

**OTIF**



**ORGANISATION INTERGOUVERNEMENTALE POUR  
LES TRANSPORTS INTERNATIONAUX FERROVIAIRES**

**ZWISCHENSTAATLICHE ORGANISATION FÜR DEN  
INTERNATIONALEN EISENBAHNVERKEHR**

**INTERGOVERNMENTAL ORGANISATION FOR INTER-  
NATIONAL CARRIAGE BY RAIL**

**INF. 3**

21 June 2013

Original: German

**RID/ADR/ADN**

Joint Meeting of the RID Committee of Experts and the Working Party on the Transport of Dangerous Goods (Geneva, 17 – 27 September 2013)

**Agenda item 6: Reports of informal working groups**

**Report of the 11<sup>th</sup> session of the working group on telematics (Tegernsee, 3 and 4 June 2013)**

**Transmitted by the Secretariat of OTIF**

1. At the invitation of Germany, the 11<sup>th</sup> session of the working group on telematics was held in Tegernsee on 3 and 4 June 2013. The meeting was chaired by Mr Helmut Rein (Germany).
2. The following States took part in the discussions at this session: Belgium, France, Germany, Netherlands, Sweden and the United Kingdom. The European Railway Agency (ERA), the Intergovernmental Organisation for International Carriage by Rail (OTIF), the European Chemical Industries Council (CEFIC), the International Road Transport Union (IRU), the International Tank-Container Organisation (ITCO), the International Union of Railways (UIC), the International Union of Wagon Keepers (UIP) and the Association of the European Rail Industry (UNIFE) also took part in the meeting (see Annex I).

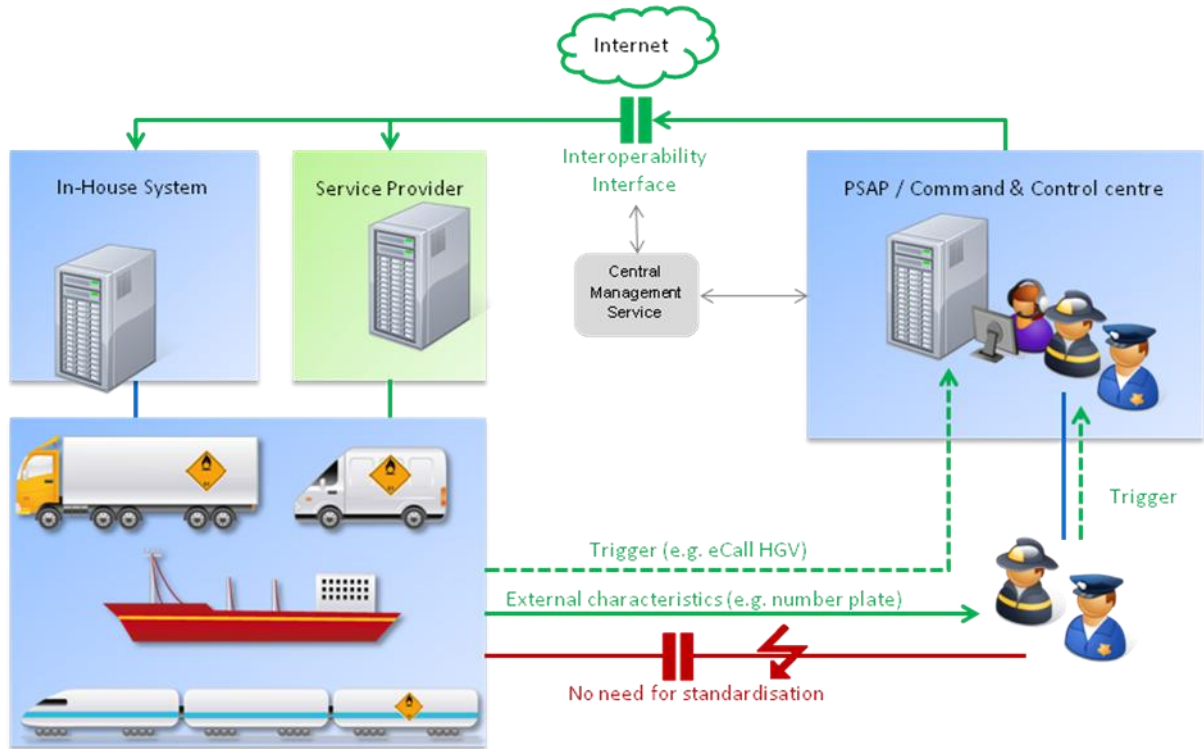
For reasons of cost, only a limited number of copies of this document have been made. Delegates are asked to bring their own copies of documents to meetings. OTIF only has a small number of copies available.

**Preliminary results of the German research project**

- The contractors carrying out the German research project, Mr Kaltwasser, Mr Otten and Mr Harrod Booth, used the presentations attached in annexes II (System Architecture), III (Standardisation) and IV (IT Security) to provide a summary of the working group's discussions to date, and to introduce a telematics system architecture for use of the electronic transport document and to improve emergency management in the carriage of dangerous goods. These could be used as the basis for further discussions and projects.

Application scenario

- The following diagram clarifies the application scenario:



The transport undertakings input all the data necessary for the transport of dangerous goods into their own database or into a database belonging to a service provider of their choice. These databases, for which existing systems can be used, are considered to be Trusted Party 2 (TP2).

In transport checks or intervention by the emergency services, externally recognisable characteristics, such as vehicle markings and wagon numbers, are transmitted by the inspection personnel or emergency services to their respective control centres, which then use an internet-based interface (central management service, Trusted Party 1) to retrieve data from Trusted Party 2. In so doing, Trusted Party 1 ensures that access to the data input by the carriers can only be obtained via authorised entities. It also checks the authorisation of the TP2 parties. The same procedure is also used for automated signals sent directly from the vehicle to the control centre (e.g. eCall).

As the systems shown on the left and right-hand sides of the diagram are already available, only the central management service has to be set up, which deals with the retrieval of and access to the data. This should preferably be set up at European Commission level as the single central body.

5. The working group unanimously welcomed the approach presented. In so doing, the representative of ERA highlighted that this approach **should be compatible** with the TAF TSI (Technical Specifications for Interoperability – Telematic Applications for Freight Transport). **However, a detailed analysis of the technical possibility of implementing the proposed concept in relation to the TAF TSI should be carried out. In addition to this, a cost/benefit analysis for rail transport should be carried out.**
6. The representative of the United Kingdom, who, at previous meetings, had expressed his general scepticism towards telematics applications because of the anticipated negative cost/benefit ratio, particularly supported this approach, as it assumed that existing hardware and software systems could be used, and it made it possible for the Member States to introduce the necessary measures simply. The relatively low investment costs would be accompanied by its usefulness both for transport undertakings, which could use existing data, and for the emergency services and control authorities, which would have rapid access to these data.

