-ordinator	Elaborated Final draft version 17.6.03
EC	18 June 03

9.9 Legal Issues........ 136

Annexes:

A: IPSec Specification
B: Database and database queries SQL / XML
C: Provisioning of Mobile Network Location - other solutions

1. EXECUTIVE SUMMARY

The report covering the results from WP 3 “Specifications of the European in-vehicle emergency call” describe a technical, functional and organisational solution of a pan European handling of a telematics based emergency call from the vehicle. The report covers a common system specification and communication protocol definition together with operational procedures and the architecture of the vehicle e-call system.

It is the view of the E-MERGE consortium that this solution is realisable on a pan-European scale only during the coming years, as the selected solution depends on the planning and realisation of the European Commission initialised E-112 initiative and thus the adoption of the ETSI/EMTEL protocol by the telecom operators and thus providing the possibility for the PSAPs to receive location information. Furthermore, the Telematics Forum standard for a global telematics protocol, which had been used in the E-MERGE concept for transmission of the vehicle data to the PSAPs and the service providers, is still to be adopted by the automotive world and implemented widely.

Nevertheless, the selected architecture and protocols provide at the time of submission of this report in the view of the E-MERGE consortiums the best basis for the adoption of a pan-European solution for in-vehicle e-calls.

The here described solution gives all involved partners the possibility to implement processes and operations of E-MERGE by interim solutions and applications. An issue for the success of the selected approach is the organisations of PSAPs locally or nation wide as the PSAPs need to be equipped to receive not only the location information but as well the “minimum set” of vehicle data, which will be made available for the PSAPs by use of E112 via the push of the minimum set of data directly to the PSAPs as data in the 112 voice call. Regulations to support this are necessary and should be defined and regulated within the EC.

The E-MERGE consortium finds that the selected approach supports strongly the realisation of the pan-European e-call available for all. In addition the selected approach supports a general opening of the telematics market and the realisation demonstrates a basic platform for additional future services and solutions.

This WP 3 Specifications of the European in-vehicle emergency call final document is dated at 17 June 2003. Information, technical changes and standards, which become known after this date, are not included anymore in this report but will naturally be taken into account in the development work within the E-MERGE project.

2. INTRODUCTION

The report D 3.0 Specification of the European in vehicle emergency call, describes the minimum recommendations for the handling of an in-vehicle emergency call of all involved parties regarding the realisation. The report covers a common system specification and communication protocol definition together with operational procedures and the architecture of the vehicle e-call system.

2.1 Background and starting point

A starting point for this work has been the state of the art and user requirement study of WP2. This input was used to derive features, technological requirements and the scenario of use from which a common architecture was defined. The work led to a general functional specification – detailing the way the vehicle emergency call chain works. The message structures and procedures and operational issues and requirements are listed. Furthermore, data security and privacy has been dealt with and it is specified how the handling of personal data occur.

This report covers:

- Recommendations for minimum technical requirements of the on-board units are outlined
- Technical requirements for the central systems are specified
- One common E-MERGE Data model is specified
- Common Message sets/formats and Exchange formats are specified
- Standardised interfaces along the E-call chain are specified
- HMI recommendations are given
- Defined communication bearer – and a technology is selected and the architecture defined
- Interoperability requirements and specifications are determined.
- A minimum standard for Quality service level is specified
- The procedure when false alarms are received is specified.
- Recommendations of common procedures for E-call service centres are specified.

The output from this report will be used in a description of the site-specific architecture at the various countries developing and testing the E-MERGE concept. The site specific architecture description follows as widely as possible the overall E-MERGE architecture, specification and definition as defined and will include:

- Mission (and Vision) of the application
- List of user needs and system requirements
- Functional architecture
- Information architecture
- Communication architecture
- Physical architecture
- Organisational architecture

In addition the relation with the overall nation-wide architecture for emergency call handling will be highlighted. The result of this task is the collection and description of the key elements that emerged as commonly necessary to implement successfully and effectively the vehicle E-call services, plus those recognised as enabling the interoperability.

The specification secure that the E-MERGE system is future proof in relation to technical performance.
All user needs from WP2 and the following defined requirements, which are discussed and adopted united, are documented, insofar they are possible from technical, organisational and process orientated illustration and feasibility.

2.2 Objectives of the specification work package

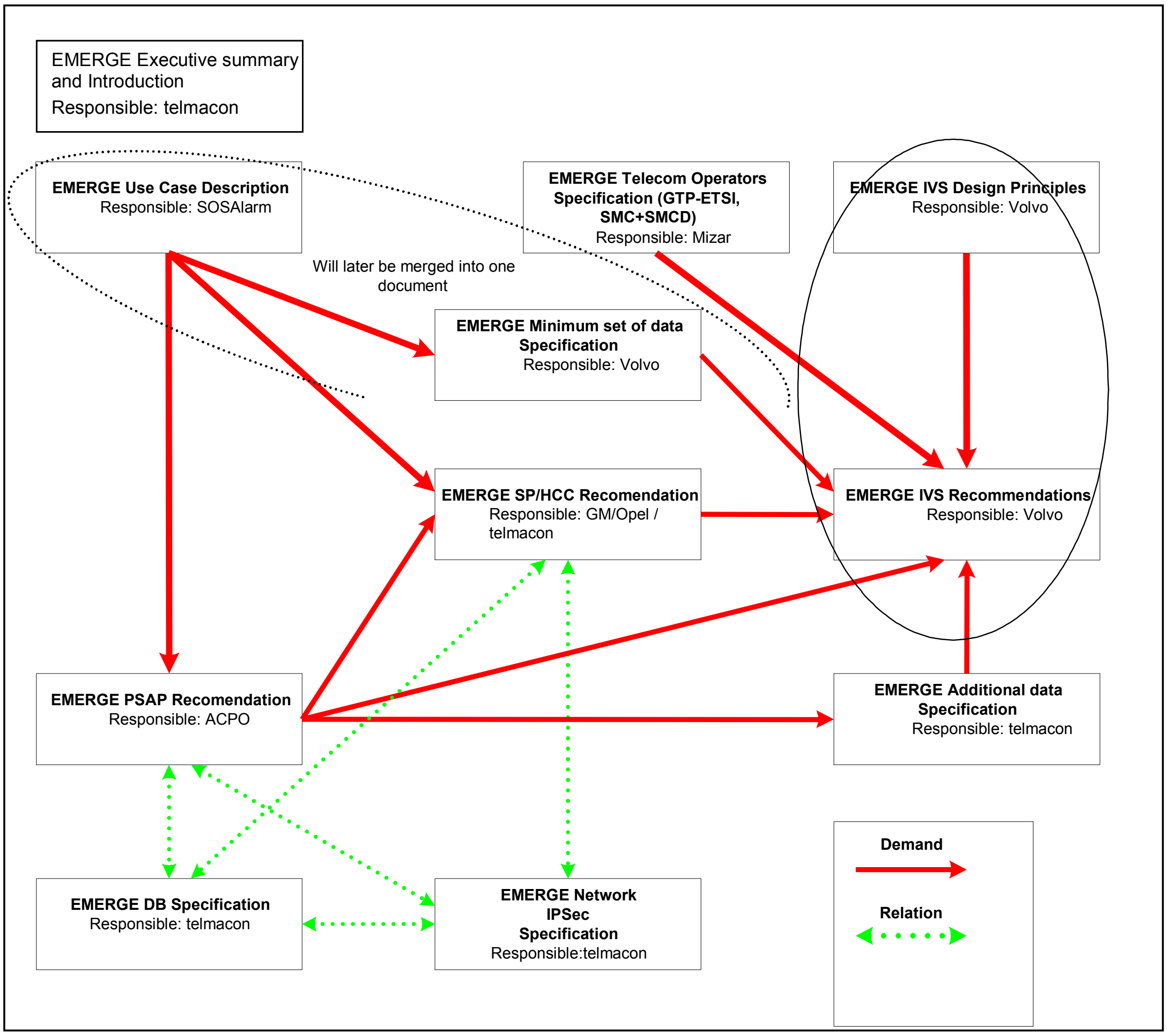

EMERGE Executive summary and Introduction
Responsible: telmacon
EMERGE Use Case Description
Responsible: SOSAlarm
EMERGE Telecom Operators Specification (GTP-ETSI, SMC+SMCD)
Responsible: Mizar
EMERGE IVS Design Principles
Responsible: Volvo
Will later be merged into one document
EMERGE Minimum set of data Specification
Responsible: Volvo
EMERGE SP/HCC Recomendation
Responsible: GM/Opel / telmacon
EMERGE IVS Recommendations
Responsible: Volvo
EMERGE PSAP Recomendation
Responsible: ACPO
EMERGE Additional data Specification
Responsible: telmacon
EMERGE DB Specification
Responsible: telmacon
EMERGE Network IPSec Specification
Responsible:telmacon
Demand
Relation

Figure 1: Overview of WP3 objectives

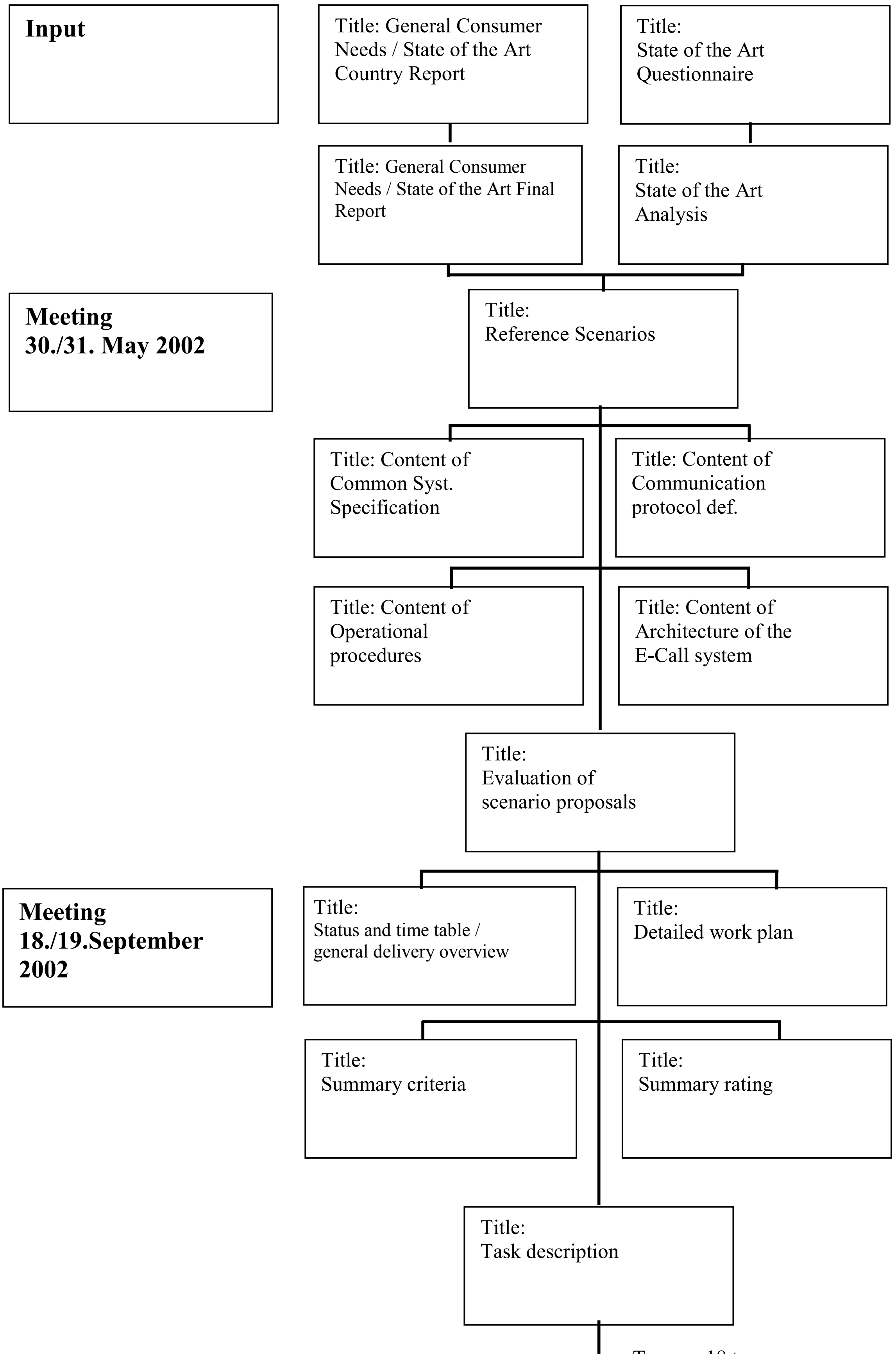
2.3 Description of the work

Based on the project definition, the E-MERGE project partners have gone through different phases of intensive discussions to reach a number of conclusions on the E-MERGE specifications. During the discussions, the partners took into account varying needs and wishes of the involved E-MERGE partners, as well as country-specific regularisations and laws. Existing solutions and technologies have been considered, as well as possible realisation periods depending on the required capital.

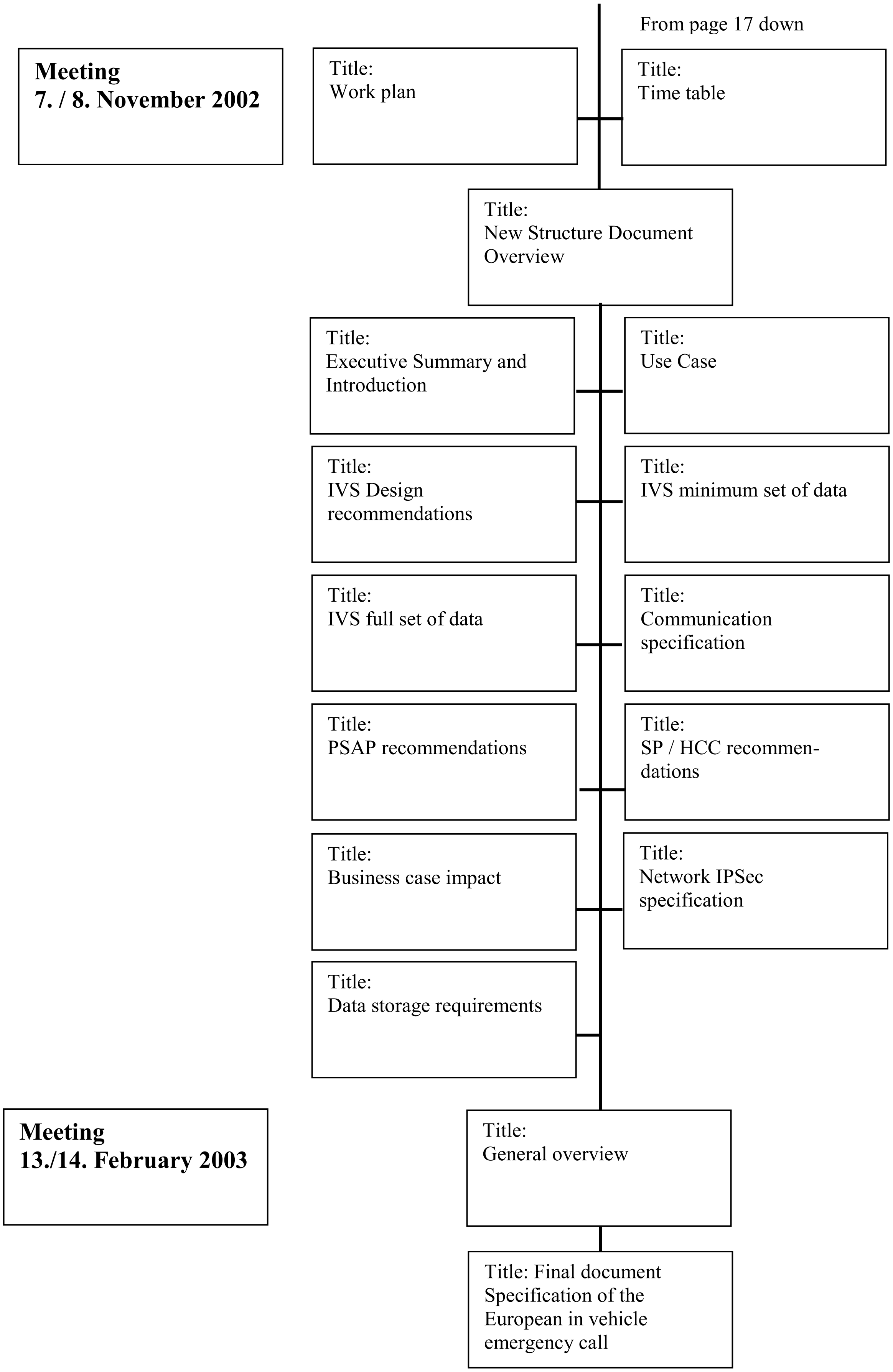
The core of this solution is:

- The integration of existing projects and standards
- The use of one IVS protocol only
- A minimum E-call function specification for IVS systems
- The availability of a minimum set of in-vehicle data, which is being send directly to the PSAP
- Time- and process-optimised procedures
- Data protection of personal data
- The Minimisation of false alarm and abuse occurrences
- A cost-optimised realisation of a pan-European data exchange between the service providers and PSAPs for additional value added data, which can be provided in case of a incident
- Solving the language problem
- Optimisation of the data exchange between PSAP and SP
- Definition of the different possibilities of an E-call and the different processes.

2.4 System Specification Document Overview


Input
Title: General Consumer Needs / State of the Art Country Report
Title: State of the Art Questionnaire
Title: General Consumer Needs / State of the Art Final Report
Title: State of the Art Analysis
Meeting 30./31. May 2002
Title: Reference Scenarios
Title: Content of Common Syst. Specification
Title: Content of Communication protocol def.
Title: Content of Operational procedures
Title: Content of Architecture of the E-Call system
Title: Evaluation of scenario proposals
Meeting 18./19.September 2002
Title: Status and time table / general delivery overview
Title: Detailed work plan
Title: Summary criteria
Title: Summary rating
Title: Task description

To page 18 top


From page 17 down
Meeting 7. / 8. November 2002
Title: Work plan
Title: Time table
Title: New Structure Document Overview
Title: Executive Summary and Introduction
Title: Use Case
Title: IVS Design recommendations
Title: IVS minimum set of data
Title: IVS full set of data
Title: Communication specification
Title: PSAP recommendations
Title: SP / HCC recommen-dations
Title: Business case impact
Title: Network IPSec specification
Title: Data storage requirements
Meeting 13./14. February 2003
Title: General overview
Title: Final document Specification of the European in vehicle emergency call

2.5 Structure of the report

This report is structured under the premise of a logical and technical process. The basis is the E-MERGE architecture, which is adopted by all E-MERGE partners as well as the different dependencies and paths of information within an E-MERGE event such as an E-call.

Chapter 1: E-MERGE Executive Summary

Chapter 2: E-MERGE Introduction

Chapter 3: E-MERGE Architecture

Chapter 4: E-MERGE Use Case

Chapter 5: E-MERGE In-Vehicle-System Design Recommendations

Chapter 6: E-MERGE Specification of IVS data (minimum set of data) to be forwarded to PSAP in case of an e-call

Chapter 7: E-MERGE Specification of IVS data (full set of data) to be forwarded to service providers / HCC in case of an e-call

Chapter 8: E-MERGE Communication Specification

Chapter 9: E-MERGE PSAP requirements

Chapter 10: E-MERGE Service Provider Recommendation

Chapter 11: E-MERGE Business case impact

Chapter 12: E-MERGE Network security

Chapter 13: E-MERGE Data storage requirements

Most interesting for:

Chapter	Car manufacturer	PSAP	SP	Telco's
1	X	X	X	X
2	X	X	X	X
3	X	X	X	X
4	X	X	X	
5	X			X
6	X	X	X	
7	X		X	X
8		X	X	X
9		X	X	
10		X	X	
11	X		X	
12		X	X	X
13		X	X	

2.6 List of abbreviations

3GPP – 3rd Generation Partnership Project

A

Ack - Acknowledge
ACP - Application Communication Protocol
ADAS - Advanced Driver Assistance System
A-GPS - Assisted Global Positioning System
AMPS - Advanced Mobile Phone System
ASCII - American Standard Code for Information Interchange
ASN.1 - Abstract Syntax Notation number One: is an international standard that aims at specifying data used in communication protocols. It is a powerful and complex language: its features are designed to describe accurately and efficiently communications between homogeneous or heterogeneous systems
ASTAP - Asia-Pacific Standardisation Program

B

C

CGALIES - Coordination Group on Access to Location Information by Emergency Services
CLI -Customer Line Identification
CRUD - Create Read Update Delete
CSD – central securities depository

D

DB - Database
DBMS - Database Management System
DIS - Draft International Standard
DMZ - Demilitarised Zone
DoS - Denial of Service
DSRC - Dedicated Short Range Communication

E

E112 - An emergency call to the number 112, including best effort location information make available by the network providers
EA - Emergency Authorities
EC - European Commission
E-call - Emergency call
EMC - Electromagnetic Compatibility
E-MERGE - name of the European emergency call standardisation project
E-OTD – Enhanced Observed Time Difference positioning method
eMLPP - enhanced Multi-Level Precedence and Pre-emption
ETSI OCG-EMTEL - European Telecommunications Standards Institute Operational Coordination Group on Emergency Telecommunications

ETSI EG – ETSI Guide
ETSI ES – ETSI Standard
ETSI TS – Technical specification
ETSI TR – Technical report
EU – European Union

F

G
GAD - Geographical Area Description
GATS - Global Automotive Telematics Standard
GMLC - Gateway Mobile Location Centre
GPRS - General Packet Radio Service
GPS - Global Positioning System
GSM - Global System for Mobiles
GTP - Global Telematics Protocol
GTSC - Global Telematics Standards Collaboration

H
HCC - Home Call Centre, the call centre or service provider to whom the driver has signed a contract.
HI - Health Insurance
HMI - Human Machine Interface
HTTP - HyperText Transfer Protocol

I
ID - Identification
IE - Information Element
IEEE - Institute of Electrical and Electronics Engineers
IETF - Internet Engineering Task Force
IMEI - International Mobile Equipment Identifier
IP - Internet-Protocol
IPSec - Internet Protocol Security
IPv4 - IP-Addresses 4 x 16 bit = 64 bit
IPv6 - IP-Addresses 8 x 16 bit = 128 bit
ISDN - Integrated Services Digital Network
ISO - International Organization for Standardisation
ITS - Intelligent Transport Systems
ITU – International Telecommunication Union
IVS – In-Vehicle System (on-board unit)

J
JDBC - Java Database Connectivity

K

L

LCC - Local Call Centre, a call centre that the HCC potentially would make a pan-European agreement with in order to better provide a European coverage.
LCS - Location Services
LDAP - Lightweight Directory Access Protocol
LIF - Location Interoperability Forum
LMU - Location Measurement Unit

M

min - minimum
MLC – Mobile Location information Centre
MLP (Lite) - Mobile Location Protocol
MSC - Mobile Switching Centre

N

NIS+ -.Network Information Service Plus

O

ODBC - Open Database Connectivity
OEM - Original Equipment Manufacturer
OSI - Open System Interconnection
OTAP - Over The Air Protocol

P

PKI - Public Key Infrastructure
PLMN - Public Land Mobile Network
PSAP - Public Safety Answering Point

Q

QoS - Quality of Service

R

RDBMS - Relational Database Management System
RFC - Request For Comments
RSA - Public key encryption technology developed by RSA Data Security

S

SDO - Standards Developing Organisation
SES Satellite Earth Stations and Systems
SIM – subscriber identity module

SMLC - Serving Mobile Location Centre
SMS - Short Message Service
SP – Service Provider
SO - Support Organization
SOAP - Simple Object Access Protocol
SPAN – Services and Protocols for Advanced Networks
SQL – structured query language
SW - Software

T
T1 - Committee T1-Telecommunications
TETRA – Terrestrial Trunked Radio
TIA – Telecommunications Industry Association
TICS - Traffic Information Control System
TIPHON – Telecommunications and Internet Protocol Harmonisation Over Networks
TCP - Transmission Control Protocol
TSAG - Telecommunication Standardisation Advisory Group

U
UK – United Kingdom
UMTS - Universal Mobile Telecommunications System
UTC - Coordinated Universal Time
UTM - Universal Transverse Mercator

V
VIN - Vehicle Identification Number
VPN - Virtual Private Network

W
WCDMA
WG – work group
WGS - World Geodetic System
WLAN - Wireless Local Area Network
WP - Work Package

X
XML - eXtensible Markup Language

2.7 Reference documents

General web-based sources – CGALIES

1. ISO 4513 Road vehicles — Visibility Method for establishment of ellipse for driver's eye location
2. ISO 2575 Road vehicles — Symbols for controls, indicators and tell-tales
3. ISO 4040 Road vehicles — Location of hand controls, indicators and tell-tales
4. ISO 3958 Road vehicles — Passenger car driver hand control reach
5. ISO (DIS) 15005 Road vehicles — Traffic information and control systems (TICS) dialogue management principles
6. ISO (DIS) 15006 Road vehicles — Traffic information and control systems (TICS) auditory presentation of information
7. ISO (DIS) 15008 Road vehicles — Traffic information and control systems (TICS) ergonomic aspects of in-vehicle information presentation
8. ISO (DIS) 11429 Ergonomics — System danger and non-danger signals with sounds and lights.

[1] URL : http://www.telematicsforum.com

[2] Telematics Forum – GTP (Global Telematics Protocol) « *Requirements* » Version 1.0, 22nd October 2002

[3] Telematics Forum – GTP (Global Telematics Protocol) « *GTP Application Protocol – Encoding Specification* » Version 1.0, 21st March 2003

[4] URL : http://www.emtel.etsi.org

[5] Hutchison 3G UK Ltd – « *LIF MLP Lite 112/999* » Version 1.0, 9th September 2002

[6] ETSI OCG-EMTEL – « *EM02td003 – Emergency Communication by Citizens with Authorities* » Version 0.1, 10th January 2003

[7] ETSI OCG-EMTEL - – « *EM02td022 - Location of Emergency 122 mobile calls in Spain* » Version 0.1, 15th January 2003

[8] MESA – Statement of requirements

[9] PNO – ISC / SPEC Specification number 013 emergency location

[10] Network Design for 999 GPS

[11] MQ Interface detail

Printed sources:

1. Huitema, C., IPv6: The New Internet Protocol, 2nd ed. Upper Saddle River: Prentice Hall, Inc., 1998.

2. Pfleeger, C.P., Security in Computing, 2nd ed. Upper Saddle River: Prentice Hall, Inc., 1997.

3. Storebø, G., Virtual Private Networks. (Spring project, Norwegian University of Science and Technology, 1998).

Web based sources:

1. Masica, K., Securing IP. SunWorld, June 1998. http://www.sunworld.com/swol-06-1998/swol-06-ipsec.html

2. Salomone, S., VPN: The Basics. InternetWeek, http://www.internetwk.com/VPN/paper.htm

3. RSA, http://www.rsasecurity.com/rsalabs/faq/3-6-1.html

4. Krawczyk, H., SKEME: A Versatile Secure Key Exchange Mechanism for Internet, from IEEE Proceedings of the 1996 Symposium on Network and Distributed Systems Security. http://www.research.ibm.com/security/skeme.ps

5. www.sql.org – The portal for SQL
6. www.xml.org – The portal for XML
7. http://www.w3c.org/ - The portal for Web services

3. E-MERGE ARCHITECTURE

The goal of the E-MERGE project is to define a common pan-European in-vehicle Emergency call infrastructure and protocol. Such a protocol will allow vehicle emergency situations to be dealt with in the same, efficient manner across the European Union. This chapter will clarify how the E-MERGE e-call infrastructure is set up, and how the different participants in the e-call procedure will communicate with each other.

Firstly, the current provisions for an emergency response to a vehicle call are outlined in order to obtain an understanding of how the European 112 call, and the E112 system works. Next, the chapter goes into how these current provisions can be expanded to cover every entity potentially involved in a road accident: These entities include.

- The vehicle and its occupants
- A Public Safety Answering Point (PSAP)
- A service provider to whom the vehicle owner has a contract with
- The Emergency Authorities/Stage 2 PSAPs/dispatchers like the police force, ambulance services, fire departments etc.

3.1 Normal 112 Call from a Vehicle using a portable phone

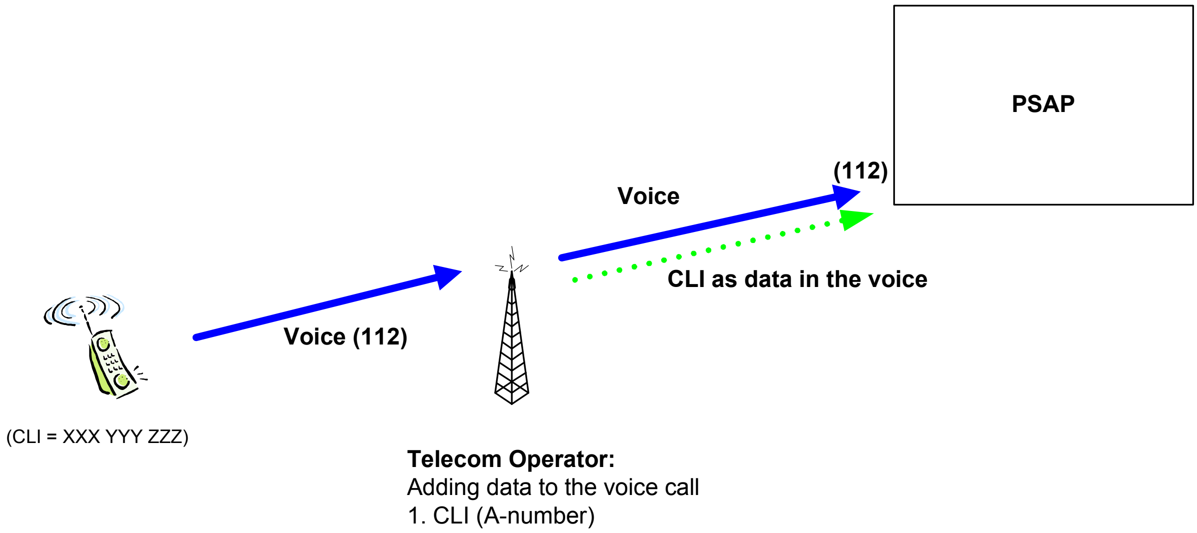


Figure 2: The driver calls 112 using the portable GSM phone

When a vehicle driver requires assistance in an emergency situation he can make a call using either the portable or fixed mobile phone to the 112 number. 112 are European emergency call number as agreed in the CGALIES initiative. This number is or will be in function across Europe. When the telecom operator detects a call to 112, it is technically possible for the operator to add the caller's line identity number (CLI) as data to the voice connection, and forwards the call to a Public Safety Answering Point (PSAP). The PSAP is a central handling point for receiving emergency calls, and notifying the Emergency Authorities or dispatchers.

3.2 A normal E-112 call using a portable phone with GSM location data

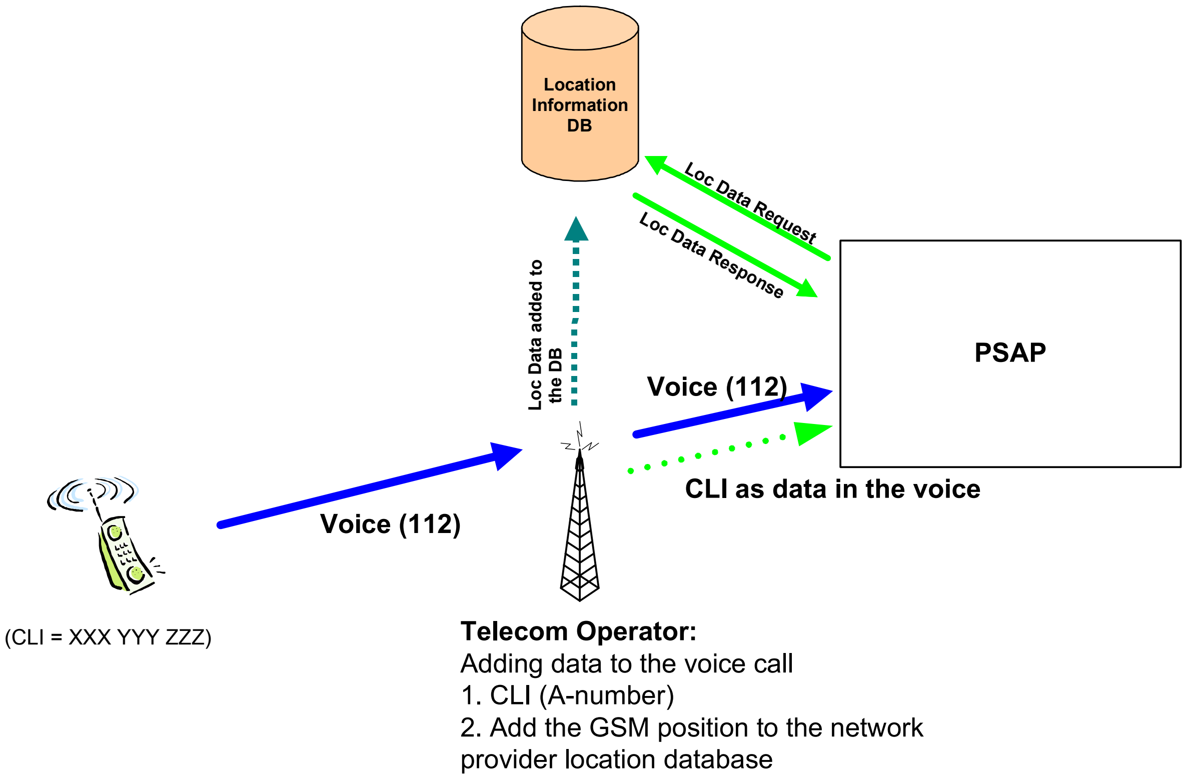


Figure 3: A 112 Call combined with CGALIES

The newly adopted E112 structure makes it possible to be able to quickly deploy the emergency services to the place of the accident, as the PSAP knows the current location of the driver involved. From July 2003 the E112 arrangements, will be a requirement under a European directive for the telecom operator to provide to the PSAPs by use of the best effort principle, GSM location (e.g. triangulation) information in addition to the CLI.

3.3 The E-MERGE E-call Infrastructure

The solutions discussed in the sections above already go a long way in facilitating emergency assistance. The E112 call can significantly speed up and improve incident handling but the handling of road incidents could be highly improved via a combination of E112 and in-vehicle e-calls, provided that a European standard protocol process, handling and service chain is available.
Specifically, the emergency assistance facilities can benefit greatly from e.g. an improved location information and information about the severity of the incident. The availability of the GPS positioning system and from advances in the field of in-vehicle hardware technologies can greatly contribute to this.
As the E-MERGE architecture build on the usage of E112 the co-operation with ETSI who specify how the network providers provide location information to the PSAPs has been extremely important. The co-operation between ETSI and E-MERGE has only in the last phase of the specification made it possible to more precisely define the E-MERGE

architecture. The starting point were the below architecture where the interrelationship between the actors can be seen and the at the time expected relationships were presented:

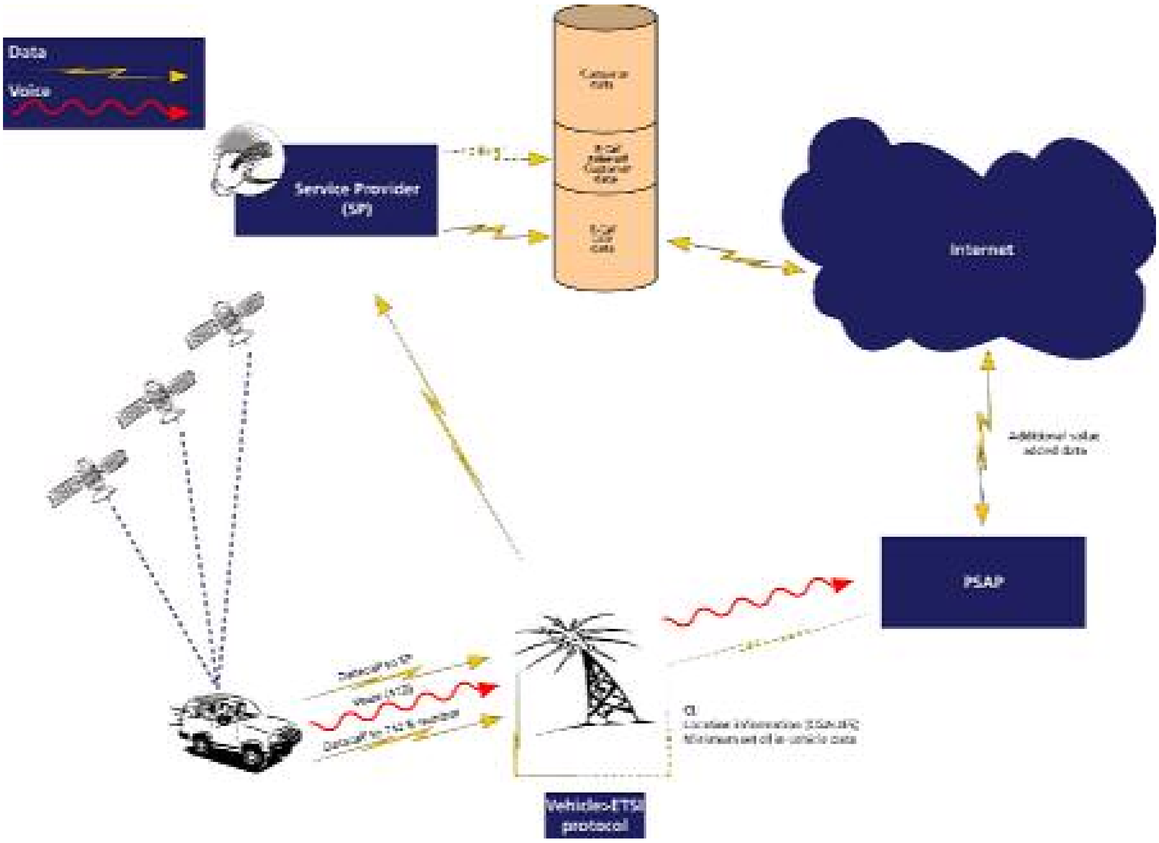


Figure 4: E-MERGE architecture as a staring point based on the E112 infrastructure

In the next sections, the E-MERGE protocol architecture will be introduced via the different players who have a role to play in the in-vehicle e-call architecture, and explaining how they interact. Finally an overview of the final solution, which is recommended, will be presented.

3.3.1 The Vehicle

Vehicle to the PSAP

The E-MERGE infrastructure consist firstly of, an In-Vehicle System (IVS), which is built into the vehicle with the aim to manually or automatically call 112 and provide the minimum required data to the PSAPs as fast as possible and thus give an optimum incident response. The IVS is an embedded computer device designed specifically for the in-vehicle environment. Among other features, the IVS should have the capability to receive GPS signals. The vehicle is also equipped with several sensors, each monitoring the condition of a vehicle part. The GSM communication model as hands free set is equipped with external microphone and loudspeaker. The IVS listens to the sensors, and will send a data message to the PSAP, when it detects that a minimum of two sensors has been activated, which is used together with specific limits (e.g. de-acceleration equals) to determine that an incident has occurred.

When an incident has occurred the various messages will be sent via a common vehicle protocol to be agreed on by the automobile manufactures. Within E-MERGE the developments and testing will be done using the Global Telematic Protocol, which is a Telematics Forum development and consist of a merger of GATS and ACP.

As will be explained in more details in chapter 8 the E112 solution being currently specified by ETSI has made it difficult for E-MERGE to define one single solution at the moment. However, two potential solutions has been established of which the latter is the one recommended by the E-MERGE consortium as also further explained within chapter 8.

3.3.1.1 Potential solution

The first potential solution involve a service provider, which has the role of receiving the minimum set of data and make this available in a specific database for the network providers to pull this based on the CLI. The architecture specified below shows a potential interim solution and not the optimised transmission way between IVS and PSAP.

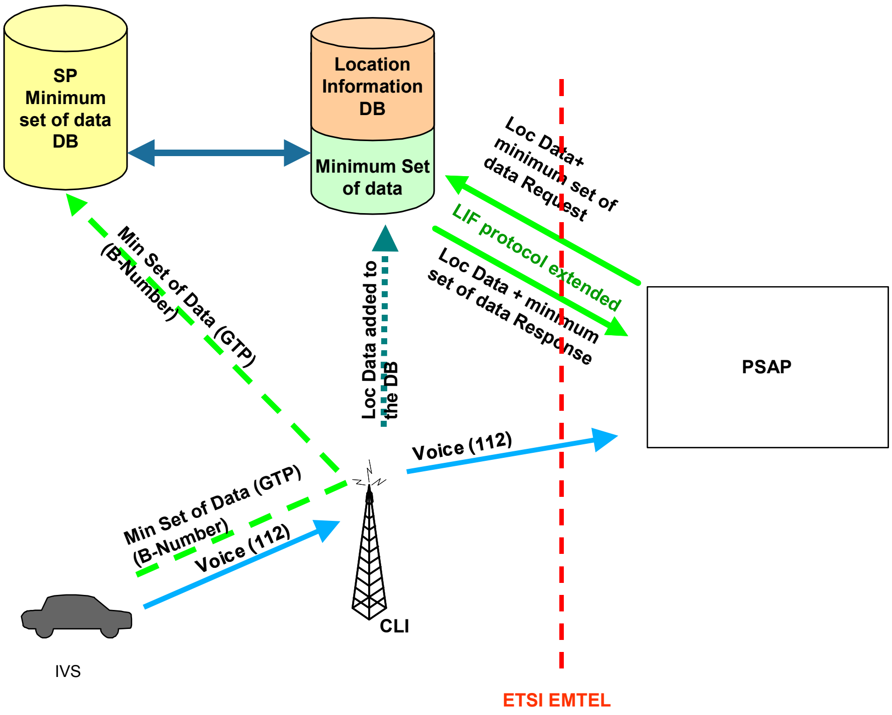

SP Minimum set of data DB
Location Information DB
Minimum Set of data
Loc Data+ minimum set of data Request
LIF protocol extended
Loc Data + minimum set of data Response
Min Set of Data (GTP) (B-Number)
Loc Data added to the DB
PSAP
Voice (112)
Min Set of Data (GTP) (B-Number)
Voice (112)
CLI
IVS
ETSI EMTEL

Figure 5: A potential vehicle PSAP link in a transition period

Workflow:

1. the IVS generates a 112 voice call and a data call with the minimum set of data (GTP) to a private SP number as indicated by the vehicle manufactures (this number should follow the vehicle brand and work even if the driver do not have a subscription to a SP);

2. the mobile operator handles the 112 voice call, forwards it to the PSAP together with the CLI and route the data call in a second communication way (minimum set of data) to the SP;
3. the mobile operator adds GSM location data of the 112 voice call in the server DB, hosted by the telco location server; the SP receives the data call (minimum set of data) together with the CLI, interprets the GTP data call and put the minimum set of data in the SP DB;
5. if a service contract with the customer exists, the IP address and the telephone number of the SP are enclosed as information in the minimum set of data.
6. the network providers location server pull the minimum set of data from SP DB via a search for the CLI at all vehicle manufactures SPs DBs;
7. the PSAP receives the 112 voice call together with the CLI and receive the location information and minimum set of data from the network provider location server according to the ETSI/EMTEL specification (pull or push) in relation to E112;
8. the location server send location data + minimum set of data response to the PSAP according to the ETSI/EMTEL specification.

3.3.1.2 Recommended solution

On the basis of discussion with ETSI a recommended architecture for the in-vehicle e-call system can be illustrated. This architecture will as far as possible be developed and tested by the E-MERGE consortium. The aim on the side of E-MERGE is to transmit in an optimal timed way the data from the IVS by utilisation of a communication way to a PSAP operator work place. In the range of intensive project discussions with ETSI, as well as partners of ETSI during May 2003, different transmission ways of data in the voice channel has been identified, which are explained in chapter 8.

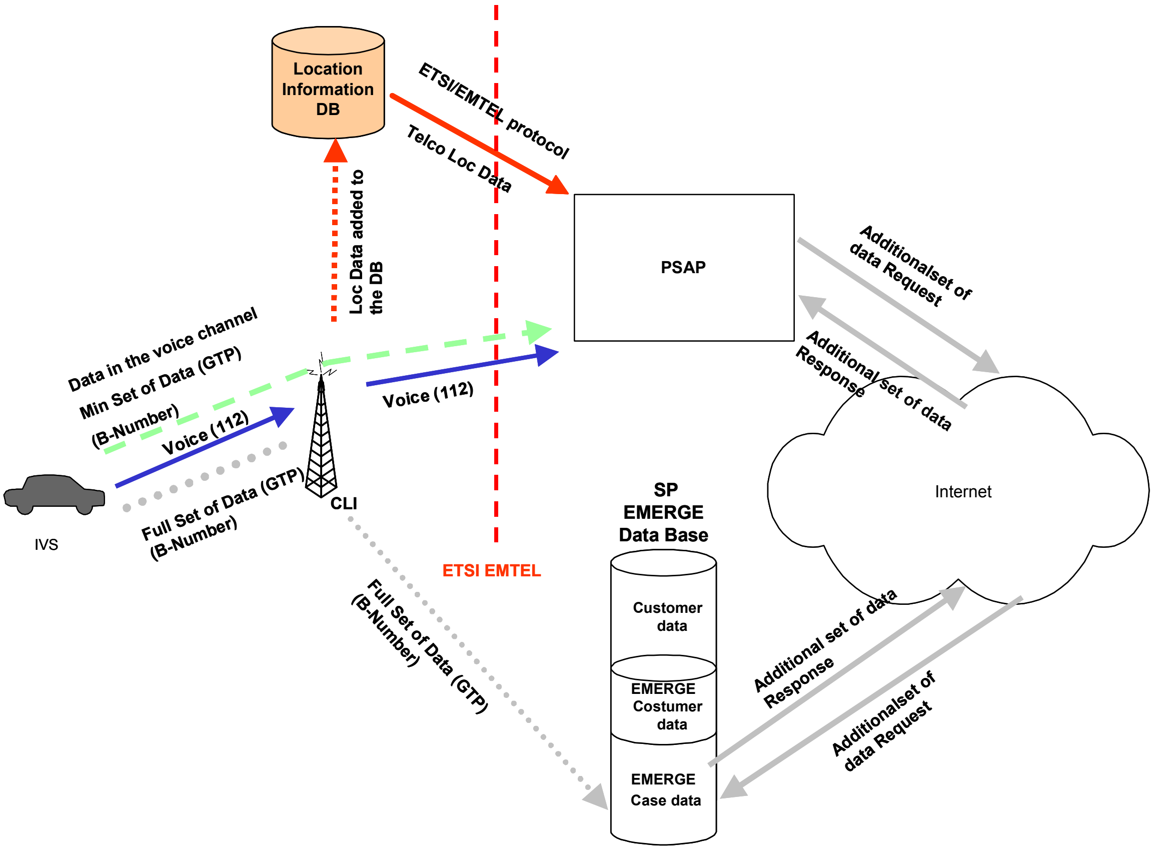


Figure 6: The recommended vehicle PSAP link

Workflow:

1. The IVS, the generating agent of the E-Merge call, sends the emergency call to a PSAP via voice channel, decomposed on two separate steps: the first one regards the data sending GSM / GPRS / UMTS technologies on a voice channel, whilst the second one is a pure 112 voice communication that uses the already opened voice channel. The data part of the call encloses the minimum set of data defined by the E-Merge project in the GTP protocol as a GTP E-Call Application. Data sending before a normal voice communication is established ensure the coverage also for those cases when the driver is not able to speak or the emergency call has been generated automatically by triggering the in-vehicle sensors.

2. The E-Merge call (data + voice) goes through the mobile network and is first handled by the TELECOM operator. The TELECOM Operator recognises that the call is an emergency call (voice + data). The TELECOM operator has the responsibility to enrich the call with the CLI (Caller Line Identification). At the same time the TELECOM operator has the duty to add the mobile location at a best effort principle into the Location Server Database. After the emergency call handling, the TELECOM Operator delivers the E-Merge call to the appropriate PSAP via the fixed line network.

3. The PSAP receives two different type of communication via the fixed line network on a common channel: the first one is data communication delivered in GTP protocol whilst the second one is a normal voice communication. The minimum set of data + CLI are delivered as transparent data together with the voice. At the same time the

TELECOM Operator push the Mobile Location to the PSAP using the Mobile Location Protocol chosen within ETSI Workgroup.