#### Design decisions

7. The working group paid particular attention to the design decisions set out in the presentation:
  - No regulations would be made as to how the system should be organised nationally. As a result, it would perhaps also be possible to equip every member of staff in the control authorities or emergency services with a portable terminal so that they could retrieve data directly, rather than via a control centre.
  - Existing certificates issued by commercial providers can be used for the central registration.
  - Each individual transport undertaking can make its own decision as to whether the transport documentation is produced in electronic or paper format. However, it is anticipated that a lot of undertakings would stop using the paper format very quickly, as they already have electronic systems available with which, for example, the delivery of a consignment is confirmed. In this respect, the system shown provided a way of arranging the possibility set out in RID/ADR/ADN 5.4.0 of using electronic systems instead of paper documents.
  - The certificates are not issued for individuals, only for organisations.
  - As for the paper document, access to the whole document is ensured for authorised organisations.
  - The certificates are used to secure the communication between the end points and for digital signatures.
  - To ensure interoperability, services must be certified.
  - No continuous monitoring is required for TP2 services. However, consideration must be given to the requirements that need to be contained in the regulations in cases where a service is temporarily unavailable.
  - TP2 services must be registered with a central registration body (TP1). A federative system for TP1 services was only considered as a secondary solution if the European Commission is not prepared to operate a TP1 service (see also paragraphs 4 and 12).
  - Use of internet for communication.
  - Use of open interfaces to enable future development.

## INF.3

- The system must firstly enable automatic retrieval on the basis of the vehicle identification number (e.g. eCall) and secondly retrieval on the basis of data provided by a casual observer (e.g. location, registration plate). It must be possible to retrieve the entire data set on the basis of these data.
  - The carrier must have all the data concerning the dangerous goods being carried.
  - The data structure must depict the organisation principles used for the paper document.
8. The working group did not call these design decisions into question, **whereas the consequences of the design decisions could not be assessed without further analysis.**

### System architecture

9. In principle, the working group was of the view that the architecture presented was good. However, none of the representatives were able to state on behalf of their State or association that this was the only possible way. In the French and Swedish projects (see paragraphs 20 to 22), this basic structure is assumed, and its assumptions will be verified in the context of these projects. The working group should prepare any further details necessary on the basis of this architecture.

### Future work

10. The final report of this research project financed by Germany, which will be available at the end of July 2013, would be sent to all delegates. The data model it describes would be freely available and could be used by software undertakings.
11. The findings will be submitted to the Joint Meeting and the European Commission's Dangerous Goods Regulatory Committee so that the RID/ADR/ADN Contracting States could give their views on the basic concept and if necessary, propose modifications that could be fed in to the working group's future work.
12. The European Commission is asked to host Trusted Party 1 (TP1) at Commission level in order to avoid a federative solution (see also paragraph 4 and the tenth indent of paragraph 7). The meeting was reminded that the Commission fulfilled a similar function for transport of animals, where there was also an interface with non-EU Member States.
13. The working group also recommended having a discussion in the Dangerous Goods Regulatory Committee with the Commission bodies responsible for telematics. In connection with this, the working group again pointed out that a number of the Commission's telematics projects addressed dangerous goods issues which were not harmonised with the working group.
14. Once the Joint Meeting had taken a decision of principle, basic provisions for RID/ADR/ADN and criteria would have to be drafted, which should be covered by standardisation. As it took at least two years to draft standards, a date of entry into force of 2017 seemed a little ambitious. It had to be remembered that not all Member States had followed the working group's activities and that they would first need information on the technical feasibility and anticipated costs.

### **Telematics in transport**

15. With the help of the presentation in Annex V, Mrs Dannelke (German Ministry of Transport) gave a general overview of satellite navigation, navigation applications and telematics in transport.

## Developments in the TAF TSI in relation to the transport of dangerous goods

16. Using his presentation (see Annex VI), Mr Gutiérrez (ERA) explained that most of the information listed in section A of the "Who does what" table would be taken over into the TAF TSI data catalogue. He emphasised that the main aim of the TAF TSI was not to improve safety, but to ensure interoperability in the exchange of data in rail freight transport. **With regard to real time applications, other developments had to be considered, for example GSM-R applications, before anything could be said about the possibility of implementing the proposed concept in a cost-effective manner.**
17. The working group noted that the TAF TSI that was presented reflected the current legal status of RID and that **therefore, in addition to the existing standard for the electronic transport document of the eRailFreight project, on which the relevant data structure of the TAF TSI was based, another system was** in place which covered rail transport in terms of the left-hand part of the diagram in paragraph 4 (TP2) and which the control centres for control personnel or the emergency services could **possibly have access to in future via a dedicated TP1**. As the TAF TSI was only binding on the EEA Member States and Switzerland, transposition into Uniform Technical Prescriptions in accordance with Appendix F to COTIF should be kept in mind.

### eCall HGV

18. Mr de Waal (Dutch Ministry of Transport) presented a film showing developments in connection with eCall for the carriage of dangerous goods (<http://www.youtube.com/watch?v=zmOCc0qFmSg>).
19. Based on the application scenario for the retrieval of complete information, as shown in the diagram in paragraph 4, in contrast to previous statements that had been made, the working group no longer considered it necessary that eCall should provide a minimum data set for dangerous goods. As both eCall signals and the retrieval of dangerous goods data took place via the emergency services' control centre, the working group thought it was sufficient to transmit a unique identification number to the control centre.

### Swedish project

20. Mrs Rydberg (Security Arena Lindholmen) referred to a Swedish project in which requirements of the competent authorities for telematics applications in the transport of dangerous goods were being evaluated.

### GeoTransMD

21. Mr Pfauvadel and Mr Méchin (French Ministry of Transport) gave the presentation in Annex VII. This concerned a French project which, based on the system architecture presented in the German research project, which was adopted by the working group (see paragraph 9), would include, among other things, testing Trusted Parties TP1 and TP2. The project, which started in June 2013, would run until 31 May 2016.
22. The working group said it wished those points that had an impact on legislation and standardisation to be brought forward so that they would be available in time to enter into force on 1 January 2019. **ERA asked if rail transport was also being considered in the scope of the project and whether the project took international and multimodal case studies into account. The representatives of France replied that they would consider involving the railway sector more closely in the project.** Other points that would have to be investigated in relation to the architecture, such as the evaluation and optimisation of the data traffic in TP1, the certification infrastructure and feasibility testing, were included directly in the presentation by France and are reflected in Annex VII.