4. The PSAP transmit acknowledge of data received to the IVS and interpret GTP minimum set of data using a GTP interpreter.
5. In case the user is a subscriber of a private Service Provider (SP) the IVS sends a full set of data via TELECOM operator to SP, after receiving acknowledge from the PSAP.
6. The SP receives the data message encoded with a proprietary protocol and it starts handling procedures, adding the additional E-Merge data in the E-Merge database in order to make these data available for the PSAPs.
7. The SP transmits acknowledge of data received to the IVS.
8. If translation is needed the SP starts on PSAP request using a toll free number a conference call with the driver.
9. If the driver is also a subscriber of a SP the PSAP start management operation accessing at the E-Merge Database in order to get full set of additional E-Merge data directly from the SP.
10. The PSAP Operator elaborates the received data.
11. The PSAP Operator dispatches the emergency details to the most appropriate Rescue Centres.
12. In a second time the PSAP communicates to the SP the involved rescue centres, to allow the SP to be able to provide additional post-accident services. This communication could happen via fixed line network as a simple phone call between the operators, or via Internet. In this last case the PSAP Operator can access to E-Merge Database and put in all the available information about the involved Rescue Centres.

Vehicle to the SP

In case that the driver has a contract to a service provider (SP) then in addition to the minimum set of data and the 112 voice communication a full set of data is sent to this SP and the SP makes these information available for the PSAPs in a specific E-MERGE case data DB as follows.

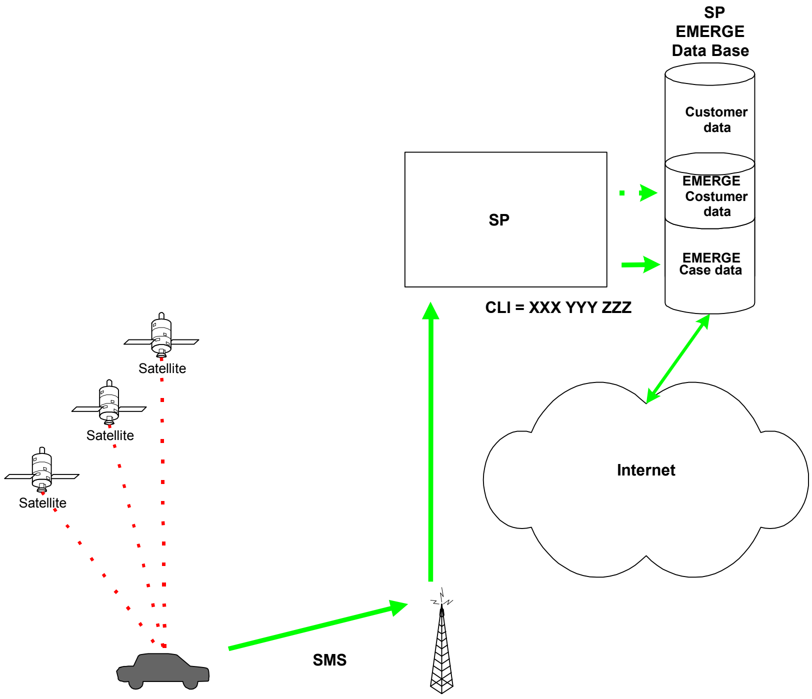


Figure 7: Data transmission to the SP

Workflow

1. the IVS generates a data call with the full set of data (GTP) to a private SP number if the driver has a contract with a SP;
2. the mobile operator route the data call (full set of data) to the SP;
3. The SP receive the full set of data from the Vehicle including the CLI
4. The SP operator add full set of data to the E-MERGE case data database.

3.3.2 The PSAP and the Emergency Authorities

The PSAP is the call centre responsible for providing a first response to an emergency 112 call and is responsible for routing the 112 call to the correct stage 2 PSAPs (dispatchers). The PSAP base currently the routing of the information to the relevant 2nd stage PSAPs on the information received by talking to the person dialling 112. In case of future in-vehicle e-calls routed directly to the PSAPs via the automatically generated data received either directly as the minimum set of data or via the SP as the additional set of data they will now in addition be able to make a more qualified routing to the appropriate stage 2 PSAPs and in addition the 2nd stage PSAPs will know what kind of incident response they should react with.

The architecture and workflow for the minimum set of data has been explained in the previous chapter. The additional data that in addition could be very useful for the PSAPs both for the initial emergency response but mainly for the after handling of the emergency is suggested handled in the following way:

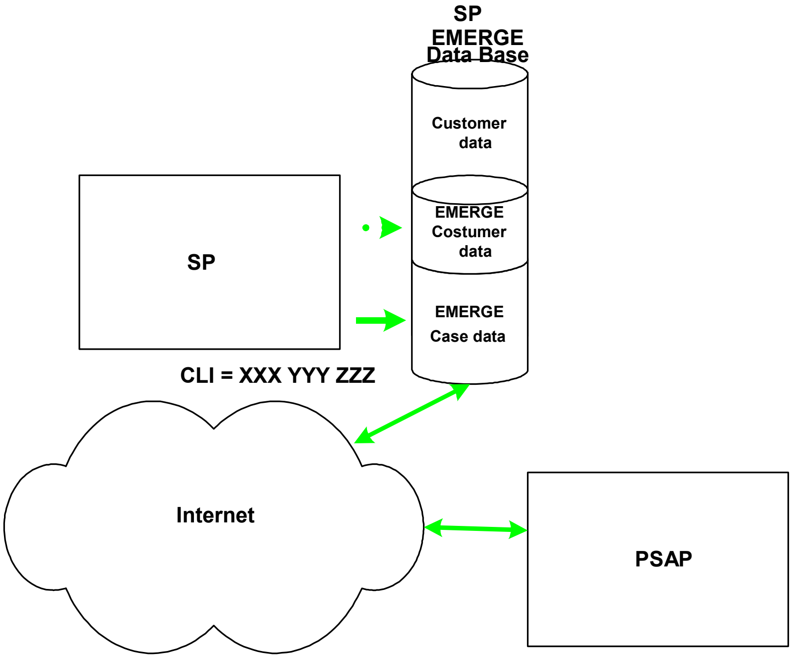


Figure 8: The PSAP connects to the E-MERGE Database

Workflow:

1. The PSAP operator identify via the minimum set of data that the driver has a subscription to a service provider
2. The PSAP identifies the SP based on the IP address given in the minimum set of data
3. The PSAP operator access the SP specific database via a secure web interface
4. The PSAP operator search for data using the CLI
5. The search via CLI generate a view of all data, which has been uploaded by the SP operator
6. The PSAP operator have a possibility to add PSAP identification (e.g. telephone number and name etc) in order for the SP to know which PSAP has received the data

3.3.3 Solving the language problem

In the case that the PSAP operator does not speak the language of the driver involved in the accident it is possible for the PSAP, if the driver has a subscription to a SP, to set up a conference voice call between the vehicle occupant, an operator at the responsible SP, and itself. The SP toll free telephone number is included in the minimum set of data. This direct contact information of the SP operator is included in the additional data SP to PSAP

4. EMERGE (e-call) Use Cases

4.1 Introduction

In this part of the document the E-MERGE (e-call) use cases are described. Figure 1 shows and overview of the use cases.

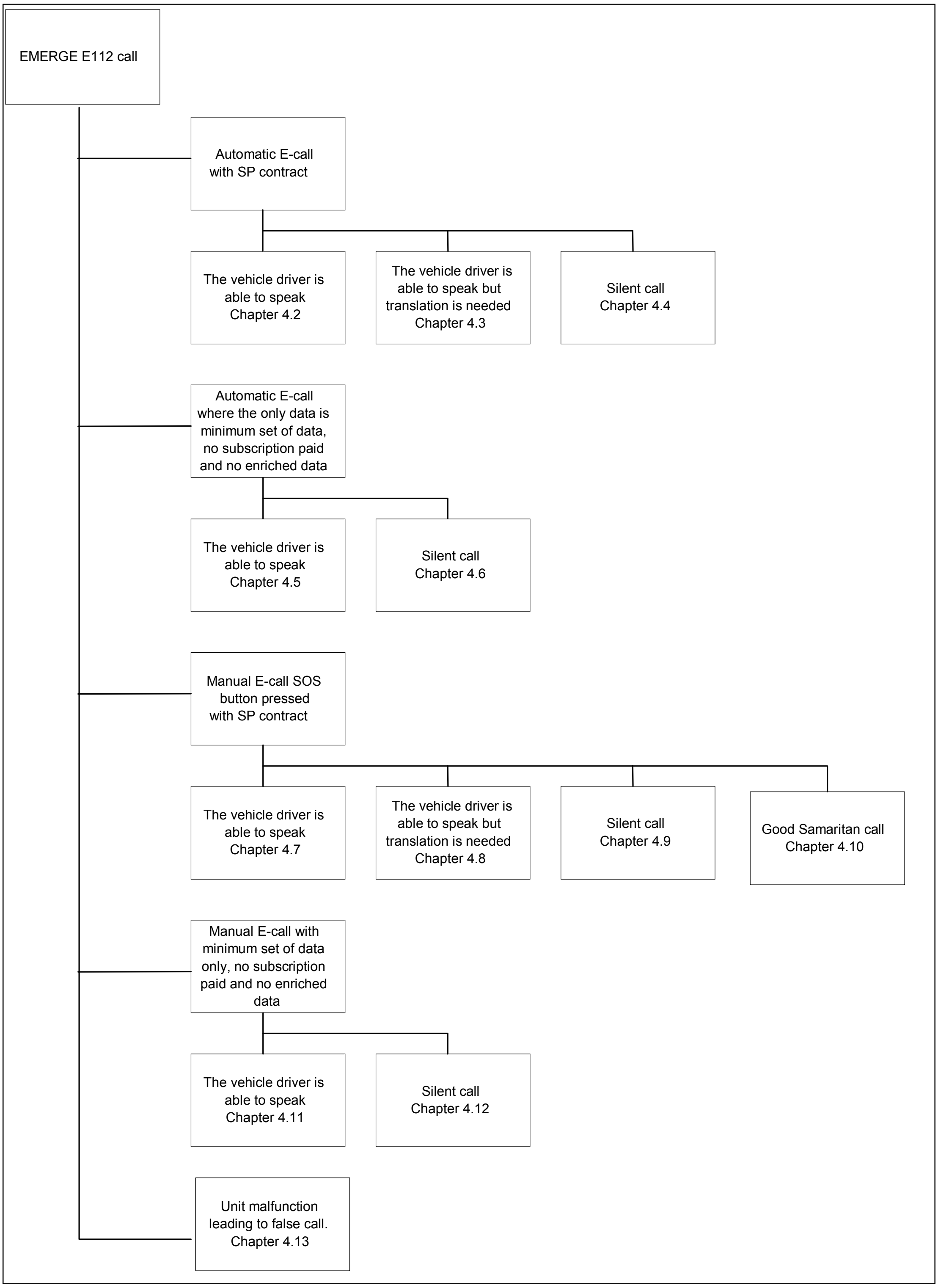

EMERGE E112 call
Automatic E-call with SP contract
The vehicle driver is able to speak Chapter 4.2
The vehicle driver is able to speak but translation is needed Chapter 4.3
Silent call Chapter 4.4
Automatic E-call where the only data is minimum set of data, no subscription paid and no enriched data
The vehicle driver is able to speak Chapter 4.5
Silent call Chapter 4.6
Manual E-call SOS button pressed with SP contract
The vehicle driver is able to speak Chapter 4.7
The vehicle driver is able to speak but translation is needed Chapter 4.8
Silent call Chapter 4.9
Good Samaritan call Chapter 4.10
Manual E-call with minimum set of data only, no subscription paid and no enriched data
The vehicle driver is able to speak Chapter 4.11
Silent call Chapter 4.12
Unit malfunction leading to false call. Chapter 4.13

Figure 9:Overview of use cases

The E- MERGE Use Cases as defined and described within this chapter, are the use cases relevant for the in-vehicle E-call as defined by the E-MERGE consortium. They are divided in five main groups:

- Automatic E-Call
- Automatic E-Call, no subscription to SP
- Manual E-Call SOS button pressed
- Manual E-Call , no subscription is paid
- Unit mall function leading to false call.

Each of the main groups have detailed descriptions of the Use Cases within the group, those are:

- The vehicle driver is able to speak
- The vehicle driver is able to speak but translation is needed
- Silent call
- Good Samaritan call (eye witness call).

The Use Cases describes the handling of the information within each Use Case, from initialisation to the end of sequence.

4.2 Automatic E-call, the vehicle driver is able to speak and subscription to SP

4.2.1 Description

This use case describes how the driver of the vehicle will be automatically connected via a voice and data connection to the PSAP. This connection is based on the E112 call including the provision of the location data by the network provider and the transmission of the minimum set of data. The voice, location information and minimum set of data is used to request emergency services and give proper response in the event of an incident. The PSAP has the opportunity, based on the SP-ID and the toll free SP telephone number, which is included in the minimum set of data, to activate a conference call to the SP for a voice connection and to pull additional data from the SP E-MERGE DB via internet. The automatic E112 call is activated when the vehicle automatically detects that a minimum of two critical sensors has been activated. The IVS unit creates the minimum set of data message to be sent to the PSAP and after acknowledge the full set of data is sent to the SP.

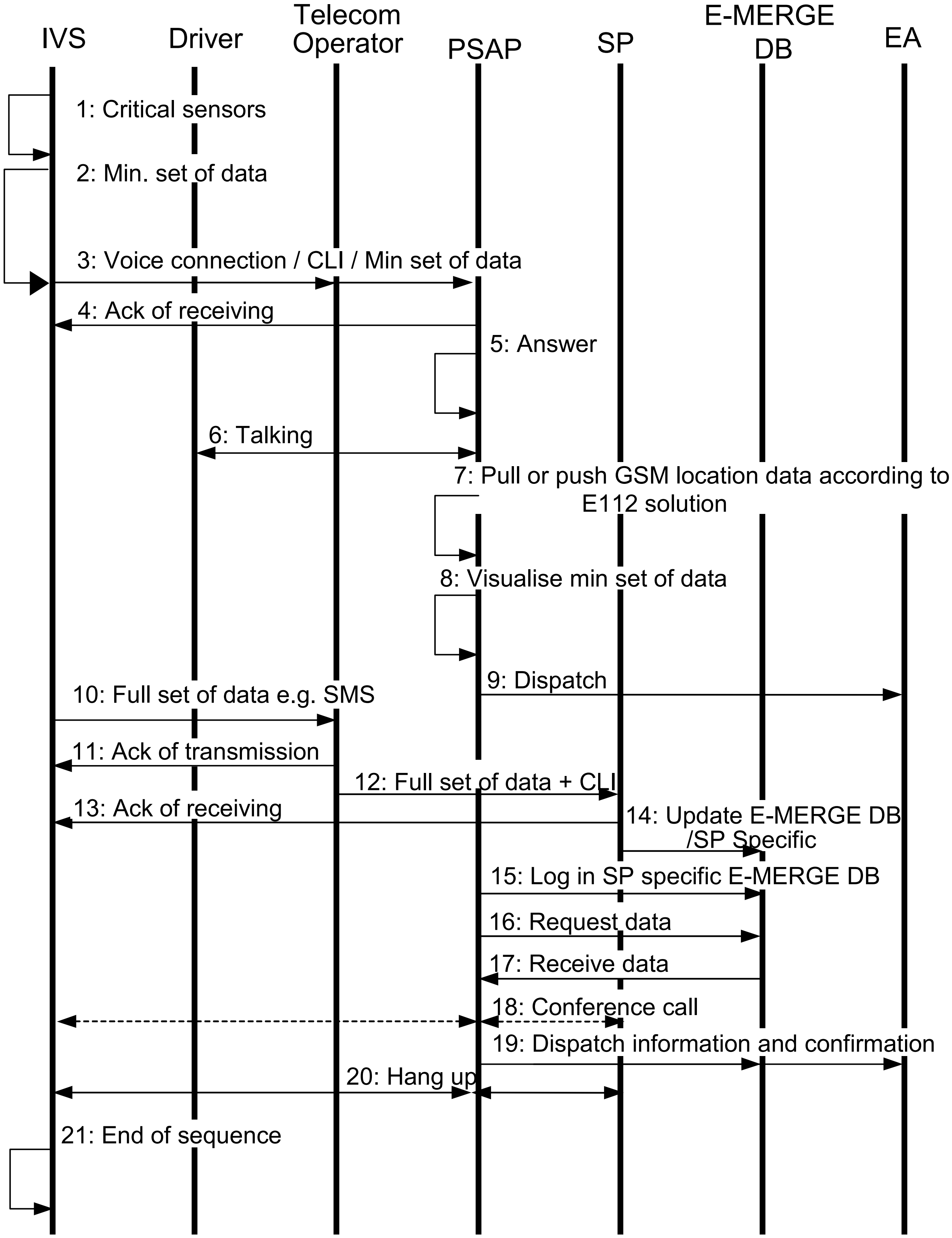
A voice call is made automatically to the PSAP allowing the PSAP representative to communicate with the driver of the vehicle. The nature of the emergency is determined and the PSAP representative contacts the appropriate Emergency Authority to request timely assistance for the driver of the vehicle. The emergency service is time and mission critical.

4.2.2 Initialisation

The service starts with:

A vehicle crash occurs and a minimum of 2 critical sensors is activated which causes the IVS unit to begin an automatic emergency sequence.

4.2.3 Sequence overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Critical sensors
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in SP specific E-MERGE DB
16: Request data
17: Receive data
18: Conference call
19: Dispatch information and confirmation
20: Hang up
21: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.2.4 Sequence of Events

1. Emergency service sequence initiated automatically via a minimum of 2 critical sensors. (e.g. airbag and roll over).
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP communicates with the vehicle driver.
7. The PSAP pull or get the minimum set of GSM location data from the telecom location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the SP specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP has the opportunity to open a conference call with the vehicle, the SP and the EA. The conference call is set up on a SP specific European free number.
19. The PSAP contact the E-MERGE data base for dispatch information and the EA for further dispatch confirmation.
20. The PSAP hangs up the voice call.
21. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.3. Automatic E-call, the vehicle driver is able to speak but translation is needed, subscription to SP

4.3.1 Description

This use case allows the driver of the vehicle to automatically contact the PSAP but as the PSAP operator dose not understand the driver a conference call with the SP, to whom the driver has a contract with, in order to speak in native language will be established. The PSAP has the opportunity, based on the SP ID and the toll free SP telephone number as content of the minimum set of data, to activate a conference call to the SP for a voice connection and to receive additional data from the SP E-MERGE DB via Internet.

The service is activated when the vehicle automatically detects that there was a minimum of two critical sensor activated. The IVS unit formulates a minimum set of data message to the PSAP and after acknowledge the full set of data is sent to the SP.

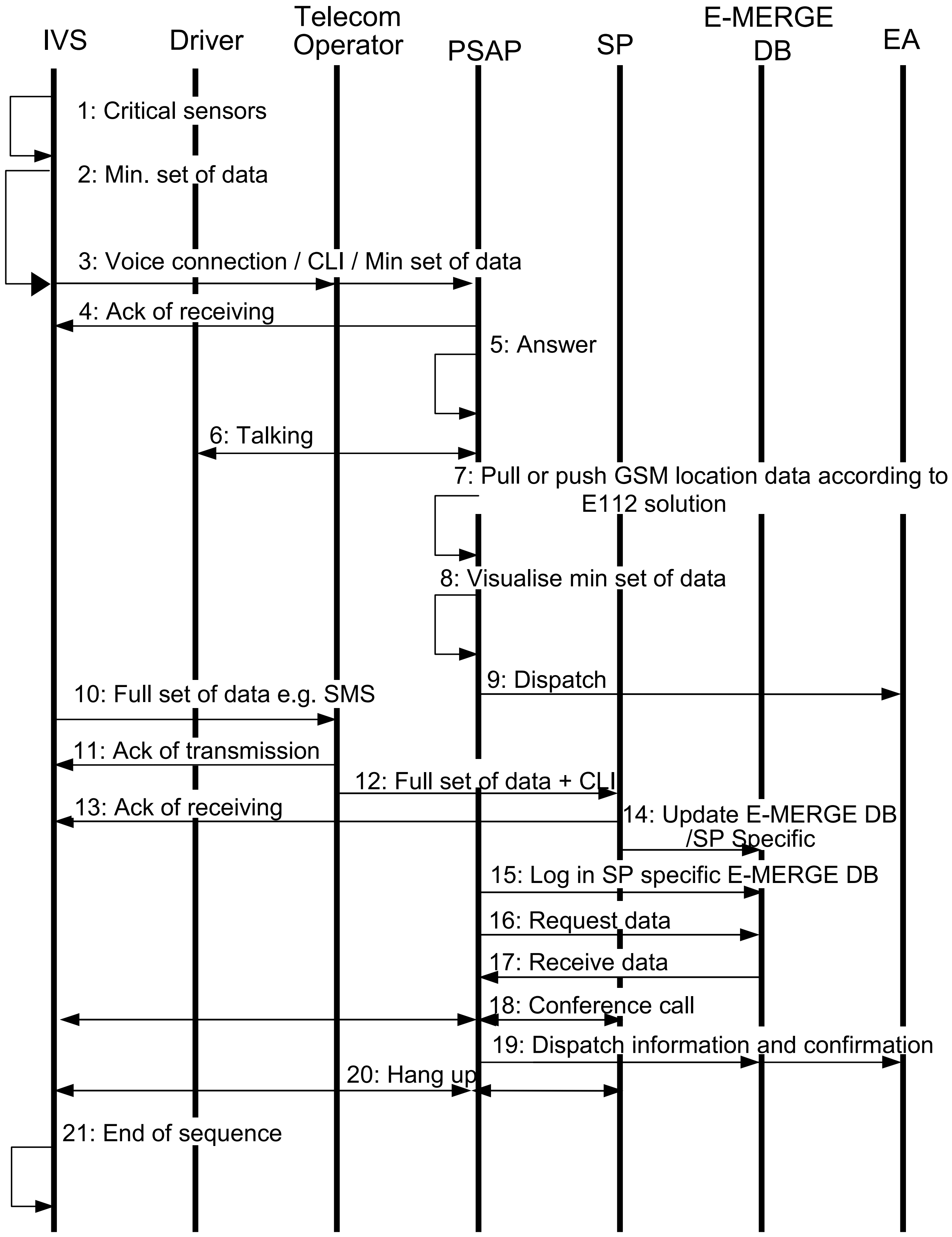
A voice call is established automatically from the vehicle to the PSAP allowing the PSAP representative to communicate with the driver of the vehicle. Here the vehicle is outside the home country and the driver is not English or speaks the language of the country to where the vehicle is located, so the PSAP operator analyse the minimum set of data to locate contact data for the responsible SP. The PSAP operator sets up a conference call with the vehicle driver and the SP operator. The nature of the emergency is determined and the PSAP representative contacts the appropriate Emergency Authority to request timely assistance for the driver of the vehicle. The emergency service is time and mission critical.

4.3.2 Initialisation

The service starts with:

A vehicle crash occurs and a minimum of 2 critical sensors is activated which causes the IVS unit to begin an automatic emergency sequence.

4.3.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Critical sensors
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in SP specific E-MERGE DB
16: Request data
17: Receive data
18: Conference call
19: Dispatch information and confirmation
20: Hang up
21: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.3.4 Sequence of Events

1. Emergency service sequence initiated automatically via a minimum of 2 critical sensors. (e.g. airbag and roll over).
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP operator cannot understand the vehicle driver, translation is needed.
7. The PSAP pull or get the minimum set of GSM location data from the telecom location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the SP specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP set up a conference call with the vehicle, the SP and the EA. The conference call is set up on a SP specific European free number.
19. The PSAP contact the E-MERGE data base for dispatch information and the EA for further dispatch confirmation.
20. The PSAP hangs up the voice call.
21. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.4. Automatic E-call silent call, subscription to SP

4.4.1 Description

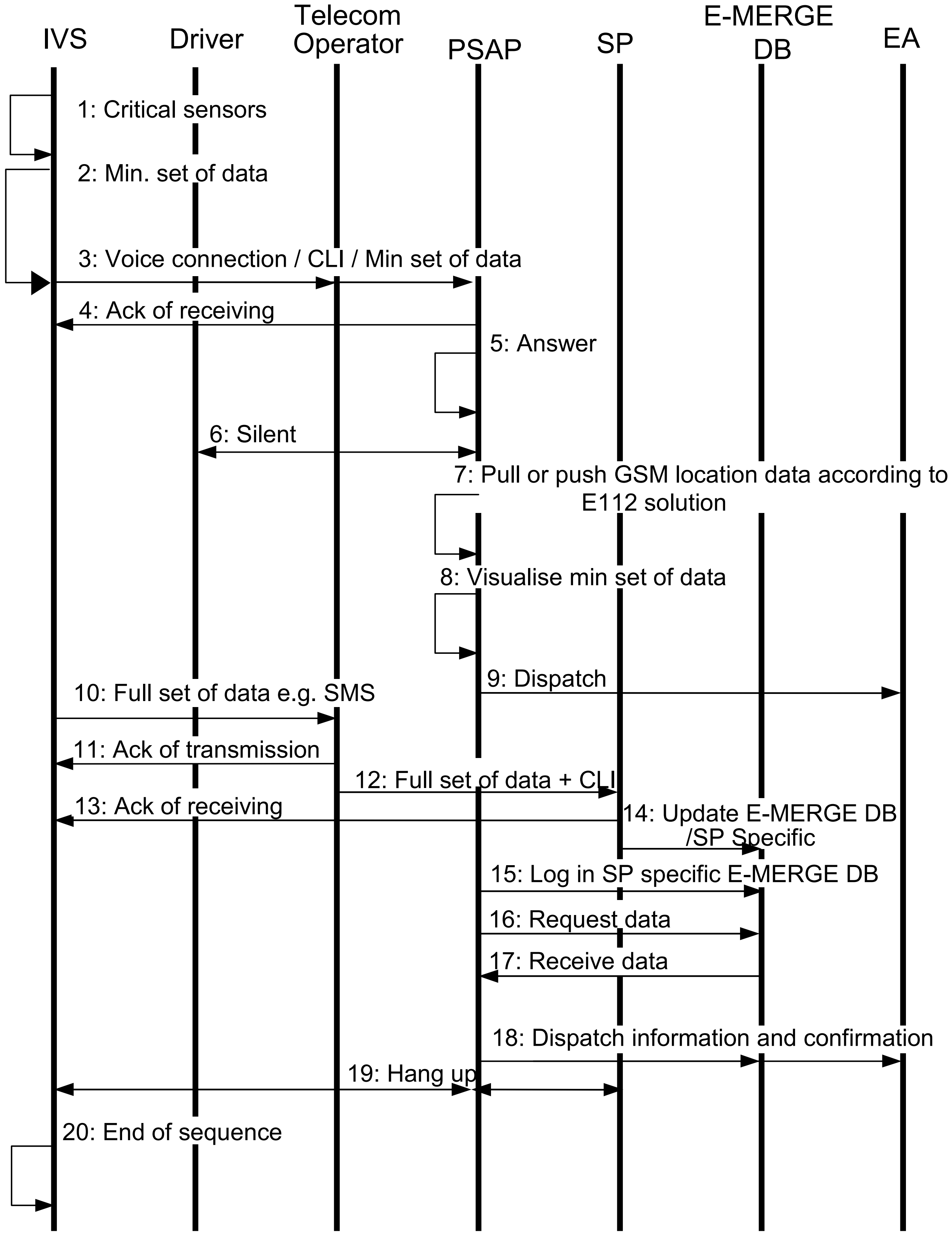
In this case the PSAP operator cannot get in voice contact with the vehicle driver over the voice link and treats the call as a silent call. The nature of the emergency has to be determined based on the minimum set of data and the full set of data. Emergency assistance may not be dispatched until after the full set of data has been received. Member states should develop their own protocols to deal with the possibility that activation has been accidental to allow the PSAP/EA to disconnect.

4.4.2 Initialisation

The service starts with:

A vehicle crash occurs and a minimum of 2 critical sensors is activated which causes the IVS unit to begin an automatic emergency sequence.

4.4.3 Sequence overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Critical sensors
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Silent
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in SP specific E-MERGE DB
16: Request data
17: Receive data
18: Dispatch information and confirmation
19: Hang up
20: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.4.4 Sequence of Events

1. Emergency service sequence initiated automatically via a minimum of 2 critical sensors. (e.g. airbag and roll over).
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP cannot hear the driver (silent call).
7. The PSAP pull or get the minimum set of GSM location data from the telecom location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the SP specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP contact the E-MERGE data base for dispatch information and the EA for further dispatch confirmation.
19. The PSAP hangs up the voice call.
20. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.5. Automatic E-call where the only data is minimum set of data, no subscription to SP, the driver is able to speak.

4.5.1 Description

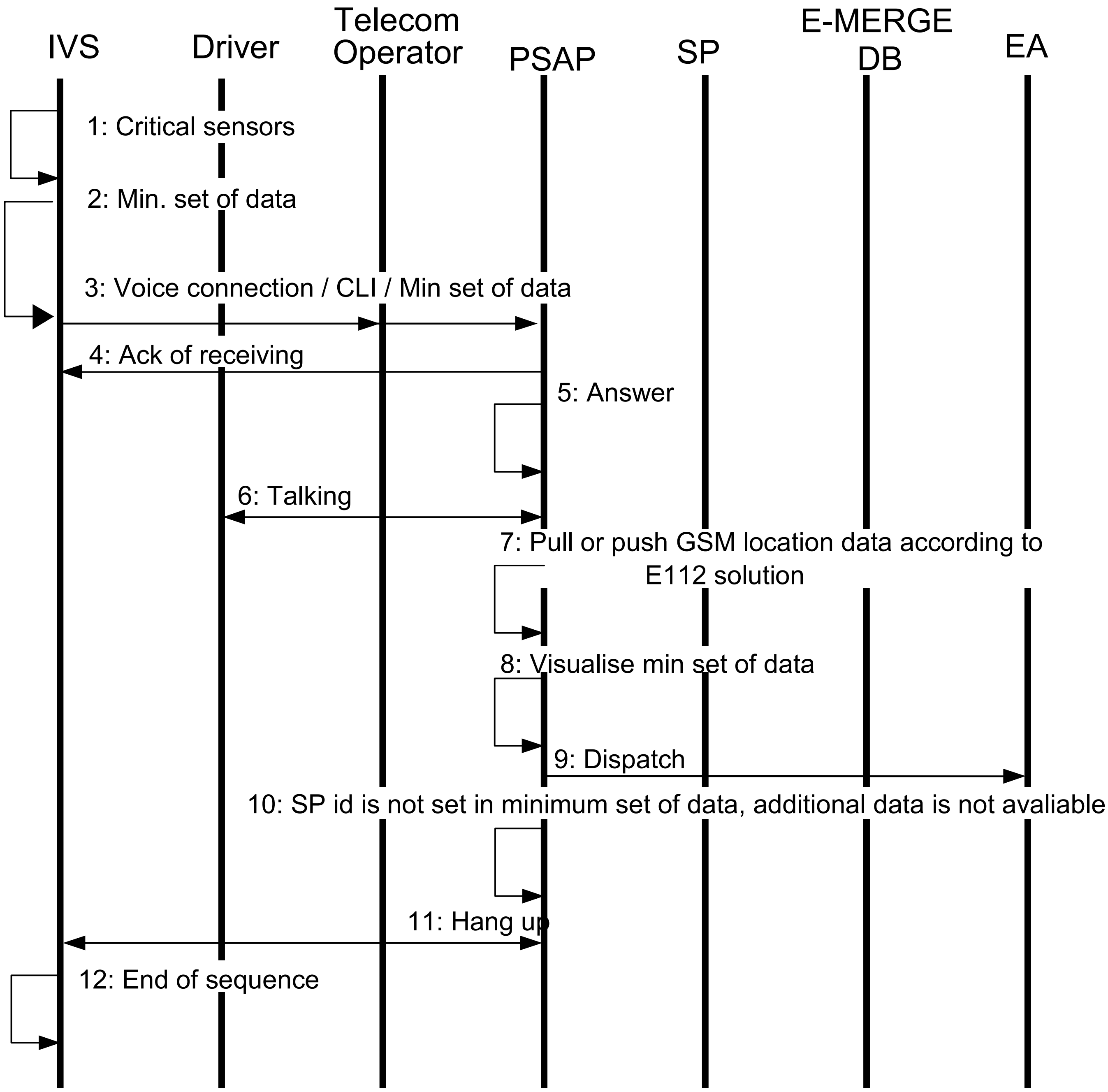
Within this use case the driver dose not have a subscription to a SP and can thus not obtain the benefits from making the additional data available for the PSAPs together with the possibility for establishing language support.

4.5.2 Initialisation

The service starts with:

A vehicle crash occurs and a minimum of 2 critical sensors is activated which causes the IVS unit to begin automatic an emergency sequence.

4.5.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Critical sensors
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: SP id is not set in minimum set of data, additional data is not avaliable
11: Hang up
12: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.5.4 Sequence of Events

1. Emergency service sequence initiated automatically via a minimum of 2 critical sensors. (E.g. airbag and roll over).
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator also from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP communicates with the vehicle driver.
7. The PSAP pull or get the minimum set of E-MERGE data from the telecom location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. SP id is not set in minimum set of data (SP id not set is the identification that no subscription is paid for E-MERGE). No additional data is available.
11. The PSAP hangs up the voice call.
12. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.6. Automatic E-call where the only data is minimum set of data, no subscription paid and silent call.

4.6.1 Description

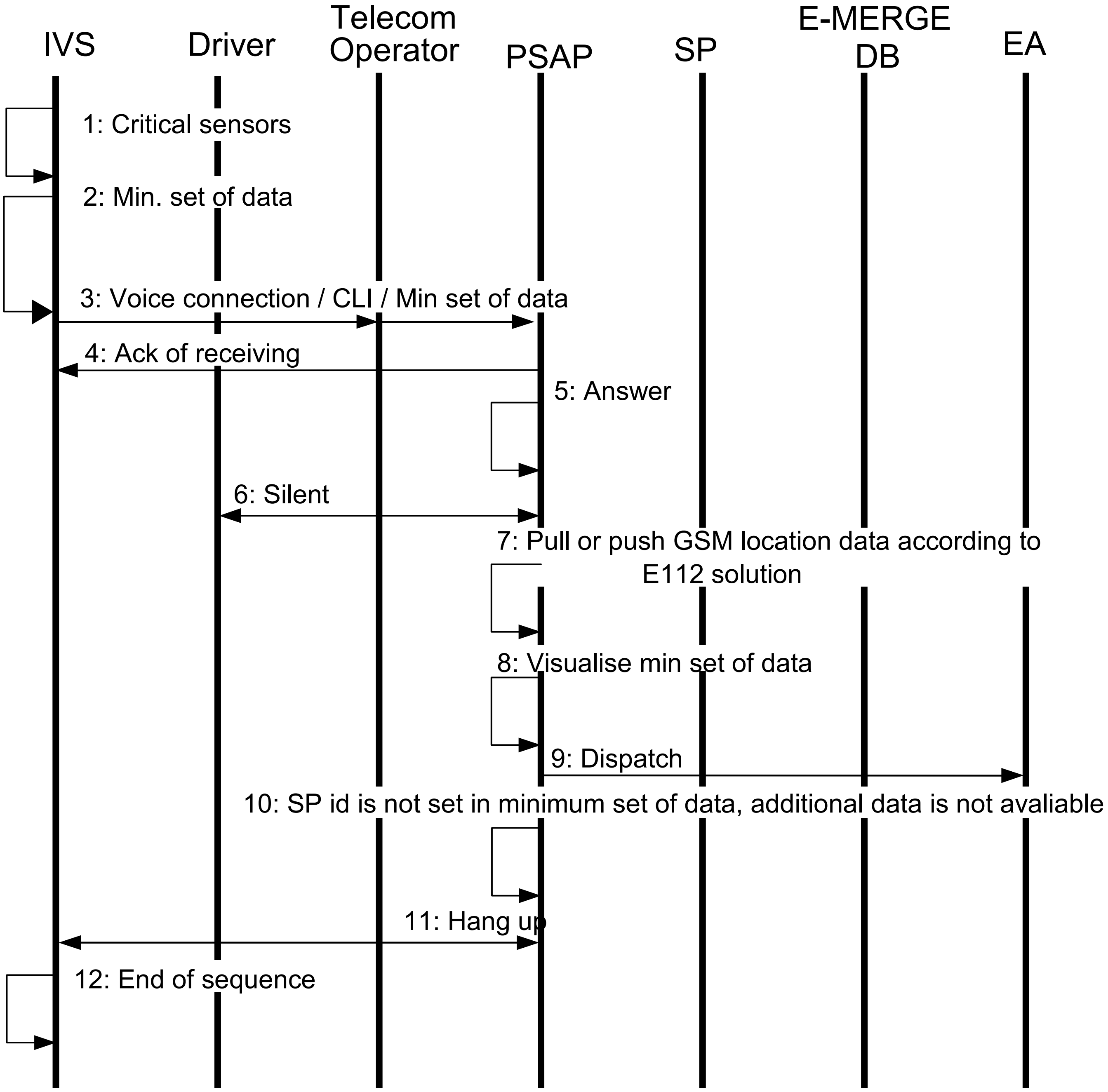
In this case the PSAP operator cannot get in voice contact with the vehicle driver. The nature of the emergency has to be determined based on the minimum set of E-MERGE data. Member states should develop their own protocols to deal with the possibility that activation has been accidental to allow the PSAP/EA to disconnect.

4.6.2 Initialisation

The service starts with:

A vehicle crash occurs and a minimum of 2 critical sensors is activated which causes the IVS unit to begin an automatic emergency sequence.

4.6.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Critical sensors
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Silent
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: SP id is not set in minimum set of data, additional data is not avaliable
11: Hang up
12: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.6.4 Sequence of Events

1. Emergency service sequence initiated automatically via a minimum of 2 critical sensors. (E.g. airbag and roll over).
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP cannot hear the driver (silent call).
7. The PSAP pull or get the minimum set of GSM location data from the telecom operator location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance, based only on the minimum set of data. The PSAP or EA may decide that there is no emergency.
10. SP id is not set in minimum set of data (SP id not set is the identification that no subscription is paid for E-MERGE). No additional data is available.
11. The PSAP hangs up the voice call.
12. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.7. Manual E-call, subscription to SP and the vehicle driver is able to speak

4.7.1 Description

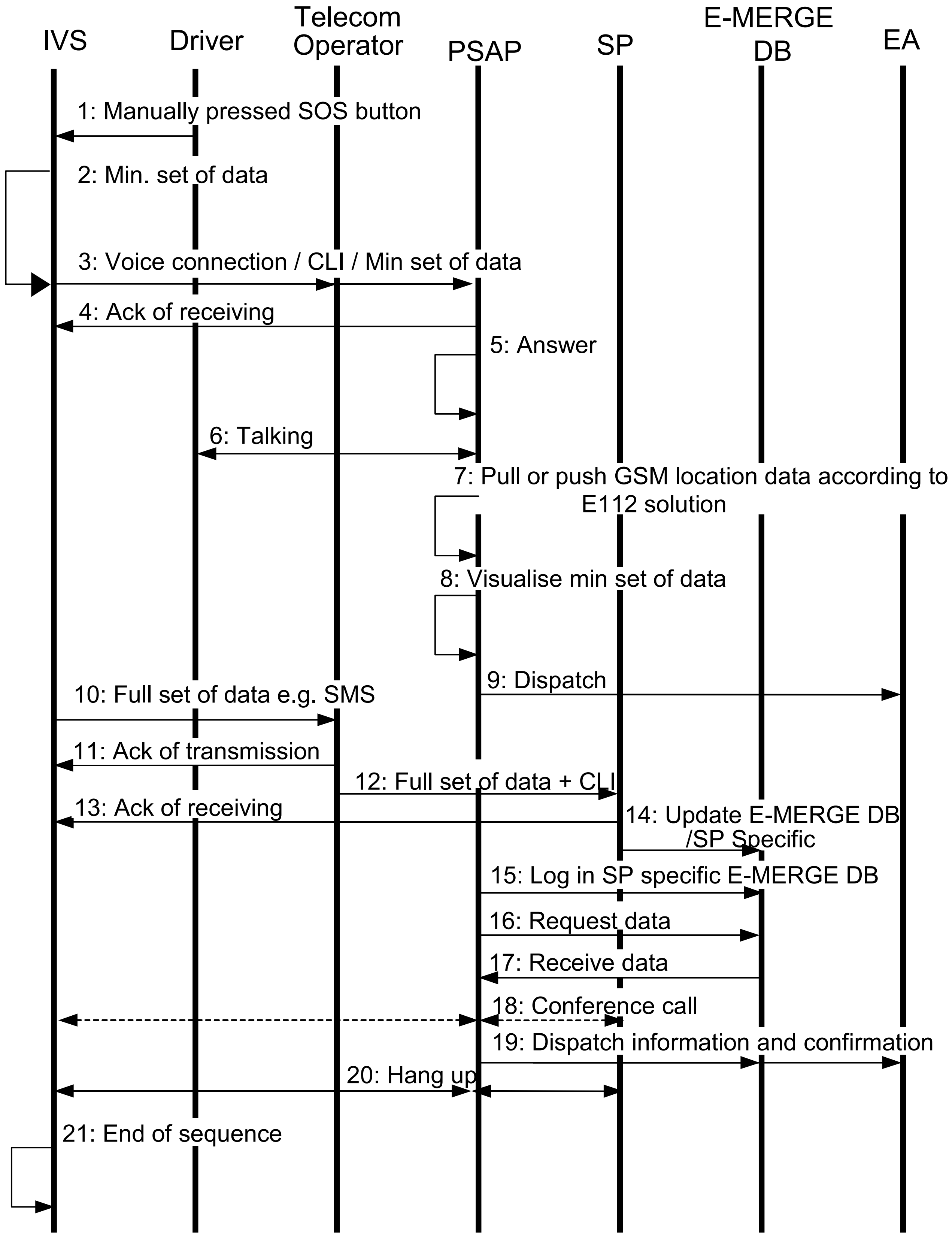
This use case allows the driver of the vehicle manually to contact the PSAP via voice channel in order to request emergency services in the event of an incident. The PSAP has the opportunity, based on the SP-ID and the toll free SP telephone number, which are included in the minimum set of data , to activate a conference call, to the SP and to receive additional data from the SP E-MERGE DB via Internet. The service is activated by manually pressing the SOS button. The IVS unit formulates a minimum set of data message to the PSAP and after acknowledge the full set of data is sent to the SP.

A voice call is made manually to the PSAP allowing the PSAP representative to communicate with the driver of the vehicle. The nature of the emergency is determined and the PSAP representative contacts the appropriate Emergency Authority to request timely assistance for the driver of the vehicle. The emergency service is time and mission critical.

4.7.2 Initialisation
The service starts with:

The vehicle driver presses the SOS button, which causes the IVS unit to begin an automatic emergency sequence.

4.7.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Manually pressed SOS button
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in SP specific E-MERGE DB
16: Request data
17: Receive data
18: Conference call
19: Dispatch information and confirmation
20: Hang up
21: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.7.4 Sequence of Events

1. Emergency service initiated by the vehicle driver manually pressing the SOS button.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP communicates with the vehicle driver.
7. The PSAP pull or get the minimum set of GSM location data from the telecom operator location database .
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the Service provider specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP has the opportunity to open a conference call with the vehicle, the SP and the EA. The conference call is set up on a SP European free number.
19. The PSAP contact the E-MERGE data base for dispatch information and the EA for further dispatch confirmation.
20. The PSAP hangs up the voice call.
21. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.8 Manual E-call, subscription to SP, the vehicle driver is able to speak but translation is needed

4.8.1 Description

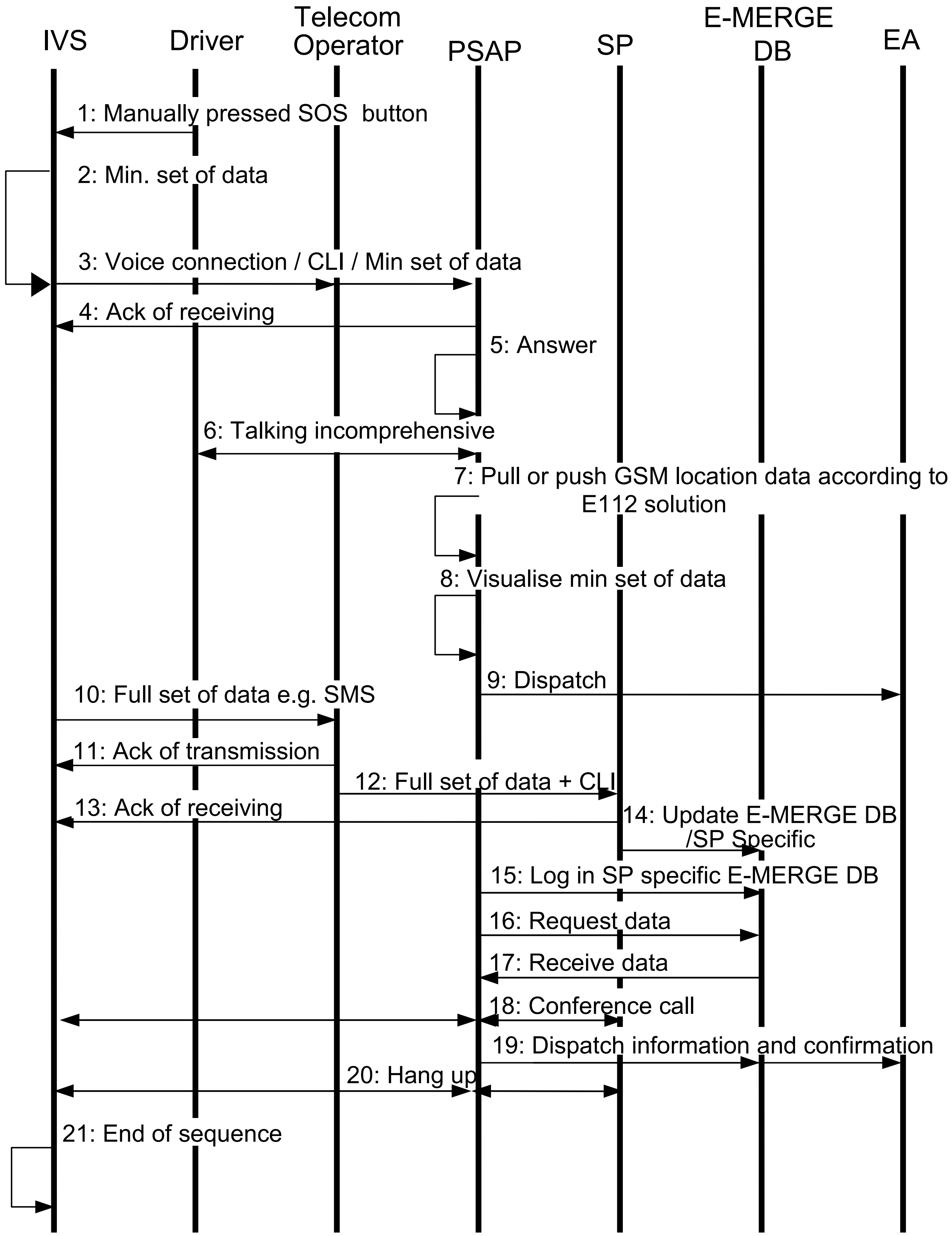
This use case allows the driver of the vehicle to manually contact the PSAP via voice channel, but as the PSAP operator does not understand the driver, a conference call in order to speak in native language with the SP, to whom the driver has a contract with, will be established. The PSAP has the opportunity, based on the SP ID and the toll free SP telephone number, which is included in the minimum set of data, to activate a conference call to the SP for a voice connection and to receive additional data from the SP E-MERGE DB via Internet.

4.8.2 Initialisation

The service starts with:

The vehicle driver presses the SOS button, which causes the IVS unit to begin an automatic emergency sequence.