**LIST OF PARTICIPANTS**  
**of the Joint Meeting working group on telematics (Tegernsee, 3-4 June 2013)**

	Name of Participant	Body represented	Address	Phone	Fax	E-mail
<b>Representatives of the Contracting States/Member States, international organisations and the European Commission:</b>						
1	Bailleux, Caroline	Belgium (Min.)	Service Public Fédéral Mobilité et Transports Rue du progrès, 56 B – 1210 Bruxelles	+32-2-277-3916	+32-2-277-4055	<a href="mailto:Caroline.Bailleux@mobilite.fgov.be">Caroline.Bailleux@mobilite.fgov.be</a>
2	Rein, Helmut	Germany (Min.)	Bundesministerium für Verkehr, Bau und Stadtentwicklung – Referat UI 33 – Robert-Schuman-Platz 1 D – 53175 Bonn	+49-228-99-300-2640	+49-228-99-300-807-2640	<a href="mailto:helmut.rein@bmvbs.bund.de">helmut.rein@bmvbs.bund.de</a>
3	Schwan, Gudula	Germany (Min.)	Bundesministerium für Verkehr, Bau und Stadtentwicklung – Referat UI 33 – Robert-Schuman-Platz 1 D – 53175 Bonn	+49-228-99-300-2641	+49-228-99-300-807-2641	<a href="mailto:gudula.schwan@bmvbs.bund.de">gudula.schwan@bmvbs.bund.de</a>
4	Dannelke, Sabine	Germany (Min.)	Bundesministerium für Verkehr, Bau und Stadtentwicklung – Referat UI 35 – Invalidenstraße 44 D – 10115 Berlin	+49-30-18-300-2660	-	<a href="mailto:sabine.dannelke@bmvbs.bund.de">sabine.dannelke@bmvbs.bund.de</a>
5	Hoffmann, Alfons	Germany (Min.)	Bundesministerium für Verkehr, Bau und Stadtentwicklung – Referat UI 33 – Robert-Schuman-Platz 1 D – 53175 Bonn	+49-228-99-300-2645	+49-228-300-99-807-2645	<a href="mailto:alfons.hoffmann@bmvbs.bund.de">alfons.hoffmann@bmvbs.bund.de</a>

6	Pfauvadel, Claude	France (Min.)	Ministère de l'Écologie, de l'Énergie, du Développement Durable et de l'Aménagement du Territoire Mission du Transports des Matières dangereuses Arche Nord F – 92055 Paris la Défense Cedex 04	+33-1-4081-8766	+33-1-40811065	<a href="mailto:claud.pfauvadel@equipement.gouv.fr">claud.pfauvadel@equipement.gouv.fr</a>
7	Méchin, Jean-Philippe	France (CETE SO)	Centre d'Études Techniques de l'Équipement du Sud Ouest (CETE SO) Département Informatique et Modernisation Rue Pierre Ramond Caupian, BP C F – 33165 Saint-Médard-en-Jalles cedex	+33-55670-6575	+33-1-40811690	<a href="mailto:jean-philippe.mechin@developpement-durable.gouv.fr">jean-philippe.mechin@developpement-durable.gouv.fr</a>
8	Leminh, Marc	France (NOVACOM)	NOVACOM-Services 8-10 rue Hermès Parc Technologique du canal F – 31520 Ramonville Saint Agne	+33-56139-5011	+33-56139-5001	<a href="mailto:marc.leminh@novacom-services.com">marc.leminh@novacom-services.com</a>
9	Dr. Ruffin, Emmanuel	ERA (Safety Unit)	European Railway Agency (ERA) Safety Unit 120 rue Marc Lefrancq BP 20392 F – 59307 Valenciennes Cedex	+33-3-2709-6707	+33-3-2709-6807	<a href="mailto:emmanuel.ruffin@era.europa.eu">emmanuel.ruffin@era.europa.eu</a>
10	Gutiérrez Domínguez, Rodrigo	ERA (Interoperability Unit)	European Railway Agency (ERA) Interoperability Unit 120 rue Marc Lefrancq BP 20392 F – 59307 Valenciennes Cedex	+33-3-2709-6764	+33-3-2709-6608	<a href="mailto:rodrigo.gutierrez@era.europa.eu">rodrigo.gutierrez@era.europa.eu</a>
11	De Waal, Johannes Frederik	Netherlands (Min.)	Ministry of Infrastructure and Environment Plesmanweg 1-6 NL – 2597 JG Den Haag	+31-70-456-6845	-	<a href="mailto:hans.de.waal@minienm.nl">hans.de.waal@minienm.nl</a>
12	Conrad, Jochen	OTIF	Intergovernmental Organisation for International Carriage by Rail (OTIF) Gryphenhübeliweg 30 CH – 3006 Bern	+41-31-359-1017	+41-31-359-1011	<a href="mailto:jochen.conrad@otif.org">jochen.conrad@otif.org</a>
13	Guricová, Katarina	OTIF	Intergovernmental Organisation for International Carriage by Rail (OTIF) Gryphenhübeliweg 30 CH – 3006 Bern	+41-31-359-1016	+41/31-359-1011	<a href="mailto:Katarina.Guricova@otif.org">Katarina.Guricova@otif.org</a>

14	Skärdin, Brita	Sweden (Min.)	Swedish Civil Contingencies Agency Hazardous Substances Section Norra Klaragatan 18 SE – 651 81 Karlstad	+ 46-10-240-5495	+46-10-240-5600	<a href="mailto:brita.skardin@msb.se">brita.skardin@msb.se</a>
15	Rydberg, Gunilla	Sweden (S&T)	Security Arena Lindholmen Sjöländ & Thyselius Box 6238 SE – 10234 Stockholm	+46-761416947	-	<a href="mailto:gunilla.rydberg@st.se">gunilla.rydberg@st.se</a>
16	Hart, Jeff	United Kingdom (Min.)	Department for Transport Dangerous Goods Division Zone 3/19 Great Minster House 33 Horseferry Road GB – London SW1P 4DR	+44-20-7944-2758	+44-20-7944-2039	<a href="mailto:jeff.hart@dft.gsi.gov.uk">jeff.hart@dft.gsi.gov.uk</a>
17	Trojanowska, Valerie	United Kingdom (Min.)	Department for Transport Dangerous Goods Division Zone 3/19 Great Minster House 33 Horseferry Road GB – London SW1P 4DR	+44-20-7944-2754	+44-20-7944-2039	<a href="mailto:valerie.trojanowska@dft.gsi.gov.uk">valerie.trojanowska@dft.gsi.gov.uk</a>
18	Dr. Kaltwasser, Josef	Germany (FV Telematik)	AlbrechtConsult GmbH Theaterstr. 24 D – 52062 Aachen	+49-241-400-29025	+49-241-500-718	<a href="mailto:josef.kaltwasser@albrechtConsult.com">josef.kaltwasser@albrechtConsult.com</a>
19	Lüpges, Christian	Germany (FV Telematik)	AlbrechtConsult GmbH Theaterstr. 24 D – 52062 Aachen	+49-241-446-89708	+49-241-500-718	<a href="mailto:christian.luepges@albrechtconsult.com">christian.luepges@albrechtconsult.com</a>
20	Dr. Otten, Marcus	Germany (FV Telematik)	Otten software GmbH Röntgenring 7 D – 40878 Ratingen	+49-2102-30964-10	+49-2102-30964-29	<a href="mailto:mo@otten-software.de">mo@otten-software.de</a>
21	Dr. Harrod Booth, Jonathan	United Kingdom (FV Telematik)	Harrod Booth Consulting Ltd. (HBC) Denton New Park Road GB – Cranleigh, Surrey, GU6 7HJ	+44-7990520404	-	<a href="mailto:jon@harrodbooth.com">jon@harrodbooth.com</a>
<b>Representatives of international and European associations:</b>						
22	Heid, Andrea	CEFIC (VCI)	Verband der Chemischen Industrie e.V. (VCI) Mainzer Landstraße 55 D – 60329 Frankfurt/Main	+49-69-2556-1444	+49-69-2556-1535	<a href="mailto:heid@vci.de">heid@vci.de</a>
23	Marmy, Jacques	IRU	International Road Transport Union (IRU) 3, rue de Varembe – P.O. Box 44 CH – 1211 Geneva 20	+41-22-918-2720	+41-22-918-2741	<a href="mailto:jacques.marmy@iru.org">jacques.marmy@iru.org</a>



24	Köppen, Jochen	ITCO (Köppen GmbH)	Köppen GmbH Arnold-Dehnen-Straße 20-24 D – 47138 Duisburg	+49-203-42993-13	+49-203-42993-34	<a href="mailto:Jochen.Koeppen@koeppen-du.de">Jochen.Koeppen@koeppen-du.de</a>
25	Gutbrod, Ralf	RAILDATA	RAILDATA Centralbahnstr. 11 CH – 4051 Basel	+41-61461-5375	+41-61461-5228	<a href="mailto:gutbrod@raildata.coop">gutbrod@raildata.coop</a>
26	Heintz, Jean-Georges	UIC (SNCF)	Union Internationale des Chemins de fer (UIC) 16, rue Jean Rey F – 75015 Paris	+33-1-5325-3028	-	<a href="mailto:heintz@uic.org">heintz@uic.org</a>
27	Kogelheide, Rainer	UIP (GATX)	GATX Rail Germany GmbH Valentinskamp 70 D – 20355 Hamburg	+49-40-36804-8232	+49-40-36804-112	<a href="mailto:rainer.kogelheide@gatx.eu">rainer.kogelheide@gatx.eu</a>
28	Haltuf, Miroslav	UNIFE (OLTIS Group a.s.)	OLTIS Group a.s. Washingtonova 1567/25 CZ – 110 00 Praha 1	+420-724001958	-	<a href="mailto:miroslav.haltuf@oltisgroup.cz">miroslav.haltuf@oltisgroup.cz</a>
<b>Interpreter:</b>						
29	Ashman, David	OTIF	Intergovernmental Organisation for International Carriage by Rail (OTIF) Gryphenhübeliweg 30 CH – 3006 Bern	+41-31-359-1024	+41-31-359-1011	<a href="mailto:david.ashman@otif.org">david.ashman@otif.org</a>

# Project of the Federal Ministry of Transport, Building and Urban Development

-

“Project to develop a telematics system architecture  
to deploy the electronic transport document and to  
improve emergency management in the transport of  
dangerous goods”

-

## Preliminary results



**Josef Kaltwasser**  
**AlbrechtConsult GmbH**

**WG on Telematics on 3-4<sup>th</sup> June 2013**

## Outline

- ▶ **Scope and framework conditions**
- ▶ **From the previous R&D project to the current project**
- ▶ **Project introduction**
  - General concept
  - Focus topics
    - IT standards and trigger mechanisms
    - IT security mechanisms
    - Data model adaptations
  - Telematics system architecture and service interfaces
  - Mock-up demo
- ▶ **Conclusions**

## Scope and framework conditions



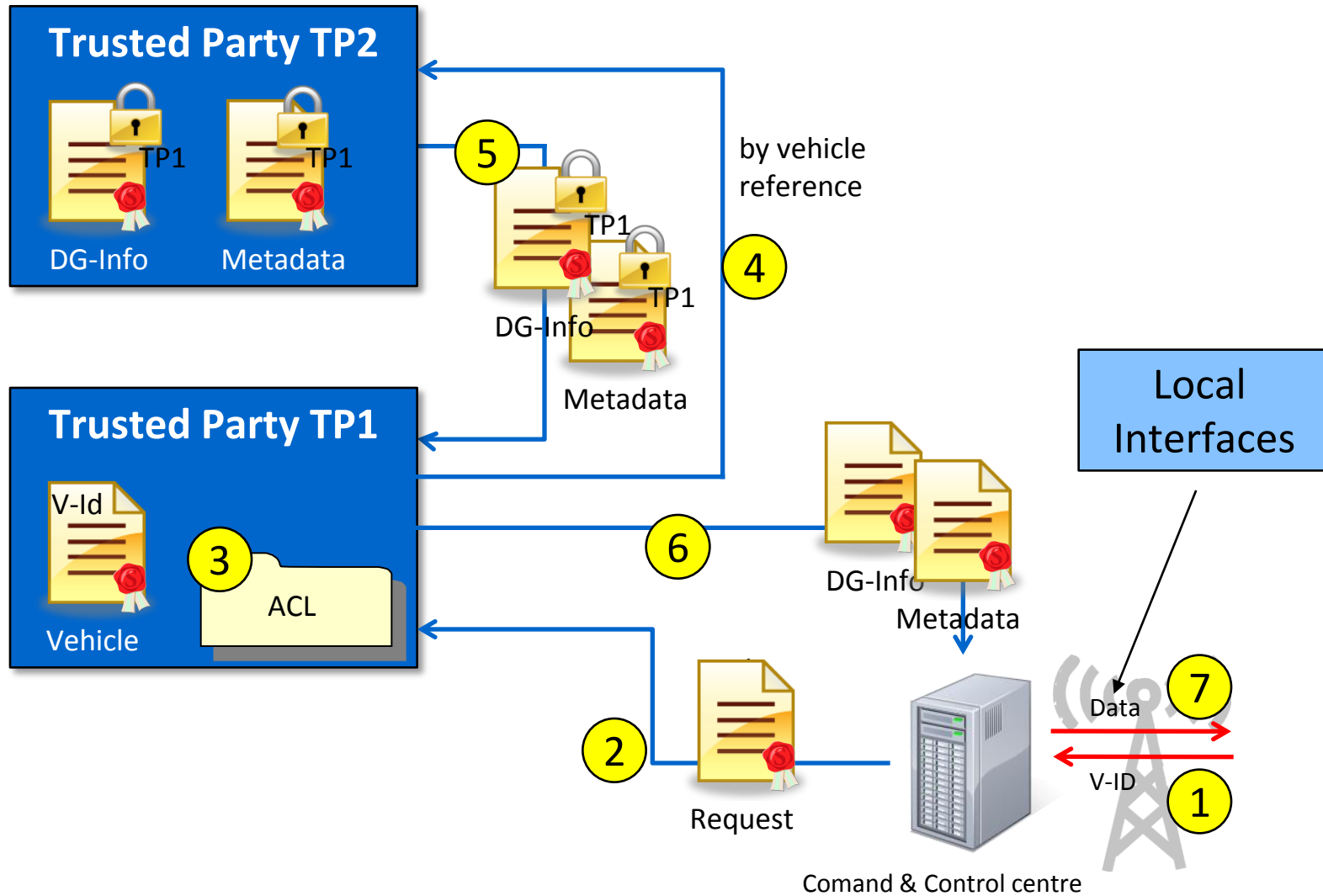
## Scope and framework conditions

- ▶ The “Joint Meeting” is maintaining the DGT regulations for inland transport (rail, road & inland waterways) on a Europe+ scope
- ▶ The regulations are substantial and technically detailed when it comes to physical, material, etc. requirements – they do so far NOT mention Telematics
- ▶ What is mentioned is the optional electronic representation of the data requirements on the transport document – but this is based on “functional equivalence” which in itself is not specified
- ▶ DGT actors have so far drawn the conclusion that paperless transport is practically impossible and increasingly complain about this fact incurring unnecessary cost to their business
- ▶ The “Joint Meeting” has mandated an informal WG on Telematics (rotating chair DE/FR) – this group has created a tabular description of relevant data, including references to stakeholder roles and use cases
- ▶ Germany has launched a study in 2010 to consider the role that Telematics could potentially play in DGT
- ▶ The results of this study have been reported to WG Telematics – they are the basis of the current work