4.8.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Manually pressed SOS button
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking incomprehensive
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in SP specific E-MERGE DB
16: Request data
17: Receive data
18: Conference call
19: Dispatch information and confirmation
20: Hang up
21: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.8.4 Sequence of Events

1. Emergency service initiated by the vehicle driver manually pressing an SOS button.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP operator cannot understand the vehicle driver, translation is needed.
7. The PSAP pull or get the minimum set of GSM location data from the telecom operator location database .
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the SP specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP open a conference call with the vehicle, the SP and the EA. The conference call is set up on a SP European free number.
19. The PSAP contact the E-MERGE data base for dispatch information and the EA for further dispatch confirmation.
20. The PSAP hangs up the voice call.
21. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.9 Manual E-call, silent call

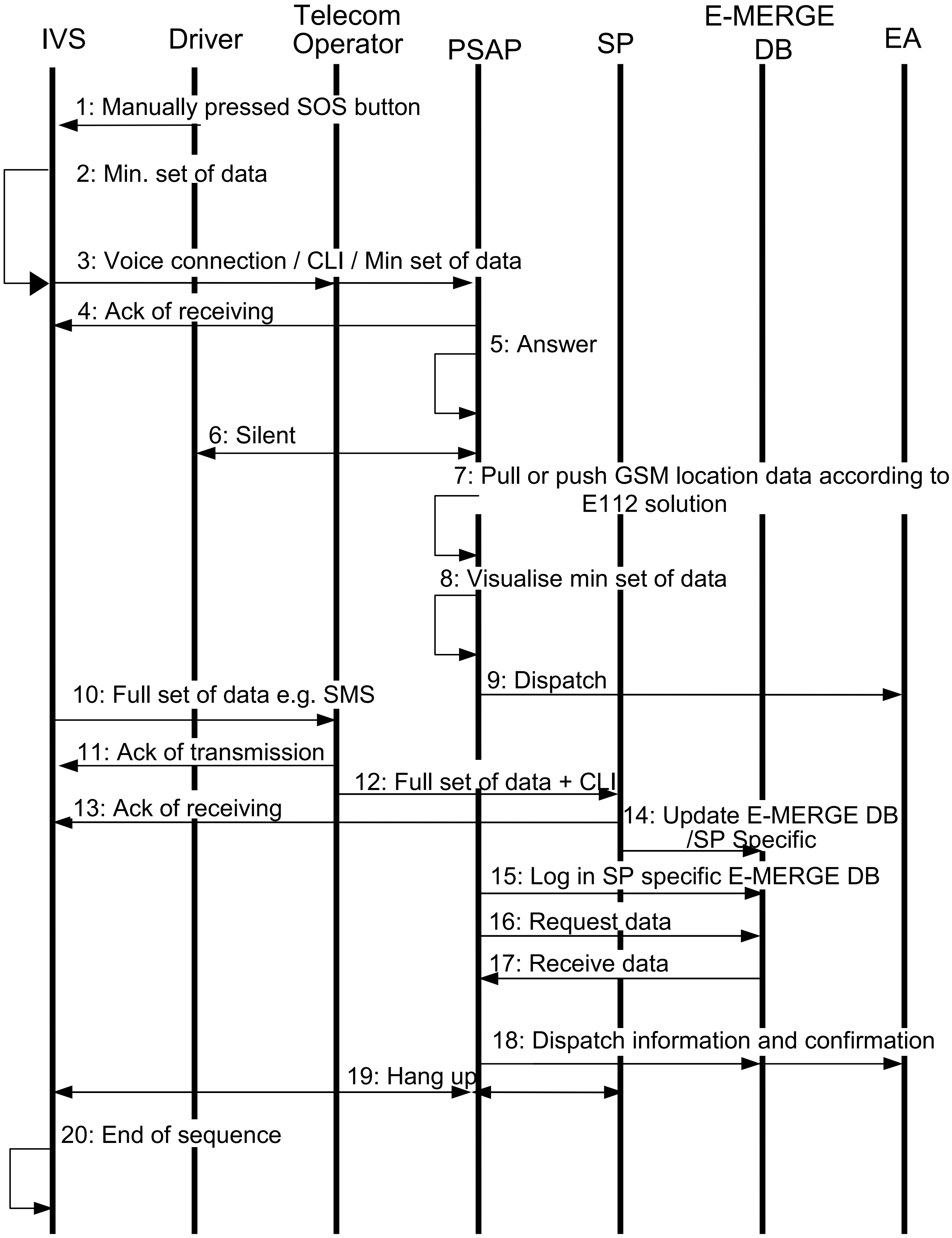
4.9.1 Description

The service is activated when the driver manually presses the SOS button. The IVS unit formulates a minimum set of data message to the PSAP and after acknowledge the full set of data is sent to the SP. A voice call is established by pressing a button allowing the PSAP representative to communicate with the driver of the vehicle. In this case however, the PSAP operator cannot get in contact with the vehicle driver. The nature of the emergency has to be determined based on the minimum and if needed also the full set data. Emergency assistance may not be dispatched until after the full set of data has been received. Member states should develop their own protocols to deal with the possibility that activation has been accidental to allow the PSAP/EA to disconnect.

4.9.2 Initialisation
The service starts with:

The vehicle driver presses the SOS button, which causes the IVS unit to begin an automatic emergency sequence.^

4.9.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Manually pressed SOS button
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Silent
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in SP specific E-MERGE DB
16: Request data
17: Receive data
18: Dispatch information and confirmation
19: Hang up
20: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.9.4 Sequence of Events

1. Emergency service initiated when the vehicle driver manually presses the SOS button.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP cannot hear the driver (silent call).
7. The PSAP pull or get the minimum set of GSM location data from the telecom operator location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the Service provider specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP contact the E-MERGE data base for dispatch information and the EA for further dispatch confirmation.
19. The PSAP hangs up the voice call.
20. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.10 Manual E-call - Good Samaritan Call, (eye witness call)

4.10.1 Description

This use case enables the driver of the vehicle to request emergency services in order to help a third party involved in an emergency/incident.

The service is activated by manually pressing the SOS button. The IVS unit formulates a minimum set of data message to the PSAP and after acknowledge the full set of data is sent to the SP.

A voice call is made manually to the PSAP allowing the PSAP representative to communicate with the driver of the vehicle.

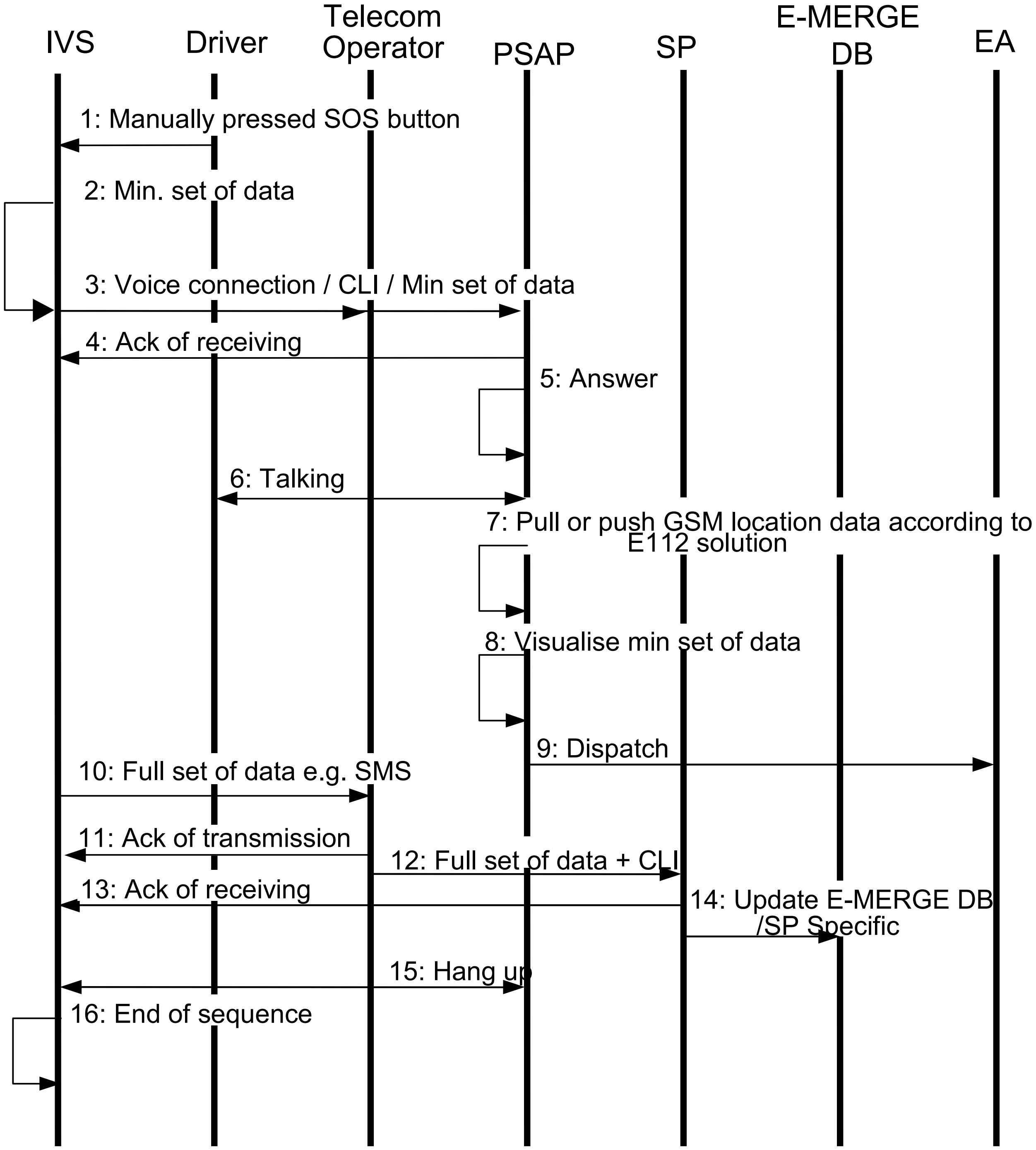
Note: According to the "E-MERGE IVS Recommendations" the IVS unit will not distinguish between an emergency directly affecting the caller or an emergency affecting a third party.

4.10.2 Initialisation

The service starts with:

Driver/passenger of vehicle A observe an accident for vehicle B or an emergency/crime affecting another person C. Driver or passenger pushes the SOS button, which causes the IVS unit to begin an automatic emergency sequence.

4.10.3 Sequence overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Manually pressed SOS button
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e.g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Hang up
16: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.10.4 Sequence of Events

1. Emergency service initiated by the vehicle driver manually pressing the SOS button.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator, from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP communicates with the vehicle driver.
7. The PSAP pull or get the minimum set of GSM location data from the telecom location database.
8. The PSAP visualises the minimum set of data – especially with a view of locate precisely from where the call was made.
9. The PSAP dispatches Emergency Assistance.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP hangs up the voice call.
16. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.11 Manual E-call where the only data is minimum set of data, no subscription paid, driver is able to speak

4.11.1 Description

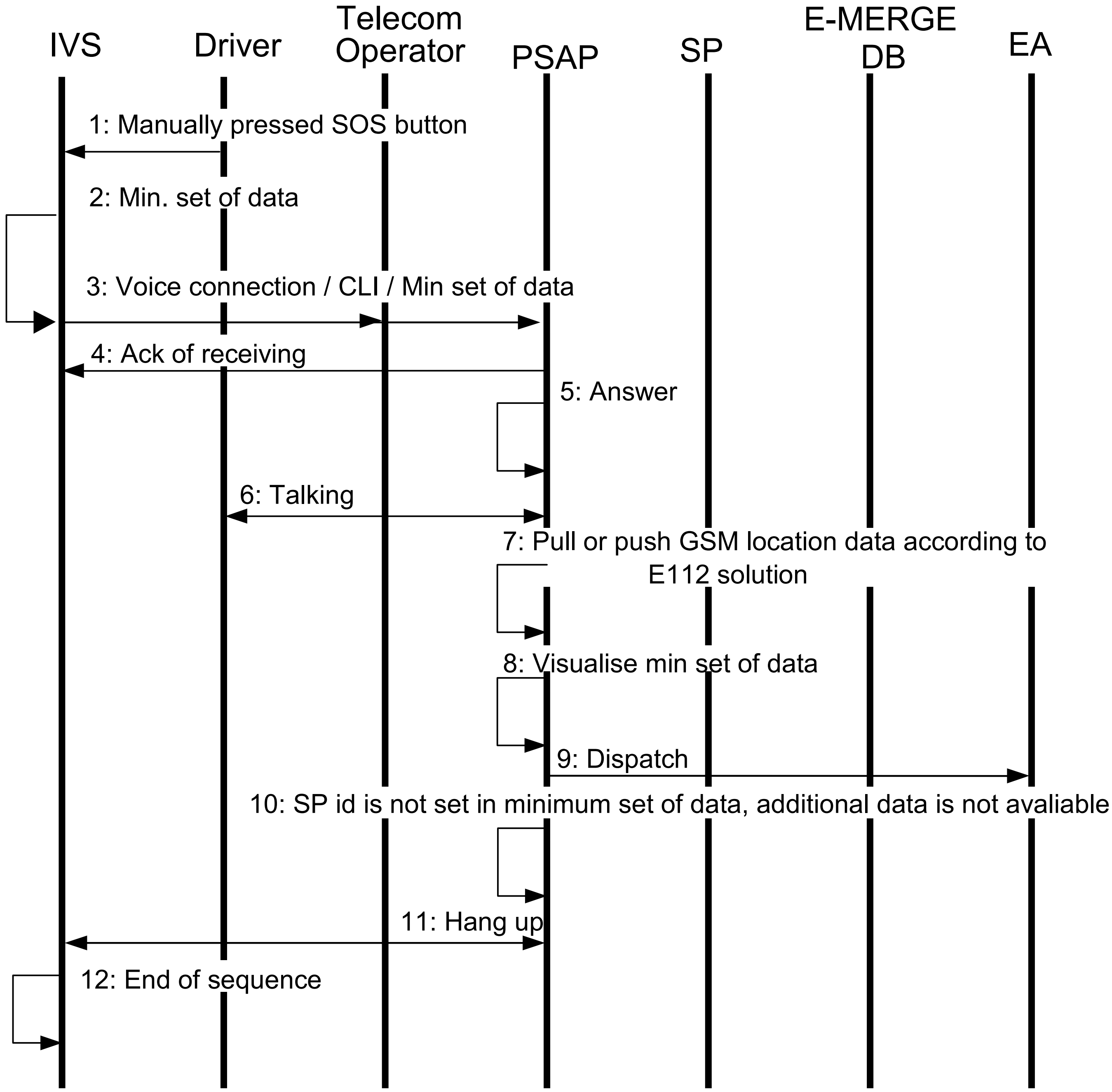
The service is activated by manually pressing the SOS button. The IVS unit formulates a minimum set of data message to the PSAP.

A voice call is established to the PSAP allowing the PSAP representative to communicate with the driver of the vehicle. The nature of the emergency is determined and the PSAP representative contacts the appropriate Emergency Authority to request timely assistance for the driver of the vehicle. The emergency service is time and mission critical.

4.11.2 Initialisation
The service starts with:

The vehicle driver presses the SOS button, which causes the IVS unit to begin an automatic emergency sequence.

4.11.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Manually pressed SOS button
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: SP id is not set in minimum set of data, additional data is not avaliable
11: Hang up
12: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.11.4 Sequence of Events

1. Emergency service initiated by the vehicle driver manually pressing the SOS button.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP communicates with the vehicle driver.
7. The PSAP pull or get the minimum set of GSM location data from the telecom location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance.
10. SP id is not set in minimum set of data (SP id not set is the identification that no subscription is paid for E-MERGE). No additional data is available.
11. The PSAP hangs up the voice call.
12. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.12 Manual E-call where the only data is minimum set of data, no subscription, silent call

4.12.1 Description

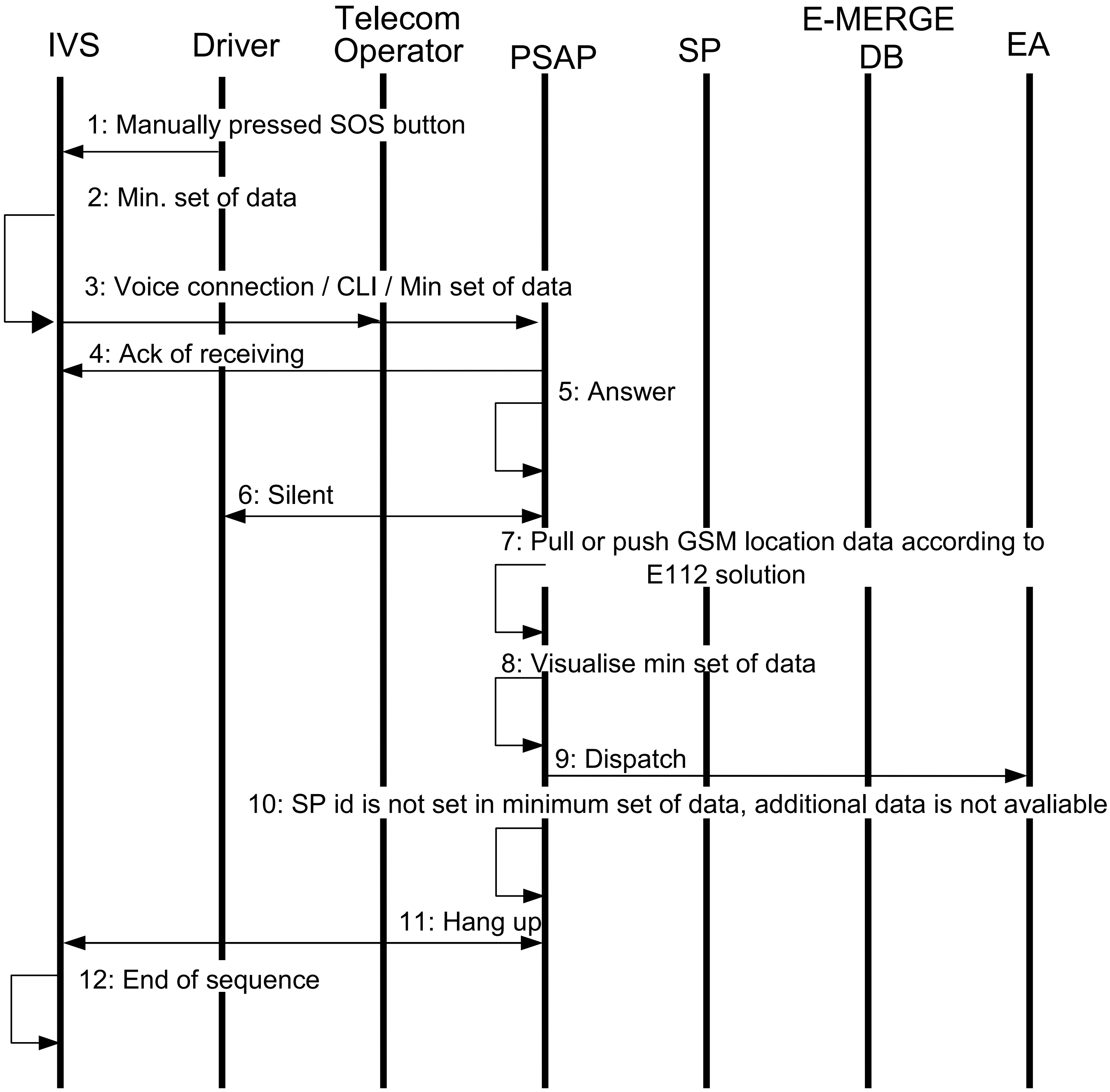
In this case the PSAP operator cannot get in voice contact with the Vehicle driver. The nature of the emergency has to be determined based on the minimum set of E-MERGE data. Member states should develop their own protocols to deal with the possibility that activation has been accidental to allow the PSAP/EA to disconnect.

4.12.2 Initialisation

The service starts with:

The vehicle driver presses the SOS button, which causes the IVS unit to begin an automatic emergency sequence.

4.12.3 Sequence Overview


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1: Manually pressed SOS button
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Silent
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: SP id is not set in minimum set of data, additional data is not avaliable
11: Hang up
12: End of sequence

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.12.4 Sequence of Events

1. Emergency service initiated by the vehicle driver manually pressing the SOS button.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator, from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP cannot hear the driver (silent call).
7. The PSAP pull or get the minimum set of GSM location data from the telecom operator location database.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance, based only on the minimum set of data. The PSAP or EA may decide that there is no emergency.
10. SP id is not set in minimum set of data (SP id not set is the identification that no subscription is paid for E-MERGE). No additional data is available.
11. The PSAP hangs up the voice call.
12. The IVS ends the emergency service sequence.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.13 Unit malfunction leading to false call

4.13.1 Description

This use case deals with the internal malfunction of the IVS, which triggers an E-call where no emergency situation exists.

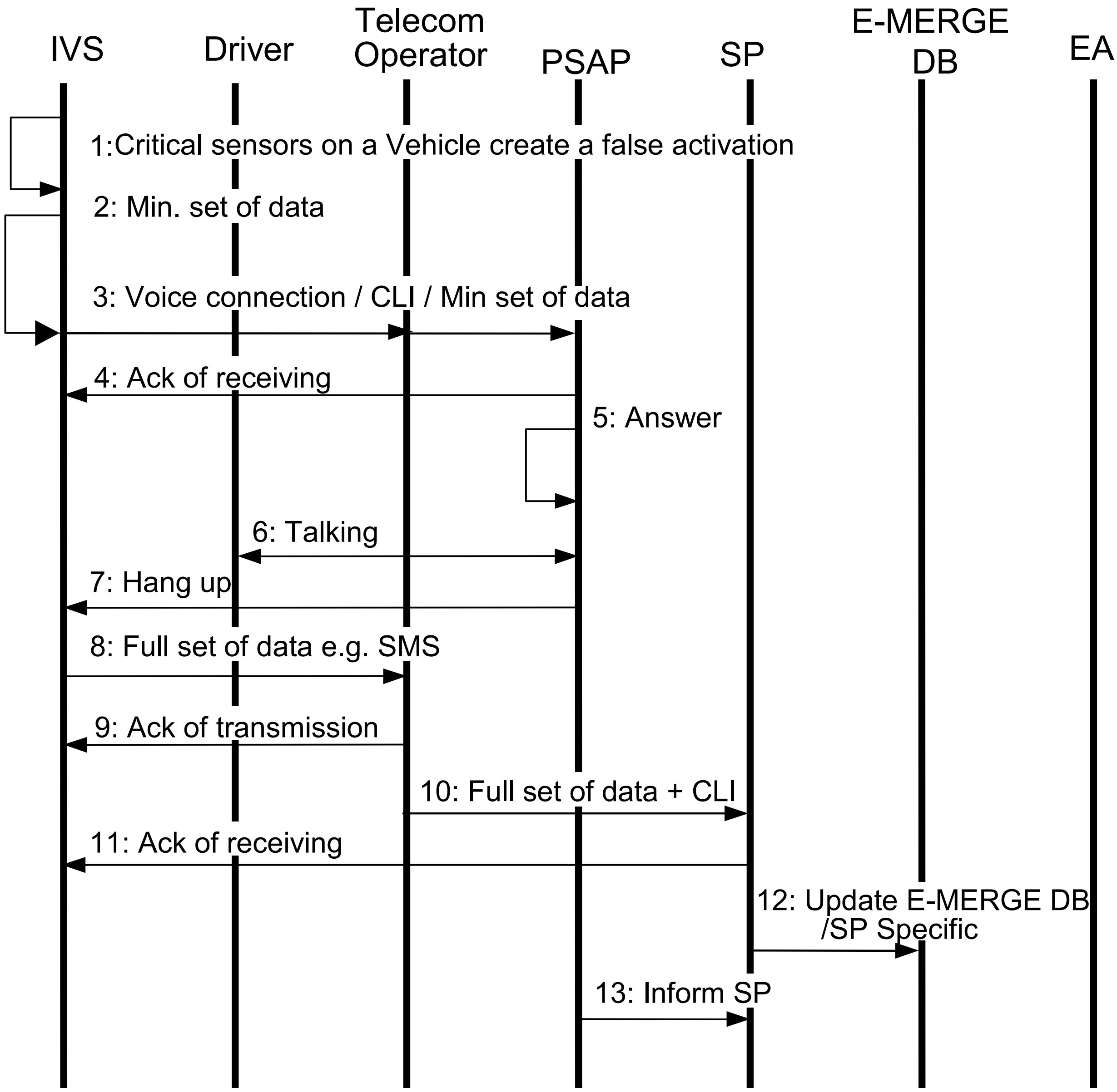
Malfunctions that lead to a false is not only based on a IVS unit malfunctioning but in addition on the possibility of a deliberate or accidental false activation of the IVS unit by a person within the vehicle.

Member states should develop their own protocols to allow the PSAP to disconnect the call if they are convinced that there is no emergency situation after establishing voice contact. However this activation could be minimised by the utilization of effective HMI for the location of the in-vehicle push button.

4.13.2 Initialisation

Critical sensors on a Vehicle create a false activation, which causes a request to the IVS unit to begin an automatic emergency sequence.

4.13.3 Sequence Overview Voice connection

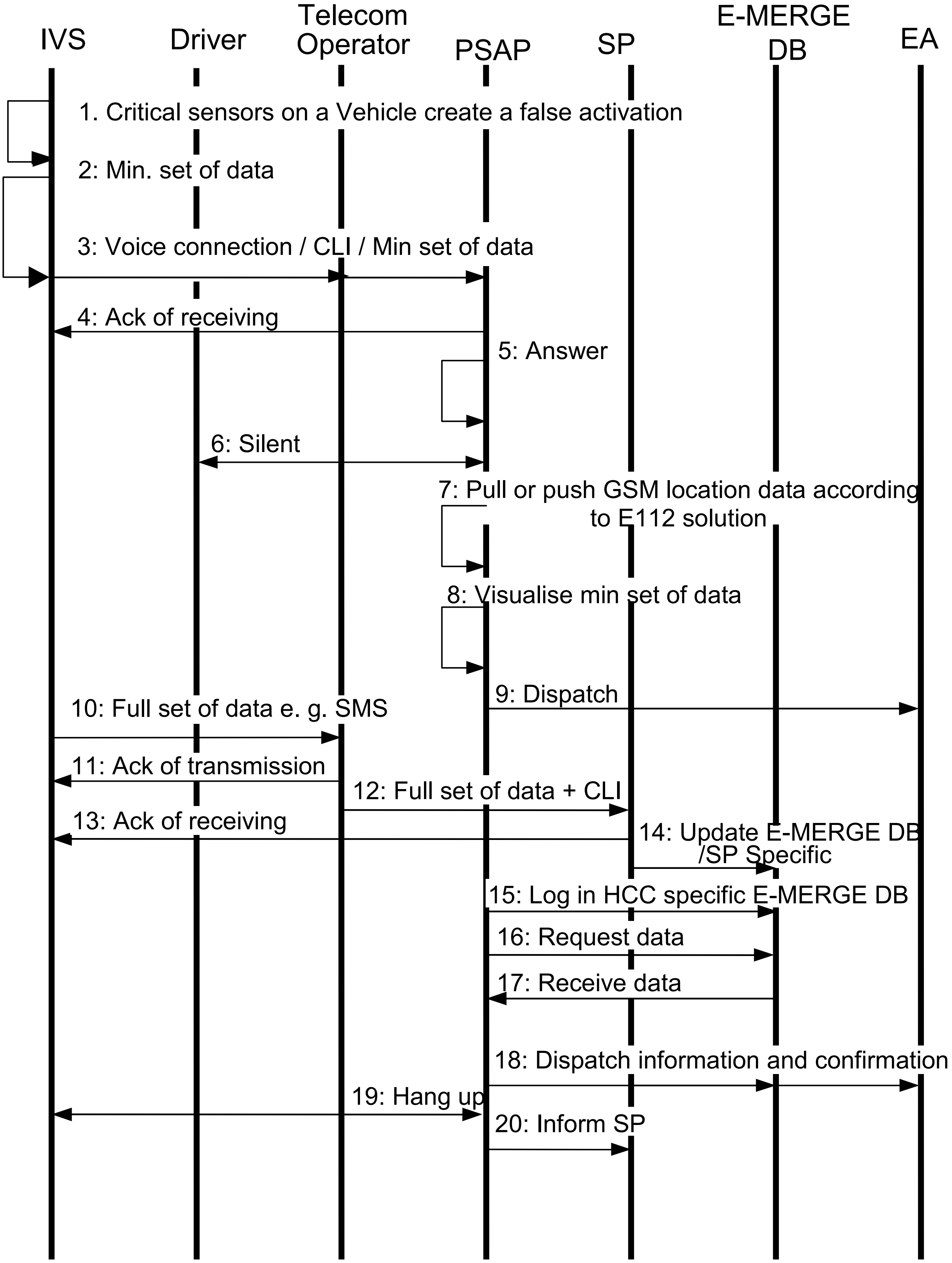

IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1:Critical sensors on a Vehicle create a false activation
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Talking
7: Hang up
8: Full set of data e.g. SMS
9: Ack of transmission
10: Full set of data + CLI
11: Ack of receiving
12: Update E-MERGE DB /SP Specific
13: Inform SP

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.13.4 Sequence of events Voice connection

1. Critical sensors on a Vehicle create a false activation, which causes a request to the IVS unit to begin an emergency sequence.
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator, from the PSAP. ***Note depends on technical solution***
5. The PSAP answers the voice call.
6. The PSAP communicates with the vehicle driver.
7. No incident, the PSAP hangs up the voice call.
8. Full E-MERGE set of data is sent to the Telecom operator.
9. The Telecom operator send the acknowledge of transmission to the vehicle.
10. The full set of data is forwarded to the SP, including the CLI-data.
11. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
12. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
13. The PSAP can on the basis of the SP identifier within the minimum set of data inform the SP, about the unit mall function in order to avoid continuous false calls.

4.13.5 Sequence Overview no Voice connection


IVS
Driver
Telecom Operator
PSAP
SP
E-MERGE DB
EA
1. Critical sensors on a Vehicle create a false activation
2: Min. set of data
3: Voice connection / CLI / Min set of data
4: Ack of receiving
5: Answer
6: Silent
7: Pull or push GSM location data according to E112 solution
8: Visualise min set of data
9: Dispatch
10: Full set of data e. g. SMS
11: Ack of transmission
12: Full set of data + CLI
13: Ack of receiving
14: Update E-MERGE DB /SP Specific
15: Log in HCC specific E-MERGE DB
16: Request data
17: Receive data
18: Dispatch information and confirmation
19: Hang up
20: Inform SP

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.13.6 Sequence of events no Voice connection

1. Emergency service initiated by the vehicle driver manually or automatically .
2. Minimum E-MERGE set of data is sent via the Telecom operator in the voice channel to the PSAP.
3. A voice call is established between the vehicle*** and the PSAP. ***Depends on the GSM module and the communication mode (GPRS).
4. An acknowledgement for the receiving of the minimum set of data is sent to the vehicle via the Telecom operator, from the PSAP. ***Note depends on technical solution***
5. The PSAP cannot receive the voice call.
6. The PSAP cannot communicate with the driver.
7. The PSAP merge minimum set of GSM location data with the voice call.
8. The PSAP visualises the minimum set of data.
9. The PSAP dispatches Emergency Assistance. The nature of the emergency is **NOT** determined.
10. Full E-MERGE set of data is sent to the Telecom operator.
11. The Telecom operator send the acknowledge of transmission to the vehicle.
12. The full set of data is forwarded to the SP, including the CLI-data.
13. An acknowledgement for the full set of data is sent to the vehicle from the SP via the Telecom operator. ***Note depends on technical solution***
14. The SP updates the Service provider specific E-MERGE database with additional customer and contract data.
15. The PSAP logs in to the E-MERGE database. The common identifier for the Service provider specific database is the network ID and /or the SP ID number / IP address.
16. The PSAP request data from the E-MERGE database.
17. The PSAP receives data from the E-MERGE database.
18. The PSAP contact EA for further dispatch confirmation. The nature of the emergency is **NOT** determined
19. The PSAP hangs up the voice call.
20. Inform SP, unit mall function.

Note: Project E-MERGE recognise that there are differing organisational and communication structure within the European Union that deal with the receipt control and dispatch of emergency rescue vehicle.

4.14 Conclusion

The E- MERGE Use Cases as defined and described by this chapter, provide the basis for a specification of the various interfaces relevant for the five main groups of calls, which has been identified as relevant for the in-vehicle e-call.

The relevant groups are:

- Automatic E- Call
- Automatic E-Call, no subscription
- Manual E-Call SOS button pressed
- Manual E-Call, no subscription
- Unit mall function leading to false call.

The main groups have been described in details with a special focus of the following special cases:

- The vehicle driver is able to speak
- The vehicle driver is able to speak but translation is needed
- Silent call
- Good Samaritan call (eye witness call).

5. IVS Design Recommendations

5.1 Introduction

This document describes the recommendation and design guidelines for the development of an In-Vehicle System for emergency calls.

5.2 Human Machine Interface (HMI)

5.2.1 Standards

Before introducing the HMI requirements for the E-call system, it is necessary to provide an overview of the different regulations existing in Europe.

On December 21, 1999, the Commission of the European Communities issued a recommendation '*on safe and efficient in-vehicle information and communication systems: A European statement of principles on human machine interface*' to its member states.

This document also contains references to specific ISO standards regulating the E-call In-Vehicle System requirements.

5.2.2 The E-call system HMI

To allow a vehicle driver or passenger to activate an emergency call manually, buttons are required. Currently, most in-vehicle systems offer a minimum of two assistance buttons, one for activating an emergency call, and another one for requesting vehicle breakdown assistance.

In order to maximise the benefits of the E-call system, the E-call HMI must be as user-friendly as possible. The ease of interaction with the unit as well as the design of button location and function must be considered critical factors for the usability of the system.

The E-call system usability requirements can be broken down into several HMI characteristics:

- Ease of use
- System Feedback to the user
- Prevention of false activation
- Prevention of driver distraction

5.2.2.1 Ease of Use

The E-call button should be placed in a location that the driver and front seat passenger can reach to activate the button, without having to leave their seats.

To assist new users that may be unfamiliar with a vehicle, the E Call Button should have a similar look-and-feel across different vehicle types and brands. The E-call system look-and-feel should be similar to help the user recognise the system, but it does not have to be identical in each vehicle.

Such a look-and-feel includes the following aspects:

- Position
- Size
- Colour
- Feel
- Shape
- Night-time button illumination

The lack of experimentation in real-life conditions prevents the specification of an E-call HMI standard. On the other hand, it is possible to provide a number of logically sound recommendations as those listed in the paragraphs below.

Position

The E-call button should be positioned in a distinct location so as to prevent the driver and other vehicle occupants from pushing the button accidentally. This position can be located in the rear mirror area, which can be reached by both front seat passengers without leaving their seats. Some vehicle manufacturers locate the E-call button on the dashboard, which can also be reached easily. In this position the E-call button needs to differ with the warning button in several aspects, so that an error from the driver can be avoided.

Colour

Most of the car manufacturers choose the red colour for the E-call button. The red colour is generally considered to indicate danger, so it is easy for the user to identify this button as an E-call button.
However, the user should not be able to confuse the E-call button with other warning buttons of the same colour. This can be achieved by using different shapes to distinguish between the buttons.

Size, Feel and Shape

These features largely depend on the interior design, but should allow the driver to easily identify the E-call button.

5.2.2.2 Feedback from the system

The system could offer either auditory or visual feedback to the user. Multimode feedback could help to assure the vehicle passengers that the system is activated.

Audio feedback

Auditory feedback could be achieved with a tone, or with a voice communication from the alarm centre.

Visual feedback

Visual feedback can be offered to the user via a display, a blinking light or with some icon on the instrument cluster. This kind of feedback is not always possible, especially in those accidents where the vehicle is severely damaged. If the feedback is provided via the display, the passengers must be able to understand the information quickly and easily.

5.2.2.3 Driver distraction prevention

In order to minimise the distraction of the driver the following recommendations are made.

- The E-call system should allow for hands-free operation after activation.
- The driver should be able to locate the E-call Button easily, without having to take his eyes off the road for more than two seconds.
- The E-call button should provide visual or audible confirmation that a message has been sent, to reassure the driver, and to allow the driver to continue concentrating on his / her primary task of driving.
- Any warnings of activation should be designed so as to prevent the driver from being started or distracted.

5.2.2.4 Good Samaritan calls

A Good Samaritan call is an E-call made by a person that witnesses an incident, but is not directly involved to help the persons directly involved. So called “Good Samaritan” calls constitute a problem, since they cause overload and information diversity at the PSAP side.

5.3 Calls where an Emergency service is not required

The reduction of the number of false or accidental calls is essential if emergency services are not to be deployed inappropriately. If an emergency service is sent to an incident where they are not required or to respond to a false call, they may not be available to respond to a genuine call which may put lives at risk. Because of these facts it is necessary to give some requirements on this problem.

False calls can be due to different factors, some related to the user (e.g. accidental activation because of a non adequate HMI) and some other related to the system itself (the failure of one or more sensors inside the vehicle).

5.3.1 Reducing the number of accidental/false calls

Minimising the number of false or accidental activations of the system is vital if the unit is to have credibility, and to make effective use of the emergency service response. While the emergency services are responding to a false or accidental activation, they will not be available for a genuine emergency. This may result in loss of life or more serious injury.

To minimise false or accidental activations:

- The E-call button should be positioned where accidental pressing is unlikely.
- The E-call button should alert the driver either visually or audibly that it has been activated.
- The E-call button should be held down for 2 seconds before activation is confirmed.
- Any other Service call button should be located sufficiently far away from the E Call button to prevent a false or mistaken activation.
- The E-call system should have the ability to cancel a call within 6 seconds to undo an accidental activation.
- The E-call system should alert the driver if it has been automatically activated by vehicle sensors.

To prevent or minimise the occurrence of false calls caused by the failure of a sensor:

- The E112 call should only be generated automatically if one or more sensors of the list below is activated.
- The E-call system should alert the driver if an attached sensor fails (5.6.6 IVS self-check capabilities).

5.4 Triggers for an automatic E-call

The IVS has to be able to provide to the PSAP/SP with the necessary information for them to determine the vehicle status. This information can be obtained from the different vehicle sensors present, which allow for the monitoring of the vehicle status after the accident.

5.4.1 Appropriate Sensors to trigger an automatic E-call

It is recommended that the following sensors should be able to trigger an automatic E-call:

- Airbag
- Crash sensor rear
- Crash sensor front
- Crash sensor side
- Roll over sensor
- Temperature sensor (fire)

5.4.2 Dealing with single sensor activation

If a single sensor activates, the *minimum set of data* is sent to the PSAP who can use a voice call to verify whether the activation requires an emergency response or other assistance. For example, a low speed crash may trigger the deployment of an air bag. The driver is uninjured, no criminal offences are disclosed, and no other party is injured. There is no requirement for an emergency service response, although the driver may require added value services.

5.5 Storage of parameters

In order to review the accident history, the following parameters could at least be stored in the IVS.

- The button push or sensors activations that triggered the call
- GPS positions
- Time stamps
- Self-check parameters
- Battery power status

The minimum set of data could also if possible and desirable be stored locally permanently (in non-volatile memory).

5.6 Redundancy

The IVS should be provided with redundancy for external components such as those described in the sections below. In case of a crash, external system components and the connections (optical and electrical) to those components will be the most likely to be damaged.

5.6.1 Antennas

An IVS equipped with an external antenna should also be provided with some type of internal antenna that can be used when the external antenna is out of order. The IVS should determine whether the antenna switch is necessary or not. The switch time should be short. The built-in back-up antenna should be a dual-band (900/1800 MHz band) antenna.

5.6.2 Battery

When the power from the main battery is lost when an E-call is requested, the IVS should be powered from a back-up battery. The talking time is limited when the back-up battery is used, and varies according to the power consumption required by IVS and the ambient temperature. It should be possible to talk for at least 10 minutes in “normal” circumstances.

5.6.3 Crash proof system

The IVS should be placed in a location as safe for exposure to pressure and damage as possible.

5.6.4 Microphone and speaker

The IVS should be equipped with an internal microphone and speaker as back-ups for the external ones. These should automatically be switched to if an E-call requires it.

5.6.5 Embedded SIM card

If the SIM card is located externally, there should be one internal back-up SIM-card.

5.6.6 Self-check

To avoid permanent failures of the system itself, and not only of the sensors and external components, the IVS should have self-check capabilities. If possible, the IVS should report failures to the HCC, or at least indicate to the driver that the system is in degraded mode.

5.6.7 Standard automotive requirements

The automotive requirements are more extensive than the consumer ones. To be compliant with the automotive standards, the devices must meet the following requirements:

- Extended operating temperature range from – 40° to + 85° Celsius.
- Low power consumption (single 12V general supply).
- EMC regulation compliant
- Functioning at high speed
- Software stability (no user input resulting in system hang-up)
- Integration with the on-board electronic system
- Fire-proof for 15 min (open flame)
- High reliability (e.g. tested in all possible car environments)

The IVS should be compliant with these requirements in order to guarantee a minimum functionality, also after an accident.

5.7 Communication attributes

5.7.1 Communication flow

The following criteria are taken into account to evaluate wireless networks for emergency services.

5.7.1.1 European coverage

The geographical coverage of the wireless network should include the European countries.

5.7.1.2 Priority

Priority means the ability to prioritise data: "emergency" data should be sent before other types of data in the wireless network.

NOTE: Mobile services in GSM/GPRS networks are *generally* prioritised in the following order (from highest to lowest priority):
1. Emergency voice call
2. Ordinary voice call
3. GSM data call
4. GPRS data call
5. SMS.

5.7.1.3 Reliability

Terminal communications should be reliable. Reliability means the probability of a successful transfer of data, e.g. the avoidance of data loss.

5.7.1.4 Confirmation

Confirmation means the possibility for the terminal to receive a confirmation that the recipient of a message has received the data. In this case, the recipient of the message is the telecom operator.

5.7.1.5 Timing

Timing means the difference between the time stamp "sent" by the terminal and time stamp "received" by the telecom operator.

5.7.1.6 Remarks

Remarks mean any extra remarks with an effect on the choice of bearers for wireless emergency services.

5.7.1.7 Overview 2003.03.07

	European Coverage	Priority	Reliability	Confirmation	Timing	Remarks
GSM-SMS	very good	no	very high	yes	< 5s	suitable for small amounts of data
GSM-Data	very good	yes/no*	high	yes/no*	5-30s	highly network-dependent
GPRS	good	yes/no*	medium	yes/no*	5-10s**	suitable for small amounts of data
UMTS	n/a	yes/no*	very high?	yes/no*	?	positioning is integrated in the standard

*) Priority depends on what the terminal requests and the network supports
**) Typical values, much higher delays may be experienced

5.7.2 Data transmission via GSM-SMS

In this section we evaluate GSM-SMS according to the communication criteria explained in the previous sections.

5.7.2.1 European Coverage

European Coverage is close to 100 % in western European countries.

5.7.2.2 Priority

There is no possibility to prioritise between different SMS messages.

5.7.2.3 Reliability

GSM-SMS offers a very high reliability. This is due to the low risk of congestion (limited network resources needed), low bit error rates (radio bearer for SMS is well protected) and the short session duration.

5.7.2.4 Confirmation

An acknowledgement is always sent to the terminal when the network has successfully received an SMS. Optionally, the terminal may also receive an acknowledgement when the SMS has been delivered to the final recipient (must be requested by the terminal when the SMS is sent).

5.7.2.5 Timing

The terminal-network transfer time is usually less than 5 seconds.

5.7.2.6 Remarks

- SMS is a widely used and preferred wireless bearer for safety services today.
- SMS is suitable for small amounts of data (in the order of a few hundred bytes).
- The service is heavily standardised with few optional features, which makes its behaviour in different networks highly predictable.

5.7.3 Data transmission via GSM data channel

In this section we evaluate GSM data channels according to the proposed communication criteria.

5.7.3.1 European Coverage

The coverage of GSM data channels is close to 100 % in western European countries.

5.7.3.2 Priority

GSM data calls can be prioritised using the "enhanced Multi-Level Precedence and Pre-emption (eMLPP) service". However, support of the eMLPP service is only a network option.

5.7.3.3 Reliability

The level of reliability depends on what type of data calls the terminal requests (low or high reliability call). High reliability calls may however not be supported by the network.

5.7.3.4 Confirmation

The network will send acknowledgements if a high reliability call is requested (see 'Reliability' above). There are no acknowledgements for a low reliability call.

5.7.3.5 Timing

There is always a delay due to the initial call establishment phase. This delay varies depending on what type of data call the terminal has requested, and what type of data calls are supported by the network. For small amounts of data (a few hundred bytes) the call establishment phase is in any case considerably longer than the actual data transfer phase.

Furthermore, there is a trade-off between reliability and delay. In case of a bad radio connection between the mobile and the network, a call with low reliability will not introduce any extra delays while a call with high reliability can introduce substantial delays.

5.7.3.6 Remarks

- GSM data is suitable for larger amounts of data (in the order of kilobytes).

- The overall 'behaviour' of a GSM data call can vary very much depending on the network operator. A data call with certain requirements can work perfectly fine in Network A, but not even be allowed in Network B.

5.7.4. Data transmission via GPRS

5.7.4.1 European Coverage

Most European GSM operators also offer GPRS. The geographical coverage, if a network offers GPRS, most often coincides with the geographical coverage of GSM. Note though that roaming capabilities are still limited (as compared to GSM).

5.7.4.2 Priority

There is a possibility of prioritising between GPRS calls using four so called 'radio priority levels'. However, the exact usage of these radio priority levels depends on the network operator.

5.7.4.3 Reliability

The level of reliability depends on what type of GPRS call the terminal requests. There are a number of reliability levels defined, but a network operator need not support all of them.

5.7.4.4 Confirmation

Whether acknowledgements are sent from the network to the terminal or not depends on the level of reliability requested (see 'Reliability' above).

5.7.4.5 Timing

The time it takes to transmit a chunk of data from the mobile to the network depends on many factors. Some of the most relevant are:
- Whether the network operator prioritises voice calls over GPRS calls
- How many active GPRS calls there are in the area
- What type of GPRS call the terminal has requested

5.7.4.6 Remarks

- GPRS is suitable for the transfer of both small and large amounts of data, as long as there are no strict delay requirements.

- The 'success rate' when trying to establish a GPRS call can vary significantly. This is due to the fact that GPRS is normally offered as a 'background' service using any network capacity that happens to be free at the moment. In many networks, a GPRS call will be disconnected in favour of a voice call or a GSM data call.

- Vodafone GPRS roaming, for example, is available to UK customers in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Hong Kong, Ireland, Italy, the Netherlands, Portugal, Spain, Sweden and Switzerland.

5.7.5 Data transmission via UMTS

5.7.5.1 European coverage

There are only a number of telecom operator test sites available at the present. No services on UMTS are offered to the public yet.

5.7.5.2 Priority

The national recommendations regarding these are currently about to be formulated. But there are large technical possibilities for prioritising emergency calls in the UMTS wireless network.

5.7.5.3 Reliability

According to standardization documents, UMTS will be able to guarantee a wide variety of strict Quality of Service requirements. This includes requirements on priority, reliability, confirmations and timing.

5.7.5.4 Confirmation

See ‘Reliability’ above.

5.7.5.5 Timing

See ‘Reliability’ above.

5.7.5.6 Remarks

All data services discussed in this document will be supported in UMTS networks as well, but with a better control over reliability and timing. Furthermore, positioning services are an integral part of the UMTS ‘package’. The standardisation documents also specify more advanced data services that might be a better/safer option than any of the data services discussed.

However, as there are no large-scale public UMTS networks in operation, it is difficult to say what will actually be *supported* by network operators in the near future.

5.7.6 Number triplets / IP addresses

5.8 Conclusion

This chapter presented an overview of the requirements and recommendations for an In-Vehicle System. The requirements for a user-friendly Human Machine Interface were discussed, as well as provisions for false emergency calls, automatic E-call triggering, equipment failure and data storage. Finally, each of the available wireless communication technologies was evaluated in terms of coverage, prioritisation capabilities, reliability, confirmation possibilities, and timing.
In the next chapters, the nature of the data transported over these networks is discussed. Chapter 6 will deal with the minimum set of data sent from the IVS to the PSAP, while chapter 7 will cover the full set of data sent from the IVS to the SP.

6. Specification of In Vehicle System data (minimum set of data) to be forwarded to PSAP in case of an E-call

6.1 Introduction

This document describes the minimum set of data that must be sent from the vehicle in case of an emergency call. This data is to be sent from the vehicle via the Telecom operator using different data transmission ways to the PSAP. The information elements in the minimum set of data have been selected on the basis of their relevance in an emergency rescue situation. This means that the minimum set of data described below is required to speed up and improve the response by a rescue service.

6.2 Information Elements

The following information elements are of interest in an emergency situation. These information elements are specified according to the **Telematics Forum, Global Telematics Protocol (GTP), Encoding Specification, 21 March 2003, Version 1.0** The references in the data table can be found in the **(GTP), Encoding Specification, 21 March 2003, Version1.0, see Annex A.**

6.2.1 Use Case Header

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (6)**
Use: Defines the actual subset of the use case.
Example: Version 1.0 (6.1 – 6.8)
Page: 15-16

6.2.1.1 Privilege

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (6.5)**
Use: Authorization levels.
Example: Version 1.0 (6.5) table 8 privilege levels bit number 1 highest privilege
Page: 16

6.2.2 Version element

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.3)**
Use: Defines Car manufacturer, Terminal ID, Software and Hardware release.
Example: Version 1.0 (22.3 and 22.3.3)
Page: 60, table 38: Version element encoding Octet\Bit 2 car manufacturer
Page: 60, table 39: Manufacturer ID Definitions

6.2.3 Time Stamp (PSAP use)

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.26)**

Use: Defines the time when the accident message was generated.

Example: 2002-11-27 19:45.21 Version 1.0 (22.26.1 up to 22.26.6)

Page: 78-79

6.2.4 Location (PSAP use)

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.10, 22.11, 22.12 and 22.19)**

Use: Defines the location of the vehicle in Lat, Long according to WGS84.

Example: N52 45.0010 E005 10.2250 (Earlier 1.2.1 GPS position)

Page: 63, 22.10 Location

Page: 63, 22.11 Best available position

Page: 69, 22.19 Current dead reckoning

6.2.5 Direction (PSAP use)

Description: Direction of travel derived from the last three GPS positions with a 30 meters interval. **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.17 and 22.18)**

Use: Defines in which direction the vehicle involved was moving.

Example: Version 1.0 (22.17 and 22.18 value ½)

Page: 68, 22.17 Area Location Way Point Coding

Page: 69, 22.18 Distance Flag

6.2.6 Vehicle Descriptor

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20)**

Use: Defines the Colour, Model, VIN, Terminal number and license plate of the car, allowing the rescue personnel to identify the vehicle involved in an accident.

Example: Version 1.0 (22.20.1 up to 22.20.8)

Page: 70 – 72 Table 56: Vehicle Descriptor

6.2.6.1 Model year (PSAP use)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.2)**

Use: Defines the model year for the vehicle. 2 Digits are sufficient to specify the year.

Example: version 1.0 (22.20.2)

Page: 70

6.2.6.2 Vehicle colour (PSAP use)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.6)**

Use: Defines the vehicle colour by means of a text string.

Example: Version 1.0 (22.20.6)

Page: 71

6.2.6.3 Vehicle model (PSAP use)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.7)**
Use: Defines the make and model of the vehicle.
Example: Version 1.0 (22.20.7)
Page: 72

6.2.7 E-call Status (PSAP use)

Description: The source of the emergency call and the number of triggers, which includes manual triggers, as well as sensor triggers: airbag, rollover, crash sensors. According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.21)**
Use: Information for the emergency operator, allowing him to dispatch rescue service(s).
Example: Version 1.0 (22.22) bit 3 set indicates the activation of an airbag.
Page: 73

6.2.7.1 Breakdown source (E-call data), (PSAP use)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.22.)**
Use: Table 67: Breakdown Source
Bit 1 manually activated
Bit 2 vehicle rolled over
Bit 3 airbag activated
Bit 4 crash sensor activated
Table 68: Breakdown Source extended octet
Bit 3 Vehicle has moved
Example: Version 1.0 (22.22.)
Page: 74

6.2.7.2 Breakdown Recognition Flag (E-call data), (PSAP use)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.23.)**
Use: Table 69-breakdown sensor
Bit 6-fuel type is gaseous
Table 70-breakdown sensor extended octet
Bit 3 manual panic alarm
Bit 7 manual E-call alarm
Example: Version 1.0 (22.23.)
Page: 75

6.2.8 Service Provider Identifier (PSAP use)

Description: Should be the fixed IP address of each SP formatted with 4 bytes, IPV4, rasp 4 quads.
Use: The use of Ipv6 as defined by the Internet Engineering Task Force (IETF) should be considered when implementing these specifications.
Example: 193.96.28.72
Page: not realized yet by GTP

6.2.9 Service Provider telephone number (PSAP use)

Description: Should be an internal toll-free number for the SP with 13 digits.
Use: This number is used be the PSAP organization across Europe to contact the SP in case an E-call language problem needs to be solved via a conference voice call between customer, country-specific PSAP and HCC / SP provider
Example: 00800 – 123 45 678
Page: not realised yet by GTP

6.2.10 Country code (PSAP use)

Description: Should be the international country indicator with a maximum of 3 characters.
Use: This code is used to identify the home country of the vehicle.
Example: D = Germany, SW = Sweden, SLO = Slovakia etc.
Page: not realised yet by GTP

6.3 Priority

Depending on the carrier (SMS, GPRS etc) used for sending the information elements the available amount of data will vary and hence there is a need for prioritisation between the information elements to make sure that the most important data is sent. When the data limit is reached the remaining information elements will not be considered. The priority of the data decided by the E-MERGE consortium is as follows:

1. GPS Position
2. Direction of travel
3. Number of triggers of the call
4. Colour, make, model of the vehicle
5. Which sensors are triggered: airbag, roll-over, front crash, side crash or rear crash sensor
6. Time stamp of the event

6.4 Minimum set of data standard

The data specified is the minimum set of data to be sent from the vehicle in order to comply with the proposed E-MERGE standard.

6.5 Message Structure

6.5.1 Emergency call request message

Description: The Terminal to request the emergency service sends this message. **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (7.3.1.)**
Example: Version 1.0 (7.3.1)
Page: 18, Table 10

6.5.2 Emergency call reply message

Description: The message is a reply from the PSAP, which sends this message to the terminal. **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (7.3.2.)**
Example: Version 1.0 (7.3.2)
Page: 19, Table 11

6.6 Conclusion

This chapter, chapter 6, has provided a detailed insight in the minimum set of data expected by a PSAP. It should be stressed that, to be fully E-MERGE-compliant, all the data items listed in 6.3 should be present and made available to the PSAP. As a result, the PSAP gets a detailed image of the nature of the accident, and any possible casualty involved. Emergency teams can then response to the accident in a significantly shorter time frame and, as a consequence, with a higher level of success.

The next chapter 7 extends this minimum data set with additional information, which can be sent from the vehicle via a HCC, to whom the driver has a contract with, to the PSAP in order to improve even more the emergency response.

7. Specification of full set of data to be made available by service providers / HCC to PSAPs in case of an E-call

7.1 Introduction

The minimum set of data defined by chapter 6 is used by the PSAP to get an initial and maybe sufficient identification of an emergency event. However, if the minimum set of data is not sufficient or in case that the PSAPs would need a more detailed insight of the incident and potentially involved actors and relatives a second set of data, in this chapter referred to as the 'full set of data' is transmitted from the vehicle to an HCC and there made available for the PSAPs. The following paragraphs define the content of this full set of data.

7.2 Information Elements

The following information elements are those of interest in an emergency situation. These information elements are specified according to **Telematics Forum, Global Telematics Protocol (GTP), Encoding Specification, 21 March 2003, Version 1.0, Annex A and (GTP)**, **Transport Protocol Encoding Specification, 12. November 2002, version 0.1, Annex B.**
The references in the data table can be found in the **(GTP), Encoding Specification, 21 March 2003, Version 1.0, see Annex A**

7.2.1 Use Case Header

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (6)**
Use: Defines the actual subset of the use case.
Example: Version 1.0 (6.1 – 6.8)
Page: 15-16

7.2.1.1 Privilege

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (6.5)**
Use: Authorisation levels.
Example: Version 1.0 (6.5) table 8 privilege levels bit number 1 highest privilege.
Page: 16

7.2.2 Version element

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.3)**
Use: Defines Car manufacturer, Terminal ID, Software and Hardware release.
Example: Version 1.0 (22.3 and 22.3.3)
Page: 60, table 38: Version element encoding \ Bit 2 car manufacturer ID
Page: 60, table 39: Manufacturer ID Definitions

7.2.3 Time Stamp

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.26)**
Use: Defines the time when the accident message was generated.
Example: 2002-11-27 19:45.21 Version 1.0 (22.26.1 up to 22.26.6)
Page: 78-79

7.2.4 Location

Description: According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.10, 22.11, 22.12 and 22.19)**
Use: Defines the location of the vehicle in Lat, Long according to WGS84.
Example: N52 45.0010 E005 10.2250 (Earlier 1.2.1 GPS position)
Page: 63, 22.10 Location
Page: 63, 22.11 Best available Position
Page: 69, 22.19 Dead reckoning data

7.2.5 Direction

Description: Direction of travel derived from the last three GPS positions with 30 meters interval. **GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.17 and 22.18)**
Use: Defines in which direction the vehicle is was moving.
Example: Version 1.0 (22.17 and 22.18 value ½)
Page: 68, 22.17 Area Location Way Point Coding
Page: 69, 22.18 Distance Flag

7.2.6 Vehicle Descriptor

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20)**
Use: Defines the Colour, Model, VIN, Terminal number, License plate of the car to allow the rescue personnel to spot the accident vehicle.
Example: Version 1.0 (22.20.1up to 22.20.8)
Page: 70 – 72 Table 56: Vehicle Descriptor

7.2.6.1 Model year

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.2)**
Use: Defines the model year for the vehicle.2 Digits are sufficient to specify the year.
Example: version 1.0 (22.20.2)
Page: 70

7.2.6.2 VIN

Description: International vehicle identification number according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.3)**
Use: Defines all manufacturer data for the vehicle.
Example: version 1.0 (22.20.3)
Page: 71

7.2.6.3 Terminal serial

Description: Terminal serial identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.4)**
Use: Defines the terminal serial number for the IVS.
Example: version 1.0 (22.20.4)
Page: 71

7.2.6.4 License plate

Description: License plate number parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.5)**
Use: Defines the license plate of the vehicle involved in the emergency.
Example: version 1.0 (22.20.5)
Page: 71

7.2.6.5 Vehicle colour

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0. (22.20.6)**
Use: Defines the vehicle colour via a text string.
Example: Version 1.0 (22.20.6)
Page: 71 and 72

7.2.6.6 Vehicle model

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 06 January 2003, Version 1.0 (22.20.7)**
Use: Defines the make and model of the vehicle.
Example: Version 1.0 (22.20.7)
Page: 72

7.2.6.7 IMEI

Description: The equipment GSM serial number identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.20.8)**
Use: Defines the GSM equipment available to the IVS.
Example: version 1.0 (22.20.8)
Page: 72

7.2.7 E-call Status

Description: The source of the emergency call and the number of triggers, which includes manual triggers as well as sensor triggers: airbag, roll-over. According to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.21)**
Use: Information for the emergency operator to be able to dispatch rescue services.
Example: to be written from GTP (Earlier 1.2.4 Triggers and 1.2.6 Sensors)
Page: 73

7.2.7.1 Breakdown source (E-call data)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.22.)**
Use: Table 67: Breakdown Source
Bit 1 manually activated
Bit 2 vehicle rolled over
Bit 3 airbag activated
Bit 4 crash sensor activated
Table 68: Breakdown Source extended octet
Bit 3 Vehicle has moved
Example: Version 1.0 (22.22.)
Page: 74

7.2.7.2 Breakdown Recognition Flag (E-call data)

Description: Vehicle identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.23.)**
Use: Table 69-breakdown sensor
Bit 2-Front sensor activated
Bit 3-Rear sensor activated
Bit 4-Side sensor activated
Bit 5-Vehicle Alarm activated
Bit 6-fuel type is gaseous

Table 70-breakdown sensor extended octet
Bit 1 hidden manual alarm
Bit 2 Remote control alarm
Bit 3 manual panic alarm
Bit 5 Distance alarm
Bit 6 Geographic region alarm
Bit 7 manual E-call alarm
Example: Version 1.0 (22.23.)
Page: 75

7.2.7.3 Breakdown data (E-call data)

Description: Additional descriptive data identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.24.)**
Use: Table 72-breakdown data type value
Value 3-Crash data
Table 74-Crash data type
Value 1-Crash intensity data
Example: Version 1.0 (22.24.1.)
Page: 76

7.2.7.4 Crash intensity data (E-call data)

Description: Additional descriptive intensity data identification parameters according to **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (22.24.1.1)**
Use: Table 75-Crash Intensity data
Octet \ bit 1
2

3
4

Example: Version 1.0 (22.24.1.1.)
Page: 77

7.3 Priority

The data shall follow the **(GTP)**, **Transport Protocol Encoding Specification, 12. November 2002, version 0.1, Annex B**. Depending on the carrier (SMS, GPRS etc) used for sending the information elements the available amount of data will vary and hence there is a need for priority between the information elements to make sure that the most important data is sent. When the data limit is reached the remaining information elements won't be considered. The priority of the data decided by the E-MERGE consortia is as follows:

1. GPS Position
2. Direction of travel
3. Number of triggers of the call
4. Colour, make, model of the vehicle
5. Which sensors that triggered, airbag, roll-over, front crash, side crash or rear crash sensor
6. VIN
7. Terminal Serial
8. License plate
9. IMEI
10. Breakdown (E-call) source
11. Breakdown (E-call) Recognition Flag
12. Breakdown (E-call) data
13. Crash intensity data
14. Time of the event

7.4 Maximum set of data standard

The data specified is the full set of data to be sent from the vehicle in order to comply with the E-MERGE standard.

7.5 Message Structure

7.5.1 Emergency call message request

Description: The Terminal to request the emergency service sends this message. **(GTP), Encoding Specification, 21 March 2003, Version 1.0 (7.3.1.)**
Example: Version 1.0 (7.3.1)
Page: 18, Table 10

7.5.2 Emergency call reply message

Description: The message is a reply from the PSAP sends this message to the terminal.
(GTP), Encoding Specification, 21 March 2003, Version 1.0 (7.3.2.)
Example: Version 1.0 (7.3.1)
Page: 19, Table 11

7.6 Conclusion

The full set of data sent to HCCs as defined within this chapter, is very similar to the minimum set of data described for the In-Vehicle data sent to the PSAP. The main difference remains the final target and use of the information. To be fully compliant with the specifications as defined by the E-MERGE consortium both the defined dataset of Chapter 6 and 7 should be provided by the IVS. Of these two chapters, the priority paragraphs (6.3 and 7.3) determine the minimum set of data, which should be provided by a IVS for both the minimal and full data set. It remains advisable to read these two chapters in concert with the GTP Protocol definition document mentioned in the previous paragraphs.

8. COMMUNICATION SPECIFICATIONS

8.1 Introduction

This document describes the communication protocol to be implemented in E-MERGE. The chapter starts with an analysis of the current available protocols and identifies the most interesting protocols available. The protocols considered are emergency-call oriented allowing a terminal to send as fast and efficiently as possible a minimum set of E-MERGE data to the PSAPs.

8.2 State of the Art

At the moment of writing various standardization organizations are defining protocols suitable for transferring emergency call oriented data. A lot of these standards have only a local, very often Country specific scope and, as a consequence, are not useful in an international context. Some of these standardization efforts however do indeed address a wider audience and could be candidates for a European wide implementation. The following paragraphs identify a few of these protocols and sketch the boundaries of their usability.

8.2.1 GTP Protocol

The Telematics Forum, more specifically a sub-group of this forum, the GTP WG, has started an effort to merge the ACP (application Communication Protocol) and the GATS (Global Automotive Telematics Standard) into a new protocol called the Global Telematics Protocol or GTP for short. ACP and GATS are the two leading protocols for telematics service delivery into the vehicle today. Both protocols have been optimised for telematics and have witnessed a rapid acceptance by the market. Today, almost all OEMs rely on one of these two protocols for their telematics solutions and several companies even use both. But as the value of telematics lies in the applications (customers do not care about which protocol is implemented in their terminal), the competition between ACP and GATS for market share has also been harmful.

8.2.1.1 Objectives

The main objective the GTP workgroup attempts to reach with the development and the implementation of GTP is to demonstrate benefits such as:

- One global OTAP (Over The Air Protocol) which reduces costs by simplifying OEM design tasks and increasing competition for components, systems and services
- Avoidance of spending resources in areas with little or no differentiation capabilities
- Enabling of customisation - thus differentiation - at the application and service level where the highest level of consumer recognition exists
- Ability to utilise the multiple bearers existing today such as AMPS, GSM, SMS, GPRS, UMTS, DSRC and WLAN without the need to make modifications to the applications
- Opportunity to build upon a proven system component with years of operation in commercial environments.

- Chance to utilise proven and desirable features of both the ACP and GATS standards.
- A scalable solution to provide what features the customer needs and will pay for today, without compromising possible upgrades in the future.
- Deployment of an open standard which protects current and future investments
- A telematics focused, and thus, telematics optimised implementation.

8.2.1.2 GTP protocol architecture

The scope of GTP is shown in the following figure. GTP is defined here as the "over the air protocol" to convey information between the central infrastructure, a private or public service access point for GTP message exchange, and the Vehicle Terminal, the In Vehicle System or IVS.

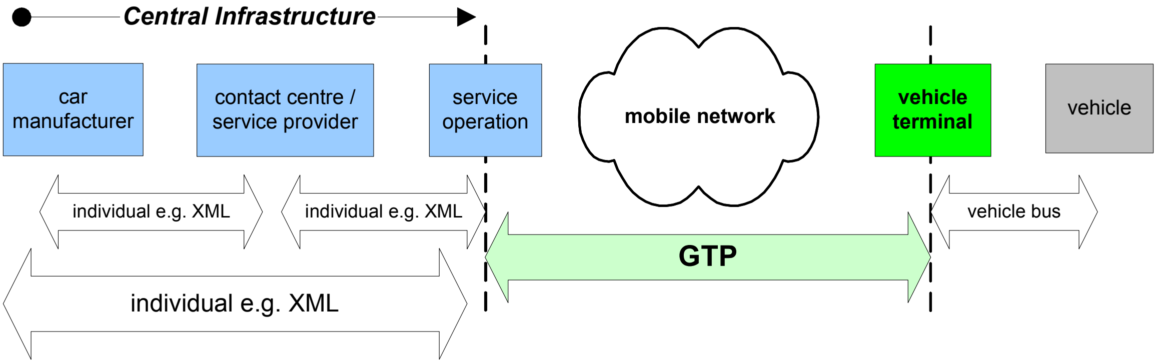


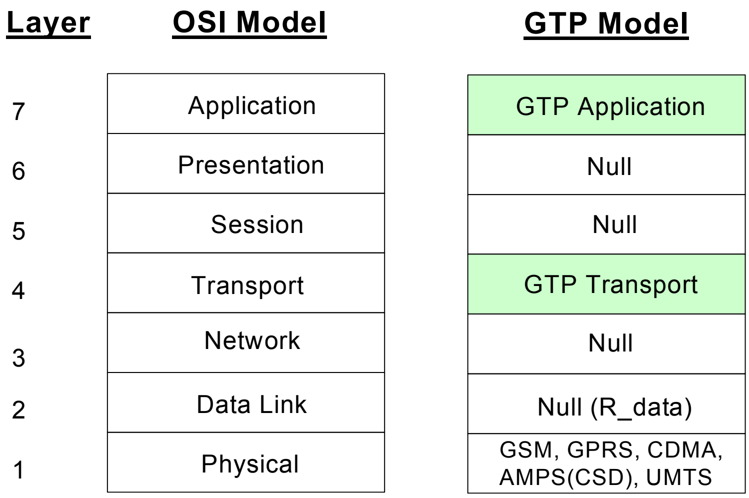
Figure 10: Overall Architecture of GTP Deployment

The protocols of GTP stacked up against the OSI 7 layer reference model is shown in figure 2 The GTP application layer protocol is used by the GTP applications to exchange information with peer GTP applications in another system component as shown in figure 3.

As an example: the Emergency application (application ID =1), which will be the specific subject of this analysis, is invoked in the vehicle. The application emergency application would use the E-call Message in the GTP application protocol suite to provide the appropriate information for the emergency, and to transfer the message down the GTP protocol stack.

The GTP Transport protocol adds its own headers to guarantee that the GTP application message is indeed transferred to the peer GTP application. The peer GTP transport layer will acknowledge receipt of the GTP application message back to the sender of the message. The GTP application message transfers up the GTP protocol stack in the peer and processed by the peer GTP application in the central infrastructure.

The OSI layered system looks much like an onion where each layer of the stack peels away its layer of the onion until, at the top level of the stack, the application layer finally consumes the pay-load data.



Layer	OSI Model	GTP Model
7	Application	GTP Application
6	Presentation	Null
5	Session	Null
4	Transport	GTP Transport
3	Network	Null
2	Data Link	Null (R_data)
1	Physical	GSM, GPRS, CDMA, AMPS(CSD), UMTS

Figure 11: OSI reference model and GTP

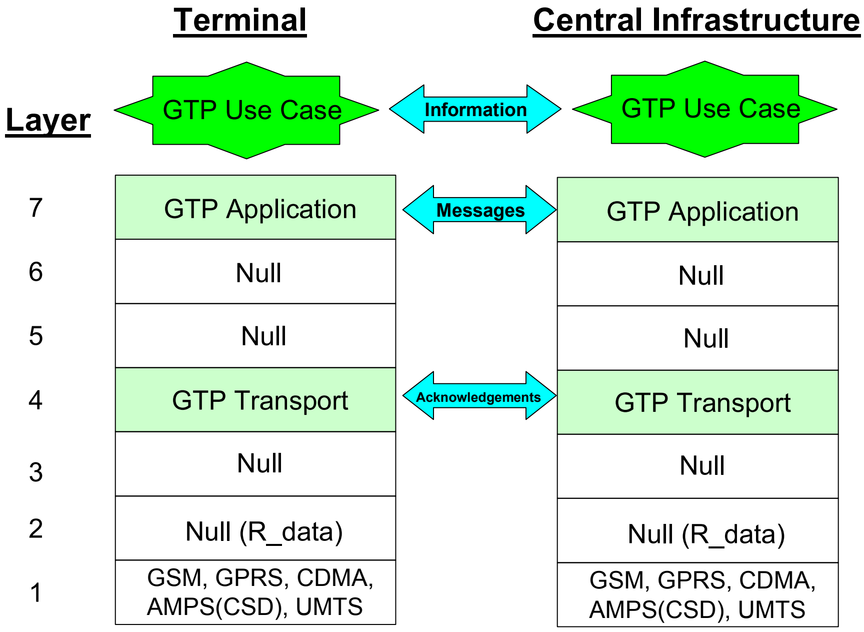


Figure 12: GTP application information exchange

8.2.1.3 GTP protocol structure

GTP is a versatile protocol, which formats information elements in meaningful messages. The basic unit of data is an information element that can be combined to form message types. These resulting message types are the atomic units used for transferring data by the transport layer.

The bits in an octet are numbered from 0 to 7 from the most significant bit to least significant bit. Multi-octet fields have the most significant octet in the in the first octet of the field. Packed decimal digits have the most significant digit in the first (Bits 0-7) of the first octet.

Generally the GTP protocol has adopted bit indicators, like the 'more' flag, which help to interpret the structure of a message. The more flag is used to indicate that an additional octet, providing an extension of information pertaining to this field, follows the actual octet. If the value is 0, then this is the last octet of continuous information before the next element. If the value is 1, then another information element octet follows this octet, as shown in the following example.

Octet \ bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	IE identifier		More Flag=0	Length (number of octets that follow)				

Octet \ bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	IE identifier		More Flag=1	Length (number of octets that follow)				
2	More Flag=0	Length						

Another indicator is the additional flag (Addl Flag), which is used to indicate when a similar element type is repeated in the successive octet. As a brief example: the GPS status provided by field A could have additional GPS status flags in fields A1 and A2. Thus the type of the element remains the same.

Octet \ bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	Addl Flag=1	Field A				Field B		
2	Addl Flag=1	Field A1				Field B1		
3	Addl Flag=0	Field A2				Field B2		

As explained above, an element is defined by a fixed sequence of bits. This fixed format record, either contains data parts, again in a pre-defined fixed format, or a 2 bit IE Identifier, More Flag, and length. The length field specifies the number of successive octets for the element that follow. If the number of follow-up octets exceeds 32, then the More Flag is set to extend the length field. An empty information element is one octet with a length field of zero.

The IE identifier can assume four different values:

- **0** - if transparent data (binary data) are used
- **1** - if text format (8 bits per character) is used
- **2** - if it consists of packed decimal
- **3** - for the extended definition

8.2.1.3.1 Application Header

Each message between the IVS and Central Infrastructure contains an application Header defined in the table below.

Octet \ bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1	Reserved Set to 0	Private Flag	Test Flag	Message Type				
2	Addl Flag=1	Version			Message Control Flag			
3	Addl Flag=0	Scenario Number				Privilege		
4…5	Message Length							

The message type field is unique for a specific message. If a message is constructed with a unique combination of message elements then that message will have a unique message type. The definition of the message is defined by the application. If the *Private Flag* is set, then this message type is a custom message. If the *Test Flag* bit is set, then this is an application test message.

The Version field represents the version of the application as defined by the application. This allows the application to be revised and identified independent of the overall GTP version number. This field is used when subsets or super sets of the same application are defined.

Message Control Flag defines various actions that are common over many applications, as shown in the following table.

Bit number	**Definition**
0	Reserved, set to 0
1	1=A GTP message is buffered at the Central Infrastructure 0=No GTP message is buffered at the Central Infrastructure
2	1=The Message Length field is 16 bits 0=The Message Length field is 8 bits
3	1=Application message response is expected 0=Application message response is not expected

Bit 3 indicates the sender is expecting an application message response message from the receiver.

The GTP scenario number indicates which transaction scenario is being used for this application, in other words which sequence of one or more GTP messages is used in one invocation of a GTP application. The scenario numbers are unique within an application. In the specific emergency call application scenarios are defined as follows:

- *Scenario 1*: assumes that a voice call is then established with the Central Infrastructure so that the Central Infrastructure can determine the nature of the emergency and take appropriate action. When the IVS requires a reply message, it should set the response expected flag, the message control flag is set 3, to get the emergency call reply message (Scenario 2) with the phone numbers. Otherwise, the voice call can be initiated immediately.
- *Scenario 2*: an emergency call message, triggered by a vehicle event, is sent from the IVS to the central infrastructure. The central infrastructure then sends an application layer reply back to the IVS to confirm message receipt. The central infrastructure then dispatches the appropriate services. The IVS then initiates a voice call to the central infrastructure in the same communication way.
- *Scenario 3*: This scenario adds an emergency terminate message so that the IVS can reliably end the emergency call session.

Privilege is intended to indicate the authorisation level of the customer initiating an application. Service will be denied if the user does not have the proper authorisation level.

The message length field can have values from 0 to 255 octets. If this field is defined as 16 bits, then the range is from 0 to 65,535. The message length is the total number of octets in the message not including the header or the message length octet.

Private flag indicates if the application message has been defined yet in the GTP protocol, or it is a proprietary message.

If the Test Flag value is 0, then this application message is to be acted upon. If the value is 1, then this application message is a test message and action is dependent upon the implementation.

8.2.1.3.2. GTP Emergency Call Application

The "Message Type" field defines the emergency call message set. If the message type value is 1, the message is an emergency call request, if the value is 2 the message is identified as an emergency call reply and if the value is 4 the message type identifies an E-call terminate message.

When the IVS requests an emergency service it sends the following type of message.

Octet \ bit	0	1	2	3	4	5	6	7
1 - 3	Application Header (see 2.1.3.1)							
4 - 8	Version (see 2.1.3.3)							
9 - 12	Time Stamp (see 2.1.3.3)							
13 – n-1	Location (see 2.1.3.3)							

n – m-1	Vehicle descriptor (see 2.1.3.3)	
m – k-1	Emergency status (see 2.1.3.3)	
k – i-1	More Flag	Length of Information Types
i – j-1	Information Type 1	
z – h-1	Information Type n	

At a minimum, the IVS must provide the central infrastructure with the date, time, location, vehicle description, and breakdown status. The breakdown status may give insight as to nature of the call and help response units to better equip themselves. The vehicle may or may not have the ability to support the optional fields. In the event the vehicle does support the detection of the optional fields, the IVS shall report them.

Remark:
In the language use of E-MERGE, the breakdown status has to be used as e-call status. An accordingly change request has been made to the GTP working group.

The vehicle shall set the length of the optional fields to 0 (zero) otherwise.

The information type field can be used to convey additional information contained by an Emergency call. This field specifies the type of information that the end user may request.

The following step consists of a reply message sent from the Central Infrastructure to the IVS confirming receipt of the emergency assistance request. The Reply Message may also be used to ask for a confirmation of the current location of the vehicle. This is managed by setting the appropriate bits in the E-call control flag2 field. The structure of the reply message is the following:

Octet \ bit	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1 - 3	Application Header (see 2.1.3.1)							
4 - 8	Version (see 2.1.3.3)							
9	Confirmation				Transmit Units			
10	EcallControlFlag2							
10 – j	Error Element							
j – z-1	More Flag	Length of Phone Number/Transmit Interval Pairs						
z – k-1	More Flag	Reserved	Transmit Interval 1					
k – n-1	Phone Number 1							

n+1 – i-1	More Flag	Reserved	Transmit Interval N
i – h-1	Phone Number N		

The central infrastructure in response to the emergency call request sends this message. It is used to inform the IVS whether or not the emergency request can be processed. If the emergency notification cannot be processed, then it specifies information allowing the IVS to proceed to its next course of action.

Some of the possible reasons for rejection are:

- The vehicle is in a country different from the SO
- The vehicle is not authorised for the service at this SO
- Use alternate SO

The transmit interval and phone number are always paired. The transmit interval is the number of transmit units to wait before re-sending the message to the phone number. It is possible to dynamically change the transmit interval of the currently used phone number by providing a new interval with a null (empty) phone number. This is used to dynamically modify the transmit interval times of the phone numbers typically during tracking.

To inform the IVS that the Central Infrastructure has terminated the voice call and the IVS should resume prior activities, the Central Infrastructure uses the following type of message.

Octet \ bit	0	1	2	3	4	5	6	7
1 - 3	Application Header (see 2.1.3.1)							

8.2.1.3.3. Emergency Call Data set

The following paragraph provides a description of the emergency call data set, described as IE Identifiers, implemented in the GTP protocol.

- Version element contains information about the car manufacturer, the IVS manufacturer, the current version of the installed hardware and the current version of the implemented software.
- The time stamp is encoded as UTC time and it is the time at which the triggering event in the IVS occurred.
- Location regards the position history of the vehicle and the entries are ordered from the most current to oldest.
- Vehicle descriptors are the VIN, the terminal serial number that identifies the wireless device consumer, the vehicle colour, the vehicle model the license plate and the IMEI of the wireless equipment.

- Emergency status identifies the nature of the emergency, including information about the source (manually activated or sensors triggered), the sensors that have initiated an automatic detected emergency and the breakdown data such as crash data.
- Confirmation element represents the confirmation status of an assistance reply message.
- Transmit units element specify the interval at which an emergency call message is sent on a regular basis, in order to track a vehicle.
- E-call control flag 2 defines additional control functions in the E-call message.
- Error element IE identifier may be either binary or text and include the nature of missing or invalid information in the message.
- Each phone number element is variable in length with the number of digits of the phone number defined by the length. If multiple phone number elements appear for a given application, it is up to the application to determine when and how to use them serially or concurrently. Norms or legal issues within a country may dictate the level of concurrency. In general the order that *Phone Number* elements appear specifies the order that the application shall attempt to use the specified bearers. The reserved octet is reserved as part of the country code. The presence of the reserved octet is dependent upon the control flag. The country code and the network code both contain leading zeros.

8.2.2. ETSI OCG-EMTEL

ETSI (the European Telecommunications Standards Institute), more specifically a sub-group of this, the OCG-EMTEL (Ad Hoc Group on Emergency Telecommunications), has started an activity of co-ordination between the various Standards Developing Organisations (SDOs), due to the recent resolutions in bodies such as the ITU Telecommunication Standards Advisory Group (TSAG), the Global Telecommunications Standards Collaboration (GTSC), the Asia-Pacific Standardisation Program (ASTAP) and various ETSI technical bodies (in relation to work on next generation networks) that highlight the need for a co-ordinated approach to emergency communications.

OCG-EMTEL is responsible for the horizontal co-ordination of emergency telecommunication standardisation activities within ETSI, which currently take place, in particular, in the following ETSI technical bodies:

1. Technical committee SPAN (International emergency preference schemes and multimedia services)
2. Technical committee SES (Satellite communications)
3. OCG SECURITY (Security)
4. Project TETRA (Mobile narrow-band and wide-band communications for public safety applications)
5. Project TIPHON (Emergency telecommunications services in IP based networks)
6. Partnership project MESA (Mobile broadband communications for public safety applications)
7. Partnership project 3GPP (Priority services and Location services for GSM and W-CDMA systems).

8.2.2.1. Objectives

The OCG EMTEL's primary role is to provide a lightweight horizontal co-ordination structure for issues related to the setting of requirements on ETSI deliverables.

The group shall concentrate on definition of requirements for:

- Communication of citizens with authorities/organisations in case of distress (emergency call handling).
- Communication between authorities/organisations during emergencies.
- Communications from authorities/organisations to the citizens during emergencies.

Giving consideration to issues such as network security, network integrity, the network behaviour in emergency situations and emergency telecommunications needs in networks.

The duties of the OCG EMTEL are:

- To co-ordinate the setting of emergency telecommunication requirements and undertake measures to efficiently continue and stimulate further co-ordinated work in this area;
- To identify relevant work outside ETSI, inform and stimulate appropriate activity in ETSI technical bodies;
- To provide mechanisms for the effective liaison between ETSI technical bodies, AIG, USER group and with external organisations such as local, national and regional government authorities, the EU commission, civil protection and disaster relief and emergency or security authorities/organisations, related activities in ITU, T1, TIA and other SDOs;
- To co-ordinate ETSI representation in external bodies such as GTSC (Global Telecommunication Standards Collaboration) on emergency telecommunication matters.

8.2.2.2 The ETSI protocol overview

The ETSI protocol as defined by this specification document comprises a wide set of standardization efforts and documents. In general, establishing of a new standard takes a few concise stages in the overall specification definition process. First a set of basic technical documents is generated which are approved and adopted by the ETSI technical body. These documents are:

- ETSI TS - The ETSI Technical Specification
- ETSI TR - The ETSI Technical report

In a second stage these basic standards are approved and adopted after voting by the members. The resulting documents are:

- ETSI ES – The ETSI Standard
- ETSI EG – The ETSI Guide

Finally the specification becomes a real standard after the approval by the Technical Body and is adopted, after voting, by the national standards bodies. The resulting document is referred to as the ETSI EN or ETSI European Standard.

ETSI already did publish a huge amount of documents and, as the market becomes more global structured many more are still to come.

For E-MERGE compliant operation a Telecom operator and a PSAP SHOULD comply to the different standards applicable to the communication between these parties.

Following ETSI requirements for communication of citizens with organisations for determining the location of an emergency caller using a mobile device the co-ordinates according to TS 101 109 V7.1.0 shall be indicated. When applying simple means only, the accuracy of location indication is linked to the size of the cell or the appropriate sector of a cell. The Cell ID together with optional additional information like Timing Advance will be translated into co-ordinates by the SMLC according 3GPP TS 03.71 (TS 101 724 V8.6.0) and transferred to the VMSC. To ensure that the location data are send to the same emergency centre to which the call is routed the VMSC adds additional information to the location data which identifies the appropriate emergency centre (e.g. the routing number used to route the call). Depending on the implementation of the interface between GMLC and the emergency centres (HTTP, TCP/IP, #7) the GMLC translates the routing information received by the VMSC into an appropriate addressable entity. In case of a ‘push service' the GMLC transmits the position data automatically to the appropriate emergency centre. It has to be insured that the position data are available at the emergency centre site within a specific time window after receiving the appropriate call.

In case of a more unlikely ‘pull service' the data are sent on request to the emergency centre. The request has to be based on the CLI of the emergency caller and the position data have to be available at the GMLC within a specific time window after the emergency centre has received the call.

The protocol layers of the interface between GMSC and emergency centre shall be implemented according LIF TS 101.

8.2.2.3 Mobile location protocol

The Mobile Location Protocol (MLP) is an application-level protocol for querying the position of mobile stations independent of underlying network technology. The MLP serves as the interface between a Location Server and a location-based application.

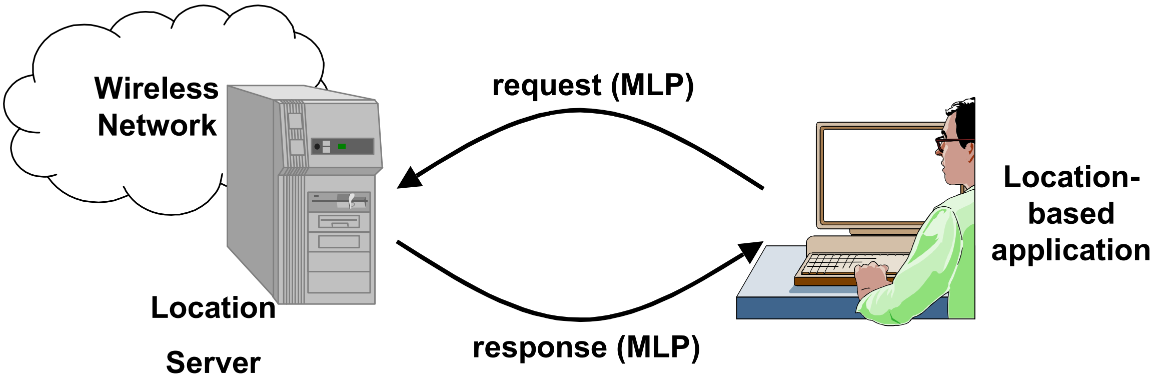
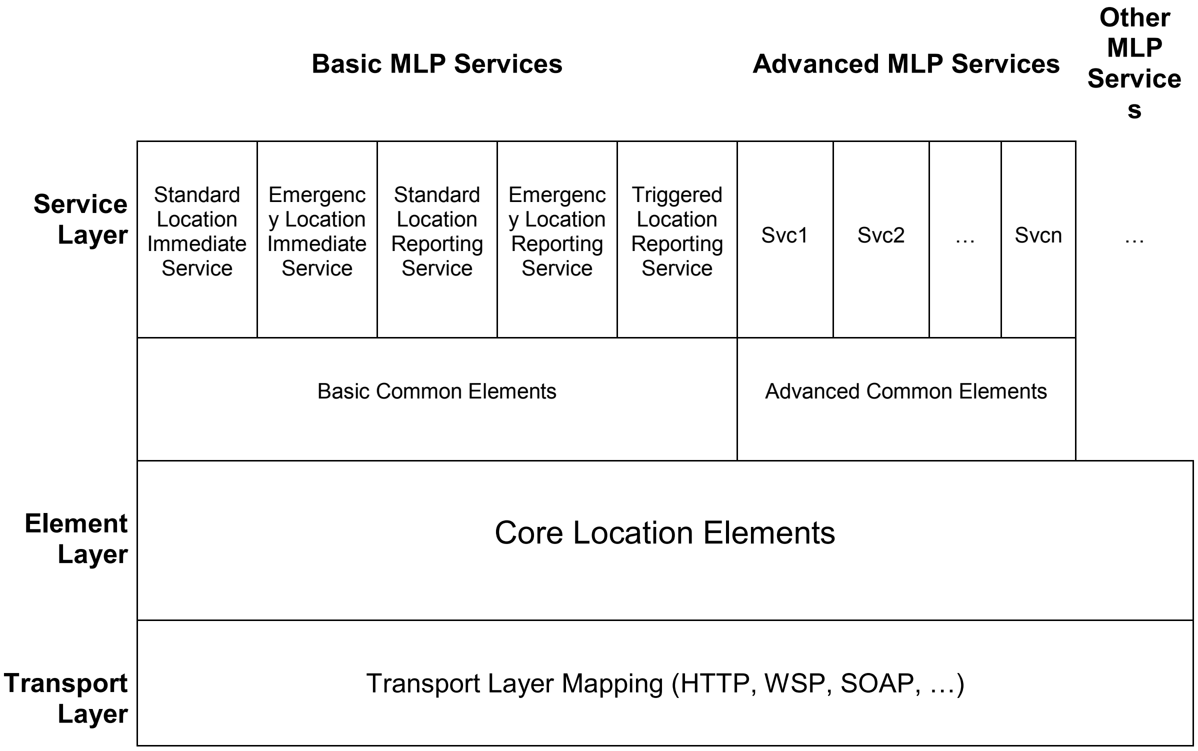


Figure 13: Mobile location protocol

Possible realisations of a Location Server are the GMLC, which is the location server defined in GSM and UMTS, and the MPC, which is defined in ANSI standards. Since the location server should be seen as a logical entity, other implementations are possible.

In the most scenarios an LCS client initiates the dialogue by sending a query to the location server and the server responds to the query.

In MLP, the transport protocol is separated from the XML content (as shown in the following table).


Basic MLP Services
Advanced MLP Services
Other MLP Services
Service Layer
Standard Location Immediate Service
Emergency Location Immediate Service
Standard Location Reporting Service
Emergency Location Reporting Service
Triggered Location Reporting Service
Svc1
Svc2
…
Svcn
…
Basic Common Elements
Advanced Common Elements
Element Layer
Core Location Elements
Transport Layer
Transport Layer Mapping (HTTP, WSP, SOAP, …)

At the lowest level, the *Transport Layer* defines how XML content is transported. Possible MLP transport protocols include HTTP, WSP, SOAP and others.

The *Element Layer* defines all common elements used by the services in the *Service Layer* which, at the same time, defines the actual services offered by the MLP framework. Basic MLP services are based on location services defined by 3GPP, whilst the advanced MLP services are additional. For E-MERGE project purpose most interesting Basic MLP Services are:

- **Emergency Location Immediate Service** is a service used especially for querying of the location of a mobile subscriber that has initiated an emergency call. The response to this service is required immediately (within a set time). This service consists of the following messages:
    - Emergency Location Immediate Request
    - Emergency Location Immediate Answer
- **Emergency Location Reporting Service** is a service that is used when the wireless network automatically initiates the positioning at an emergency call. The position and related data is then sent to the emergency application from the location server. Which

application and its address are defined in the location server. This service consists of the following message:

- Emergency Location Report

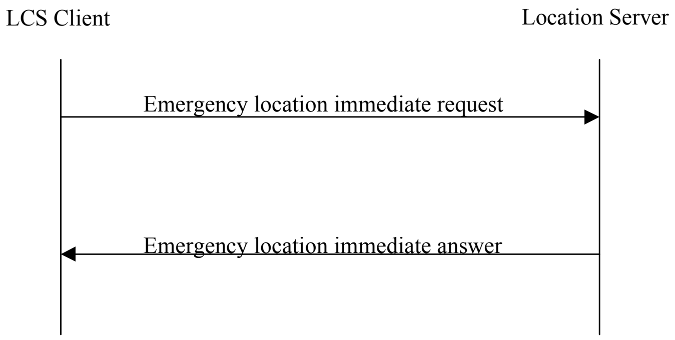
8.2.2.3.1 Emergency location immediate service

The emergency location immediate service is used to retrieve the position of a mobile subscriber that is involved in an emergency call or have initiated an emergency service in some other way.

The service consists of the following messages:

- Emergency Location Immediate Request
- Emergency Location Immediate Answer

The following message flow encapsulates this service:


LCS Client
Location Server
Emergency location immediate request
Emergency location immediate answer

8.2.2.3.1.1 Emergency location immediate request DTD

```
<!-- MLP_EME_LIR -->

<!ENTITY    % extension.param       "">
<!ELEMENT   eme_lir                 ((msids | (msid, gsm_net_param)+), qop?,
                                    geo_info?, loc_type? %extension.param;)>
<!ATTLIST   eme_lir
            ver CDATA               #FIXED "3.0.0">
```

8.2.2.3.1.2 Emergency location immediate answer DTD

```
<!-- MLP_EME_LIR -->

<!ENTITY    % extension.param       "">
<!ELEMENT   eme_lia                 ((eme_pos+ | (result, add_info?))
                                    %extension.param;)>
<!ATTLIST   eme_lia
            ver CDATA               #FIXED "3.0.0">
```

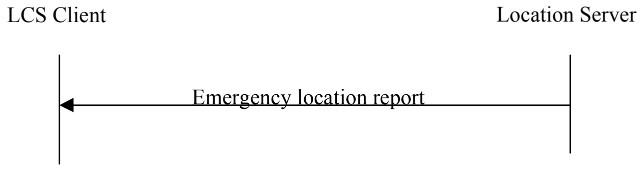
8.2.2.3.2 Emergency location reporting service

If the wireless network spontaneously initiates a positioning when a user initiates or releases an emergency call, an emergency location report is generated. The application(s) that the emergency location report should be sent to is defined within the location server. Data as required geographical format and address to application is also defined within the location server.

The service consists of the following message:

• Emergency Location Report

The following message flow encapsulates this service:



8.2.2.3.2.1 Emergency location report DTD

```
<!-- MLP_EME_LIR -->

<!ENTITY    % extension.param      "">
<!ELEMENT   emerep                 (eme_event  %extension.param;)>
<!ATTLIST   emerep
            ver CDATA              #FIXED "3.0.0">
```

For more details about elements and attributes in DTD please see Annex H "LIF TS 101 Specification"

8.2.2.4 Milestones

The availability of ETSI EMTEL protocol is expected at least by the date of application of the "*Universal service directive*", 25th of July 2003.

8.2.3 Location information and CGALIES

Location information is without any doubt one of the most important data elements presented to a PSAP. The coordination group on Access to Location Information for Emergency Services (CGALIES) estimates the lack of adequate emergency response due to location inaccuracy up to 3.5 million calls a year. Even worse, in 2.5 million cases the PSAP could not dispatch the required emergency service simply due to missing location info. Each year 40 million real emergency calls are sending from mobile devices. Automated and improved location information would greatly reduce the time lag for emergency service dispatching in all cases. The CGALIES final report version 1.0 identifies the relevant implementation issues related to the enhancement and improvement of emergency location in Europe.

8.2.3.1 CGALIES technology overview

The network architecture for location services (LCS) will comply with existing standards and will evolve with new standards as and when they are defined. In LCS two new network elements are necessary to provide Location Services.

1. Serving Mobile Location Centre (SMLC). This unit is responsible for the collection and co-ordination of all the necessary information in the network to give a position estimate of the mobile subscriber;
2. Gateway Mobile Location Centre (GMLC). This unit manages the external interface to LCS clients and Emergency service providers. It performs authorisation and privacy functions as well as provisioning and billing.

There is also a new optional unit called the Location Measurement Unit (LMU), which provides assistance data to the network for some location technologies (E-OTD and some implementations of A-GPS). The LMU can be deployed anywhere but typically would be deployed at a cell site and is co-ordinated from the SMLC.
The interface between the GMLC and LCS clients (Le interface) will be standardised and will support any standardised LCS technology. It is the Le interface that could be used for connection with the emergency services.

The network architecture for the emergency services network is diagrammed in the next figure. This is a generic view of the architecture, and meant as a reference. There may be localised variations, such as Primary and secondary PSAP operations being co-located.