## From the previous R&D project to the current project



# IT-Security Concept

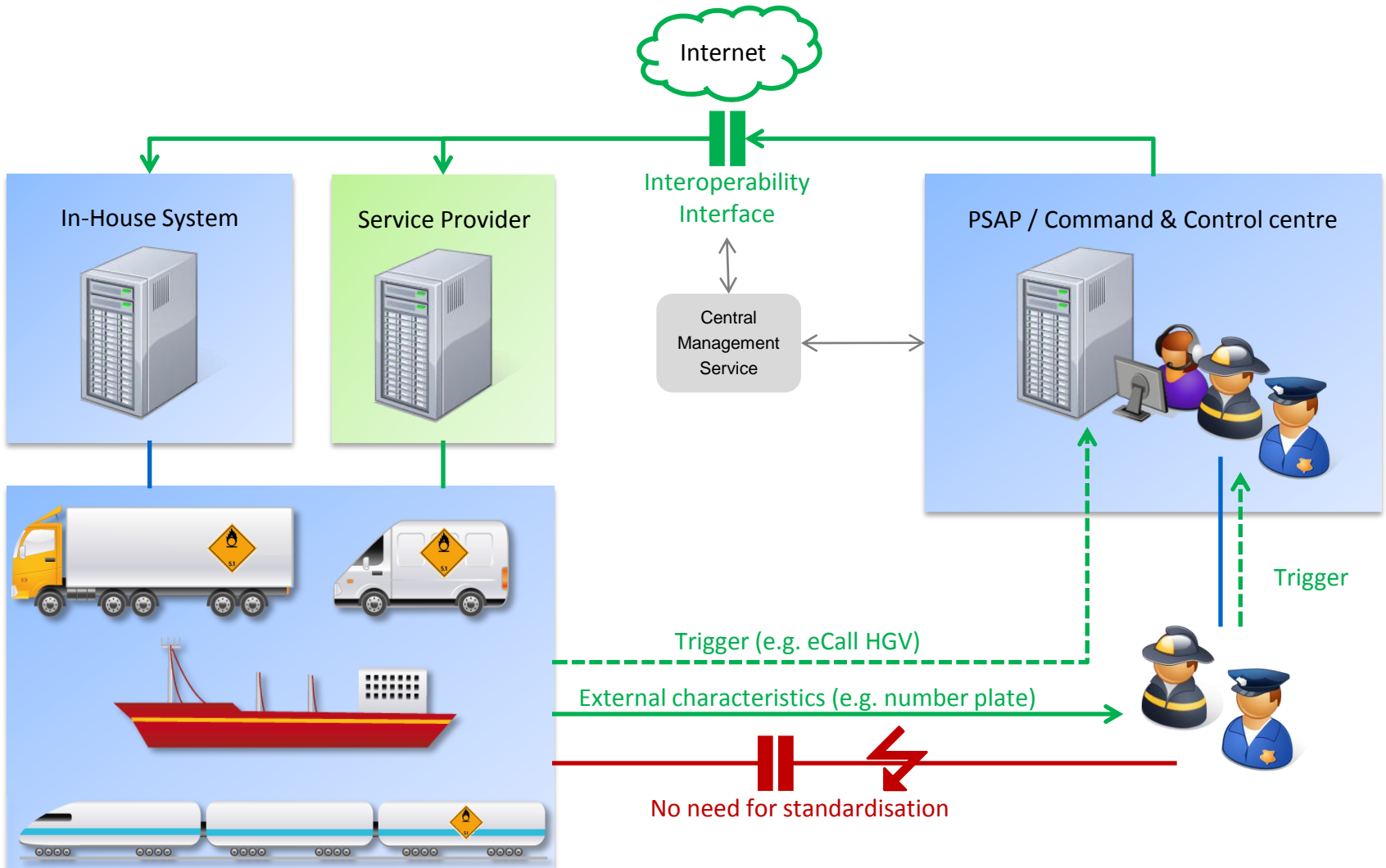


## How has this proposal evolved since 2011?

- ▶ **The original proposal implied that DG data was by default forwarded to external entities (the Trusted Parties 1 & 2)**
- ▶ **The split in two disparate TPs was deliberate to reduce the risk of fraud or theft of data – only cooperating TPs 1 & 2 could actually read the data**
- ▶ **BUT: Users were reluctant to accept data stores where data for each single transport would need to be delivered!**
- ▶ **Alternative proposal: rather than stipulating the use of a central database to store the data, stipulate the provision of a standardised interface that allows justified access to the data when needed!**
- ▶ **Such an interface can be implemented by the carrier himself (e.g. large companies with mission critical IT) or by (private!) service providers contracted by the carrier (e.g. ‘white van man’)**
- ▶ **The actual data access interface takes the place of TP2**
- ▶ **A central service still is needed, e.g. to manage security features – this central service takes the place of TP1**



# Basic application scenario with federated services



## Perceptions

- ▶ **Project findings and recommendations have been confirmed by the Working Group on Telematics**
  - Use of widely used IT standards (e.g. WSDL, XML, SOAP, http) that makes the introduction of the telematics system simple
  - Consider IT(S) standards as trigger mechanisms (e.g. eCall/TARV)
  - Use of IT security mechanisms (e.g. certificates, digital signatures encryption) that makes the system secure
  - Use of the dangerous goods data model that has been validated as an adequate replacement for the of the transport paper document
- ▶ **Aim is to use the telematics system architecture for field tests / pilot implementations**
- ▶ **A fully elaborated technical specification is required first that allows for producing the appropriate software and ensured comparable results**

## General concept



## General system concept

- ▶ **Replace access to paper documents with (electronic, machine-to-machine) access to a back-office system**
- ▶ **The back-office service can be provided by the carrier or by a service provider (⇒ many instances of this service – needs addressing)**
- ▶ **Central (mainly) administrative tasks will be located in a central service (maybe implemented by a set of federated services)**
- ▶ **Each transport must uniquely be identified to access data:  
access credentials = service address + transport ID**
- ▶ **Access credentials can be carried by today's / future standards, e.g. for vehicle initiated emergency notification**
- ▶ **There need to be further 'lookup' services resolve access credentials in case of access based on external observations**
- ▶ **Access must be controlled and data protection must be ensured  
⇒ up-to-data cryptographic technology needed**
- ▶ **The interface should easily integrate into the existing landscape of Freight & Logistics IT services ⇒ use of web services & XML technology**