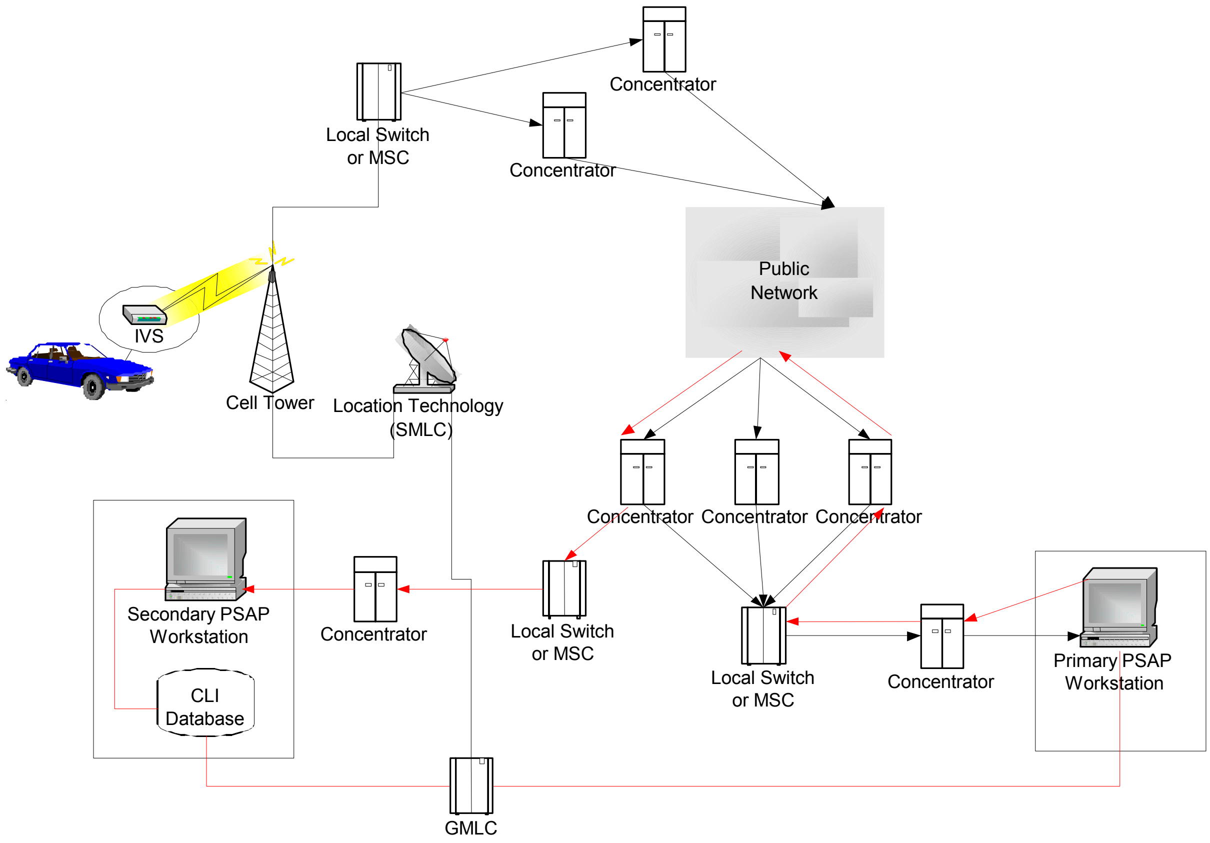


Figure 14: Network Architecture

The Call Flow on Mobile Network consists of the following steps:

1. Mobile network telephone dials 112.
2. The tower sends the call to the Mobile Switching Centre (MSC).
3. Call is forwarded to a concentrator to be sent to the PSAP on the public network.
4. Received by a local concentrator.
5. Forwarded to a local switch serving the Primary PSAP.
6. Forwarded to a concentrator for the Primary PSAP.

7. SMLC (or other methods of location) send location information to the MSC.
8. MSC forwards location information to the GMLC.
9. Call answered by Primary PSAP.
10. Location Information, if available, is requested by the PSAP from the GMLC.
11. Call forwarded to secondary PSAP for Dispatch Response.
12. When call reaches secondary PSAP, more refined location information, if available, is requested by the PSAP either directly from the GMLC or through the CLI database to the GMLC.

8.2.4 Other solutions

Waiting for the development of an official LIF standard or other ETSI/EMTEL solution to be adopted for emergency telecommunications some countries has already proposed nationwide specific solutions. These solutions are explained in Annex H.

To this running activities, which needs new infrastructure measures, should be checked following thoughts appendages from ETSI and their associated organisations and appraised due to the feasibility and realisation time.

8.2.4.1 DTMF – signalling in the voice channel

DTMF signalling is possible in principle and is used already long-time. The transition from the mobile network into the fixed network take place in the MSC's of the GSM provider. DTMF signalling can not be used for the data transmission of bigger volumes due to the realisation time per signal (circa 400 – 500 msec). DTMF can be used as reference for the PSAP. If DTMF is used, the PSAP can get knowledge, before the change data to voice based on the DTMF signal, that in an external data base are available further data.

8.2.4.2 Data transfer before utilisation of the voice channel by voice

This relative simple variant based on the usage and frequency of the air interface with 12 kbit/sec. An automatically switch in the IVS mobile set can be realised similar a fax preselector function. In the MSC occurs the frequency translation of 12 kbit/sec air interface over a transcoder to 64 kbit/sec.

8.2.4.2 User to user signalling

The utilisation of user to user signalling is defined as standard in the SCCP protocol ITUT-Q711-715.

Our approach for the widened usage user to user signalling based on the available and really used data volume in the USD string. The USD string has 272 bytes as standard. As per telecom regulatory authority are 256 bytes available. As per enquiry, will be used from the network provider, country specific varying, between 50 and 100 bytes. Thus give a available usage amount of circa 150 bytes. With 150 bytes availableness can be transmitted the IVS / E-MERGE minimum set of data as per our suggestion. On the side of the GSM network provider, this function will be supported by BSSAP. The transition into the fixed network takes place in the MSC. On the fixed network side, this function and availableness is defined and implemented in the standard ISUP 761-766.

8.2.4.3 Extended utilisation of user to user signalling

An interesting extended function on the protocol level and as standard ITUT – Q 737, execution 06/97 adopted, is the possibility to transmit data during the connection with a defined size of 128 kilobyte. ITUT – Q 737 "supplementary service" offers here three service categories. Interworking is guarantee, insofar the bidirectional utilisation also. On the GSM producer side, the function must be supported. Today it is not possible to give a statement over all GSM provider regarding to the implementation of this standard, as this standard is no duty.

8.3. Communication Architecture

Reminding that one of the scopes of the E-Merge project is to test and to implement new technology based protocol solutions, in the following there is a description of the communication architecture to be implemented in E-Merge concept, in order to reach the objectives of the whole project.

It is important to specify that the adoption of this architecture as a final solution to be implemented widely across Europe is strictly depending by the work and adoption E112 and the adoption of the GTP protocol. .

It is fundamental to specify that in this phase of the study, the E-Merge project is dealing uniquely with communication flows involving the IVS, the Telecom Operator and the PSAP, because the communication between the IVS and the Service Provider could use a proprietary communication protocol based on commercial agreements, but E-Merge takes a focus on SP operational procedure in order to make sure that the PSAP is able to access to SP additional data.

8.3.1. Communication flow

The communication flow between the actors involved in the emergency calls management chain, which is shown in the following figure 5, could be summarised in the following steps :

1. The IVS, the generating agent of the E-Merge call, sends the emergency call to a PSAP via voice channel, decomposed on two separate steps: the first one regards the data sending GSM / GPRS / UMTS technologies on a voice channel, whilst the second one is a pure 112 voice communication that uses the already opened voice channel. The data part of the call encloses the minimum set of data defined by the E-Merge project in the GTP protocol as a GTP E-Call Application. Data sending before a normal voice communication is established ensure the coverage also for those cases when the driver is not able to speak or the emergency call has been generated automatically by triggering the in-vehicle sensors.
2. The E-Merge call (data + voice) goes through the mobile network and is first handled by the TELECOM operator. The TELECOM Operator recognises that the call is an emergency call (voice + data). The TELECOM operator has the responsibility to enrich the call with the CLI (Caller Line Identification). At the same time the TELECOM operator has the duty to add the mobile location at a best effort principle into the Location Server Database. After the emergency call handling, the TELECOM Operator delivers the E-Merge call to the appropriate PSAP via the fixed line network.
3. The PSAP receives two different type of communication via the fixed line network on a common channel: the first one is data communication delivered in GTP protocol whilst the second one is a normal voice communication. The minimum set of data + CLI are delivered as transparent data together with the voice. At the same time the TELECOM Operator push the Mobile Location to the PSAP using the Mobile Location Protocol chosen within ETSI Workgroup.
4. The PSAP transmit an acknowledge of data received to the IVS and interpret GTP minimum set of data using a GTP interpreter.
5. In case the user is a subscriber of a private Service Provider (SP) the IVS sends a full set of data via TELECOM operator to SP, after receiving the acknowledge from the PSAP.

6. The SP receives the data message encoded with a proprietary protocol and it starts handling procedures, adding the additional E-Merge data in the E-Merge database in order to make these data available for the PSAPs.
7. The SP transmits an acknowledge of data received to the IVS.
8. If translation is needed the SP starts on PSAP request using a toll free number a conference call with the driver.
9. If the driver is also a subscriber of a SP the PSAP start management operation accessing at the E-Merge Database in order to get full set of additional E-Merge data directly from the SP.
10. The PSAP Operator elaborates the received data.
11. The PSAP Operator dispatches the emergency details to the most appropriate Rescue Centres.
12. In a second time the PSAP communicates to the SP the involved rescue centres, to allow the SP to be able to provide additional post-accident services. This communication could happens via fixed line network as a simple phone call between the operators, or via Internet. In this last case the PSAP Operator can access to E-Merge Database and put in all the available information about the involved Rescue Centres.

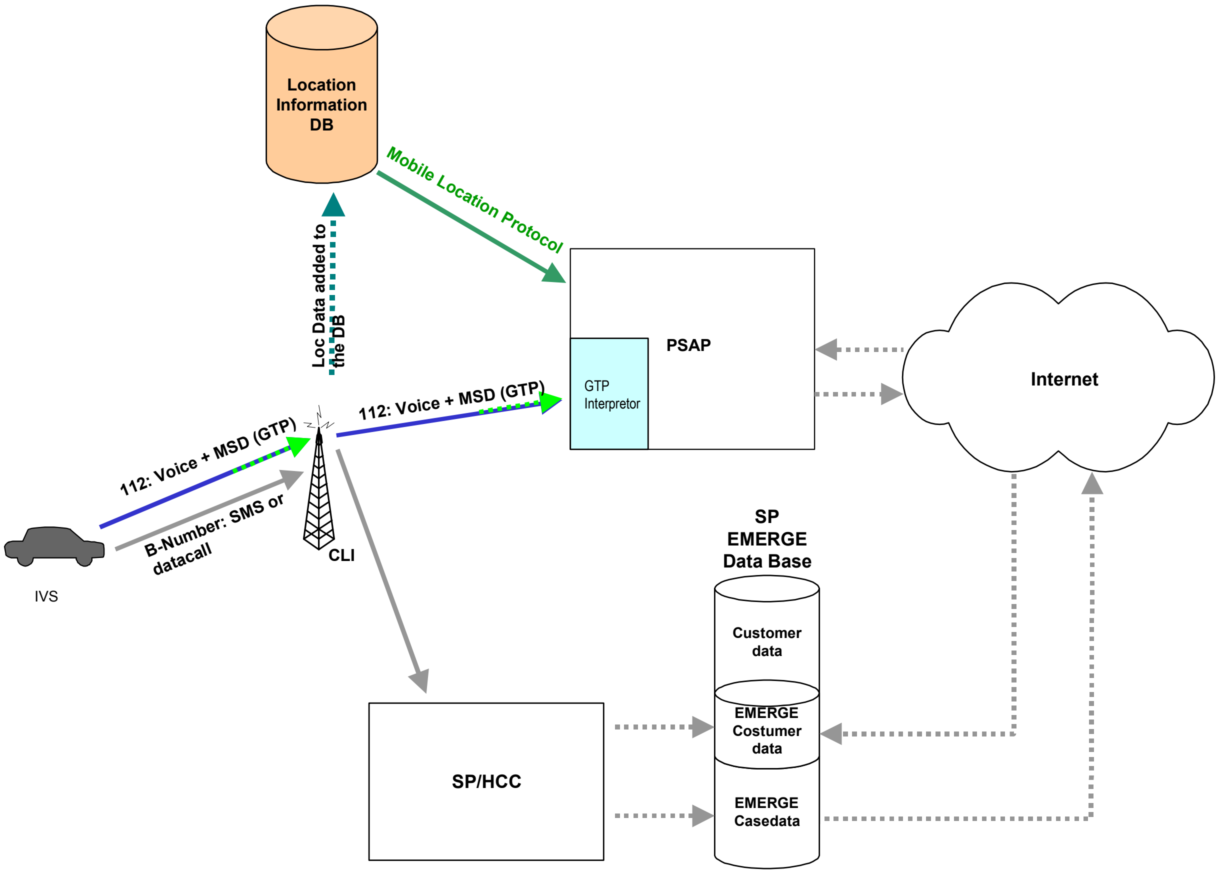


Figure 15: Communication Architecture

8.3.2. Analysis

This is an optimised communication architecture, in terms of effectiveness and clear responsibilities. This architecture represents the most onerous situation for the PSAP because the PSAP interface has to deal with two different protocols, the Mobile Location protocol, and above all, it must translate the data call from GTP. Based on the results of ETSI / EMTEL protocol work optimisation could potentially be possible.

The communication between Mobile Network Provider and SP is made using proprietary protocols and a specific bearer, and the data call is directed to a private B-Number. The quality of the service in terms of redundancy, routing and priority is regulated by a specific contract or commercial agreement.

Due to the importance for the SP to have the possibility to provide additional post-accident services, it is fundamental the availability of some base information. These information regard more specifically the availability of Rescue Centres references such as *« Who has kept the vehicle? »*, or *«Which is the Hospital that received the driver ? »*, and so on.

It is important to note that this analysis is technology independent, in fact, this solution could be implemented into the 2G GSM Network Architecture, ensuring that data together with voice are delivered at the same PSAP and last, but not least, voice connection link is always established, so TELECOM Operator could add Mobile Location to the communication with complete benefits from EC Regulation.

8.3.3. Specifications

The following paragraph derives a set of specifications from the previous analysis. These specifications have been divided according to the main actors involved in the communication chain and they consider uniquely the requirements for the management of the communication flow.

8.3.3.1. IVS

The IVS should have the capability :

- To discriminate which type of bearer use (GSM, GPRS, SMS,...back up system in case of lack of coverage) ;
- To generate a 112 voice call on mobile network using a single channel;
- To include in the 112 voice call the minimum set of data ;
- To handle a normal voice call using the already open voice channel ;
- To handle GTP protocol ;
- To generate a data call to a private B-Number (Service Provider) including additional data ;

8.3.3.2. Telecom Operator

The Telecom Operator should have the capability :

- To receive a 112 call generated by different types of device (GSM, GPRS, UMTS, ...) ;
- To handle 112 call generated by a mobile device;
- To prioritise 112 call ;

- To add CLI to a 112 voice call ;
- To add Mobile location to a 112 voice call ;
- To interpret Mobile Location protocol ;
- To route the call to the appropriate PSAP;
- To match deliver both voice and data, sent on a sigle voice channel, to the appropriate PSAP ;
- To guarantee the security on data transmited related to 112 call ;
- To guarantee the integrity on data transmited related to 112 call ;
- To guarantee the quality of the service in terms of redundancy, routing and priority ;
- To manage a conference call when translation is needed ;
- To receive a private call generated by different types of device (gsm, gprs,...) ;
- To route the data call to the appropriate SP;
- To guarantee contract terms with the SP ;
- To manage a conference call, when translation is needed.

8.3.3.3. PSAP

The PSAP should have the capability :

- To handle 112 voice call ;
- To receive Mobile Location data from the fixed network ;
- To interpret Mobile Location protocol ;
- To receive data in a workable format ;
- To receive correct and complete data ;
- To elaborate Mobile Location protocol ;
- To visualise the CLI ;
- To visualise the Mobile location;
- To visualise accurate position ;
- To visualise the minimum set of data ;
- To send an acknowledge based on the GTP protocol to the IVS
- To access internet network ;
- To access E-Merge Database ;
- To access additional E-MERGE data ;
- To put information in the E-Merge Database ;
- To communicate a post-accident information to the SP ;

8.3.3.4. SP

The SP should have the capability :

- To handle a call (voice + data);
- To receive data independently by the used infrastructure ;
- To interpret the proprietary protocol ;
- To receive a feedback of the Rescue Service involved ;
- To send an acknowledgement to the IVS ;
- To ensure E-Merge Database security ;
- To endure data privacy ;
- To provide additional post-accident services ;

8.4 Communication Mobile Network Provider to PSAP

8.4.1 Communication flow

The communication flow from the mobile network provider to the PSAP has been discussed in the previous paragraph, and regards more specifically a part of the whole emergency-call management chain. The communication flow relevant to this subchapter, as shown previously, could be summarised as follows:

[1] The TELECOM operator enriches the incoming E-Merge call with the CLI (Caller Line Identification) and adds the mobile location into the Location Server Database. After the emergency call handling, the TELECOM Operator delivers the E-Merge call to the appropriate PSAP via the fixed line network.

[2] The PSAP receives two different type of communication via the fixed line network on a common channel: the first one is data communication delivered in GTP protocol whilst the second one is a normal voice communication. The minimum set of data + CLI are delivered as transparent data together with the voice. At the same time the TELECOM Operator push the Mobile Location to the PSAP using the Mobile Location Protocol chosen within ETSI Workgroup.

[3] The PSAP transmit acknowledge of data received to the IVS and interpret GTP minimum set of data using a GTP interpreter.

8.4.2 Analysis

According to the communication architecture adopted by the E-MERGE project, we can summarise some important aspects involved in this part of the communication chain and conduct a technology independent analysis. First of all the mobile network provider has to route the call to the appropriate PSAP via fixed line networks and it has to provide the CLI to the PSAP.

This solution, identified as the best one, could be implemented into the 2G GSM Network Architecture, ensuring that data together with voice are delivered at the same PSAP and the voice connection link is always established, so TELECOM Operator could add Mobile Location to the communication with complete benefits from EC Regulation.

8.5 Communication Mobile Network Provider to HCC (SP)

8.5.1 Communication flow

The communication flow between the mobile network provider and the HCC is regulated by a private commercial agreement between the parties and this case does not represent a focus of the E-MERGE project, but it is important to give some recommendations.

The communication flow could be summarised in the following steps:

[1] When it has been generated by an IVS and the driver is also a subscriber of an service provider (HCC), after sending the original E-MERGE call, a second data call is generated to the HCC. This goes through the mobile network and the GSM operator first handles it. The GSM operator treats this call as a normal private call and applies the normal deliver procedure to a B-Number and carries the call as it is to the appropriate HCC.

[2] The HCC receives the data message encoded with a proprietary protocol and it starts handling procedures, adding the additional E-MERGE data in the E-MERGE database in order to make these data available to the PSAPs.

[3] The HCC transmits an acknowledgement for data received, to the IVS.

[4] If translation is needed the PSAP starts a conference call with the HCC and the driver.

8.5.2 Analysis

The communication between the parts is made using proprietary protocols and a specific bearer, and the call is directed to a private B-Number. The quality of the service in terms of redundancy, routing and priority is regulated by a specific contract or commercial agreement.

8.5.3 Specifications

In the following there is a set of specifications deriving from the previous analysis. These specifications have been divided for the main actors of the considered communication chain and they consider uniquely the requirements for the management of the communication flow.

8.5.3.1 Telecom Operator

The Telecom operator should have the capability.

- To receive a private call generated by different types of device (GSM, GPRS,...).
- To handle a call generated by a mobile device.
- To route the call to the appropriate HCC.
- To guarantee the contract terms.
- To manage a conference call, when translation is needed.

8.5.3.2 HCC

The HCC should have the capability:

- To handle a call (voice + data).
- To receive data independently by the used infrastructure.

- To interpret the proprietary protocol.

8.6 Communication PSAP to HCC (SP)

8.6.1 Communication flow

The communication flow between the PSAP and the HCC could be regulated by a private commercial agreement between the parts and this case does not represent a focus of E-MERGE project. Also if it is not a duty of E-MERGE project to oblige PSAP to provide information to the HCC, it is however, important to give some recommendations.

The communication flow, shown in the following figure 6, could be summarised in the following steps:

[1] When the PSAP receives the 112 call, it receives the minimum set of data + CLI + GSM location, from the GSM operators location databases on the basis of the CLI.

[2] The PSAP transmit an acknowledge of data received to the IVS

[3] If the driver is also a subscriber of a HCC the PSAP start management operation accessing at the E-MERGE database in order to get additional E-MERGE data directly from the HCC and to be capable to arrange the best needed rescue service. The identifier is the IPSec address and the toll free number of the HCC in the MSD.

[4] After this the PSAP forward the rescue request to the rescue centres.

[5] In a second time the PSAP communicates to the HCC the involved rescue centres, to allow the HCC to be able to provide additional post-accident services. This communication could be regulated by particular agreements between the parts and it could happen via fixed line network as a simple phone call between the operators, or via the Internet. In this last case the PSAP operator can access to E-MERGE database and put in all the available information about the involved rescue centres.

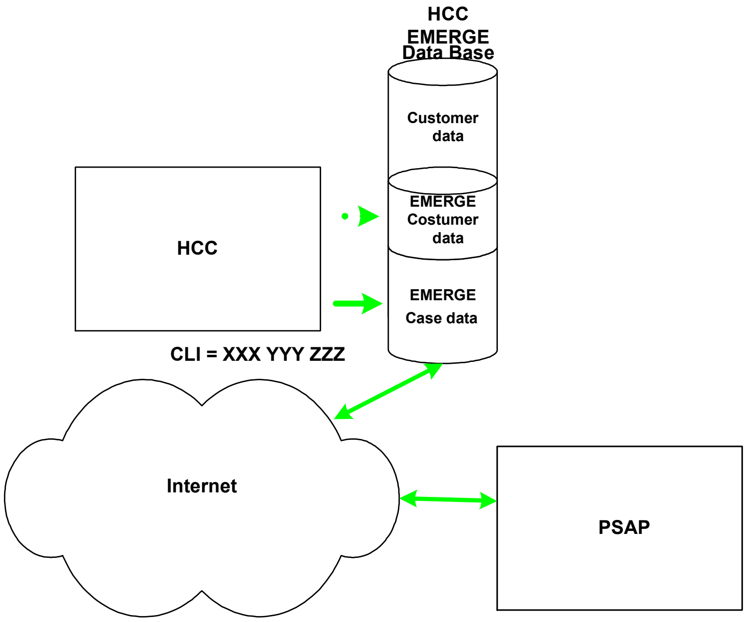


Figure 16: Communication PSAP to HCC

8.6.2 Analysis

Due to the importance for the HCC to have the possibility to provide additional post-accident services, it is fundamental to have some basic information available. This information regards more specifically the availability of rescue centres references such as *« Who has kept the vehicle? »*, or *«Which is the Hospital that received the driver? »*, and so on.

As previously mentioned, this type of communication could happen via different ways, and it could be also regulated by particular agreements.

To conclude, it would be desirable to implement an operational procedure for this type of information provisioning.

8.6.3 Specifications

In the following there is a set of specifications deriving from the previous analysis. These specifications have been divided for the main actors of the considered communication chain and they consider uniquely the requirements for the management of the communication flow.

8.6.3.1 PSAP

The PSAP should have the capability to:

- Communicate post-accident information to the HCC.
- Access Internet network based on an IPSec solution.
- Access E-MERGE database.
- Put information in the E-MERGE database.

8.6.3.2 HCC

The HCC should have the capability:

- To receive a feedback of the rescue service involved.
- To ensure E-MERGE database security.
- To endure data privacy based on IPSec solution.
- To provide additional post-accident services.
- To be able to receive a conference call in several languages from a PSAP

8.7 Conclusion

This chapter defined the E-MERGE specification from the communication perspective. The different protocols and standards involved in the communication between the IVS and telecom provider on the one side and the telecom provider and the PSAP and HCC on the other side. One communication event in different solutions is defined for the communication between the IVS and telecom operator. Basic is the GTP protocol to sent data over the public telephony network, whatever the bearer technology might be.

A first data and eventually voice communication schema handles the first contact between the emergency originator or victim and the Public Safety Answering Point (PSAP) organisation. In this first case the telecom operator should be able to transmit the GTP protocol via a protocol defined by the OCG EMTEL standardisation committee. A second communication event happens when the IVS eventually sends an extended set of data to a service provider. This service provider will act as a home call centre and provides additional services on behalf of the victim, the PSAP and any other third party involved in the post processing of the E-call.

From these different use cases the necessary requirements to be supported by the different parties were determined and specified.

9. E–Merge PSAP Requirements

9.1 Introduction

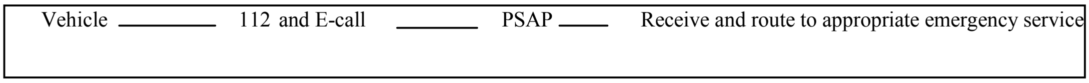
While Chapter 8 described the E-MERGE requirements on the side of the telecom operator, this chapter will list the requirements for the PSAP player in the E-call emergency response chain. A PSAP should comply with the requirements explained in this chapter to be able to take part in that chain, as it forms a vital link between vehicle drivers and passengers that may or may not be injured, and emergency authorities such as casualty rooms, ambulances and fire departments. It is responsible for passing on all information relevant to emergency services such as the number of injured, the nature of injuries, the location of the vehicle and the data learnt from the vehicle sensors on the condition of the vehicle, and so forth.

Before it goes into the actual requirements, this chapter will briefly define the PSAP, and the data it should receive from the other actors. In addition, the operational procedures a PSAP should follow to handle an E-call are described. The chapter continues with an overview of the technical requirements, the PSAP requirements on the database and the performance requirements for the PSAP. Finally, a number of legal issues in connection with the PSAP are addressed, such as the issue of data protection and legal liability.

9.2.Definitions

9.2.1 PSAP

A **Public Safety Answering Point (PSAP)** is a **physical** location where emergency calls and E-MERGE calls are received. This may be a public authority, possibly a public/private partnership or a telecommunications operator licensed by a public authority.
They will be responsible for ordinary 112 voice calls via landline and mobile networks. The PSAP is responsible for informing the Emergency Authorities.



9.2.2 Critical sensor

A critical sensor within E-MERGE is defined as an in-vehicular sensor, which is designed to monitor critical events within a vehicle immediately before, during or after a collision. The PSAP requirement for an automated activation of the E-MERGE emergency system is that no less than 2 of these defined sensors will have activated.

9.2.3 Minimum set of data

The minimum set of data should be transmitted as defined in chapter 6.

9.2.4 Additional data and categories

The additional data provided by the service provider will include the minimum set of data, as a confirmation that the information transmitted is correct. This information transmitted from the service provider via a web browser function should differentiate between the additional data and the minimum set of data. This could be achieved by the use of differently coloured text for the two sets of data.

Sensor	SubGroup	HCC	Other
Vehicle Unique identification (Registration Mark)			
Speed			
Deceleration			
Radial Speed			
Tilting			
Persons on Board	In numbers Heart rate		
Temperature	Engine Compartment Passenger Cell		
Smoke Sensor	Engine Compartment Passenger Cell		
Wearing of Seat Belts	Child seat indication		
Point of Impact	Number of sensors to locate impact points		

Table 1: Additional Vehicle Sensor data

Sensor	Subgroup	HCC	Other
Details of Collision of data recorders on vehicle	How to access the additional data and where		
Up-to-date contact details for vehicle owner/driver			
Insurance Details			
Driving Licence			
Evidence of Road worthiness (Test			

Certificate)			
Persons to inform (Next of Kin)			
Incident Manager (Free phone)			
Service Offered for the member	Persons to inform Deal with property from vehicle Vehicle removal and repair Additional services based on contract		
Incident Reference details/Common unique reference			

Table 2: Additional Data from the service provider

9.3. Reference list

9.3.1 Reference list IVS data to PSAP

The data list sent by the IVS to the PSAP contains the minimum set of data:

- Use Case Header
- Privilege Level
- Version Element
- Time Stamp
- E-MERGE ID
- Vehicle Location
- Vehicle Direction
- Vehicle Descriptor

For more information, please consult chapter 6: minimum set of data description.

9.3.2 Reference list SP data to PSAP

The data list sent by the SP to the PSAP contains the additional data:

- Use Case Header
- Privilege Level
- Version Element
- Time Stamp
- E-MERGE ID
- Vehicle Location
- Vehicle Direction
- Vehicle Descriptor
- Vehicle Model Year
- Vehicle Identification Number
- IVS terminal serial number
- License plate number

- Vehicle Colour
- Vehicle Model
- IMEI GSM equipment number
- E-call status: source and number of triggers
- Breakdown Recognition parameters
- Breakdown data
- Service Provider identifier
- Service Provider telephone number
- Country code
- Other Data

9.4 Data base content for the PSAP

9.4.1 DB1 Customer information.

This data set contains data related to the actual customer available at the HCC databases and which potentially could be made available for the PSAP and EAs. This data is further divided in the following three sub-sections:

DB1.1 Customer general data
Provides basic information about the customer.
Data Provider: Information entered by the service provider after closing the contract with the Customer.

Field	Description	Length (in Bytes)
Customer First name	Customer's First Name.	40
Customer Surname	Customer's Last Name	40
Customer Middle name	Customer's Middle name	40
Customer Title	Customer's Title	10
Inbound Mobile Telephone Number 1	Mobile Telephone number	20
Inbound Mobile Telephone Number 2	Secondary Mobile Telephone number	20
Back-up SIM Telephone Number	Back-up SIM Telephone number.	20
Contract Number	Contract number as registered by the SP	20
Customer Registration Number	Customer identification number	20
Contract Status	The status of the contract	10
Contract Type	If applicable the Contract type	20
Preferred Language	The preferred language of the customer	20
Country Code	The international Country Code	3

For a known customer the following customer details should be available to the operator upon request:

Field	Description	Length (in Bytes)
Customer Date of Birth	Data of birth	8 (format YYYYMMDD)
Customer Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Customer's full address	512
Home Telephone Number or digital network	Customer's home telephone number	20
Work telephone Number	Customer's work telephone number	20
Mobile Phone number	Mobile phone number	20
Identity Card State of issue	The international Country Code of the ID card issuing state.	4
Identity card number	Number marked on the ID Card. This is a 12 character number marked on the front of the ID card	12
Passport number	If applicable the number of the customers passport	20
Passport Country Code of Issue	The international Country Code of the Passports issuing state.	3
Country Code	Country Code the user	3
User Code	A User Code if applicable	20

DB1.2 Customer Health insurance data
This data set provides more specific data on the health insurance(s) owned by the customer.
Data Provider: Information entered by the service provider after closing the contract with the customer.

Field	Description	Length (in Bytes)
Health Insurance Organisation	Name of the Health Organisation. Where applicable this should be the legal Health Insurance organisation	40
Health Insurance Customer number	Customer number known to the Health Insurance Organisation.	40
Health Insurance Address Address Line 1 (Office	Address of the Health Insurance organisation.	512

Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)		
Health Insurance Telephone Number or digital network	HI Telephone number	20
Health insurance valid until date	Expiry date of the HI contract.	8 (format YYYYMMDD)
Private Health Insurance Customer number	If the customer posses a private Health Insurance Policy this field contains the customer number.	40
Private Health Insurance Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Address of the private Health insurance organisation.	512
Private Health Insurance Telephone Number or digital network	HI Telephone number	20
Private Health insurance valid until date	Expiry date of the HI contract.	8 (format YYYYMMDD)

DB1.3 Customer credit card data
Credit card information could automate the payment transactions for such services as towing, ambulance, emergency organisation interventions and so forth.
Data Provider: The service provider enters this information while closing the contract procedure.

Field	Description	Length (in Bytes)
Credit Card Organisation	Name of the Credit Card organisation e.g. VISA, American Express etc.	20
Name of Credit Card owner	Name of the Credit Card owner as indicated on the card.	40
Credit Card number	Credit Card Number	16
Expiry Date	Expiry Date marked on the Credit Card.	8 (format YYYYMMDD)

DB1.4 Driver license

Organisations such as the police department could use this information to identify the victim of an accident.

Data Provider: The service provider enters this information when setting up the contract.

Field	Description	Length (in Bytes)
Driver License Number	Number provided on the driver license form.	10
Driver License Issue date	Date the issuing organisation handed out the Drivers License	8 (formatted YYYYMMDD)
Driver License Issue organisation	Issuing organisation.	40
Country Code of issue organisation	International Country code of issuing organisation.	3

DB 1.5 Customer contact details

This information will be useful for an operator in case of an emergency call. It allows the service provider to contact the customer's relatives or any additional contact persons.

Data Provider: The service provider should enter this information during the setup of the contract. This version of the specifications defines up to three contact person entries.

Field	Description	Length (in Bytes)
Level 1 Name of Contact	Full name of the first contact person.	40
Level 1Contact Telephone Number	First contact person's telephone number.	20
Level 1 Contact Person Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the first contact person.	512
Level 2 Name of Contact	Full name of the second contact person.	40
Level 2 Contact Telephone Number	Second contact person's telephone number.	20
Level 2 Contact Person Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the second contact person.	512

Level 3 Name of Contact	Full name of the first contact person.	40
Level 3 Contact Telephone Number	First contact person's telephone number.	20
Level 3 Contact Person Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the first contact person.	512
Free text	Free remarks and additional information	1024

9.4.2 DB2 Service Provider contract data

This information is partly related to the service provider itself but should be completed by the operator at the moment a PSAP request arrives.
Data Provider: service provider and service provider operator.

Field	**Description**	**Length (in Bytes)**
SP Organisation	Name of the service provider	40
SP Contract number	Number of the contract registered with the SP	20
SP Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the service provider organisation.	512
SP Telephone Number or digital network	service provider Telephone number	20
SP Fax Number	service provider Fax number	20
SP Email address	E-Mail address of the service provider	40
SP Contract valid until date	Contract expiry date	8 (format YYYYMMDD)
SP Operator Name	Full name of the operator handling the emergency call	40
SP Operator Direct Phone	Direct telephone number of the operator	20

SP Operator Email address	Direct E-Mail address of the operator handling the emergency call	40
SP Country Code	International Country Code of the service provider's location.	3
SP IP Address	Fixed IP address attributed to the service provider. The need for a fixed IP address is a requirement imposed by the Security architecture. See also chapter 12 for more details.	15 (A sequence of 4 numbers separated by a dot ex. 123.456.789.123)
Incoming Data Time Stamp	Time Stamp when receiving the request from the PSAP	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)
Outgoing Data Time Stamp	Time Stamp when sending out the response to the PSAP	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)

9.4.3 DB3 Vehicle data

DB 3.1 IVS-data
This information is obtained from the in vehicle telematics system.
Data Provider: The information is sent out by the IVS as part of the request process.

Field	**Description**	**Length (in Bytes)**
Manufacturer	Full name of the manufacturer	40
SW- Version	Software Version if applicable	5
Message protocol	If applicable formatting protocol of the message sent from the IVS	10 (ex. HTTP, SOAP, ASCII etc.)
Acknowledge	Indicates if the message needs and acknowledge	1
Serial number	Serial number of the device	40
Incoming message	Content of the incoming message.	1024
IMEI	International Mobile Equipment Identity Number	20 (ex. Nnnnnn/nn/nnnnnn/n)

DB 3.2 Full set of information provided by IVS (Chapter 7)
Data provided by the IVS and reflects the status of the vehicle and provides the service provider with the technical incident data. This data is part of the full set of information made available by a HCC. The values provided by the IVS SHOULD be formatted according to According to (GTP), Encoding Specification, 21st March 2003, Version 1.0

Data Provider: The in-vehicle telematics system.

Field	Description	Length (in Bytes)
E-call status	The source of the emergency call and the number of triggers, which includes manual triggers as well as sensor triggers: airbag, roll-over.	1 (See also the GTP Encoding Specification Version 1.0 page 73)
E-call source	Vehicle identification parameters.	1 (See also the GTP Encoding Specification Version 1.0 page 74)
E-call Recognition flag	Vehicle identification parameters.	1 (See also the GTP Encoding Specification Version 1.0 page 75)
E-call Crash Data	Additional descriptive data identification parameters.	n exact number of bytes depends on the amount of data made available by the IVS. (See also the GTP Encoding Specification Version 1.0 page 76)
E-call Crash Intensity Data	Additional descriptive intensity data identification parameters	4 (See also the GTP Encoding Specification Version 1.0 page 77)

DB 3.3 Vehicle insurance data
Data related to the insurance of the vehicle itself. This information will be indispensable to contact the insurance organisation of the victim.
Data Provider: The insurance company. The information is gathered from the insurance forms provided by the customer when setting up the contract.

Field	Description	Length (in Bytes)
Vehicle Insurance Organisation	Full name of the Vehicle insurer	40
Vehicle Insurance contract number	Insurance Contract number	20
Vehicle Insurance Address Address Line 1 (Office Name) Address Line 2 (Street	Full address of the insurer	512

Name) Address Line 3 Address Line 4 (Post Code)		
Vehicle Insurance Telephone Number or digital network	Telephone number of the insurance organisation	20
Vehicle Insurance valid until date	Insurance expiry date	8 (format YYYYMMDD)
Vehicle Insurance valid from date	Insurance initiation date (Date from)	8 (format YYYYMMDD)
Vehicle Insurance code	Insurance code attributed by the Insurance organisation	20

9.4.4 DB4 Manufacturer data

Vehicle manufacturer data information provided mostly by the IVS system and originating from the car's manufacturer. The information contained by database belongs to the full set of data described in chapter 7 of these specifications. As for the data elements provided by the DB3 data set, some elements are encoded according to (GTP), Encoding Specification, 21st March 2003, Version 1.0 (22.20), page 70 the vehicle descriptor. Not all elements however are contained by this protocol. For these elements missing a length estimate is given.
Data Provider: the car's in-vehicle telematics systems. The data is initially set by the car's manufacturer.

Field	**Description**	**Length (in Bytes)**
Chassis Number (VIN)	Vehicle Identification Number	17 (See page 70 of the GTP Protocol table 56)
Vehicle Registration Number	Registration number of the Vehicle attributed by the governmental authorities	20
Vehicle Manufacturer	Full name of the Car Manufacturer	40
Vehicle Model	Car model	40
Vehicle Colour	Colour	20
Vehicle Registration Date	Registration date	8 (formatted YYYYMMDD)
Vehicle Maximum Total Weight	Maximum total weight of the vehicle. This element is missing from the GTP protocol definition.	10 (ASCII representation of a decimal value)
Vehicle License plate	License plate. This value is rather Country dependent but may be standardised in the future	20
Vehicle User Code	User groups	4

9.4.5 DB5 Service Provider Data (HCC)

Part of the E-MERGE event record, which identifies the HCC. In this case the request was received by a HCC that has a contract with a LCC. The information is obtained from the static data provided by the service provider.
Data Provider: The service provider static database.

Field	Description	Length (in Bytes)
HCC Organisation	Full name of the HCC service provider	40
HCC Event number	Sequence number for the generated event	12
HCC Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the HCC	512
HCC Telephone Number or digital network	Telephone number of the service provider	12
HCC Fax Number	Fax number of the service provider	12
HCC Email address	Valid E-Mail address of the service provider	40
HCC operator Name	Name of the operator dealing with the event call.	40
HCC operator Direct Phone	Direct phone number of the operator dealing with the event.	12
HCC operator E-mail address	operators E-Mail address	40
HCC Country Code	International Country Code of the HCC location.	3
HCC IP Address	Fixed IP address attributed to the service provider. The need for a fixed IP address is a requirement imposed by the Security architecture. See also chapter 12 for more details.	15 (A sequence of 4 numbers separated by a dot ex. 123.456.789.123)
HCC Information time stamp	Time Stamp marking the creation time of this record.	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)

9.4.6 DB6 Service Provider Data (LCC)

Part of the HCC is, that it identifies the LCC –, local partner of the HCC. The information is obtained from the static data provided by the service provider.
Data Provider: The service provider static database

Field	Description	Length (in Bytes)
LCC Organisation	Full name of the LCC service provider	40
LCC Event number	Sequence number for the generated event	12
LCC Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the LCC	512
LCC Telephone Number or digital network	Telephone number of the service provider	12
LCC Fax Number	Fax number of the service provider	12
LCC Email address	Valid E-Mail address of the service provider	40
LCC operator Name	Name of the operator dealing with the event call.	40
LCC operator Direct Phone	Direct phone number of the operator dealing with the event.	12
LCC operator Email address	operators E-Mail address	40
LCC Country Code	International Country Code of the LCC location.	3
LCC IP Address	Fixed IP address attributed to the service provider. The need for a fixed IP address is a requirement imposed by the Security architecture. See also chapter 12 for more details.	15 (A sequence of 4 numbers separated by a dot ex. 123.456.789.123)
LCC Information time stamp	Time Stamp marking the creation time of this record.	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)

9.4.7 Field lengths and Field formats

The following conventions may help the implementers of these specifications to handle the data transported amongst the E-MERGE parties:

- Data elements or fields as specified in the tables above are always represented as ASCII character sequences. This is true for genuine string data but also for numerical data.
- Dates are always represented by 8 bytes and formatted as follows:
  YYYYMMDD Example: 20030306.

Timestamps are formatted with a character sequence of 14 bytes:
YYYYMMDDHHMMSS Example 200303061417

9.5 Operational procedures

The initiation of an E-MERGE call should take place in the following order

- Acknowledgement Recognition of the incident
  - i. By the driver
  - ii. Automatically by the sensor (No less than two critical sensors for confirmation)
- The call is accepted by the PSAP
  - iii. If Verbal contact with the driver is established
  - iv. Or at least two critical sensors have been activated
  - v. If silent calls are received with no sensor data, normal silent call procedures will apply.
- The caller is questioned by the PSAP and the minimum set of data is visualised Where silent call and sensor information is received, the minimum data set is visualised.
- PSAP passes the information to the EA
- PSAP or EA could indicate that they wish additional data to be pushed to them or pulled by them from the HCC.
- EA dispatches rescue vehicles
- EA rescue vehicle deals with incident
- EA contact service provider for value added services if required.
- Scene cleared in-vehicle *e*-system reset

9.6. PSAP Technical Requirements

The technical requirements are for:

- High-speed error-free messaging of the data transmission from PSAP to the telecom operator in order to receive the minimum set of data and the GSM location and in addition to pull the additional data from the SP.
- Recognition of an English data dictionary to deal with the above issue (Recognising that English is the official emergency language)
- A system providing a high degree of coverage through the mobile phone network providers for voice communication. As voice communication can reassure callers and acts as a prompt for the mobilisation for the emergency services.

- PSAPs to be able to receive and handle the E 112 calls (Voice, minimum set of data and pull of data).
- Error-free links between the PSAP and the service provider Database, to provide fast secure and reliable communication.
- Being able to call the HCC European Free phone number for value-added services or language support
- Internet link for transmission of value-added data.

9.6.1. Operator infrastructure

The following operator infrastructures are mandatory in addition to the normal PSAP operator Infrastructures for handling a 112 call.
Additional operational infrastructures are:

- Software to receive and visualise Minimum set of E-MERGE data.
- Maps for the visualisation of the accurate position, preferably Digital mapping software.
- Browser software to log into an internet address. If the communication over internet is secured, security software is also needed.
- Software to send case data to the SP.

9.6.1.1Personnel

- Availability 24 hours at 365 day
- 4 shift model
- Multilingualism, minimum English
- Psychological stress training
- Continuing education

9.6.2. Telephony infrastructure

The following telephone infrastructures are mandatory in addition to the normal PSAP telephone Infrastructures for handling a 112 call. For more information, please refer to chapter 8.

The additional telephone infrastructures are:

- The telephone system should be able to pull the additional data set from the SP database when the 112 voice and data has been received
- To protocol all actions, which are in connection with an E-call / E-MERGE event, with a timestamp
- Building up a conference call
- Routing of voice and data to the assigned working places
- Implementation of the assigned working places into a conference call
- As contractually agreed – voice recording
- Forwarding the call to E-MERGE working places
- Direct dialling to E-MERGE working places
- Administration of groups

- Visualisation of the incoming number
- Supervisor functions like:
    - To listen in
    - To intervene
    - To adopt
- Save the connectivites with timestamp for tree months
- Demonstration and allocation of the active work place for all E-calls
- Priority handling for E-call events
- Visualisation of all incoming and outgoing call numbers for the operator
- Administration of a defined operator number tape of the E-call group in order to enable the HCC to talk to the responsible operator directly
- Knocking function with visualisation of caller
- Over plugging function
- Safe all voice activities to the E-call data base
- Facsimile
- Internal and external conference call

9.6.3. Network infrastructure

Within Chapter 12 the network infrastructures mandatory is illustrated in addition to the normal PSAP network Infrastructures for handling a 112 call.

The Additional network infrastructures are:

- Internet connection

9.7. Data base PSAP requirements

The databases maintained by the HCC and telecom operators should meet the following requirements:

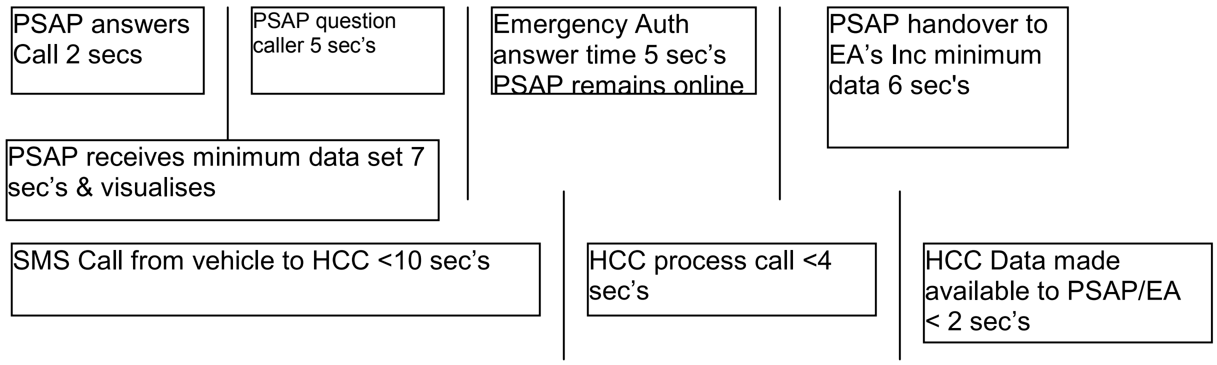
- Access to a database provided by a service provider must comply or exceed the existing UK timing performance criteria
- The databases should be maintained to a high degree of accuracy
- Transmission should be over a secure network
- Any transmissions to the PSAP or the emergency authorities must be of a common communication protocol
- The language used should be English
- A differently coloured text should be used to differentiate between the minimum set of data and additional data categories during transmission to prevent duplication or possible error
- They should be capable of providing the location data in the format required by the host PSAP for the EAs they serve.
- Data Protection and accuracy issues will be the responsibility of the service providers

- service providers should be of a sufficient standard to operate as an effective service provider using a nationally recognised standard (ISO 9000)

9.8 Performance standards

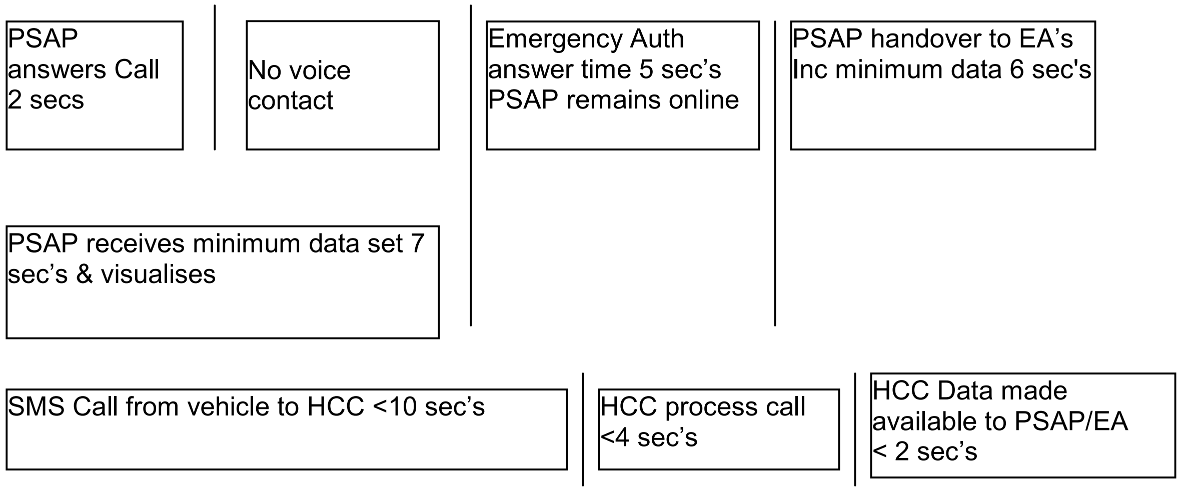
Voice call with minimum data and additional data

Call generated by person in vehicle pushing the E-call button or automatic activation:


PSAP answers Call 2 secs
PSAP question caller 5 sec's
Emergency Auth answer time 5 sec's PSAP remains online
PSAP handover to EA's Inc minimum data 6 sec's
PSAP receives minimum data set 7 sec's & visualises
SMS Call from vehicle to HCC <10 sec's
HCC process call <4 sec's
HCC Data made available to PSAP/EA < 2 sec's

Data call with minimum data and additional data

Call generated by automatic activation following the activation of 2 critical sensors:


PSAP answers Call 2 secs
No voice contact
Emergency Auth answer time 5 sec's PSAP remains online
PSAP handover to EA's Inc minimum data 6 sec's
PSAP receives minimum data set 7 sec's & visualises
SMS Call from vehicle to HCC <10 sec's
HCC process call <4 sec's
HCC Data made available to PSAP/EA < 2 sec's

9.8.1 Work flow

Chapter 4 E-MERGE Use Case in this document describes the workflow for each use case.

9.8.2 Timing

In case of a **manual activation of the E-call**, the PSAP operator should answer the call within 2 seconds. Upon answering the call, the operator should learn as much information (What? Where? What is needed?) from the driver as he possibly can in 5 seconds.

Just before the voice call is initiated, the minimum set of data is made available using the voice channel to send the data as "data in the voice". This is then visualised by the PSAP. It should be done within 7 seconds.

Based on the information from the voice call and the Minimum set of data, the PSAP contacts the Emergency Authorities who have 5 seconds to answer the call.

The PSAP has 6 seconds to hand over the first information about the incident to the EA.

Slightly later than the minimum data set and voice, the PSAP pull the full set of data from the HCC. This information should be available at the HCC in less than 10 seconds after the initiation of the voice call to the PSAP. In less than 4 seconds, the HCC should process the SMS. Then, the HCC should be able to make the HCC data available to the PSAP and the Emergency operators in less than 2 seconds.

In case of an **automatic activation** by the critical sensors, the procedure is very similar. The PSAP operator has 5 seconds to try and establish contact with the vehicle driver via the automatically initiated voice call. After those 5 seconds, the procedure continues without any voice information from the driver.

9.9 Legal Issues

9.9.1 Data protection

The data protection issues with regard to this area of the rescue chain are not within the protection granted by the 112-call area, as they do not form part of the immediate call for assistance. As such there would need to be an agreement by the person from whom the data is generated that the HCC or Central Data base has permission to store that data. The person storing the data would have a requirement to ensure accuracy. There is a to the value of the data and who would own it.

9.9.2 Legal liability (accuracy)

The owner of the database would have in partnership with the person whom the data was generated to assure accuracy. There would need to be an indemnity on behalf of the PSAP and the emergency services if they carried out any action (or not) as a result of receiving inaccurate information.

9.9.3 Legal liability (failure of communication)

The PSAPs and the HCC or central database would need to indemnify themselves against the non-receipt of information on the failure of the communication chain resulting in the worsening of the emergency situation. In addition there would also be a need for the EAs to deal with this issue.

9.9.4 Legal liability (incorrect information)

The PSAP/EA would need to indemnify them against the receipt of the information which was incorrect and upon which they acted, which resulted in a worsening of the emergency situation.

9.9.5 Human rights

This proposal has been audited for Human Rights Compliance and is affected by Articles 1,2 and 8 of the First Protocol of the Human Rights Convention. There is also an issue with relation to the Osman Ruling, which expands the duty of care for public authorities, and how they respond to a known risk for a member of the public.

9.10 Other solutions

In Europe is the WGS84 format generally in the utilisation of telematics user.

For UK, the GRID reference design is used, which need a transmission of the WGS84 data into GRID data. This procedure is described in different standards. Following documents are required at BT – British Telecom to realise the implementation:

- BT 999 GPS – Network Design 999 GPS
- BT 999 GPS – MQ Interface
- BT EDSP Message Standards

9.11 Conclusion

To be E-MERGE compliant, a European PSAP centre should meet the requirements and follow the procedures and recommendations provided in this chapter. The requirements explained in this chapter include recommendations in terms of information input and output, technical infrastructure, call handling procedures and time limits. Of course, it was also necessary to include a number of legal requirements and issues in the discussion.
Now the recommendations for E-MERGE compliant PSAPs have been clarified, we need to address the requirements on the side of the service provider, as the SP is one of the most important sources of information for the PSAP. This will be the subject of Chapter 10.

10. Service Provider Recommendations

10.1 Introduction

In the previous descriptions it has been stated several times that the cooperation of the service provider in E-call in relation to providing additional services to the PSAPs in relation to in-vehicle emergency calls is of value for the emergency response efficiency. At this time many service providers are already involved in E-call handling. Experience with E-call handling and customer databases is thus available. Experience combined with the possibility to further develop telematics based services makes the service providers important partners in the E-MERGE system.

Services today range from pure E-call handling, safety & security services (alert and/or breakdown call handling, accident and post-accident management, vehicle tracking & tracing, door lock/unlock, etc.), traffic/travel related location based services (traffic information, navigation, vehicle oriented services (remote diagnostics, monitoring), Fleet Management Services, Infotainment services.

The main task in relation to the in-vehicle emergency call is to receive and handle incoming data in relation to in-vehicle E-calls, and make available the up-to-date data set to the responsible PSAP as well as to provide defined services for the customer (e.g. post-accident services).

This chapter describes recommendations to the service providers about how to establish and arrange the provision of value added data in the E-call service chain within the E-MERGE system.

10.2 Definition

The following terms and abbreviations are used in this section and the remainder of the document:

10.2.1 SP Service provider or HCC Home call centre

A **service provider (SP)** or **Home Call Centre (HCC)** is a **physical and functional** component, responsible for providing telematics based services to its subscribers – the drivers - (e.g. breakdown calls handling and management, IVS communication handling, accurate location detecting like tracking and tracing of the vehicle based on GPS/GALILEO technology, fleet-management services, etc.) The HCC is located in the home country of thesubscriber. In case the accident will happen in the home country of the subscriberthe LCC and HCC will be the same but in case that the incident will happen in another country a agreement between a HCC and a LCC could have been made.

10.2.3 LCC Local call centre

The **Local Call Centre (LCC)** is a **functional** component to whom the HCC can have a contract to and which is located in the country where the accident has happened.

10.2.4 E-MERGE Call

The **E-MERGE call** or E-call is a telematics emergency call originated by IVS based on mobile communication technology combining primarily data transmission via SMS or data channel, which includes GPS/GALILEO location, additional data and voice transmission, adopting the E-MERGE protocols. The E-MERGE call could be activated manually by S.O.S. button or automatically by processing of car signals activated. The E-MERGE call is the only type of call treated by E-MERGE project;

10.2.5 PSAP

A **Public Safety Answering Point (PSAP)** is a **physical** location where emergency calls and E-MERGE calls are received. This may be a public authority, possible in a public/private partnership, or a telecommunications operator licensed by a public authority, responsible also for ordinary voice calls landline and mobile; The PSAP is responsible to inform the Emergency Authorities.

10.2.6 EA

The **Emergency Authority (EA)** is an agency like police, ambulance, or fire brigade responsible for dealing with the call and managing the most appropriate response (e.g. dispatching vehicles, providing rescue service, …);

10.2.7 IVS

The **In-Vehicle System (IVS)** is an on-board telematics device with different specific function of generating "E-MERGE calls";

10.3 Service Types and Definitions

The following gives an overview of the service categories that can be distinguished in relation to the full set of data.

We have created four different categories:

1) Customer related services
2) Vehicle related services
3) Personal customer environment related services
4) Technical support services
5) Additional support services

10.3.1 Customer related services

	PSAP Need	Source of information	Value-added services	Source of information
Customer related	Number of passengers	Voice: Customer input Data: Seat sensors	Who is hurt?	Voice: Customer input Data: CLI/Telecom operator
	Number of adults/children	Voice: Customer input Data: Seat sensors with weight control	Customer identification (is the registered customer in the car?)	Voice: Customer input Data: if customer starts engine with a personal chip key to identify himself

	Total number of people hurt	Voice: Customer input Data: Absence of voice call = all are hurt / impact speed above a threshold = all are hurt / roll over sensor positive = all are hurt, etc	Contact list	Voice: Customer input Data: SP database
	Severity of injuries to dispatch appropriate services (e.g. helicopter, special treatment)	Similar to previous item: Voice: Customer input Data: Absence of voice call = all are severely hurt / impact speed above a threshold = all are severely hurt / nº of roll over => severity, etc.	Car insurance details, health insurance details (privately insured, special conditions), patient authorization, acknowledgement, storage of critical/ confidential information (credit card numbers, passwords, bank accounts, driver license, passports, etc.)	Voice: Customer input Data: SP database
	Exactly know what kind of support is needed	Voice: Customer input Data: Sensor information from vehicle	Translation service, telephone conference capability,	Voice: Customer input Data: SP database
	CLI to follow up on silent calls or false alarms	Voice: Customer input Data: Telecom operator		

10.3.2 Vehicle related services

	PSAP Need	Source of information	Value-added services	Source of information
Vehicle related	How many triggers caused the automatic call (minimum 2)	Vehicle sensor data (Minimum standard between OEMs required)	GPS dead reckoning, gyros information, storage of crash data, critical vehicle component monitoring,	Voice: Customer input Data: Vehicle sensors, in-vehicle memory
	Which triggers caused the automatic call	Vehicle sensor data	Hazardous goods/cargo monitoring/information	Voice: Customer input Data: SP Fleet-Management information
	Brand, model, type, colour, petrol type	Voice: Customer input Data: VIN number	Details on service coverage according to SP service fee: (Tracing and tracking, salvage of vehicle, towing to professional workshop, garaging, expert opinions on potential repair and cost estimate, initiating appropriate repair, timely provision of parts, provide rental car, return service, etc.)	Voice: Driver input Data: SP database
	License plate	Voice: Customer input Data: IVS memory	License plate	Voice: Customer input Data: SP database
	Direction	Voice: Customer input Data: IVS (GPS), pearl chain information		
	Impact speed, deceleration speed	Voice: Customer input Data: IVS (GPS)	Impact speed, deceleration speed	Voice: Customer input Data: IVS (GPS)
	Number of vehicles involved in accident.	Voice: Customer input Data: Vehicle sensor data		
	Kind of technical support needed (fire brigade, towing, etc.)	Voice: Customer input Data: Vehicle sensor data		

10.3.3 Personal customer environment

	PSAP Need	Source of information	Value-added services	Source of information
Personal environment			Details on service coverage according to SP service fee: Accident Management services (organisational support), safeguarding property, removing vehicle from the road, psychological treatment, disability insurances and mobility insurance, hotel bookings, medical care, accompany children or relatives returning home, home transport of dead body, funeral service, driver training after accident, reintegration in job and education)	Voice: Driver input Data: SP database

10.3.4 Technical environment

	PSAP Need	Source of information	Value-added services	Source of information
Technical environment	Green wave for emergency vehicles, Reduction of false alarms and integration of good Samaritan calls	Local authorities, Software issue	Active safety support services (pre-information on upcoming risks), digital traffic warning light information, weather/road conditions push service, voice command, voice recognition, back-up battery and antenna, OTA capability, structural alterations (flat), handicap vehicle,	Hardware and software issue: Information sent to IVS from outside devices: Short-range communication systems, vehicle to vehicle communication, ADAS (active safety systems, mathematical methods/software, specialized service providers

10.3.5 Additional support services

	PSAP Need	Source of information	Value-added services	Source of information
Additional support services			Deal with insurance, tax authorities, local legal support, hospital administration support, selection of hospital and rehabilitation clinic, pre-financing/credits	SP service offer provided by specialists, Services listed in SP database
	Navigation and guidance support (rescue force need)	Public Traffic information/ Radio Stations, Telematics service providers		

In order to provide all these value-added services to the PSAPs, the creation of a common approach to a HCC specific database at each service provider is essential. The database at the HCC should be accessible via a specific IP address (HCC identification) by all PSAPs in Europe.

It is thus decided that the database should be held and kept accurate by the HCC. Each HCC should create a database for its customers. . More information on the content of the database can be found in 10.4.

10.4 HCC database content

The following paragraph provides an overview of the different databases maintained by a service provider. For each of the different databases the information type of the data is given, the source of the information identified and a list of fields given.

10.4.1 DB1 customer information.

This data set contains data related to the actual customer. This data is further divided in the following three sub-sections:

DB1.1 Customer general data
Provides basic information about the customer.
Data Provider: Information entered by the HCC after closing the contract with the customer. For a known customer the following details must be presented (e.g. are mandatory) to an operator in conjunction with the voice connection.

Field	Description	Length (in Bytes)
Customer First name	Customer's First Name.	40
Customer Surname	Customer's Last Name	40
Customer Middle name	Customer's Middle name	40
Customer Title	Customer's Title	10
Inbound Mobile Telephone Number 1	Mobile Telephone number	20
Inbound Mobile Telephone Number 2	Secondary Mobile Telephone number	20
Back-up SIM Telephone Number	Back-up SIM Telephone number.	20
Contract Number	Contract number as registered by the SP	20
Customer Registration Number	Customer identification number	20
Contract Status	The status of the contract	10
Contract Type	If applicable the Contract type	20
Preferred Language	The preferred language of the customer	20
Country Code	The international Country Code	3

For a known customer the following customer details should be available to the operator upon request:

Field	Description	Length (in Bytes)
Customer Date of Birth	Data of birth	8 (format YYYYMMDD)
Customer Address Details Address Line 1 (House Name)	Customer's full address	512

Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)		
Home Telephone Number or digital network	Customer’s home telephone number	20
Work telephone Number	Customer’s work telephone number	20
Mobile Phone number	Mobile phone number	20
Identity Card State of issue	The international Country Code of the ID card issuing state.	4
Identity card number	Number marked on the ID Card. This is a 12 character number marked on the front of the ID card	12
Passport number	If applicable the number of the customers passport	20
Passport Country Code of Issue	The international Country Code of the Passports issuing state.	3
Country Code	Country Code the user	3
User Code	A User Code if applicable	20

DB1.2 Customer health insurance data

This data set provides more specific data on the Health Insurance(s) owned by the Customer.

Data Provider: Information entered by the HCC after closing the contract with the customer.

Field	**Description**	**Length (in Bytes)**
Health Insurance Organisation	Name of the Health Organisation. Where applicable this should be the legal Health Insurance organisation	40
Health Insurance Customer number	Customer number known to the Health Insurance Organisation.	40
Health Insurance Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Address of the Health Insurance organisation.	512
Health Insurance Telephone Number or digital network	HI Telephone number	20

Health insurance valid until date	Expiry date of the HI contract.	8 (format YYYYMMDD)
Private Health Insurance Customer number	If the customer posses a private Health Insurance Policy this field contains the customer number.	40
Private Health Insurance Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Address of the private Health insurance organisation.	512
Private Health Insurance Telephone Number or digital network	HI Telephone number	20
Private Health insurance valid until date	Expiry date of the HI contract.	8 (format YYYYMMDD)

DB1.3 Customer credit card data
Credit card information could automate the payment transactions for such services as towing, ambulance, emergency organisation interventions and so forth.
Data Provider: The HCC enters this information while closing the contract procedure.

Field	**Description**	**Length (in Bytes)**
Credit Card Organisation	Name of the Credit Card organisation e.g. VISA, American Express etc.	20
Name of Credit Card owner	Name of the Credit Card owner as indicated on the card.	40
Credit Card number	Credit Card Number	16
Expiry Date	Expiry Date marked on the Credit Card.	8 (format YYYYMMDD)

DB1.4 Driver license
Organisations such as the police department could use this information to identify the victim of an accident.
Data Provider: The HCC enters this information when setting up the contract.

Field	**Description**	**Length (in Bytes)**
Driver License Number	Number provided on the driver license form.	10
Driver License Issue date	Date the issuing organisation handed out the Drivers License	8 (formatted YYYYMMDD)
Driver License Issue organisation	Issuing organisation.	40

Country Code of issue organisation	International Country code of issuing organisation.	3

DB 1.5 Customer contact details
This information will be useful for an operator in case of an emergency call. It allows the HCC to contact the customer's relatives or any additional contact persons.
Data Provider: The service provider should enter this information during the setup of the contract. This version of the specifications defines up to three contact person entries.

Field	**Description**	**Length (in Bytes)**
Level 1 Name of Contact	Full name of the first contact person.	40
Level 1Contact Telephone Number	First contact person's telephone number.	20
Level 1 Contact Person Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the first contact person.	512
Level 2 Name of Contact	Full name of the second contact person.	40
Level 2 Contact Telephone Number	Second contact person's telephone number.	20
Level 2 Contact Person Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the second contact person.	512
Level 3 Name of Contact	Full name of the first contact person.	40
Level 3 Contact Telephone Number	First contact person's telephone number.	20
Level 3 Contact Person Address Details Address Line 1 (House Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the first contact person.	512
Free text	Free remarks and	1024

	additional information	

10.4.2 DB2 HCC contract data

This information is partly related to the HCC itself but should be completed by the operator at the moment a PSAP request arrives.
Data Provider: HCC and HCC operator.

Field	Description	Length (in Bytes)
HCC Organisation	Name of the HCC	40
HCC Contract number	Number of the contract registered with the HCC	20
HCC Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the HCCorganisation.	512
HCCTelephone Number or digital network	HCC Telephone number	20
HCC Fax Number	service provider Fax number	20
HCC Email address	E-Mail address of the HCC	40
HCC Contract valid until date	Contract expiry date	8 (format YYYYMMDD)
HCC operator Name	Full name of the operator handling the emergency call	40
HCC operator Direct Phone	Direct telephone number of the operator	20
HCC operator Email address	Direct E-Mail address of the operator handling the emergency call	40
HCC Country Code	International Country Code of the HCC's location.	3
HCC IP Address	Fixed IP address attributed to the HCC. The need for a fixed IP address is a requirement imposed by the Security architecture. See also chapter 12 for more details.	15 (A sequence of 4 numbers separated by a dot ex. 123.456.789.123)
Incoming Data Time Stamp	Time Stamp when receiving the request from the PSAP	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)

Outgoing Data Time Stamp	Time Stamp when sending out the response to the PSAP	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)

10.4.3 DB3 vehicle data

DB 3.1 IVS-data
This information is obtained from the in vehicle telematics system.
Data Provider: The information is sent out by the IVS as part of the request process.

Field	Description	Length (in Bytes)
Manufacturer	Full name of the manufacturer	40
SW- Version	Software Version if applicable	5
Message protocol	If applicable formatting protocol of the message sent from the IVS	10 (ex. HTTP, SOAP, ASCII etc.)
Acknowledge	Indicates if the message needs and acknowledge	1
Serial number	Serial number of the device	40
Incoming message	Content of the incoming message.	1024
IMEI	International Mobile Equipment Identity Number	20 (ex. Nnnnnn/nn/nnnnnn/n)

DB 3.2 Full set of information provided by IVS (Chapter 7)
Data provided by the IVS and reflects the status of the vehicle and provides the HCC with the technical incident data. This data is part of the full set of information made available for the PSAP. The values provided by the IVS SHOULD be formatted according to (GTP), Encoding Specification, 21st March 2003, Version 1.0

Data Provider: The in-vehicle telematics system.

Field	Description	Length (in Bytes)
E-call status	The source of the emergency call and the number of triggers, which includes manual triggers as well as sensor triggers: airbag, roll-over.	1 (See also the GTP Encoding Specification Version 1.0 page 73)
E-call source	Vehicle identification parameters.	1 (See also the GTP Encoding Specification Version 1.0 page 74)
E-call Recognition flag	Vehicle identification parameters.	1 (See also the GTP Encoding Specification Version 1.0 page 75)
E-call Crash Data	Additional descriptive data identification parameters.	n exact number of bytes depends on the amount of data made available by the IVS. (See also the GTP Encoding Specification Version 1.0 page 76)
E-call Crash Intensity Data	Additional descriptive intensity data identification parameters	4 (See also the GTP Encoding Specification Version 1.0 page 77)

DB 3.3 Vehicle insurance data
Data related to the insurance of the vehicle itself. This information will be indispensable to contact the insurance organisation of the victim.
Data Provider: The insurance company. The information is gathered from the insurance forms provided by the customer when setting up the contract.

Field	Description	Length (in Bytes)
Vehicle Insurance Organisation	Full name of the Vehicle insurer	40
Vehicle Insurance contract number	Insurance Contract number	20
Vehicle Insurance Address Address Line 1 (Office Name) Address Line 2 (Street	Full address of the insurer	512

Name) Address Line 3 Address Line 4 (Post Code)		
Vehicle Insurance Telephone Number or digital network	Telephone number of the insurance organisation	20
Vehicle Insurance valid until date	Insurance expiry date	8 (format YYYYMMDD)
Vehicle Insurance valid from date	Insurance initiation date (Date from)	8 (format YYYYMMDD)
Vehicle Insurance code	Insurance code attributed by the Insurance organisation	20

10.4.4 DB4 Manufacturer data

Vehicle manufacturer data information provided mostly by the IVS system and originating from the car's manufacturer. The information contained by database belongs to the full set of data described in chapter 7 of these specifications. As for the data elements provided by the DB3 data set, some elements are encoded according to (GTP), Encoding Specification, 21st March 2003, Version 1.0 (22.20), page 70 the vehicle descriptor. Not all elements however are contained by this protocol. For these elements missing a length estimate is given.
Data Provider: the car's in-vehicle telematics Systems. The data is initially set by the car's manufacturer.

Field	**Description**	**Length (in Bytes)**
Chassis Number (VIN)	Vehicle Identification Number	17 (See page 70 of the GTP Protocol table 56)
Vehicle Registration Number	Registration number of the Vehicle attributed by the governmental authorities	20
Vehicle Manufacturer	Full name of the Car Manufacturer	40
Vehicle Model	Car model	40
Vehicle Colour	Colour	20
Vehicle Registration Date	Registration date	8 (formatted YYYYMMDD)
Vehicle Maximum Total Weight	Maximum total weight of the vehicle. This element is missing from the GTP protocol definition.	10 (ASCII representation of a decimal value)
Vehicle License plate	License plate. This value is rather Country dependent but may be standardised in the future	20
Vehicle User Code	User groups	4

10.4.5 DB5 HCC Data

Part of the E-MERGE event record which identifies the HCC. In this case the request was received by a home control centre. The information is obtained from the static data provided by the HCC.
Data Provider: The HCC static database.

Field	Description	Length (in Bytes)
HCC Organisation	Full name of the HCC service provider	40
HCC Event number	Sequence number for the generated event	12
HCC Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the HCC	512
HCC Telephone Number or digital network	Telephone number of the service provider	12
HCC Fax Number	Fax number of the service provider	12
HCC Email address	Valid E-Mail address of the service provider	40
HCC operator Name	Name of the operator dealing with the event call.	40
HCC operator Direct Phone	Direct phone number of the operator dealing with the event.	12
HCC operator E-mail address	operators E-Mail address	40
HCC Country Code	International Country Code of the HCC location.	3
HCC IP Address	Fixed IP address attributed to the service provider. The need for a fixed IP address is a requirement imposed by the Security architecture. See also chapter 12 for more details.	15 (A sequence of 4 numbers separated by a dot ex. 123.456.789.123)
HCC Information time stamp	Time Stamp marking the creation time of this record.	14 (Time Stamps should be given in the format YYYYMMDDHHMMSS)

10.4.6 DB6 Service Provider Data (LCC)

Part of the HCC is, that it identifies the LCC – SP, local partner of the HCC. The information is obtained from the static data provided by the service provider.
Data Provider: The service provider static database

Field	Description	Length (in Bytes)
LCC Organisation	Full name of the LCC service provider	40
LCC Event number	Sequence number for the generated event	12
LCC Address Address Line 1 (Office Name) Address Line 2 (Street Name) Address Line 3 Address Line 4 (Post Code)	Full address of the LCC	512
LCC Telephone Number or digital network	Telephone number of the service provider	12
LCC Fax Number	Fax number of the service provider	12
LCC Email address	Valid E-Mail address of the service provider	40
LCC operator Name	Name of the operator dealing with the event call.	40
LCC operator Direct Phone	Direct phone number of the operator dealing with the event.	12
LCC operator Email address	operators E-Mail address	40
LCC Country Code	International Country Code of the LCC location.	3
LCC IP Address	Fixed IP address attributed to the service provider. The need for a fixed IP address is a requirement imposed by the Security architecture. See also chapter 12 for more details.	15 (A sequence of 4 numbers separated by a dot ex. 123.456.789.123)
LCC Information time stamp	Time Stamp marking the creation time of this record.	14 (Time Stamps should be given in the format YYYYMMDDHMMSS)

10.4.7 Field lengths and Field formats

The following conventions may help the implementers of these specifications to handle the data transported amongst the E-MERGE parties:

- Data elements or fields as specified in the tables above are always represented as ASCII character sequences. This is true for genuine string data but also for numerical data.
- Dates are always represented by 8 bytes and formatted as follows: YYYYMMDD Example: 20030306.
- Timestamps are formatted with a character sequence of 14 bytes: YYYYMMDDHHMMSS Example 200303061417

10.5 Operational procedures HCC

10.5.1 Handling E-MERGE call by HCC

- The full set of vehicle data arrives at the HCC
- The data call is routed to the available operator
- The operator receives the full set of information and checks its local emergency support database for additional information under the E-MERGE (CLI) identifier
- The operator finds both customer data (e.g. contact addresses, contracted services like mobility insurance, towing, legal support, etc.) as well as vehicle data (VIN#) like license plate number, car insurance information, etc.)
- The operator combines all data into one data protocol and puts it into a data file (CLI identifier) as part of its database from where the PSAPs have the possibility to pull the data if needed to improve the emergency response efficiency.
- When activated by the PSAP via a predefined free HCC telephone number the operator at the HCC could be asked to set up a conference call with PSAP and customer
- All handlings are stored at the service provider
- Database is updated

10.5.2 Dealing with the E-MERGE information

As mentioned above, data about the accident should be stored at the service provider and merged with already existing (static) data. Potential data coming from the PSAP side should be added to the service provider database after the accident. All data between the HCC and PSAP must be sent over a secured internet link.

10.5.3 Visualisation of the data

The way the HCC visualizes the received additional data can differ from HCC to HCC. The merger with the already existing (static) data should be done within a predefined timeslot. (see10.8.2) The additional data in the service provider database visible for the PSAPs should be presented in English.

10.5.4 Transmitting the data

The HCC do not have the information about what PSAP is handling the Emergency call, it is thus not possible for the HCC to push the information to the PSAP. Therefore the task for the service provider is to process the data into the database within the given time constraints. (see

10.8.2). The PSAP knows via the identification of the service provider (IP address given in the minimum set of data) that after a predefined timeslot the additional data is available at the HCC database. The data can then be pulled via a secure internet link. By doing so, the HCC will know which PSAP is handling the call and can start taking care of post-accident services.

10.6 Technical requirements

The technical requirements are a recommendation. E-MERGE only defines a minimum of equipment and organisation to do justice to the temporal and process conditional definitions for the data exchange and voice communication.

10.6.1 Telephone infrastructure

- The telephone system should have following functions:
  receive of data from IVS and whose registration and allocation to the assigned working places
- To protocol all actions, which are in connection with an E-call / E-MERGE event, with a timestamp
- Building up a conference call
- Routing of voice and data to the assigned working places
- Implementation of the assigned working places into a conference call
- As contractually agreed – voice recording
- Forwarding the call to E-MERGE working places
- Direct dialling to E-MERGE working places
- Administration of groups
- Visualisation of the incoming number
- Supervisor functions like:
  - To listen in
  - To intervene
  - To adopt
- Save the connectivites with timestamp for tree months
- To assign the toll-free number to the E-call / E-MERGE working places automatically
- Demonstration and allocation of the active work place for all E-calls / E-MERGE
- priority handling for E-call / E-MERGE events
- visualisation of all incoming and outgoing call numbers for the operator
- Administration of a defined operator number tape of the E-call / E-MERGE group in order to enable the PSAP to talk to the responsible operator directly
- Knocking function with visualisation of caller
- Overplugging function
- safe all voice activities to the E-call / E-MERGE data base
- Implementation of receive and send functions of:
  - GSM / SMS
  - GSM / data channel
  - GPRS
  - UMTS
- Facsimile
- Internal and external conference call

10.6.2 Operational infrastructure

E-MERGE sees following points and items as minimum requirements:

10.6.2.1 Personnel

- Availability 24 hours at 365 day
- 4 shift model
- Multilingualism, minimum English
- Psychological stress training
- Continuing education

10.7 Additional data HCC to PSAP

Additional data could be transmitted, if these data are agreed contractual and available (customer / service provider).

Additional data could be:

Customer information	chapter 10.4.1 db 1.1
Customer health insurance data	chapter 10.4.1 db 1.2
Customer credit card data	chapter 10.4.1 db 1.3
Customer driver license	chapter 10.4.1 db 1.4
Customer contact details	chapter 10.4.1 db 1.5
Service provider contract data	chapter 10.4.2 db 2
Vehicle data	chapter 10.4.3 db 3
IVS data	chapter 10.4.3 db 3.1
Full set of information provided by IVS	chapter 10.4.3 db 3.2
Vehicle insurance data	chapter 10.4.3 db 3.3
Manufacturer data	chapter 10.4.4 db 4
HCC data	chapter 10.4.5 db 5
Service provider data (LCC)	chapter 10.4.6 db 6

10.8 Performance Standards

10.8.1 Workflow

The flow of work that is handled at the HCC can be derived from the diagram displayed below:

- The full data set arrives at the HCC.
- Data set completed with additional vehicle and customer information from the HCC database

- Transfer data into database, now accessible for requesting PSAP,
- Confirmation received that PSAP has collected additional data.

10.8.2 Timing

The time scheme where the SP should work by is displayed in the diagram.

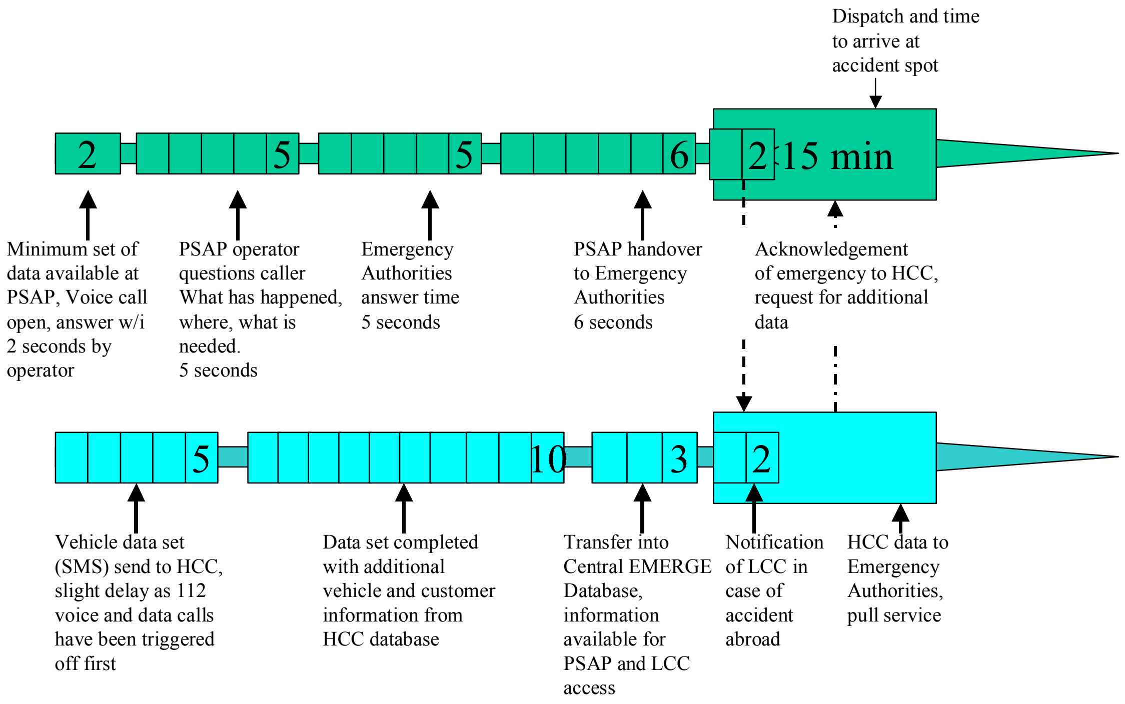

Dispatch and time to arrive at accident spot
2
5
5
6
2
15 min
Minimum set of data available at PSAP, Voice call open, answer w/i 2 seconds by operator
PSAP operator questions caller What has happened, where, what is needed. 5 seconds
Emergency Authorities answer time 5 seconds
PSAP handover to Emergency Authorities 6 seconds
Acknowledgement of emergency to HCC, request for additional data
5
10
3
2
Vehicle data set (SMS) send to HCC, slight delay as 112 voice and data calls have been triggered off first
Data set completed with additional vehicle and customer information from HCC database
Transfer into Central EMERGE Database, information available for PSAP and LCC access
Notification of LCC in case of accident abroad
HCC data to Emergency Authorities, pull service

Figure 17: Timing

10.8.3 Fall Back

In case of an overflow of information on the network, the normal voice 112 gets priority above all other calls. As a voice 112 is established at all times in case of the initialisation of an in-vehicle emergency call and as the minimum set of data follows this 112 call there is a certain guarantee that this reach the PSAP. However, there is no fall back for the additional data.

10.9. HCC Legal Issues

10.9.1 Data protection issues

The data protection issue with regard to the expanded areas of the rescue chain are not within the protection granted by the 112-call area (Universal Service Directive 2002/22/EC, Directive on Privacy and Electronic Communications 2002/58/EC), as they do not form part of the immediate call for assistance.
As such there would need to be an agreement from the person from whom the data is generated that the service provider has permission to store, use and forward that data to the PSAPs in case of an accident.
The organisation storing the data would have a requirement to ensure accuracy.

As there is a value of the data, ownership needs to be determined.

Directive 2002/22/EC requires public telephone operators to forward caller location information to authorities handling emergencies, to the extent technically feasible, for all calls made to the single European emergency call number 112.
Directive 2002/58/EC establishes the conditions for use of location data by emergency services. Member States should ensure that there are transparent procedures governing the way in which a provider of a public telecommunications network and/or a publicly available electronic communications service may override the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of data, on a per-line basis for organisations dealing with emergency calls and recognised as such by a Member State, including law enforcement agencies, ambulance services and fire brigades, for the purpose of responding to such calls[1].

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data stipulates that personal data may be processed where the processing is necessary in order to protect the vital interest of the data subject.

10.9.2 Legal liabilities

10.9.2.1 Accuracy

The owner of the database would need to have a partnership with the person for whom the data was generated to assure accuracy. In other words, the customer is obliged to report changes to his personal situation and answer regular up-date letters.
There need to be an indemnity on behalf of the PSAP and the emergency services when they carry out any action (or not) as a result of receiving inaccurate information.

10.9.2.2 Failure of communication

A malfunction of the system may imply a manufacturer's liability. The PSAPs and/or the HCC and the Central Database Host might need to compensate the customer for the non-receipt of information due to failure of the communication chain (other than telecommunication network) resulting in the worsening of the emergency situation.
There is also a need for the Emergency Authorities to deal with such a situation.

10.9.2.3 Incorrect information

The PSAPs and emergency authorities need to be compensated when actions have been executed based on incorrect (false) information. Incorrect information can result from misuse (HMI issue), intentional misleading the authorities (criminal offence), technical defects (software issue) and incorrect data provided by the customer or storage mistakes.

10.9.3 Contractual aspects

According to Article 26 of the Universal Service Directive, calls to the single European emergency number, 112, including location enhanced E112 must be provided free of charge for all end users of publicly available telephone services, including users of public pay phones.

[1] Draft: Commission Recommendation on the processing of caller location information in electronic networks for the purpose of location-enhanced emergency call services

10.9.4 Human rights

Emergency service proposals have been audited for "Human Rights Compliance" and were found effected by Articles 1, 2 and 8 of the First Protocol of the "Human Rights Convention". There is also an issue with relation to the "Osman Ruling", which expands the duty of care for public authorities, and how they respond to a known risk for a member of the public.

11. Network Security

11.1 Introduction

Especially in these situations where personal and confidential data is transported over the internet, security becomes of the utmost importance. Communication between the different parties involved in an E-MERGE call should assure a complete protection against any infringements or security violations. The data transport architecture described should as a minimum requirement support the following aspects involved in a secure Virtual Private Network:

- **Data confidentiality** - A third party should not be able to decrypt confidential information sent between two parties.
- **Authentication** - The communicating parties should be sure about the identity of their correspondent.
- **Authorization**- A partner in the network should be either allowed or prevented from using resources made available in an E-MERGE network.
- **Access control** - In no way should it be possible for third parties to enter the system without proper authorisation.

These are by no means the only security breaches a system could witness, and that a secure system should at least protect against. This specification effort provides a minimal set of features a secure E-MERGE network should support. This does not exclude any additional features, but those features depend greatly on the actual implementation of the system, and on the facilities provided by a third party security authority. A full discussion of IPSec and Virtual Private Networks is provided in Annex F. You may want to read this chapter in concert with Annex F to get a better and profound understanding of the technology and different issues involved.

11.2 IPSec and secure IP data transport

The widespread use of the Internet and the enormous data flow carried by this world wide network demands for a cautious examination of the security issues listed above. IPSec, which is short for IP Security, provides a security layer on top of the IPv4 data transport protocol, and fills the security gaps still present in this standard. As an alternative, the newer IPv6 standard could be proposed as well, but for this version of the specification, an E-MERGE compliant-system SHOULD implement or use the IPSec suite running on top of IPv4. The general specification which governs the IPSec standard is described by the IETF in the Request for Comment document RFC2401. The IPSec suite of protocols provides two main sub-protocols each described in their proper RFC documents. These protocols support the following functionality:

- Authentication by means of the Authentication Header specified by RFC2402

- Confidentiality by means of the Encapsulating Security Payload protocol specified by RFC2406.
- Data integrity by means of implementing the RFC2402 and RFC2406 specifications.

The data frames sent between the different parties of an E-MERGE system SHOULD comply with these specifications, or use the necessary soft- and hardware which provides the same functionality.

11.2.1 Transport and tunnel mode

An IPSec secured IP data transport may occur in two modes:

- Transport mode
- Tunnel mode

Transport mode mainly supports a data link between two hosts, while Tunnel mode mainly pertains to Security gateways. To be compliant to the E-MERGE specifications, a **host** SHOULD at least support Transport mode while **a node** providing external security support, and as a consequence acting as a **Security Gateway,** SHOULD support Tunnel data transport mode.

11.2.2 Virtual private networks

An E-MERGE compliant Internet Data Transport SHOULD be implemented as a virtual private network. This means that each party should support, either by means of software or by means of hardware, the following features:

- Data encryption
- Authentication
- Data integrity

These are the same features as set forward by the minimum security requirements listed in paragraph 1. The bottom line of the approach proposed by this specification is simply summarized as follows:

> *A connection between E-MERGE parties should be as secure as that same connection realised by means of a private WAN. At the same time, the openness and flexibility of the internet should not be compromised.*

Setting up a Virtual Private Networks in itself is not sufficient. A Virtual Private Network should be guarded by a Firewall. Host machines such as those installed by a PSAP or SP should reside on the DMZ side of the network.

11.2.3 Firewalls and IPSec

IPSec solves two main issues: authentication and data integrity. This may lead to the belief that IPSec in its own is sufficient to establish a full and absolute secure network. While indeed guarding against infringements and assuring data integrity, IPSec on itself does not safeguard the host system against malicious attacks launched from the perilous world wide internet.

In addition to the features provided by the IPSec protocol, an E-MERGE host SHOULD shield its internal hardware and software by means of a Firewall function.

One additional remark should be made on the actual implementation of a firewall. In general, two types of firewall infrastructures are identified: the network layer and application layer firewall. The first type of firewall acts on the lower level of the data stream, and is mostly implemented by hardware devices. The latter firewall type is better known as a proxy server and in general provides a better control over the data flow. However, since this kind of firewalls is implemented by software, they tend to influence the response time of a system. In all situations, a trade-off should be made between both systems. The E-MERGE specifications do not rigidly impose one or the other firewall implementation but only recommends a specific infrastructure relative to the demands of the party and the use cases involved.

11.3 Architectural overview

The subject of this discussion more specifically relates to the Internet cloud linking the following systems:

- PSAP to SP/HCC
- PSAP to SP/LCC
- Telecom operator to SP/HCC

The data transport between the E-call originator and the Telecom operator is not subject to the security requirement. The same goes for the communication between the Telecom Internet gateway and the PSAP. This last connection uses the European Telecommunications Standards Institute (ETSI) OCG-EMTEL protocol. More in depth information about ETSI and the use of this protocol can be found in Chapter 8.

11.4 Minimum requirements

The actual infrastructure specified by the E-MERGE consortium pertains to the minimum requirements set forward by the IPSec standard itself. However, a central security authority could impose additional requirements. In the context of this specification, these basic requirements are listed for each of the participants in the E-MERGE-compliant system. Furthermore, we do not impose a specific implementation type, and do not exclude whatever solution found in the market. Solutions may either be implemented by a set of software applications, or to the contrary implemented by means of hardware devices.
Whatever the final solution will be, to be E-MERGE-compliant, the architecture SHOULD implement the minimum IPSec requirements as specified by RFC2401.

11.4.1 IPSec requirements for the PSAP Infrastructure

The PSAP infrastructure should be shielded from the network by means of a Firewall function. This Firewall should provide the following minimal features:

- Protection against Denial Of Service (DoS) Attacks
- Prevention of third party access to vulnerable data and servers.
- Prevention of upstream data flows. This may be the case if a Trojan horse wants to connect to a spy host, for instance.
- Protection against spoofing attacks.

Furthermore, the Firewall SHOULD preferably be implemented as a Network layer system. Network layer systems work on the lower level of the OSI 7 layer model and work faster than their application layer counterparts. The Firewall in itself could either be implemented as hardware or software solution.
A network layer firewall is very often implemented by means of a router device.
As a second requirement, the E-MERGE specification imposes the need for a FIXED IP Address.

The PSAP software and hardware SHOULD be compliant to the RFC2401, RFC2402 and RFC2406 IPSec specifications.

Finally, it should be noted that both a software and hardware solution may be envisioned for the implementation of both the Firewall and IPSec functionality. The E-MERGE specifications would recommend using a hardware solution if possible. Especially large and intensive customer base applications will benefit from this strategy. Software solutions should mainly find their use in test and small business model solutions.

11.4.2 HCC infrastructure

Similarly to the PSAP infrastructure, the service provider or Home Call Centre needs to implement a fast VPN. As a consequence, the requirements are rather identical to those specified for the PSAP environment. These minimal requirements are set forward for the service provider and Home Call Centre environments:

The HCC infrastructure should be shielded from the network by means of a Firewall function. This Firewall should provide the following minimal features:

- Protection against Denial Of Service (DoS) Attacks
- Prevention of third party access to vulnerable data and servers.
- Prevention of upstream data flows. This may for instance be the case, if a Trojan horse wants to connect to a spy host.
- Protection against spoofing attacks.

Furthermore, the Firewall should implement a network layer system. Network layer systems work on the lower level of the OSI 7 layer model, and work faster than their application layer counterparts. The firewall in itself could be implemented as hardware or software solution.

A network layer firewall is very often implemented by means of a router device.

As a second requirement, the E-MERGE specifications impose the need for a FIXED IP Address.

The SP/HCC host and client software and hardware SHOULD be compliant to the RFC2401, RFC2402 and RFC2406 IPSec specifications.

Finally, it should be noted that both a software and hardware solution may be envisioned for the implementation of both the firewall and IPSec functionality. The E-MERGE specifications would recommend using a hardware solution if possible. Especially large and intensive customer base applications will benefit from this strategy. Software solutions should mainly find their use in test and small business model solutions.

11.4.3 SP/LCC infrastructure

The minimal requirements for this E-MERGE sub-system are very identical to the set-up described for the SP/HCC infrastructure. Here again, speed will be the deciding factor in the overall system layout. As a consequence, the approach or strategy accepted for both the PSAP and SP/HCC infrastructure should be applied for this leg of the system as well. This SHOULD imply the preference of a hardware solution above a software solution for the IPSec implementation as well as the implementation of the Firewall function.

The necessity for a fixed IP address remains eminent.

11.4.4 Secondary SP infrastructure

Secondary SP systems do not directly communicate with a Front-end PSAP, but serve as an additional information base for the Home and Local call centres. These Back-end systems do not have to respond to emergency situations in the same timeframe as expected or specified for Front line systems. For this kind of systems, a software IPSec or Firewall implementation is fully acceptable.

Again, the necessity for a fixed IP address remains of utmost importance.
Secondary SP infrastructures are strictly not in the scope of the E-MERGE project. However, if a secondary SP infrastructure exists, it SHOULD comply with the requirements put forward in this paragraph.

11.5 Database security

As some systems query data from back-end data systems in a client-server fashion, some precautions should be taken to preserve both the consistency and security of the data.

11.5.1. A database management system should provide:

11.5.1.1 A secure connection to the DBMS backend

Genuine CRUD[2] operations modify or retrieve data from a relational database. This information could fall victim to snooping, malicious hi-jacking or playback operations. It is therefore crucial that any data transfer between a data consumer and data producer happens in a secure manner. A DBMS Client-Server connection, subject of Chapter 13, SHOULD provide all necessary means to allow a secure connection from Client system to a DBMS Server System. The client in this case is the SP/HCC or SP/LCC partner. The Server is the Database Management System containing the actual data. The actual implementation is due to the technological restrictions imposed by a traditional and less rigidly specified Client/Server environment. Therefore the matter of secure database access is left over to the actual implementation by means of a commercial DBMS solution. In no way should databases be exposed directly on the Internet: Therefore, they should be located in the DMZ. Data transport between the different players in the E-MERGE network is always carried out in a fixed format record structure, running over IPSec secured sockets.

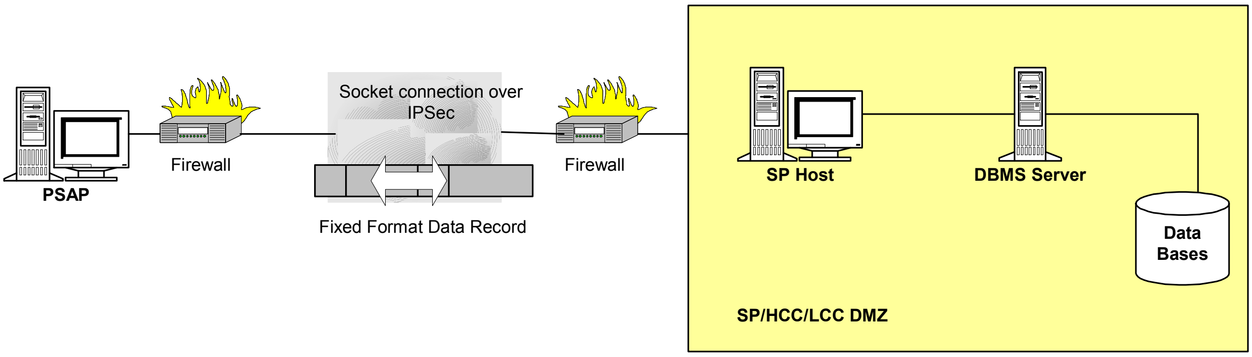


Figure 18: DBMS Server Security concepts

11.5.1.2 A single point of access

Single point login or Single point of access remains a very important topic in a secure internet environment and should be considered very cautiously. A single point of login significantly simplifies, and speeds up the communication between parties. When a single point of access

[2] Create Read Update and Delete

is used, the authorization and security data is propagated from system to system or directed from a centralized system such as an LDAP or NIS+ server. This may indeed facilitate the authentication effort, but could as well compromise the secrecy of the user and his associated password. To be compliant with the E-MERGE specifications, a Single Point of access should be implemented in a secure and guarded fashion. Since much of these features are dependent on the facilities provided by a specific product no further normative recommendations are made by this specification.

11.5.1.3 Guarded user names and passwords

User names and passwords should be guarded from discovery by a third party.

11.5.1.4 Data loss and backup strategy

The data provider should ensure a rigid strategy for preserving the persistent information important to the PSAPs and SPs. A service provider, responsible for storing data on behalf of PSAPs or secondary SPs should implement a rigid back-up procedure.

11.6 The central security authority

Still need to elaborate on this idea. According to the information obtained from Mr. Schütz, a central security authority should be assigned by the different E-MERGE network partners (PSAP, SP etc…). This Security authority takes ownership of the security in the network. The main functions of such an authority are:

- Controlling the authorization and access in the E-MERGE network.
- Providing PKI certificates and acting as the certifying authority in the network
- Providing Security Gateway functionality by setting up a secure tunnel between two E-MERGE parties.

Such a centralized approach has the benefit of having one single point of access for an entire E-MERGE network. Authorization information is not scattered over the network, but resides in the safe hands of a security officer. As a consequence, the different parties in an E-MERGE network obviously SHOULD support the requirements imposed by this central authority.

11.7 Conclusion

Security is, without any doubt, one of the most important issues today related to the widespread use of the internet. The availability of a rigid security architecture is therefore one of the greatest challenges introduced by the Internet. An E-MERGE architecture SHOULD support an IPSec based VPN connection between the following parties:

- PSAP
- SP
- HCC
- SP/LCC
- Telecom to HCC

Each of these parties involved should, as a minimum, support the minimal requirements imposed by the IPSec protocol suite as specified by RFC2401.
The IPSec mode used in between hosts should be transport-based and implement a Virtual Private Network over a Firewall infrastructure.