## IT standards and trigger mechanisms



## IT security mechanisms



## **Data model (adaptions of result from R&D project)**



## Provision of a telematics system architecture and service interfaces





## Design decisions (I)

- ▶ **No regulations for Member States or emergency responders**
  - Their internal behaviour and how they make use of the system is entirely up to them
- ▶ **Existing PKIs will be (re-)used**
  - This implies a central registry where certificates are registered and assigned to roles
- ▶ **Certificates are associated to organisations, not to individuals**
  - This may have impact of organisational procedures and does have an impact on non-repudiation
- ▶ **Access is not distinguished on content (e.g. no dedicated access right for particular Dangerous Goods classes)**
- ▶ **Certificates are used for securing the end-to-end link and for digital signatures of the content**
  - Data is not encrypted outside the communication channel

## Design decisions (II)

- ▶ **Services can (and shall) be certified in the future to ensure interoperability**
  - There is a need to consider the establishment of the organisational framework for accredited certification organisations
- ▶ **The Service Level of the TP2 services will not be constantly monitored**
  - The basic legal assumption is the equivalence to the current (paper) situation: the carrier is responsible for the service to work when needed
  - Nevertheless, suitable service levels – ideally based on internationally accredited standards – shall be specified, but no SLAs
  - There should be provisions regarding DoS attacks in the service level descriptions
- ▶ **TP2s shall register with a central registration service (→ TP1)**

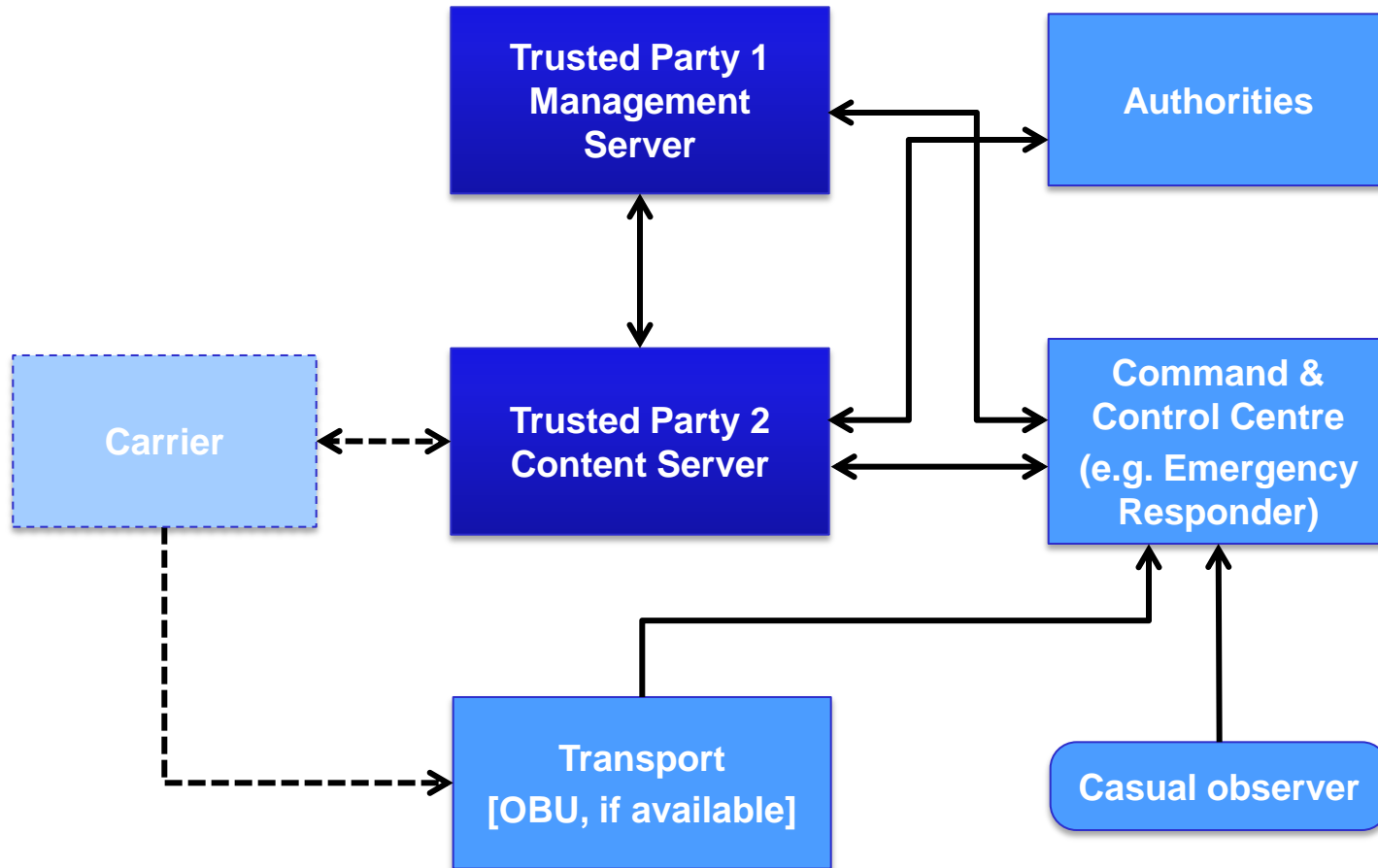
## Design decisions (III)

- ▶ **VPNs (e.g. eTESTA) shall not be required for the backbone, but associated IT-security issues must be taken into account**
- ▶ **The service interfaces shall be fully specified (WSDL & XSD)**
  - The actual development of the services will be WSDL-first
- ▶ **The system specification shall contain self-inspection methods in order to support migrations paths in case of future evolution**
- ▶ **A logging interface shall provide access to evidence (details, e.g. storage period, to be determined)**
- ▶ **The system shall support two different types of access scenarios:**
  - Access with knowledge of service end point and vehicle ID
    - e.g. “electronic trigger” via eCall, TARV, etc.
  - Access with context knowledge only (e.g. location, number plates...)
    - e.g. “casual observer”
  - The latter implies services to look up service end point and vehicle ID depending on descriptive parameters, depending on mode of transport (it needs to be considered how existing services like RIS, EUCARIS, etc. can be used here)
  - There are two basic alternatives: caching the data of current transports in a central service (TP1) or specifying multicast / broadcast enquiries on TP2s

## Design decisions (IV)

- ▶ **One single successful data access shall provide ALL DGT data needed for emergency response / control**
  - The carrier has to have the full data of the goods transported – it is not enough to have a reference to another system operated, e.g. by the consignor system
- ▶ **The data structure should reflect the organising principles used currently for paper documents for the different modes of transport (e.g. by wagon for trains)**