Security measures should not be restricted to the communication or transport of data between the different parties, but should also involve the Database back-end. Finally, a centralized security strategy could improve or result in a high-grade-secure system.

12. Data Storage Requirements

12.1 Introduction

The E-MERGE data-handling infrastructure in general deals with two main types of data:

- Data provided by the IVS system.
- Data kept and maintained by the different types of service providers.

The data produced by the IVS system as a result of an emergency call is either produced by the different sensors in the car itself and reflect the status of the car at the moment the incident occurs or in the second case, is initialised by the car maker, terminal hardware and software producer or the car-dealer. The customer itself may even provide some of this last type of information. In the E-MERGE specification effort, these data sets are referred to as the minimal and full data sets sent from the Car to the PSAP and SP. Chapters 6 and 7 discussed these two data sets respectively.

The service provider itself manages a second type of data, sometimes referred to as static data. Chapter 10 provides a detailed overview of the different data elements, which are part of this *static* data set. A lot of this information is provided by the service provider while setting up the contract.

Combined the data provided by the IVS and the data stored by the service provider feed a new set of data which identifies an incident or event and allows all parties involved, to post-process the data of the reported incident. This final dataset is referred to as the E-MERGE database, discussed by the architectural chapter, Chapter 3. Providing a PSAP with additional information on the persons involved in the incident is a second, major task of the information stored in this E-MERGE database

As a consequence, an E-MERGE compliant service provider SHOULD provide the necessary infrastructure to store the information specified by Chapter 10. This infrastructure SHOULD comply with the security requirements specified by Chapter 11 and SHOULD furthermore comply with the requirements indicated here after.

Towards the external world, data is transported in a platform independent format. Basically this is a fixed format type where each field has a fixed length and is formatted by means of bytes representing characters from the ASCII table. This for a great deal abstracts the actual infrastructure behind the service provider's front-end computer. However the service provider remains responsible for the captured data. More specific MUST the service provider respect the following constraints:

- **Data Integrity** - The data provided to the different parties in the E-MERGE network should be correct, up to date and structured according to the requirements specified in chapter 10.
- **Confidentiality** – The data contained by the service provider contains personal information, which falls under the privacy infringement law. This kind of information is very sensible and certainly should not leave the boundaries imposed by the ruling regulations.
- **Accessibility** – Data should be available to any authorized E-MERGE party in a swift and timely manner.

- **Backup and recovery** – The service provider SHOULD install a rigid backup and recovery procedure, guarding the system against data-loss.
- **Data entry** – The service provider SHOULD provide the necessary interfaces allowing authorized personnel and sub-sub systems to enter data into the databases.
- **Database management and operation** – The service provider SHOULD take all precautions to operate and manage the DBMS in a secure fashion. This includes such information as passwords and usernames.

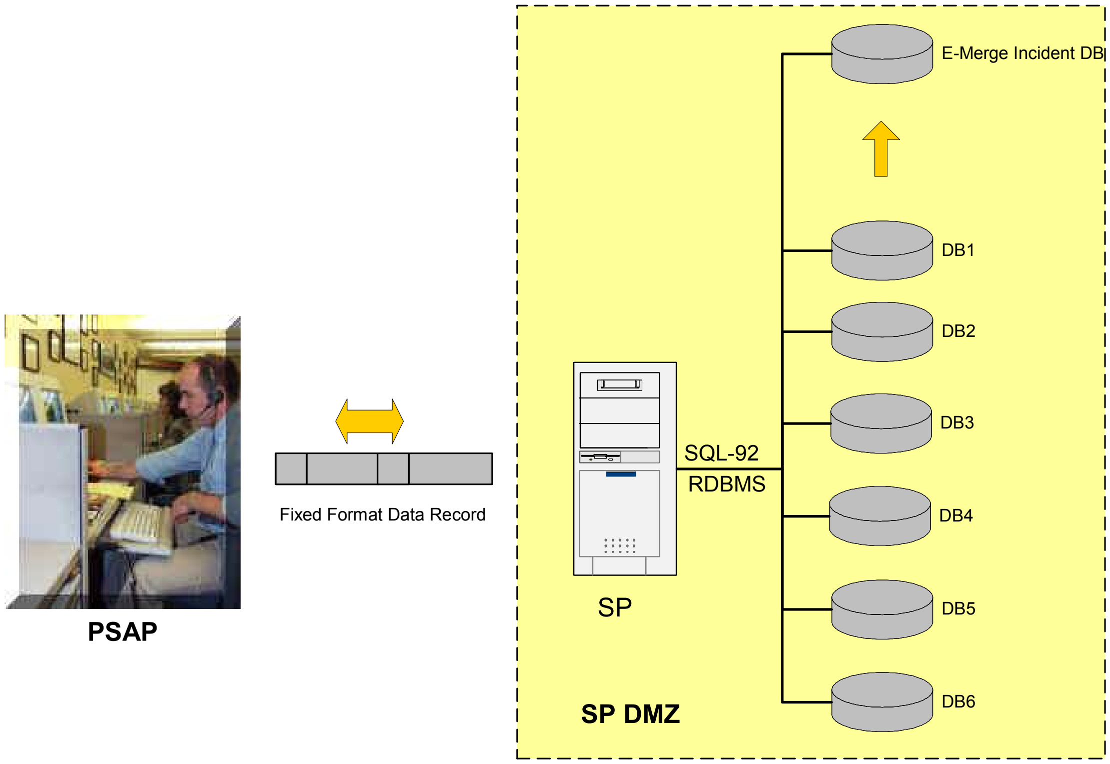


Figure 19: Data Storage Logical Architecture

12.2 Additional literature

Some of the technological concepts and terminology used in this text are very specific to Database Management Systems and the world of SQL and data handling. Annex G of this specification provides a short introduction in Database Management Systems and SQL and explains most of the terminology found in this chapter. You may want to browse over this annex if some of the terms used are not clear or are less obvious to you.

12.3 Database requirements

The above paragraph did sketch the overall requirements imposed by this specification. Not much has been specified about the actual nature of the data storage area. As explained above how exactly the data is stored by the back-end system is pretty much abstracted by the specified data transport format. From a technical viewpoint both I/O interfaces, the one implemented on the PSAP and the one implemented on the SP side, SHOULD be able to parse the record formats described by Chapter 10 and SHOULD be able to construct data-frames compliant again with the format specified in Chapter 10. The priority of the specification goes to the requirements set forward by paragraph 163 of this chapter. The following requirements should, as a consequence, be read as recommended. However, since the importance of the subject, implementers are advised to follow the guidelines published hereafter:

- Data SHOULD be stored in databases
- These databases SHOULD be of the relational type.
- The Relational Database Management System (DBMS) controlling the actual data storage should support transactions.
- The DBMS should strictly be compliant to the SQL-92 Specifications.
- CRUD[3] operations should be implemented by strictly applying the SQL-92 database query and command language. It is advisable not to use vendor specific functions and other vendor specific constructs which do not belong to or are specified by SQL-92.[4]
- The DBMS should provide a transaction log feature.
- Data retrieval and storage should be fast and without delays imposed by the DBMS itself. DBMS systems providing some sort of caching mechanism should be preferred above systems, which do not support these kinds of features.

12.4 Database drivers and connectivity

The actual connection technology used to connect an SP application to the back-end DBMS is not in the scope of this specification it might be useful to indicate the most common technologies in use. An E-MERGE network is a very distributed system with an SP acting as a front-end system to a back-end database. The service provider side in this respect functions as a two-tier traditional Client\Server system. The data obtained by the SP Host Server, converts the result set to the fixed format described by Chapter 10 or generates the necessary SQL Commands to update the database with the information provided by the PSAP and other parties involved. Such a front-end processor connects to a database either:

- By means of a native driver provided by the DBMS vendor.
- By means of an ODBC driver. If such a driver is used the version should be at least version 2.x or higher.
- By means of a type 1, 2, 3 or 4 JDBC driver. If a JDBC driver is used the version should be at least compliant to the JDBC 2.0 specifications or higher.

locates the Database tier in the DMZ of the service provider. If the database tier does not reside in the same secured environment the connection to this external DBMS server should run over an IPSec secured VPN connection as prescribed by Chapter 12.

12.5 Performance

Database access should be without any delays and as fast as possible. This requirement enforces the implementers of the back-end database system to carefully consider all performance and tuning issues pertaining to the use of industrial databases. As a guideline an implementer should consider the following issues:

[3] Create, Read, Update and Delete

[4] The reason for this requirement is not linked to the actual E-MERGE specification itself but eliminates porting issues and incompatibilities between the different DBMS systems on the market.

12.5.1 Optimistic and pessimistic locking

An optimistic locking algorithm has the preference above a pessimistic locking strategy. When implementing optimistic locking all data in the database remains available to concurrent users. A pessimistic locking strategy to the contrary, blocks concurrent access to data and may as a consequence induce delays. The decisive factor for the selection of either an optimistic or pessimistic locking algorithm is simply the chance that an identical data row gets modified concurrently so by multiple users or automated services.

12.5.2 Native drivers versus ODBC or JDBC drivers

Native tend to work faster but restricts the portability of an application. A trade-off should be made at this level as well.

Carefully consider the database design
In general, data redundancy should be avoided by all means.

12.5.3 DBMS tuning and optimisation

Carefully consider the different tuning options provided by a DBMS brand or vendor. Some settings work best if large datasets are retrieved from the database while another setting provides the best performance for regular and bulk data updates. Depending on the load of the back-end system the best strategy should be selected and tested.

12.6 SP/HCC and SP/LCC hardware requirements

Part of the performance issue is very often related to the processor speed and memory available on the back-end system. Determining an exact figure for both the processor speed and memory amounts is clearly out of the scope of this specification it is however advised to make the DBMS server a dedicated machine tailored to the demands of the database and the expected workload. This machine should contain an appropriate amount of:

- Volatile memory
- Persistent memory
- Processor speed

A second consideration should be hardware redundancy. This may imply a redundant infrastructure for hard disk, power supply and other vulnerable systems.

12.7 Distributed data handling

Data SHOULD be handled in a transactional fashion. The term transaction refers to the execution of a set of SQL commands as if it were one single atomic block. If the transaction fails the original situation is restored, the transaction is rolled back in other words or to the contrary if the transaction runs successful the data may be persisted or committed to the database.

12.7.1 Transactions

An E-MERGE compliant back-end system SHOULD execute CRUD operations in a transactional fashion. The support for transactions MAY be limited to local transactions. Distributed transactions or so called two phase commit transactions are not excluded but the impact on the performance of the overall system should be verified. As a bare minimum FLAT transactions should be supported.

12.7.2 Isolation levels

Most Relational Database Management Systems allow the database manager to set the isolation level. Isolation levels specify concurrency at a high level. These levels may vary from basic to very strict. The higher the isolation level the stricter the control of concurrent access and data updates becomes and the more the performance of the systems gets compromised. In general isolation levels address the following problems:

- Dirty reads
- Unrepeatable reads
- Phantom reads

More information on isolation levels can be found in annex G. The actual isolation level is not specified by the E-MERGE specifications but an E-MERGE compliant system SHOULD make the best trade-off between performance and data integrity. A lot depends on the actual environment or application and is therefore implementation dependent.

12.8 Data archiving

All parties involved in the creation and usage of E-MERGE data SHOULD archive this data for a period of three months as a minimum time span. Having this information at hand allows governmental organisations to retrieve statistical information from the E-MERGE data system for instance. Or, as a second example, allows the police forces to use the information stored by the E-MERGE parties during the course of an investigation. It is recommended to retain information even for a longer period. After the required three months period E-MERGE data may transferred to a secondary storage medium such as a CD-Rom and DVD.
Additionally to this requirement the different parties SHOULD comply to any local requirements legally imposed by the local government.

12.9 Conclusion

An E-MERGE system is set-up in such a fashion that the actual storage is abstracted from the operation of the system. Data transport between the different parties happens in a fixed and specified format. Each party should be able to understand and speak this common language without any dependence on the systems residing behind the interface layers. However, a secure and reliable data storage strategy is of a primordial importance for a time and mission critical application such as the emergency assistance systems subject of this specification. The specification requires therefore storing information by means of a secure, reliable and high performing Relational Database Management System. Data access and updates are done by means of the SQL-92 data query and command language. The specifications as presented by this version require a good trade-off between performance, reliability and data integrity. Some of the most important of the techniques used are listed in this chapter.

E-MERGE

Annex A: Network IPSec Specification

Version 0.1

28.02.2003

Produced by:
Telmacon

E-MERGE is co-financed by the
European Commission DG Information Society

ist
information
society
technologies

Programme name:	Information Society Technologies (IST)
Project ID:	IST-2001-34061
Project acronym:	E-MERGE
Project name:	Pan-European Harmonisation of Vehicle Emergency call Service Chain
Dissemination level[1]**:**	Public

Deliverable number:	IR 3.1
Contractual date of delivery:	25. October 2002
Actual date of delivery:	
Title of deliverable:	**Network IPSec Specification**
Work package:	WP 3
Nature of the deliverable:	Confidential
Author(s):	Gerhard Wolfien
Project co-ordinator:	Michael Nielsen (ERTICO) Tel: +32 2 400 07 49, fax: +32 2 400 07 01 E-mail: m.nielsen@mail.ertico.com

Abstract:. This document describes the Network IPSec Specification

Keyword list:

[1] This is either: Public, restricted to other programme participants, restricted to a group specified by the consortium, confidential – Information about dissemination level can be obtained in 9.5 of the Technical Annex.

Document Control Sheet

Electronic reference:

Main author(s) or editor(s): Gerhard Wolfien

Version history:

Version number	Date	Main author	Summary of changes

Approval:

	Name	Date
Prepared	Gerhard Wolfien	
Reviewed		
Reviewed	Gerhard Wolfien	
Authorised	Michael Nielsen	

Circulation:

Recipient	Date of submission

1 Network IPSec Specification

1.1 Preface and project description

The EMERGE project involves Europe wide transmission and exchange of personal data. Existing data and telecommunications directives demand for protection from unauthorised access. Telematic services shall comply with the same rules and standards for privacy protection.Virtual Private Networks (VPNs) are becoming increasingly popular with the low cost and widespread availability of the Internet. This paper discusses the basic security methods needed to create a VPN, and how VPNs can be built with the IPSec Protocol suite.

1.1.1 IPSEC based Virtual Private Networks (VPN)

The generic security standards already developed describe general methods and principles for secure services in open networks. Such security services may, amongst other purposes, be employed for secure implementation of virtual private networks, i.e. private networks implemented by connecting a Local Area company networks or network segments through the public network. Assurance that the security services give adequate protection can be built over time through experience gathered by extensive use of pilot installations. General security aspects that need to be considered include (the list is not exhaustive):

- Confidentiality (encryption)
- Authentication
- Data Integrity (cryptographic checksums)
- Non Repudiation (Digital signatures, Trusted Third Parties (TTPs))
- Authorization (Security Management)
- Access Control
- Revision (accountability)
- Key Management (TTPs, Key Recovery, Key Life Cycle aspects)

1.1.2 Abstract

The goal of this assignment is to introduce the concept of security in Virtual Private Networks (VPNs), and how such networks can be constructed with the IP Security (IPSec) protocol suite.

IPSec will come in widespread use on the Internet, because of the increasing importance of this worldwide information medium, and because of increasing demand for secure communication on the Internet. IPv4, which is the current standard transport layer protocol on the Internet, does not have security features in itself. These features have to be provided by other means. IPSec is designed to offer secure IP connections over the Internet with IPv4

IPSec promises to solve the security problems with the current version of the Internet Protocol (IPv4). If IPSec support for IPv4 becomes widespread, this may delay the deployment of IPv6 to the Internet. However, because of the expansion of the Internet, the need for a larger address space will make the migration to IPv6 unavoidable. Thus, IPSec for IPv4 can only be considered an intermediate step on the way towards an IPv6 based Internet.

1.1.3 Introduction

As people and companies become more and more dependent on information stored in computers, it is only natural that security in computer networks becomes increasingly important. Computer security has been an active field of research for many years. However, it is only recently, with the explosive growth of the Internet, that security has become an area of interest for the general public.

The availability and inexpensive access of the Internet, has resulted in an increasing demand for Virtual Private Network (VPN) solutions. VPNs provide the means to conduct secure communication of private information on the open and rather insecure Internet.

Since 1995, the Internet Engineering Task Force (IETF) has been working on a suite of protocols, collectively called IPSec (IP Security), that are designed to enable secure IP connections over the Internet. IPSec offers security services with IPv4, which is the current standard transport layer protocol on the Internet, and is mandatory for future IPv6.

2 Background

2.1 Definition of terms

As a preparation for our discussion of Internet security and Virtual Private Networks (VPNs), it would be useful to give some definitions of basic security aspects and terms the way the authors understand and use them in this paper. Later we will discuss the technology behind some of these terms in further detail.

Access Control: The property of filtering access and blocking unwanted users from the system. Access control is normally achieved by using authentication methods.

Authentication: The process and methods of verifying that the claimed sender of received data is the actual sender.

Authorization: The property of granting and restricting access to resources in a computer network.

Confidentiality: The property of performing communication so that only the intended recipient may determine what was being sent.

Encryption: Mapping data to a format that makes it unreadable for anyone but the intended recipient or owner. Employing encryption is the common way of providing confidentiality.

Integrity: The property of ensuring that data transmitted from source to destination cannot be altered without the receiver being able to detect that is has been changed.

Non-repudiation: The property of a receiver being able to prove that the received data was in fact sent by the party who claims to be the sender of this data.

Virtual Private Networks

What is a Virtual Private Network (VPN)? Using VPNs basically means employing a number of security techniques and methods to allow secure communication on an open network (the Internet). VPNs encrypt IP datagrams, use strong authentication before allowing communication, and check data integrity to ensure packets arrive at their destination unchanged.

Why are VPNs used? The use of VPNs is motivated by the need of secure communication between computer networks in different locations. This is especially important for large enterprises which need connectivity between geographically divided branch offices and business partners. Traditionally, many large enterprises have maintained costly wide area networks (e.g. X.25) for this purpose. Today the Internet provides a relatively inexpensive way to communicate between networks.

One of the advantages of VPNs over closed wide area networks (WANs) is the accessibility of the Internet, which makes life easy for nomadic users. The possibility to connect to the corporate network through the Internet can be valuable to many business travellers.

While users want the security services provided by a VPN, most people do not want this to affect their routines. They want security services to be provided transparently. Applications should be able to run without any knowledge of the VPN security services, which are provided on a lower layer. Transparency is a very important requirement for a VPN.

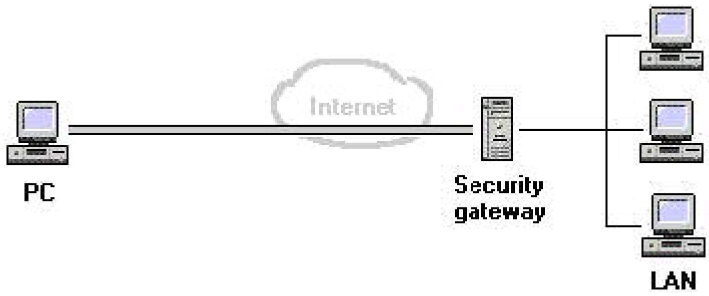


Figure 1: A Virtual Private Network

VPNs aim to provide network-layer confidentiality, integrity, and authentication. Many existing applications provide similar services at the transport layer. Putting these services at the network layer allows the system to provide these as generic services for all applications, including services without any knowledge of security. This allows the enforcement of system policy requirements for network security services

Tunnelling

To ensure secure communication through the open Internet, VPNs establish secure tunnels with encrypted traffic. Tunnelling is a fundamental feature of all VPN implementations. There are two generic classes of tunnels. The first is end-to-end tunnelling where, for example, the tunnel extends from a remote user's PC to the server to which the user is connected. In this scenario, the VPN devices at each end of the connection must handle the establishment of the tunnels, and encrypt and decrypt the data passed between the two points.

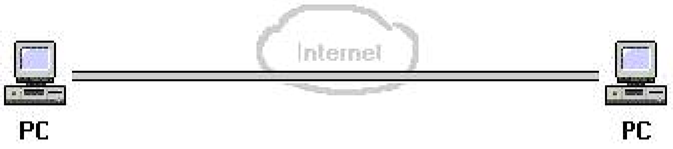


Figure 2: End-to-end tunnelling

The second type is node-to-node tunnelling, where the tunnel terminates at the edge of the network. This type of tunnel could be used to connect LANs in different locations. In such a configuration, all the traffic on each LAN is unchanged. Once traffic passes through a VPN security gateway on the edge of the LAN, it is encrypted and tunnelled to a similar device on the other LAN, where the data is decrypted and put onto the LAN in its original format.

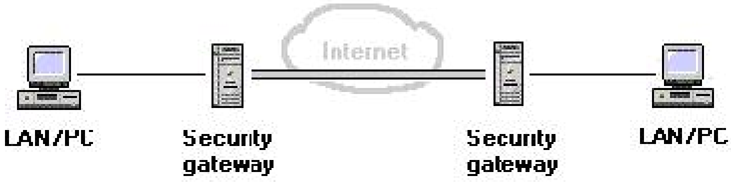


Figure 3: Node-to-node tunnelling

Firewalls

In addition to using secure tunnels to protect communication in a VPN over an entrusted network, it is also essential to protect the VPN itself. This is achieved by the use of firewalls between the trusted networks and other entrusted networks (the Internet).

A firewall is a device that protects one network from another entrusted network, most commonly the Internet. This is achieved by using two simple mechanisms, one that blocks traffic, and another, which permits traffic according to certain criteria.

In many cases, people do not need all the features of a VPN. Simply using a firewall to restrict access to the network in addition to an encrypted message or file transfer service may be enough to fulfil security needs.

One of the most important features of firewalls is the ability to prevent unauthenticated logins to the network, by blocking traffic from entrusted networks or by some other criteria. Firewalls are also important because they provide a single "choke point" where security and audit function can be imposed. To ensure this, it is essential that all communication with the outside world passes through the firewall, and that there are no "back doors" such as dial-in modem connections inside the network.

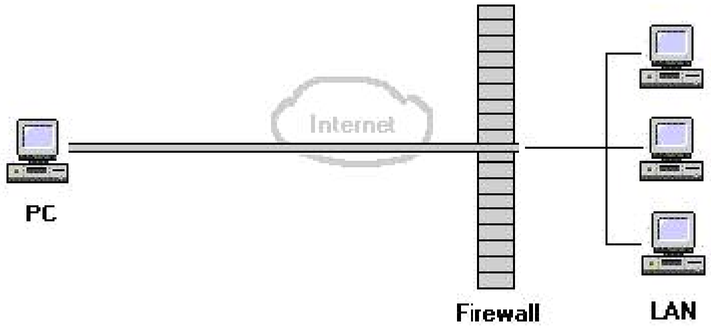


Figure 4: Firewall

The term firewall is used rather loosely. There are two different types of firewalls: screening routers and proxy gateways. (Proxies are sometimes distinguished further into proxy firewalls and guards.)

The screening router is the simplest type of firewall. It is simply a router set up to block incoming packets from entrusted networks, based on the source address, destination port number or other header information.

A more sophisticated type of firewall is the proxy gateway, which, in addition to reading protocol header information, also looks at the data inside the packets. The proxy intrudes in the communication between the outside sender and the receiver inside the firewall, screening the data transfer to ensure that only acceptable protocol commands are sent to the destination

Network security basics

All VPN solutions should include some core security technologies, most importantly encryption, authentication, key management and access control.

Encryption

VPNs use encryption to ensure the confidentiality of data as it passes over the Internet or service provider's network. Encryption is also a necessary tool to achieve authenticity and integrity. The encryption technologies used in VPNs are the same ones used in any other networking scenario where data is encrypted. As a result, the same questions arise: What size encryption key can we use? How do you manage the distribution of encryption keys to users?

All encryption is based on the use of encryption keys that are known only to the involved parties. Encryption methods are either asymmetric or symmetric.

Asymmetric encryption algorithms are based on the use of public and private keys. Each user has two keys: a public key, which the user can publish freely, and a private key that must be kept secret. The public key is used to encrypt sensitive data to this user, who is the only person holding the private key needed to decrypt this information. Public key systems have the advantage that anyone who was able to obtain an entity's public key can send encrypted data to this entity.

Symmetric encryption algorithms are based on the involved parties sharing a common secret key. This key is used both for encryption and decryption. Thus, symmetric encryption systems provide two-way channels between two or more users. This is simple and a feasible solution for small closed groups of users. However, when the number of users sharing a secret encryption key increases, the shared key becomes a security threat in itself. In practice it is therefore necessary to hold one secret key for every party with whom one wishes to share a secure communication channel.

Two widely used public encryption algorithms are the Rivest-Shamir-Adelman (RSA) algorithm and the Data Encryption Standard (DES) algorithm. These are well described in other security literature. Only DES will be presented in this paper. As we will see later it is the only algorithm that is required by the IPSec standard

Data Encryption Standard (DES)

The Data Encryption Standard (DES) was developed by the U.S. government for public use. DES is a symmetric encryption system, which is relatively easy to implement.

The DES algorithm combines the two fundamental building blocks of encryption: substitution and permutation. Input to DES is divided into blocks of 64 bits, permuted by an initial permutation, and transformed using a 64-bit key. The DES encryption algorithm then runs in cycles:

This process is repeated 16 times. After the last cycle, there is a final permutation, which is the inverse of the initial permutation.

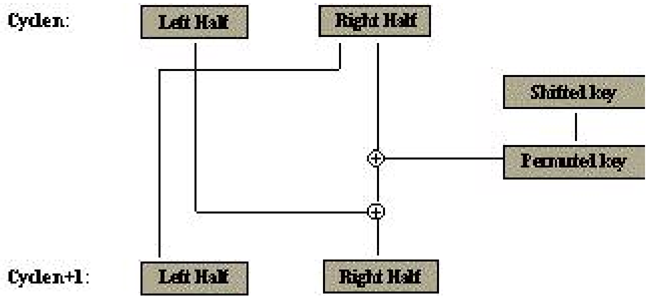


Figure 5: DES cycle

DES with Cipher Block Chaining (DES-CBC) mode

Because DES treats each block of cleartext independently, it is prone to block replay attacks. There is an easy solution to this, called block chaining.

With block chaining, each block is combined with the exclusive or of previous blocks. Let Bx be cleartext blocks, E() the encryption function and Cx encrypted blocks. Then

$$\begin{aligned} C1 &= E(B1) \\ C2 &= E(C1 \oplus B2) \\ C3 &= E(C2 \oplus B3) \end{aligned}$$

and so on. DES in cipher block chaining mode is commonly known as DES-CBC. With DES-CBC identical cleartext blocks does not necessarily produce the same encrypted text.

Today it is most common to use triple DES (also denoted 3DES), which is simply DES applied to the data three times.

A serious objection raised towards DES is the key length of only 56 bits. It has been argued that as hardware costs continue to fall and hardware performance increases, an exhaustive search attack of a DES encryption may become trivial in the near future.

Consideration of key size applies to all situations where keys are employed, including encryption and authentication. The choice of key size depends on many factors, including such obvious ones as the importance of keeping the data confidential and the security of the network that the data will pass over. In addition, the performance cost of encryption and decryption using a large key should also be considered.

Access Control/Authentication:

One of the most important elements of security for a VPN is identifying the user or process that is trying to gain access to the system. This process is called authentication, and is essential in order to control authorization of what resources the person or process has access to and is entitled to use.

Authentication provides proof to both parties in a transaction of the other party's identity. This is fundamental for services such as online banking over the Internet and any other transmission of sensitive information.

An entity, which is to be authenticated, proves its identity by showing its knowledge of a secret. The mechanisms are defined as information exchanges between entities, and where required, information exchanges with a trusted third party (TTP).

The primary means of authentication is a password: a word or string that only one person or a small group of persons know. Such methods are secure only as long as the password remains a secret. Other authentication methods are based on encryption. Such authentication methods are mostly based on secret keys, and can roughly be distinguished into three different classes: symmetric, asymmetric and zero knowledge methods.

Symmetric authentication methods are based on the involved parties sharing a common secret authentication key. It is also possible for the claimant and the verifier to share a secret authentication key with a TTP. This key is used to encrypt specific data. The encrypted data can be deciphered and its contents validated by anyone sharing the entity's secret authentication key. Authentication can also be performed by using a cryptographic hash function, which will be described below.

Authentication with asymmetric signature methods is based on public key algorithms. The claimant corroborates its identity by demonstrating its knowledge of its secret signature key. The signature can be verified by anyone knowing the claimant's public verification key. One way of obtaining a valid public key is by means of certificates distributed by a TTP or any other mutually agreed means.

Finally, there are authentication methods based on the principle of zero knowledge. One method involves using a trusted certificate authority (CA), which provides each claimant with a private digital certificate, based on the claimant's identification data and the certificate authority's private key. Zero knowledge methods can be either symmetric or asymmetric.

All of these core authentication technologies have been used in remote access scenarios for years. Companies have selected from these methods to connect their remote users and their branch offices.

Hash Functions

Hash functions produce a condensed representation (digest) of a block of data such that most changes to the data will also change the reduced form. A message digest is calculated on a block of data prior to being sent and then again after the data has been received. If the two computed digests are equal, then the block of data was most likely not altered during transmission.

Cryptographic hash functions use a cryptographic function as part of the hash function, thus producing a digest that is impossible to fabricate without knowledge of a secret encryption key. Hash functions are used to provide data integrity and authentication for network communication.

Providing a way to check the integrity of information transmitted over or stored in an unreliable medium is a prime necessity in the world of open computing and communications. Mechanisms that provide such integrity check based on a secret key are usually called message authentication codes (MACs). Typically, MACs are used between two parties that share a secret key in order to validate information transmitted between these parties.

Hashed Message Authentication Code (HMAC) [RFC 2104]

HMAC is a MAC mechanism based on cryptographic hash functions. HMAC can be used in combination with any iterated cryptographic hash function. The most widely used such functions are MD5 and SHA. In addition, HMAC also uses a secret authentication key for calculation and verification of the message authentication values.

Message-Digest Algorithm number 5 (MD5) [RFC 1321]

MD5 is derived from the Message-Digest Algorithm number 4 (MD4). The algorithm takes as input a message of arbitrary length and produces as output a 128-bit message digest of the input. It is conjectured that it is computationally infeasible to produce two messages having the same message digest, or to produce any message corresponding to a given message digest.

The MD5 algorithm is a secret key algorithm. MD5 was originally not intended to be used as a keyed hash algorithm, but is primarily intended for digital signature applications, and was designed to be fast.

Secure Hash Algorithm (SHA)

The secure hash algorithm is another variant of the Message Digest algorithm number 4 (MD4). As with MD5, SHA is designed to make it computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which will produce the same message digest.

For a message of length up to 264 bits, the SHA-1 produces a 160-bit message digest. Thus, SHA-1 appears to be a cryptographically stronger function than MD5. The algorithm is well described in Pfleeger

Key exchange

Once encryption and authentication is introduced, VPNs, like other systems that use cryptographic keys, must have a mechanism for distribution of keys to communicating entities.

All key distribution is based on the involved parties already having the means of confidential communication. In symmetric systems, the involved parties need to share a common secret key. In asymmetric systems, they need to hold pairs of private and public keys. These keys are necessary for negotiating or distributing new keys.

Key distribution may be performed either with or without a central key repository. In symmetric systems, it is necessary that both parties wishing to acquire a common secret key have already established a secure way of communication with the key repository. If this is the case, the trusted key repository can supply both parties with a new secret key. Asymmetric key exchange via a key repository can be performed when only one of the parties has an available secure connection with the key repository. Party A may request the public key of party B from the key repository; this key may then be used to communicate the public key of party A to party B.

Most key management protocols support one or more methods to periodically agree on new cryptographic keys. This complicates an entrusted third party's opportunity to break confidentiality by analyzing a large amount of encrypted data, which may be acquired over time by wiretapping the communication lines.

And important principle for development of key management protocols is Perfect Forward Secrecy (PFS). This term refers to the notion that compromise of a single key will permit access only to data protected by this single key. For PFS to exist the key used to protect transmission of data must not be used to derive any additional keys. Furthermore, if the key used to protect transmission of data was derived from some other keying material, that material must not be used to derive any more keys.

The Diffie-Hellman key exchange

This procedure was one of the first practical methods developed for key exchange, and is still very popular. The Diffie-Hellman protocol allows two parties that have never met before to establish a shared secret known only to these parties. The protocol has two public parameters p and g. Parameter p is a large prime number, and parameter g is an integer less than p. Furthermore, for every integer n between 1 and p-1, there is a power k of g such that gk = n mod p.

The procedure of negotiating a secret key between two parties A and B, can be described in six simple steps.

The result is two equal keys, key_a and key_b, that are equal to gxy mod m. Only A and B are able to generate this value. A third party who wishes to calculate this key needs to know the values of both a and b.

However, the Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. An opponent C may intercept A's public value and send his own public value to B. When B transmits his public value, C can substitute it with his own and send it to A. C and A thus agree on one shared key and C and B agree on another shared key. After this exchange, C simply decrypts any messages sent out by A or B, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This weakness is due to the fact that Diffie-Hellman key exchange does not include authentication of the participants. Possible solutions include the use of digital signatures and other protocol variants.

For further details about the Diffie-Hellman key exchange, please refer to [RSA98] or other relevant security literature.

2.2 IP Security (IPSec)

2.2.1 Introduction to IPSec

IPSec is a suite of protocols designed to enable secure IP connections over the Internet. IPSec is developed by the Internet Engineering Task Force (IETF) IP Security Working Group, and the ongoing work since 1995 has resulted in a number of Internet Draft documents (IDs) and Request for Comment documents (RFCs). They all play a part in defining a broad and flexible security infrastructure for the Internet. A good place to start amidst the jungle of IPSec documents is the IP Security Document Roadmap [RFC 2411].

The goal of the IPSec working group was to define protocols that can provide the security features that are lacking in IPv4. The IPSec specification documents define two protocols that are used to provide security services in IPv4 and IPv6. These protocols are the "IP Authentication Header (AH)" [RFC 2402] and the "IP Encapsulating Security Payload (ESP)" [RFC 2406]. The protocols specify two header types that can be used separately or together, depending on what security services are required.

In addition to AH and ESP, the key management protocol is also an important part of IPSec. The current default key management protocol for IPSec is the Internet Key Exchange Protocol (IKE) [RFC 2409], but other key management protocols may be used.

2.2.2 Security Associations

The concept of a "Security Association (SA)" is fundamental in IPSec. The SA contains information about the AH or ESP security services used by a given connection, and is uniquely identified by the triple consisting of the Destination IP Address, the Security Parameter Index (SPI) and the type of security service (AH or ESP).

The SA consists of all the parameters needed to fully specify the security contract, items such as the authentication and encryption algorithms to be used, keying material, key lengths, and key lifetimes. These parameters are organized into a structure called the Security Parameter Index (SPI).

The SPI is an arbitrary value chosen upon establishing the SA. The value zero (0) may be used to indicate that a SA has not yet been established, while the values 1-255 are reserved for future use.

A Security Association can be viewed as a unidirectional channel, offering either AH or ESP security. Note that each SA can only offer one of these security services, so in order to achieve host-to-host communication using both AH and ESP, four SAs are needed.

2.2.3 IP Authentication Header (AH) [RFC 2402]

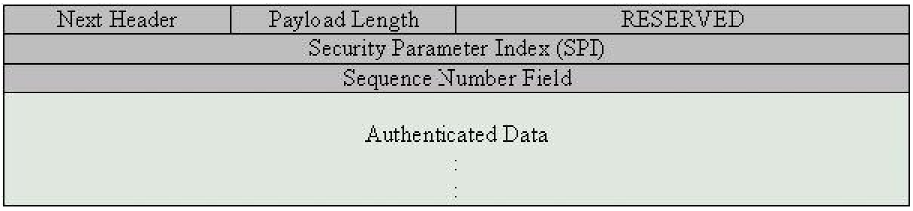
The main purpose of the Authentication Header is to provide data origin authentication of IP datagrams. This is done by computing a cryptographic authentication function over the IP datagram using a secret authentication key in the computation. The receiver verifies the correctness of the authentication data upon reception. Certain fields which must change in transit, such as the "TTL" (IPv4) or "Hop Limit" (IPv6) field, which is decremented on each hop, are omitted from the authentication calculation.

The AH protocol is designed to work with many different authentication algorithms. Presently, two authentication algorithms are considered mandatory for compliance with IPSec. The required algorithms are HMAC-MD5 and HMAC-SHA1.

In addition to authentication, AH also provides connectionless integrity and replay protection. Data integrity is assured by the checksum that is calculated by the message authentication function in use, while replay protection is provided by the use of an AH Sequence Number field.

The AH protocol does not provide confidentiality to IP datagrams. The lack of confidentiality ensures that implementations of the Authentication Header will be widely available on the Internet, even in locations where the export, import, or use of encryption to provide confidentiality is regulated.

Non-repudiation might be provided by some authentication algorithms used with the Authentication Header.



Next Header	Payload Length	RESERVED
Security Parameter Index (SPI)		
Sequence Number Field		
Authenticated Data : :		

Figure 6: AH format

The format of the Authentication Header (AH) is shown in Figure 6. The usage of each of the fields is described below.

Next header: This field simply contains an 8-bit value identifying the following header type. The values are defined by the Internet Assigned Number Authority (IANA).

Payload Length: This 8-bit field specifies the length of the AH in 32-bit words, minus 2.

RESERVED: This 16-bit field is reserved for future use, and is set to 0. Security Parameter Index: This 32-bit field together with the IP destination address, identify the Security Association. The SPI is an arbitrary value chosen upon establishing the SA. The value 0 may be used to indicate that a SA has not yet been established, while the values 1-255 are reserved for future use.

Sequence Number: This 32-bit field indicates the packet's position in a sequence. The sequence number is initialized to 0 upon establishing a SA, and is incremented by one with each sent packet. If replay protection is enabled, this value must never be allowed to cycle. When all sequence number values have been used, a new SA and thus a new key must be established.

Authentication Data: This field contains the Integrity Check Value (ICV) generated by the authentication algorithm. The length of this field is not fixed, and depends on the algorithm specification.

Usage of the Authentication Header will increase the IP protocol processing costs in participating systems and will also increase the communications latency. The increased latency is primarily due to the calculation of the authentication data by the sender and the calculation and comparison of the authentication data by the receiver for each IP datagram containing an Authentication Header.

AH can be used in either transport mode or tunnel mode. This will be described later.

2.2.4 IP Encapsulating Security Payload (ESP) [RFC 2406]

The IP Encapsulating Security Payload (ESP) protocol provides security services for IP datagrams, most importantly confidentiality, which is not provided by AH. ESP optionally also provides the services provided by AH, namely data origin authentication, connectionless integrity and replay protection.

Confidentiality is achieved by encapsulating either an entire IP datagram or only the upper-layer protocol (TCP, UDP, ICMP) data inside the ESP, encrypting most of the ESP contents, and then appending a new cleartext IP header to the now encrypted Encapsulating Security Payload. This cleartext IP header is used to carry the protected data through the entrusted network.

When encapsulating an entire IP datagram, we are operating in tunnel mode. Because this hides the source and final destination IP addresses, we have not only achieved data confidentiality as in transport mode, but also traffic flow confidentiality.

The ESP packet format is designed to keep as much information as possible confidential. Only the information needed to decrypt the payload data on the receiving side is sent as cleartext.

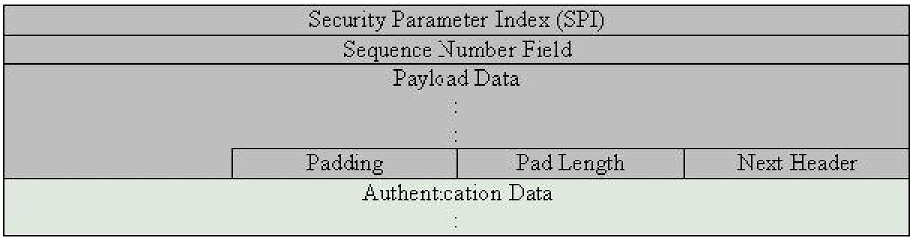


Figure 7: ESP format

The format of the Encapsulating Security Payload (ESP) is shown in Figure 7, and the use of each of the fields is shown below.

It is common to distinguish between the ESP Header, EPS Payload and ESP Footer. The ESP Header consists of the Security Parameter Index (SPI) and the Sequence Number Field, while the ESP Footer consists of the Pad Length, Next Header and the Authentication Data fields.

Security Parameter Index (SPI): This 32-bit field together with the IP destination address, identify a Security Association. The SPI is an arbitrary value chosen upon establishing the SA. The value 0 may be used to indicate that a SA has not yet been established, while the values 1-255 are reserved for future use.

Sequence Number: This 32-bit field indicates the packet's position in a sequence. The sequence number is initialized to 0 upon establishing a SA, and is incremented by one with each sent packet. If replay protection is enabled, this value must never be allowed to cycle. When all sequence number values have been used, a new SA and thus a new key must be established.

Payload Data: This is the actual data carried by the packet, and the type of data is indicated by the Next Header Field. Any cryptographic synchronization data required by the encryption algorithm, e.g. an Initialization Vector (IV), may be carried explicitly in the Payload field. An encryption algorithm that requires such explicit, per-packet synchronization data must indicate the length, any structure for such data, and the location of this data.

Padding: The padding field contains 0-255 randomly generated bytes of data, and can be used for several purposes:

Pad Length: The Pad Length field indicates the number of pad bytes immediately preceding it. The range of valid values is 0-255, where a value of zero indicates that no Padding bytes are present. The Pad Length field is mandatory.

Next header: This field simply contains an 8-bit value identifying the following header type. The values are defined by the Internet Assigned Number Authority (IANA). The Next Header field is encrypted and not possible to reveal until decryption has been performed.

Authentication Data: This field is optional, and is included only if the authentication service has been selected for the SA in question. The Authentication Data field contains the Integrity Check Value (ICV) generated by the authentication algorithm. The length of this field is not fixed, and depends on the algorithm specification.

Confidentiality is achieved by encapsulating data in the encrypted ESP payload. ESP can be used in either transport mode or tunnel mode. This will be described below.

Usage of ESP will increase the IP protocol processing costs in participating systems and will also increase the communications latency. The increased latency is due to encryption and decryption of the ESP Payload, as well as the calculation of the authentication data by the sender and the calculation and comparison of the authentication data by the receiver.

2.2.5 Modes of operation

As we have seen earlier, both AH and ESP can be used in two different modes: tunnel mode and transport mode. The difference between these two modes is that tunnel mode keeps the original IP datagram and packs it into a new packet with additional headers, while transport mode adds new AH and/or ESP headers between the original IP header and the payload. Generally, tunnel mode encapsulates IP layer packets, while in transport mode encapsulates upper layer protocol packets such as TCP and UDP packets.

2.2.5.1 AH transport and tunnel mode

In transport mode the Authentication Header is placed between the original IP header and the IP payload.

In the figures of protocol header formats, the following color codes will be used:

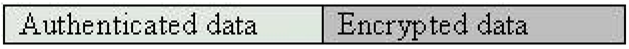


Figure 8: Color codes

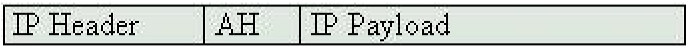
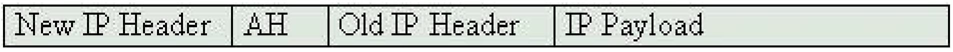


Figure 9: AH, transport mode

The entire original datagram, as well as the AH itself, is authenticated by the authentication mechanism designated by the corresponding Security Association (SA). However, the datagram is transmitted as cleartext, and is vulnerable to wiretapping.

In tunnel mode the original IP datagram is preceded by the AH, which in turn is preceded by a new IP header. The entire datagram is authenticated by the AH protocol, but as with transport mode, the datagram is still transmitted as cleartext. The difference is that the outer IP header is addressed to the unit at the end of the secure tunnel, while the final destination is only visible in the inner IP header.

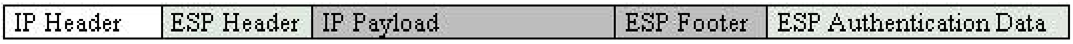


New IP Header	AH	Old IP Header	IP Payload

Figure 10: AH, tunnel mode

2.2.5.2 ESP transport and tunnel mode

Confidentiality is achieved by encapsulating data in the encrypted ESP data. In transport mode only the upper-layer protocol (TCP, UDP, ICMP) data is encapsulated, while the original IP header is retained.

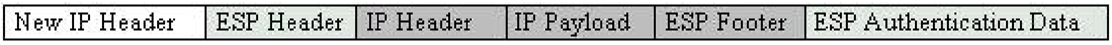


IP Header	ESP Header	IP Payload	ESP Footer	ESP Authentication Data

Figure 11: ESP, tranport mode

The original IP payload is authenticated and encrypted, but not the original IP header. Hence, the source and destination addresses in the outer header are visible while the packet is in transit.

As with AH, we can also choose to encapsulate the entire original IP datagram, and apply a new IP header to the encrypted ESP data. This cleartext header is used to carry the protected data through the entrusted network.

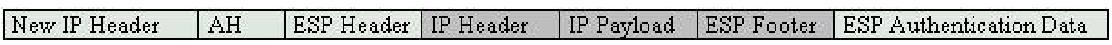


New IP Header	ESP Header	IP Header	IP Payload	ESP Footer	ESP Authentication Data

Figure 12: ESP, tunnel mode

In tunnel mode, the entire original IP datagram is encapsulated in an ESP. Because this hides the source and final destination IP addresses, we have not only achieved data confidentiality as in transport mode, but also traffic flow confidentiality. An ESP tunnel hides internal addressing information, restricting the possibilities for outside parties to perform traffic analysis.

As mentioned earlier, we can also apply both AH and ESP to an IP datagram. The resulting packet format depends on the modes used for AH and ESP. In the case where ESP is applied in tunnel mode and AH in transport mode is shown in Figure 13.



New IP Header	AH	ESP Header	IP Header	IP Payload	ESP Footer	ESP Authentication Data

Figure 13: AH transport mode, ESP tunnel mode

The entire original IP datagram is encapsulated by ESP, and a new IP header generated. AH is then applied between this new IP header and the ESP packet.

Finally, we need to consider when to use transport mode and when to use tunnel mode. Transport mode is normally used between the end points of a connection, while tunnel mode is used to set up secure tunnels between networks. Thus, it is possible for two machines to have a transport mode connection spanning over a secure tunnel between two security gateways. This may result in nesting of AH and ESP. An example of nested AH and ESP and combining modes is shown in Figure 13.

2.3 The Internet Key Exchange (IKE) [RFC 2409]

To allow secure communication with IPSec, a secure protocol for exchanging keys is necessary. The Internet Key Exchange (IKE) is the default protocol for managing keys and Security Associations (SAs) under the IPSec domain, and it is described in [RFC 2409].

IKE is a hybrid protocol that uses a combination of three protocols to negotiate and establish one or more IPSec SAs:

Oakley and SKEME each define a method to authenticate and establish a key exchange, and IKE implements both methods combined with ISAKMP to negotiate and set up keys for the IPSec security association. Parts of the SKEME protocol is also used for fast re-keying using an exchange of random numbers (called nonces).

Before two network nodes can use IPSec to communicate they must first perform authentication to prove their identity, and then establish two Security Associations: The ISAKMP SA and the IPSec SA. The two types of negotiation is performed in two phases:

Phase 1: Authentication and establishment of the ISAKMP SA. This can be considered as a "secure channel" where the two parties agree on how to protect further negotiation traffic between themselves.

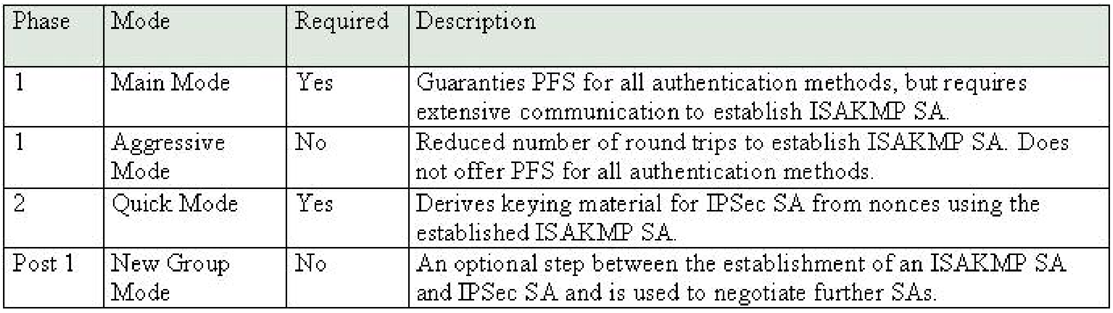
Phase 2: Negotiation of one or many Security Associations on behalf of services such as IPSec or any other services which need keying material and/or parameter negotiation.

The phase term is a part of the ISAKMP protocol described in [RFC 2408].

Both phases may use different exchange types, called modes, to negotiate Security Associations. Phase 1 may use either Main Mode or Aggressive Mode. Main Mode is required by IKE specification, while support for Aggressive Mode is recommended but not required from the implementation. The difference between the two modes is that Aggressive Mode uses fewer transactions to establish the ISAKMP SA, but at the expense of not providing Perfect Forward Secrecy (PFS) for all authentication methods.

Currently phase 2 may use Quick Mode only. There is also a mode called New Group Mode which is not really a phase 1 or phase 2 mode, but may be used after phase 1 to establish a new Diffie-Hellman group to be used in future SA negotiations using Diffie-Hellman exchanges. The Mode term is taken from the Oakley protocol description [RFC 2412]. An IKE implementation may not switch modes in the middle of an exchange.

The table below gives a brief summary of the different modes and their relation to the two phases.



Phase	Mode	Required	Description
1	Main Mode	Yes	Guaranties PFS for all authentication methods, but requires extensive communication to establish ISAKMP SA.
1	Aggressive Mode	No	Reduced number of round trips to establish ISAKMP SA. Does not offer PFS for all authentication methods.
2	Quick Mode	Yes	Derives keying material for IPSec SA from nonces using the established ISAKMP SA.
Post 1	New Group Mode	No	An optional step between the establishment of an ISAKMP SA and IPSec SA and is used to negotiate further SAs.

3.6.1 Phase 1, establishing an ISAKMP SA

When establishing the ISAKMP SA the IKE implicated implementations must negotiate the following attributes:

- encryption algorithm.
- hash algorithm.
- authentication method.
- information about a group over which to do Diffie-Hellman.

For these attributes the IKE specification requires support for:

- DES in CBC mode with weak and semi weak key check.
- MD5 and SHA.
- authentication via pre-shared keys.
- Diffie-Hellman modular exponentiation group 1 (referred to as MODP in Oakley).

The IKE RFC also recommends support for 3DES for encryption, Tiger for hash, the Digital Signature Standard (DSS), RSA signatures and authentication with RSA public key encryption, and MODP group number 2.

Possible authentication methods in addition to the required support for authentication by pre-shared secret are:

- Authentication with signatures. The two parties use certificates acquired from a trusted certificate authority (CA) to identify each other.
- Authentication with public key encryption. The two parties know each other's public keys from a trusted third party and uses RSA Diffie-Hellman algorithms to prove the knowledge of their own private keys.
- Authentication with a revised mode of public key encryption. A simplified public key exchange method which retains the advantages of authentication using public key encryption, but does this with the half public key operations.
- Authentication with a Pre-Shared secret key. The two network nodes share a secret key, which depends on the IP-address of both parties, and uses this key for authentication.

2.3.1 Phase 2, establishing an IPSec SA

After the ISAKMP SA has been established, negotiation of the IPSec SA may be initiated by setting the message ID of the ISAKMP header. As mentioned, communication in phase 2 is done using Quick Mode. The communication is used to derive key material and negotiate shared policy for non-ISAKMP SAs, in our case, one or more IPSec SAs. The phase 2 negotiation is protected by the ISAKMP SA. Quick Mode negotiation is done by exchanging nonces that provide replay protection by frequently generating fresh key material that protects against attackers generating bogus security associations. The key-refresh interval is agreed on in phase 1.

2.4 IPSec summary

In summary, the main features provided by IPSec is network-layer confidentiality, integrity and authentication.

Confidentiality is provided by the Encapsulating Security Payload (ESP). With encryption enabled, it guarantees that information sent over the network cannot be read by parties other than the intended recipients.

Integrity is provided by either or both of the Authentication Header (AH) and ESP with integrity enabled, and guarantees that information sent over the network cannot be changed in transit without the receiver being able to detect that a change was made.

Authentication is provided by AH and/or ESP together with IKE, guarantees that information received from the network was actually sent by the party who claims to have sent it.

E-MERGE

Annex B: Databases and database queries SQL / XML

Version 0.1

28.02.2003

Produced by:
Telmacon

E-MERGE is co-financed by the European Commission DG Information Society

ist information society technologies

Programme name:	Information Society Technologies (IST)
Project ID:	IST-2001-34061
Project acronym:	E-MERGE
Project name:	Pan-European Harmonisation of Vehicle Emergency call Service Chain
Dissemination level[1]**:**	Public

Deliverable number:	IR 3.2
Contractual date of delivery:	25. October 2002
Actual date of delivery:	
Title of deliverable:	Databases and database queries SQL / XML
Work package:	WP 3
Nature of the deliverable:	Confidential
Author(s):	Gerhard Wolfien
Project co-ordinator:	Michael Nielsen (ERTICO) Tel: +32 2 400 07 49, fax: +32 2 400 07 01 E-mail: m.nielsen@mail.ertico.com

Abstract:. This document describes the Databases and database queries SQL / XML

Keyword list:

[1] This is either: Public, restricted to other programme participants, restricted to a group specified by the consortium, confidential – Information about dissemination level can be obtained in 9.5 of the Technical Annex.

Document Control Sheet

Electronic reference:

Main author(s) or editor(s): Gerhard Wolfien

Version history:

Version number	Date	Main author	Summary of changes

Approval:

	Name	Date
Prepared	Gerhard Wolfien	
Reviewed		
Reviewed	Gerhard Wolfien	
Authorised	Michael Nielsen	

Circulation:

Recipient	Date of submission

1 Databases and database queries SQL / XML

Preface
This document covers the DBMS and RDBMS Databases. It descripts the SQL Structured Query Language and the modern XML Schemata's from the view of databases.

2 Databases – DBMS and RDBMS.

Databases are the most common way to store Information. The most common databases called DBMS (Databank-Management-System) – and stores the information in tables, that can be inspect by programs.
An extension to the traditional databases was build up by the theory of rational databases (Rational DBMS or RDBMS) – that not only store the information's in tables, that also define a concept how these information's are related, i.e. that defines how the tables store Information that correspondent to other tables.

Most of the actual legacy databases implements RDBMS schemata's.
In the beginning of implementing databases it was a common way to write specific programs with funktioncalls to read and write the information.

2.1 The Concept of DBMS /RDBMS Systems

The DBMS consist of tables or lists usually are stored on disks – and an engine that manages these tables.
The tables consist of 1 or more columns that store data of a specific type and contents, so as i.e. the first name of a person, a country or the date of an order.
Every table groups a list of columns that have the same structure, i.e. all information of an address (first name, last name, street , city, country) or order information (customer, price, order date).
Every table (list) have zero to many rows, where every row reflects an entry that collects the information.

In former DBMS there was no theory behind the information how they would be store in tables, but RDBMS has changed the view of that.
The information in a table is the minimum information that is needed to reflect the context of the business information, so an orderable does not contains the information of the address. There will be build an extra table for the address – with a uniq identifier, i.e. the customer number. With use of this identifier – named "primary key" every row is clearly addressed.
In the orderable there was implemented a "foreign key" with the contents of the primary key of the address.
So the foreign key points to a row in the address table. To extract the information of an order table it is so needed to read the foreign key – search the primary keys in the address table and return the address information of this row.
This transformation from a universal table – that contains all information's to two or more tables will be called "normalizing" the DBMS.

Another view of that is that specific Information shall be not store in more than one table.
So contains an order table and an invoice table the same addresses. This addresses may be removed and changed to the "primary – foreign key" construct.
A real RDBMS contains hundreds of linkages, so it is for human not longer easy to extract the information of i.e. order tables, and programs take this process.

2.2 Start of SQL

With the start of design of the relational datamodell (1970 IBM) IBM has also designed a query language of storing and retrieving the data from the RDBMS (1974 IBM) which was published 1986 as ANSI Standard SQL-1 or SQL-86 and 1987 as ISO standard.
Today there is standard SQL-3 released (1998) – and most RDBMS databases implements this standard. It includes support for objects. SQL-4 is today in design and implementation.

2.2.1 The Data Manipulation Statements, Select, Insert, Update, Delete

This language was designed as an easy way for humans to retrieval information of the databases.
It consists of keywords that will followed by names that specified the different information's in the database.
i.e.: the keyword SELECT will be followed by the columnames that are in interest for the user; the keyword FROM will be followed by the names of one or more table.
There are additional Keywords that specified relations to the contents of columns

SELECT FirstName, Street, City FROM Address table;
Means in handling language: give me the columns First names, Streets and Cities from the table Address table.
i.e.: *SELECT * FROM Addresstable WHERE City = "Chikago";*
Means: give me ALL columns from the address table where the content of City is Chicago.

The Data Manipulation Statements of SQL are:
SELECT - This will start an extracting of information from the database
INSERT - This will start a storing of information to the database
DELETE - This will start a deleting of information
UPDATE - This will start a changing of information in the database.

Every statement will be followed by other clauses that specify tables or constrains
FROM – will be followed by the table names that will be used
WHERE – will be followed by limitations / constrains for the queries i.e. rules that follows arithmetic rules. So WHERE City = "Chicago" or price = 1200 selects columns that contains Chicago or 1200.
"=" equals
">" greater than; ">=" greater or equals
"<" less than "<=" less or equals

"Like" – i.e.: WHERE City LIKE "Tex%" – all cities that start with "Tex" and followed by none or any characters.
Additional there are a set of logic operators
AND – and i.e. WHERE City = "Chicago" AND Name="Fritz" means select all rows that contains cities with name "Chicago" and also the name "Fritz"
OR – or – Select all that have the one or the other criteria, or that have both criteria's
NOT – not - Select all that have not these criteria.
SQL has a lot of more statements and arithmetic expressions – that will here not be explained, but there are functions to format and convert items, to manipulate the result data and there are arithmetic operations for calculations.

Every statement need necessary the tables on which it will be operate – and columns, and can be followed by limitations.
But the syntax was build near the English language – so it will be different for the SELECT, INSERT, UPDATE, DELETE – clauses.
i.e.:
SELECT Name FROM Table;
INSERT INTO Table (Name, City) VALUES("Fritz","Chikago");
DELETE FROM Table WHERE City = "Chicago"
UPDATE Table SET Name="Fritz", City = "Chicago".

2.2.2 The Columns of SQL-Tables

Every column in SQL consist of a name, a data type, and rules for the filling with information i.e. the data types. There are a large number of data types and so we will here only show some examples.
The most groups are DECIMALS that includes formats for numbers, with or without floating-point, the CHARACTERS and STRINGS formats that contains letters, words and sentences of words , and the groups that contains binary data – that can be interpreted as pictures, program code or whatever we can store on computers.
These groups differ between also by fixed length – and floating length storing information.
So will the data type CHARACTER can specified by a length – so
CHARACTER(20) will store fixed length sentences of characters up to 20 characters.
The CHARACTER VARYING or shorter VARCHAR(20) defines the same Information – but the internal representations differ.
The DEZIMAL group contains INTEGER, SMALLINT, FLOAT, REAL, DOUBLE PRECISION.
There are additional data types for DATE and TIME, for TIMESTAMP and INTERVAL, and also BINARY OBJECTS or BLOBS – that can store any digital information's.

And there are rules for columns, as the can contain information – so it can contain also sometimes nothing – that will named NULL.

With rules the database designer can check some aspects of the inserted data – so the definition VARCHAR(20) City NOT NULL; defines a column of cities names that can contains city names up to 20 characters, and the rule is that it must be entered.

2.2.3 The creation of SQL – Tables

Data tables in SQL will be build by the Statement
CREATE TABLE *Name* which is followed by a list of column names, her data type and additional rules.

So the Statement

```
CREATE TABLE Addresstable {
   VARCHAR(20) CustomerNumber NOT NULL;
   VARCHAR(20) FirstName;
   VARCHAR(15) LastName NOT NULL;
   VARCHAR(30)  Street       NOT NULL;
   VARCHAR(20)  City         NOT NULL;
   DATE              StartDate;
  PRIMARY KEY  (CustomerNumber);
}
```

Defines an Address for a person, where Firstname and Statedate can be omitted at inserting. If there are no LastName the Database will trap an error or if the Streetname is not present. If the Streetname is longer than 30 charakters some databases will send an error or truncated that to 30 characters.

The special keyword PRIMARY KEY defines one or more columns that are used by references from other tables, i.e. ordering Table where

```
CREATE TABLE Ordertable {
    VARCHAR(20) CustomerNumber;
    …….
    FOREIGN KEY (CustomerNumber) Addresstable;
}
```

defines that the CustomerNumber in Ordertable builds a constraints to CustomerNumber in Addresstable.

2.2.4 The SQL-Relations Attributes

With the definition of “Primary-“ and “Foreign Keys” in the creation of tables, and some attributes for Creating , Inserting, Deleting and Updating, that handles the executing of the manipulating the data some aspekts of the rational concept can reflect. Related tables will be updated in order to the statement.

So controls the database by setting the attribute KASKADE, that on inserting a new entry in order table there is an entry (PRIMARY KEY) in Addresstable that will fulfils the containments of the FOREIGN Key contents.
Or in deleting a entry in an master table, correspondings entrys in detail tables will delete also.

2.2.5 Building of SQL Select - Statements

The most needed statement is the select statement – as it is need to extract the information's from the database.

For more clearly we will assume that we have two tables, an "Addresstable" and an "Ordertable". For the Addresstable the contents may be:

```
CustomerNumber, FirstName, LastName, Street, ZipCode
A00012,Smith,Franz,Hirschweg 12,63456
A001045,Schmidt,Richard,Haselbaumstr. 45a,34333
```

And for the Ordertable

```
CustomerNumber, OrderNumber, OrderDate, Price
A00010,R0000,1.1.2000.100.00
A00012,R0012,20.5.2002,1345,00
A00012,R0013,22.5.2002,234,00
A001045,R001,16.7.2002,1111,00
```

The SELECT Statement for retrieving only OrderInformation will be:

```
SELECT * FROM Ordertable WHERE OrderDate >= 18.5.2002,
```

This will result in only 3 Outputs –

```
A00012,R0012,20.5.2002,1345,00
A00012,R0013,22.5.2002,234,00
A001045,R001,16.7.2002,1111,00
```

That matches the criteria Orderdate greater > 18.5.2002

If we want to select also the address information, we need additional the address table – and the linkage criteria.

```
SELECT AddressTable:*, OrderTable:*
  FROM AddressTable, OrderTable
  WHERE   OrderTable.CustomerNumber = AddressTable.CustomerNumber
      AND   OrderDate >= 18.5.2002
      AND   ZipCode >= 60000;
```

That will result in the answer of the Database with:

```
A00012,Smith,Franz,Hirschweg 12,63456,  A00012,R0012,20.5.2002,1345,00
A00012,Smith,Franz,Hirschweg 12,63456,  A00012,R0013,22.5.2002,234,0
```

But this is not the only way to write the Select – there are more possible solutions as in.

```
SELECT AddressTable:*, OrderTable:*
  FROM AddressTable, OrderTable
  WHERE   ZipCode >= 60000
        AND  Addresstable.CustomerNumber =
           (SELECT OrderTable.CustomerNumber
      FROM OrderTable
     WHERE OrderDate >= 18.5.2002)
```

The difference in this way is not the result – it is the time for executing the Statement and they can be differ from seconds to minutes or hours.

2.2.6 The SQL Insert, Delete, Update Statements

This statements are similar to the select statement, and in the WHERE clause can be construct like in the select statement – but the differ in an important thing.
As we can collect information's from many tables in a SELECT statement – this three Statements can work only of one table.
If we wont to insert an new order, we must wrote two statements, one for the insert data in the address table if necessary, and one for the order itself. Problems of this type are also in delete and update statements so that the real sql statements have a great complexity, and it will be necessary to write a lot of statements for some simple problem.

2.2.7 The SQL-DDL Statements, Transactions

As it is necessary to bundle more than one statement SQL has two additional Statements, COMMIT and ROLLBACK the Transactions statements.
COMMIT bundles statements – at the moment as it will executed ALL previous statements must success – or every single statement rolls back – what will say that the changes that the have make will be undo.
The ROLLBACK statement will force this also.
And finical transactions need also this bundle. So requires a finance transaction the decreasing of the account of the buyer, and the increasing of the account for the seller.
Only if both transactions are complete and successful the transaction is complete.

2.3 The SQL-Interpreter

The SQL Interpreter resists between the User interface – which can be a Terminal as minimum and the database-engine that works with the tables. The interpreter analysed the received statement – locate columns, tables, and calculate the necessary operations that the engine execute. In trivial it is like a Basic program – it interprets and for every clause it calls a special function with the parameters (tables, columns).
But in effect today the Interpreter does more. It optimized one or more statements, calculates the need of temporary tables to store intermediate data, and it controls the flow of Statements from the user to the engine – and the data from engine to the user interface.
And here are some not standard extensions to SQL implemented. Often this are needed as the standard does not follow the theory and implementations of RDBMS, and often some extensions are Vendors interest of distinct his product from others.
So we have the situation that we have a standard SQL 3 – but some of the Statements can't be execute on different machines – or result in different results by query.

2.3.1 The SQL- Stored Procedures

As the problem that the most SQL-Statements can't work alone – there was the need to write little programs, but every Vendor has done this on his own way.
The concept of it was mixture languages – Lisp , C , PL/I , Pascal – an implement in the syntax and the parser features to write SQL statements direct in the programs. The names of these languages were build i.e. PL/SQL (Vendor Oracle) what will say that is a mixture of PL/I and SQL.
With this mixed languages most problems can be solved.. As the will received the statement from the user, can do many manipulations – and send them to the SQL-Interpreter
In fact in these procedures the internal database design can be hidden from the user interface, so that a user 'think' he works with an address table – but in fact the information came from different tables.

But – and here is one great problem – there is no standard for stored procedures. Every Vendor has its own design of that – and so it can be not transferred between different types of databases.

2.3.2 The RDBMS and SQL design process

The design of RDMBS databases will be follow the theory and descript in ERP diagrams, and this will today done for the designer with graphical Software – that helps to plan the design – to locate the needed linkages – and helps to control the needed linkages.
There are a lot of tools, some from Vendor side, and some that will be inspirited from the theory.

But the view of the designer is a data-view – his description and design is focused on minimum tables, effective and fast executing for sql-statement – his view is not necessary the view of the business processes, and so there is much communication needed between the business designer and the database designer.

Changing of the database design when the business processes change is a hard way, sometimes it is impossible to change the design in a manner that reflects new business processes.
The Inspiration of Object Orientated Design will be reflecting in RDBMS Systems – but is today in process, there is no fix standard nor there are all the needed SQL Extensions defined for OO design. So the implementations that we found reflect at most standards with Vendor extensions.

2.3.3 SQL More Statements

The SQL-Language has many more statements, attributes and parameters.

So there are spezial names for the WHERE-clause if there are related to links, there are statements for roles and grants of tables and for trusted databases statements that can control the grants on every column.
There are constructions to build views, i.e. predefined sql-statements in the database, that looks likes tables – but most restricted to read only.
And some databases have concepts to handle remote databases like tables store in the database itself.
Spezial statements controls "alias"-names – or controls the controlflow, and constructions that helps automatic processes start.
And from SQL-3 there are statements that helps Object Oriented Designs to reflect in the database. But this process is not finished.

2.4 SQL- summary

SQL was extending in the past years from his beginning – and it works fine and well. But there are today a lot of Problems with it.
First – every Vendor of database engines implements a set of additional Statements and Keywords and sometimes different rules for executing or error trapping.
The design of databases may follow the standard – and need additional programs around it to fulfil the businessreqierments, or it uses the Vendor specific extensions – and will not be run on other Vendor databases.

The useful stored procedures will work only on one Vendor database, and if the are used in design of a database the design is not move to another Vendor, and the same SQL-statement will produces different effects and results on different databases.

SQL, the standard and the vendor specific extensions makes SQL in real world very complicated. A programmer must not only known the SQL Standard – he must be a specialist for a special vendor database.

And – the problem of transactions over more than one database requires additional Software that must reflect the specific characteristics of the different databases.

Transactions with more than one database are not standard, the need always external programming.
The conversation of the columns is often need by different databases, as the internal representations are quit little different.

Information retrieval from different databases often results in large analysis of the internal structure of the databases, often followed by different SQL-Statements for the different databases, a lot of external programming.

As result of this and as a consequence of the internationalisation of information the humans have search for a better way to descript Information, the relations between them and a format to exchange Information.
One of the important solutions is XML – an all around that.
This will cover in the next chapters.

3 The XML-Schema.

For the last years some peoples, institutions and companies build up a new way to define data in a way that based on structures like HTML, but in a universal and uniq way.

XML Focus Topics are:

XML and Business
ebXML (Presentations, Articles, Specifications)
XML Fundamentals & Programming Environment
XML Beginner's Guide, XML Tools (for Java, Windows, Perl, PHP, C/C++, ...)
XML Parsing, Processing and Databases
Data Binding, DOM, SAX, XSL/XSLT/XPATH, XLINK
XML & Databases ...
XML Presentation
XHTML, CSS/XSL/XSL-FO, SMIL, WSUI ...
XML Messaging, Metadata & Web Services
SOAP & XML-RPC, RDF, UDDI, WSDL, Web Services ...
Other XML Topics
XML Security, VoiceXML, ...
(Source: http://www.xml.org)

XML Schemata's can describe any data in a way that can be easily read by human, but also by programs, that use program components called parsers – to analyse and extract the information's in XML files.
A very short excurse to XML and it is use for databases will follow.

3.1 The XML-Schemata in Design

XML is syntax to describe data and the context of data. It has a syntax that is like HTML that will be used for design of web pages. But where the use of HTML is focused of the description of text-styles, the implementation of pictures and text, the focus for XML is to describe datastructur.

The base concept is that data will be explained by tags, like text-styles in HTML.
Every data item will enclosed by an opening tag with a name – and ends with a closing Tag.
The syntax of a tag is very simple it starts with "<" and ends with ">".
Between "<" and ">" there will be the name of the tag. The end tag will be start with "</"
An example of the address looks like that:

```
<ADDRESS>                                    -- Start tag of Address
   <LASTNAME>Smith</LASTNAME>
   <FIRSTNAME>Oliver</FIRSTNAME>
   <STREET>Michigan Road</STREET>
   <COUNTRY>Texas</COUNTRY>
</ADDRESS>                                   -- End tag of Address
```

The implementation of this structure is plain-ASCII-Text, and the writing in different lines is only for human-readability.

This data can be transferred between all servers, computers and programming languages, and can be interpreted by programs in a way that will restore the original context of data. This will be done by parsers, that are reflect the programming schemata for full parsing and then processing or event parsing – that parses and process on the flow of program.

Without the data items this XML-Schemata can describe also the design of database tables. So will

```
<CUSTOMERPAYMENTS>
    <ADDRESSTABLE>
       <CUSTOMERID>A00012</CUSTOMERID>
       <CUSTOMERNAME>Smith</CUSTOMERNAME>
       …..
    </ADDRESSTABLE>
    <PAYMENTTABLE>
      <CUSTOMERID>A00012</CUSTOMERID>
      <PAYMENTNO> R0012</PAYMENTNO>
       <PAYMENTDATE>20.5.2002</PAYMENTDAY>
        …..
    </PAYMENTTABLE>
    <PAYMENTTABLE>
      <CUSTOMERID>A00012</CUSTOMERID>
      <PAYMENTNO>R0013</PAYMENTNO>
      …..
     </PAYMENTTABLE>
</CUSTOMERPAYMENTS>
```

Describe the answer of the above SQL-Query without losing the information of the columns.

3.2 XML-Schemata for definition of Database-Tables

XML –Schemata's can be also used to define the database tables and the references between them, if we omit the dataentrys in the table and define the names or aliases of the tables.

```
<CUSTOMERPAYMENTS>
   <ADDRESSTABLE>CustomerTable1</ADDRESSTABLE>
    <PAYMENTTABLE></PAYMENTTABLE>
</CUSTOMERPAYMENTS>
```

3.3 XSQ-Schemata for Queries

As the data-answer the XML-Schemata can also be used for queries to a database (XSQ), if we use little additional definitions – where we have a little example like the first query.

```
<ADDRESSTABLE>
     <PLZ_LOW>60000</PLZ_LOW>
     <PLZ_HIGH>99999</PLZ_HIGH>
```

```
    <CUSTOMERNO></CUSTOMERNO >
    <CUSTOMERNAME></CUSTOMERNAME >
     ...
<ADDRESSTABLE>
```

This will be interpreted by program to find all entries in the table ADDRESSTABLE in the Range from 60000 to 99999, and send the result as XML answer.

3.4 XML-Schemata to Views , XSL

As the XML-Schemata can be used to describe tables and data items, it also can be used to build up the human readable pages – for example to build up an internet page.
For this there is an special form of XML-Schemata's – XSL (Extended Style Language), that will be describe the transformation from XML Data to fonts, colours etc. to an HTML page by example. This will be done by programs – called XML-processors that will merge data output from XML-Data files with XSL-Files – that describe the viewing of pages.

3.5 XML- for Data transfer, SOAP, UDDI

As XML are in practice only simple ASCII-Textiles, they can be transferred over all existent Networks in an easy way, and between different platforms. It can be done by hand and traditional transfer but also by protocols like SOAP (Simple Object Access Protocol) or UDDI Universal Description, Discovery and Integration specification), by example.
All of these protocols are implementations for so named web services, but here goal is to transfer data from databases to other databases (B2B Communication) or to clients of databases in a uniq and interpretable manner.

As XML is not based on a specific database it will be the modern way to query different databases in a uniq manner.

3.6 XML-Based Concepts

About the universality of XML there are a lot of specialised designs and programs around it – to solve problems in data definitions, data storing, data processing and data viewing, and most of them have names that will start with the X at the beginning. XML-Parsers are used for extracting and analysing, XSL-Style sheets are used for transforming and viewing data, XSQ are for query of databases. But also XML will be used for configuration files up to definition of business processes up to scientific formulas, used to define process flow and the structure of programs.
XML is an international project of the most impotents vendors in the whole world and it's hosted by http://www.xml.org. All that will be coordinated by the W3C (World Wide Web Consortium http://www.w3c.org/) which is not restricted to the internet services – the functionality grows up to telecommunication, finance services and also scientific researches.

3.7 The Middleware between Databases and XML

As XML is so universal for data transfer and datadefinion all database vendors have implemented XML-Interfaces to her databases – or in the phase of implementing interfaces for that – so that in the future XSQ queries and XML-Answers can be direct routed to databases. For legacy systems – that has today no XML interfaces and/or is the need of additional functionality there is an easy way to migrate to XML files.

With the use of XML to database converters it is possible to generate program-interfaces for C++ and Java that will be automatically build up a middleware between programs and the databases.

On one “side” of this components are for the programming language specific functions or method calls – on the other side is an automatic generation of SQL statements – to solve the queries to the database. The queries will be filled with data from program, and the result will be filled in the components.
All this will be generated by definition an XML file that descripts the database.

An important result of this process is that SQL is not longer focused in design process of programs – or in the transfer between different databases.

The way from the Architecture of Business Processes to Business Programs and to databases needs not longer the additional step of handwritten SQL-Statements – and a lot of problems in design and configuration of databases will be hidden to programmers and business designers.

Additional there are a lot of more positive aspects – there is no special vendor of databases needed, or an specific database, the automatic generation process of the middleware makes it easy to switches from one vendor of database to another, or to integrate an another foreign database in the information process.

3.8 XML and another Programs

There are a lot of additional programs that can direct interact with XML-Files – starting from adressbooks up to Spreadsheets and a lot of business- and finance programs. Modern handheld phones can receive and send XML-data, and a lot of customer devices will understand XML in a direct way, so for the future there is no longer need to fill databases with SQL statements – they can read and write them in the direct way.

Annex C: Provisioning of Mobile Network Location - other solutions

Version 0.1

28.02.2003

Produced by:
MIZAR Automazione SpA

*E-MERGE is co-financed by the
European Commission DG Information Society*

Programme name:	Information Society Technologies (IST)
Project ID:	IST-2001-34061
Project acronym:	E-MERGE
Project name:	Pan-European Harmonisation of Vehicle Emergency call Service Chain
Dissemination level[1]**:**	Confidential, only for members of the consortium

Deliverable number:	IR 3.0
Contractual date of delivery:	25. October 2002
Actual date of delivery:	
Title of deliverable:	Telecom Operators Specification
Work package:	WP 3
Nature of the deliverable:	Confidential
Author(s):	Alessandro Murro (MIZAR Automazione SpA) Gino Franco (MIZAR Automazione SpA) Mario Grippa (Comune di Milano)
Project co-ordinator:	Michael Nielsen (ERTICO) Tel: +32 2 400 07 49, fax: +32 2 400 07 01 E-mail: m.nielsen@mail.ertico.com

Abstract:. This document describes other solutions proposed for communication protocol to be implemented by UK and Spain in order to be able to provide GSM Location to PSAPs.

Keyword list: Telecom Operator, GSM, GPRS, Protocol, Standard

[1] This is either: Public, restricted to other programme participants, restricted to a group specified by the consortium, confidential – Information about dissemination level can be obtained in 9.5 of the Technical Annex.

Document Control Sheet

Electronic reference: \\Mizarsrv\SERVIZI\E-MERGE\Docs\WP3\Annex H.doc

Main author(s) or editor(s): Alessandro Murro

Version history:

Version number	Date	Main author	Summary of changes
0.1	28/02/2003	Alessandro Murro	First Draft and review based on Utrecht meeting

Approval:

	Name	Date
Prepared	Alessandro Murro	
Reviewed	Mats Orblom	
Reviewed	Gerhard Wolfien	
Authorised	Michael Nielsen	

Circulation:

Recipient	Date of submission

Table of Contents

1 Introduction

This document describes other solutions proposed for communication protocol to be implemented by UK and Spain in order to be able to provide GSM Location to PSAPs. In fact, waiting the development of an official standard to be adopted for emergency telecomunications, some country specific solutions have been proposed.

2 United Kingdom

UK solution for delivering location data from the Telecom Operator to the PSAP is called « MLP Lite 112/999 », and uses a subset of the Location Interoperability Forum (LIF) Mobile Location Protocol (MLP) Version 3.0.0 (6th June 2002) which is sufficient for mobile operators and Emergency Number Service Operators to implement an initial service where the Emergency Number Operator can request the location of a phone from the Mobile Operator and receive either a valid response or an error response in reply [1]. After initial implementation, some Mobile Operators will implement the functionality to initiate a position fix on the origination of a call to 112 or 999 by the user and push the resulting location information to the Emergency Operator.

MLP Lite is a XML based protocol which currently considers two kind of services:

1. Emergency Location Immediate Service (LIF defined service);
2. Emergency Location Reporting Service (LIF defined service).

The *emergency location immediate service* is used by the Emergency Operator to retrieve the position of a mobile subscriber that has initiated an emergency call from the Mobile Operator. The response to the service is required immediately.

The service consists of the following messages:

- Emergency Location Immediate Request, implemented as HTTP POST (Service Initiation) ;
- Emergency Location Immediate Answer, implemented as HTTP Response (Service Result).

The *emergency location reporting service* is used by the Mobile Operator to push the position of a mobile subscriber that has initiated an emergency call to the Emergency Operator, without a request from the Emergency Operator. Report triggered by the user either originating or releasing a call to 999/112.

The service consists of the following messages:

- Emergency Location Report Request, implemented as HTTP POST (Service Result) ;
- Emergency Location Report Answer, implemented as HTTP Response (Status_code).

MLP Lite considers some error messages such as Generic Error Response, if the request is not accepted, and Position Error Response, if the request is accepted but the position is not available.

3 Spain

The transposition of the European Union 112 number for emergency calls is regulated in Spain by Decree 903/1997. Some major aspects of this regulation are the compatibility of the 112 service with existing emergency telephone numbers, the regional competence –Autonomy Community- to provide the emergency call service in their geographical territory, the cost -free of charge for the citizen- and the provision of the caller localisation [2].

Further regulation has been issued in Spain to develop the conditions to provide the information of the mobile caller location to the emergency services through the European 112 number issued by Order 14 October 1999. The main conditions related to the caller location are the following:

The mobile operator will provide to the Emergency Call Service Provider the automatic line identification and the location of the service cell where the 112 call is originated.

The accuracy of the caller location will be improved according to the technical evolution of the mobile network operator.

No dead lines for the implementation are specified in this Order.

In Spain the main E112 players are the 19 regional Emergency Call Service Providers and the 3 GSM operators – Amena, Telefónica Móviles and Vodafone.

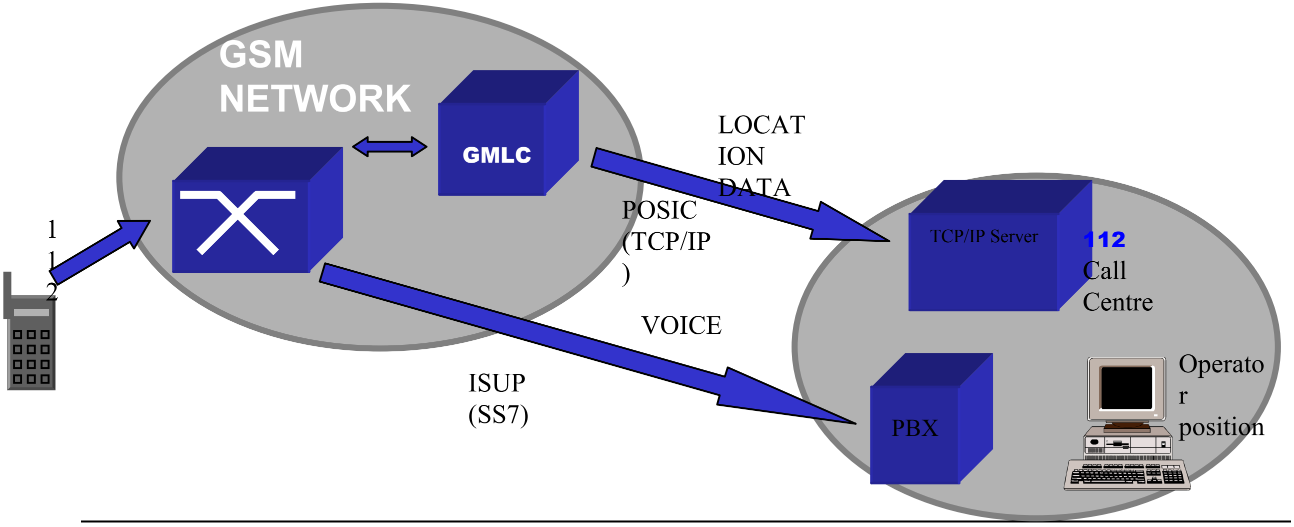
Since November 1999 Spanish GSM operators have carried out efforts to achieve a complete solution for Emergency Services. One first goal was attained in July 2000, when the first location emergency call was routed from the Telefónica Móviles Network to the emergency service operator enriched with the mobile location information.

Following the Madrid 112 demand to GSM operators to achieve a common solution and interface between mobile operators and PSAP, in March 2002 the baseline features were agreed to get a general architecture and protocol.

On the PSAPs side, Madrid 112 has leaded this project by coordinating PSAPs and GSM operators. Since September 16th 2002 Madrid is the one county having emergency service based upon mobile caller location. However, shortly, It is expected all the other Autonomy Communities will implant the E112 service.

3.1 Description of the E112 service

The E112 service implements voice call routing and location data management. When the user makes a call to 112 number, the call is routed to the GMLC so that the location coordinates estimated can be obtained from the Cell Id. Attending to the estimated position the call is routed to the right emergency centre. At the same time, location data is sent via TCP/IP to the same emergency centre employing a protocol called POSIC [2].



The Gateway Mobile Location Centre (GMLC) supports the following functions:

- Provisioning of PSAP;
- Location Calculation;
- Statistics;
- Data management.

When the mobile user calls to 112 a Network Induced method is used to manage the call routing and request the location to the GMLC. The E112 application calculates the Emergency Centre Public Telephone Number according to the estimated caller location and sends the location data to the Emergency Centre through the Public Data Network.

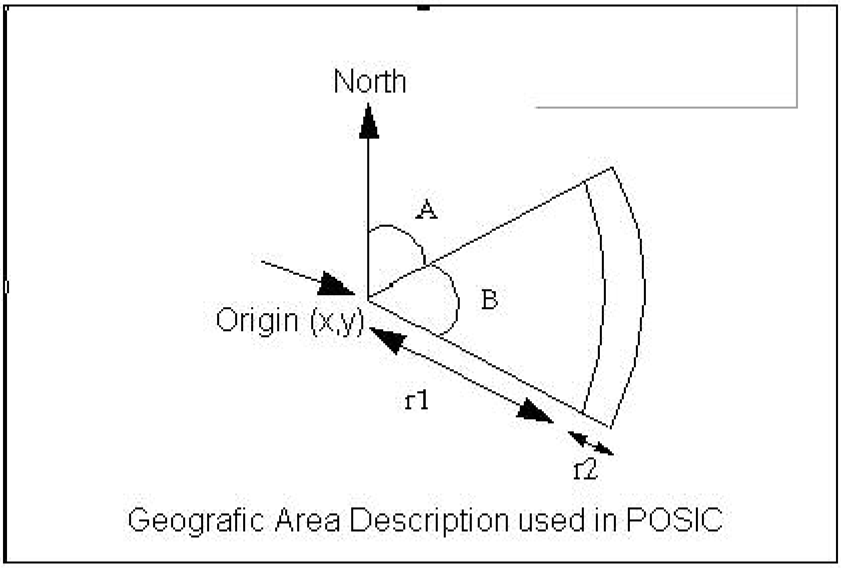
The POSIC (TCP/IP) protocol has been specified to match the particular requirements of the E112 service and features an effective way to transmit short location data messages form PLMN to PSAP in a very efficient mode.

3.2 Interface to the Emergency Call Service Provider (PSAP). POSIC112

When calling 112, location information is sent from PLMN to the PSAP using POSIC protocol over TCP/IP. The information is coded with ASN1 language and includes fields like Service Code, Calling Number, TimeStamp, Quality of Service, Postal Code, County, Province, Number of Zones, Location coordinates and probability radius according to ETSI TS 101 109 V7.1.0) Universal Geographical Area Description (GAD) [2].

3.2.1 POSIC Basic Types Used

- IntegerType. This type is codified in two bytes. The first byte will be the least significant byte and the second the most significant byte.
- ISDNNumberType
- LongIntegerType. This type is an integer codified in four bytes. The first byte will be the least significant byte and the fourth the most significant byte.
- SectorConIncertidumbre. This type of data allows to define a circular sector crown and the probability that the mobile station was inside this circular crown. This type is an adaptation of Ellipsoid Arc type defined in GSM 03.32 document version 7.1.0 (ETSI TS 101 109 V7.1.0) Universal Geographical Area Description (GAD) to give the reference position in UTM co-ordinates. We can see a graphical representation of a sector with a uncertainty radius in the figure below:



A: Offset angle, North origin point clockwise full range
B: Aperture angle, North origin point clockwise with a rage between 1 and 360 degrees.
R1: inner radius.
R2: outer radius.

- Origin: Sector origin point, it is represented by UTM zone in UTM co-ordinates X and Y.
- StringType. StringType is coded as a string that indicate the borrow service. In the case of emergency service 112 it will be ‘112’.
- TimeStampType. In this string it is shown the time in which it was made the position measure. The measure is composed of a set of digits with the next format: yyyyMMddhhmmss
  yyyy: four digits to indicate the year
  MM: two digits to indicate the month
  dd: two digits to indicate the day
  hh: two digits to indicate the hour
  mm: two digits to indicate the minutes
  ss: two digits to indicate the seconds

4 References

[1] Hutchison 3G UK Ltd – « *LIF MLP Lite 112/999* » Version 1.0, 9th September 2002

[2] ETSI OCG-EMTEL – « *EM02td022 - Location of Emergency 122 mobile calls in Spain* » Version 0.1, 15th January 2003

GST RESCUE Newsletter - March 2005

RESCUE Part of GST

Realising GST RESCUE

Rapid delivery of the appropriate emergency services can be the difference between life and death for a road accident victim. To help reduce the number of casualties on Europe's roads each year, the recently launched EC-supported and ERTICO co-ordinated GST RESCUE project, which is a three-year sub-project within the Integrated Project GST (Global System for Telematics). GST RESCUE aims to optimise the delivery of data from in-vehicle emergency call systems and its subsequent use by stakeholders in the emergency service chain. Not only will in-vehicle emergency calls deliver to the dispatch centre such critical information as location and accident severity data, but the emergency vehicles themselves will use this information to employ a navigation solution and warning system permitting them to arrive safely on the scene as quickly as possible.

The GST vision is that all future vehicles will be equipped with various communication means to interact with each other and their environment based on a common architecture and standard interfaces. Drivers and occupants will be able to rely on their on-board, integrated telematics system to access a dynamic offer of on-line safety-, efficiency- and comfort-enhancing services wherever they drive in Europe.

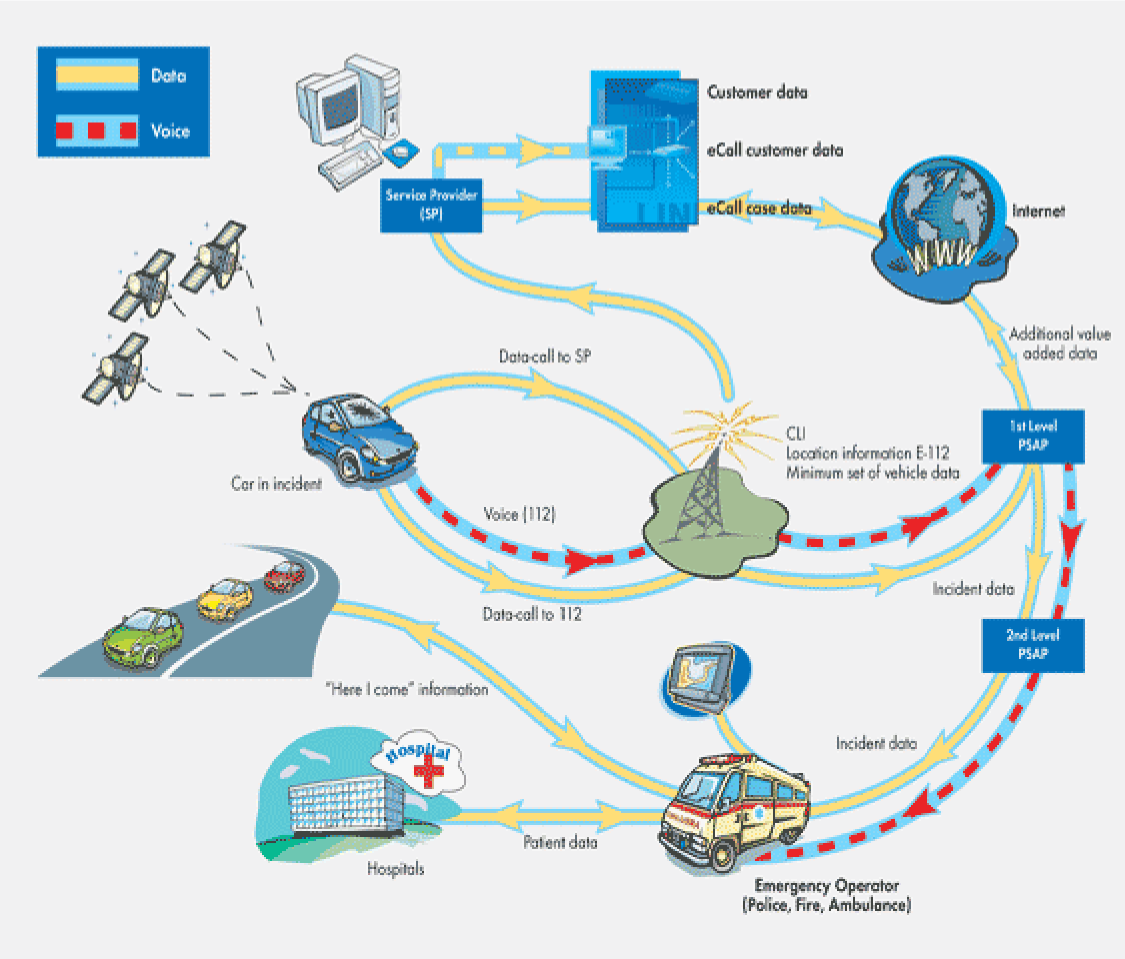
The work of GST and its subprojects will feed directly into the efforts of GST RESCUE to improve the information flow and operation of the rescue chain. Managed by ERTICO, the project has 11 consortium members representing car manufacturers, network operators, public safety answering points (PSAPs), technology providers and emergency operators. This variety of input ensures a complete view of the emergency service chain.

Optimising eCall

Until it wraps up its work in February 2007, GST RESCUE will optimise the initialisation of the in-vehicle eCall via an expert system and the data delivery to the emergency dispatch centers and emergency vehicles. The in-vehicle data will be similar to those defined and agreed on by the stakeholders in the eSafety Driving Group on eCall and the E-MERGE and AIDER projects. When the emergency vehicles have the proper incident information, a hybrid navigation solution will help guide the driver to the scene.

In addition, the project intends to test vehicle-to-vehicle communication methods that will enable the use of a "blue corridor" system to notify other drivers of an emergency vehicle's approach as well as a coning system to warn approaching vehicles of the scene. Finally, when the emergency vehicles leave the scene, it will be possible to remotely report and transfer data (e.g. about the patient) to hospitals or other rescue units. Specifically, it will test the transmission of eCall voice and data between all elements in the GST RESCUE service chain (see figure for complete GST RESCUE overview).

Ultimately the success of the developed solution will be evidenced in shorter reaction time, safer response, more complete incident information, and increased communications amongst the various players which will lead to faster and better medical intervention and thus reduced casualties.



First GST workshop
As part of the GST Forum Workshop held 7-8 September 2004 in Brussels, GST RESCUE had a breakout session in order to get input from the GST RESCUE Forum regarding the GST RESCUE user requirements. The GST RESCUE consortium took a visual approach and showed a video illustrating the various parts of the rescue chain. A good discussion about GST RESCUE Use Cases followed as participants were able to easily see in the video the problems that GST RESCUE is trying to solve.

One of the session's main discussions focused on what triggers an automatic eCall. The main conclusion was that the consortium must identify the number of existing sensors in the vehicle today and prioritise them according to the expected severity of the incident. (For example, a triggered heat sensor might not have the same impact as an air back sensor.) Another question related to the thresholds for triggering a sensor - which is pertinent to the vehicle manufacturers. Thus, the main conclusion was that GST RESCUE will examine the thresholds and discuss its findings with the vehicle manufacturers in order to make a joint decision.

The session also discussed:

- What information is needed for the route guidance system to be fitted in the emergency vehicles?
- How can the “Blue Wave” - emergency vehicles transmitting a virtual blue light to other road users - be demonstrated and realised?
- Can the Virtual Cones be extended to other road users in a data light method?

Thanks to these discussions, the Consortium has a clearer idea of what its next activities will be. The input from the GST RESCUE Forum regarding the user requirements was also beneficial to clarify some of the issues for the upcoming architectural phase.

The next activity within GST RESCUE is to complete the architecture and specifications. GST will host an Architecture Workshop 24-25 May, with the objective to validate and discuss the approach taking by GST and GST RESCUE. Apart from the 49 GST Partners, anyone which has an interest in GST project or its subprojects is welcome to participate.

Join the GST RESCUE Forum!
To encourage the widest possible participation in the project and to gain consensus on proposed solutions, GST RESCUE has created a Forum. Members of the Forum:

- Have access to all important documents
- Are encouraged to provide comments and reactions
- Are invited to participate in future workshops

Membership of the Forum is open to all interested actors, although it is envisaged to be of particular interest to car manufacturers, service providers, automobile clubs, public authorities, emergency operators, civil protection authorities and related industry such as equipment manufactures and map providers. Membership is free, including attendance to the workshops, but members are responsible for their own travel, accommodation and other costs for attending the workshops.

Currently, the GST RESCUE Forum has 204 members representing a wide range of stakeholders. To become a member, please visit the **GST RESCUE website**.

For more information, please contact GST RESCUE Project Coordinator **Rasmus Lindholm**

GST RESCUE Consortium Partners
ERTICO, CRF, France Telecom, Kreis Offenbach, Mizar, Motorola, Orange,
Petards, Sussex Police, TNO, Volvo