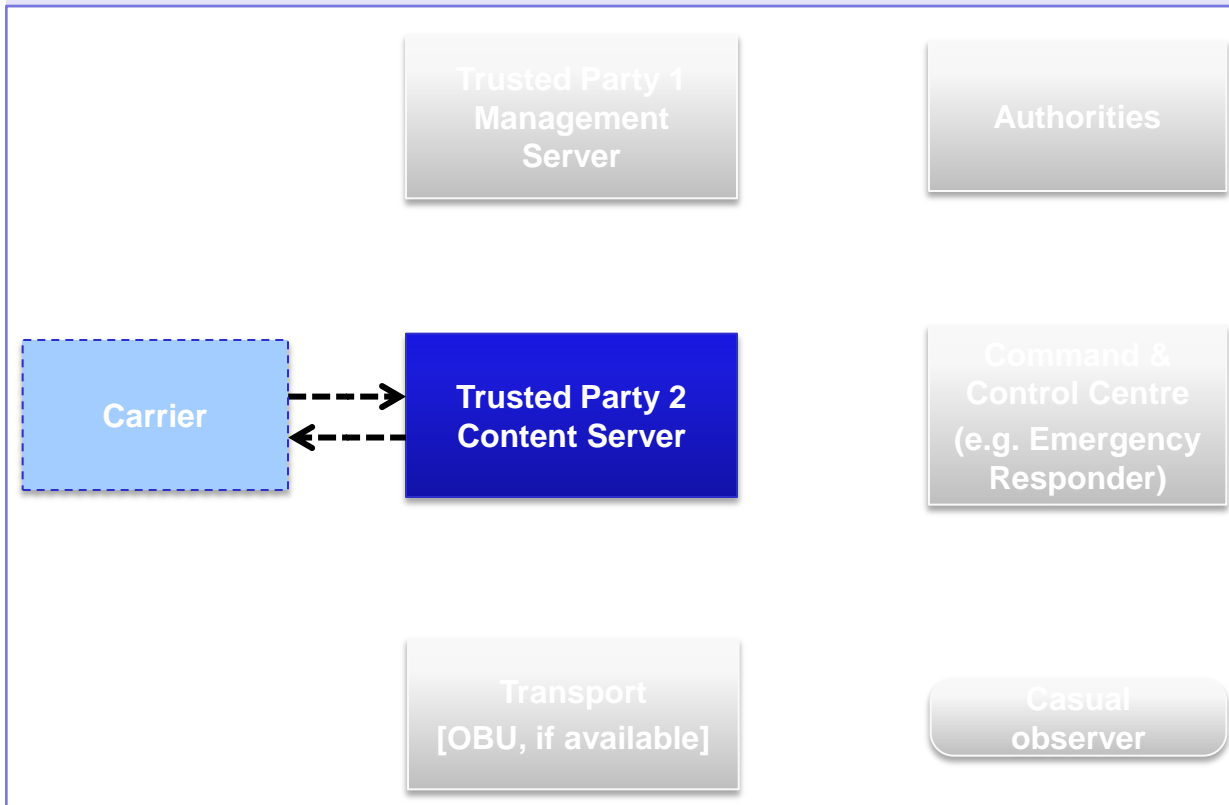
# Telematics system architecture



# Telematics system architecture

## I. Carrier stores Dangerous Goods Transport Document in TP2

- Carrier may provide a TP2 himself → this interface becomes internal!
- No standardised interface between carrier and TP2

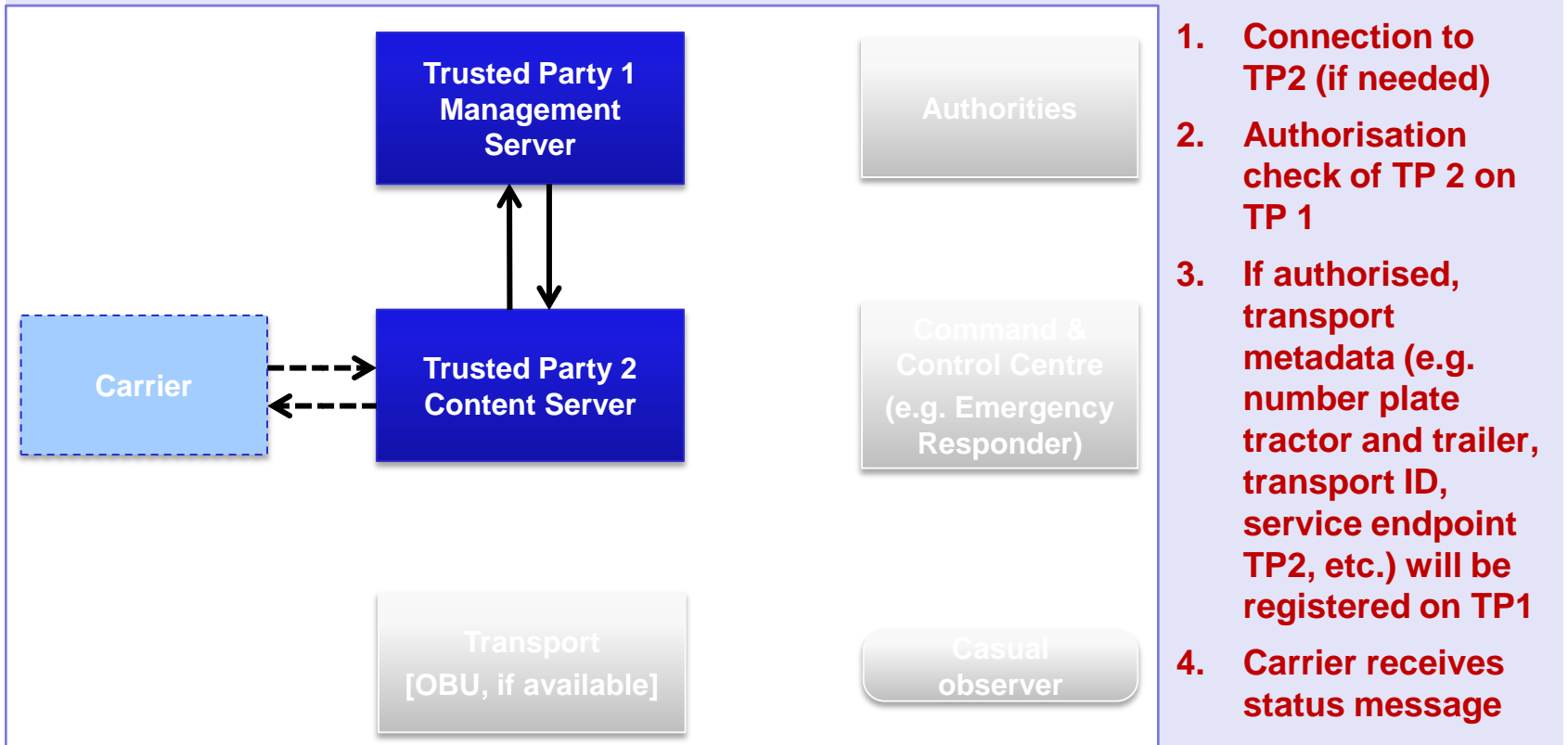


- Carrier saves DG Transport document**
- Carrier receives transport ID**

## Telematics system architecture

### II. Carrier registers DG transport on TP1

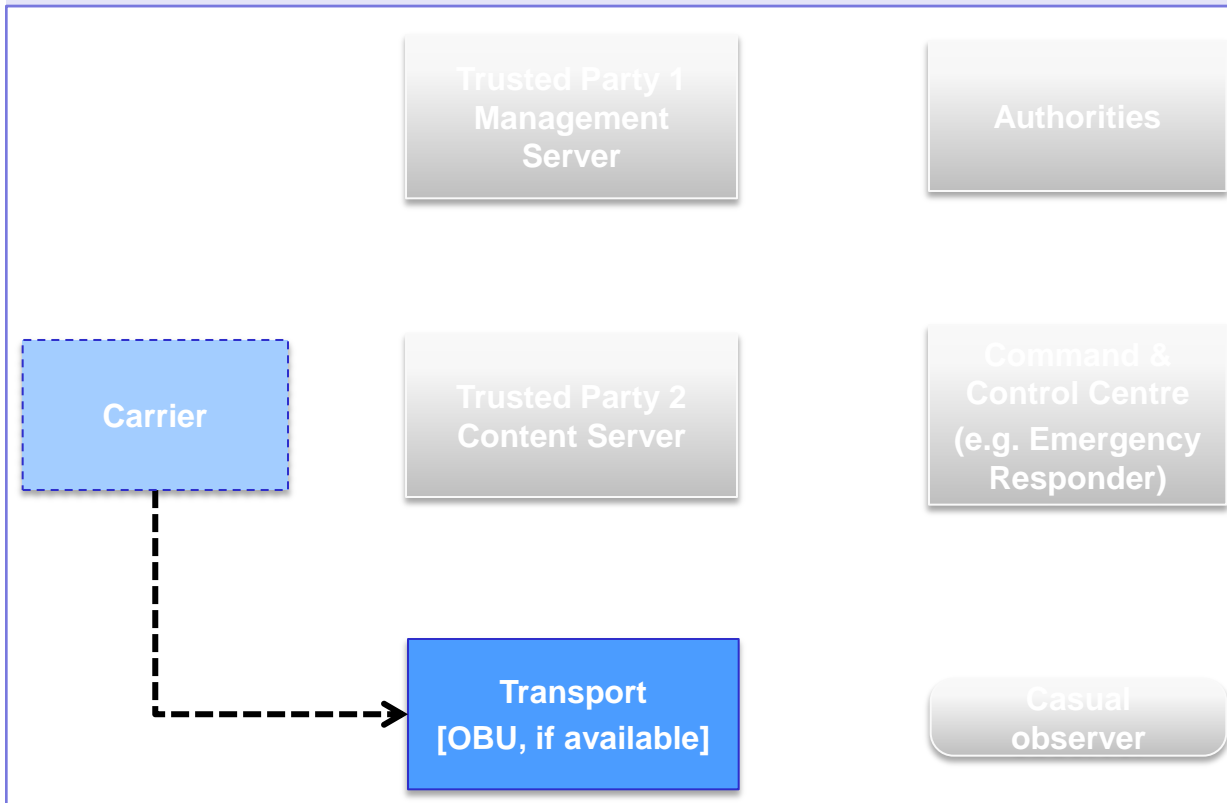
- TP2 registers transport when it starts (and de-registers when it ends)
- Carrier has to provide lookup criteria (e.g. number plates, etc.)



## Telematics system architecture

### III. Carrier saves transport ID and service endpoint TP2 in an OBU

- Only if OBU is available and vehicle initiated alerts are supported (e.g. HGV eCall)
- No standardised interface!



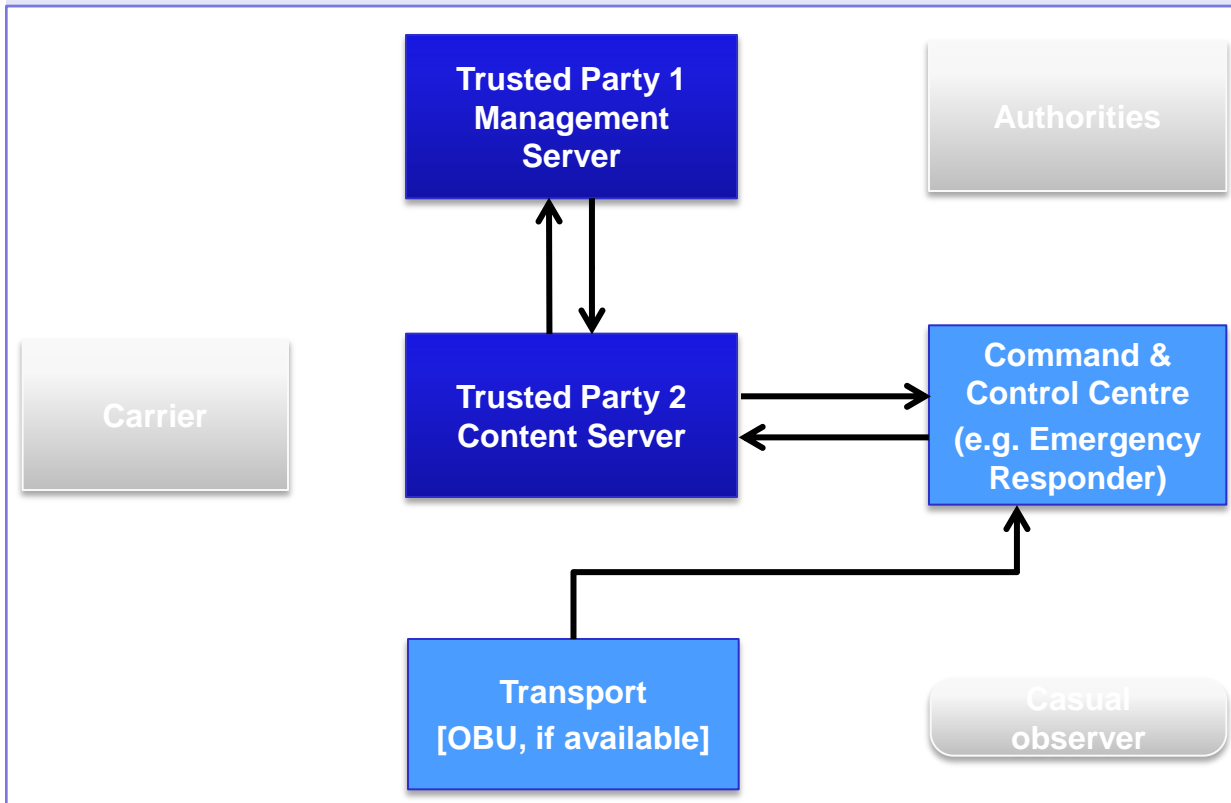
1. Carrier saves transport ID and service endpoint TP2 in OBU
2. If storing full access credentials is not possible, store unique lookup criteria (e.g. VIN)



## Telematics system architecture

### IV. Emergency situation with vehicle initiated emergency call (e.g. eCall HGV)

- Vehicle initiated emergency call is available and able to carry access credentials
- CCC has free access to the internet (redirect mode via TP1 is applicable)

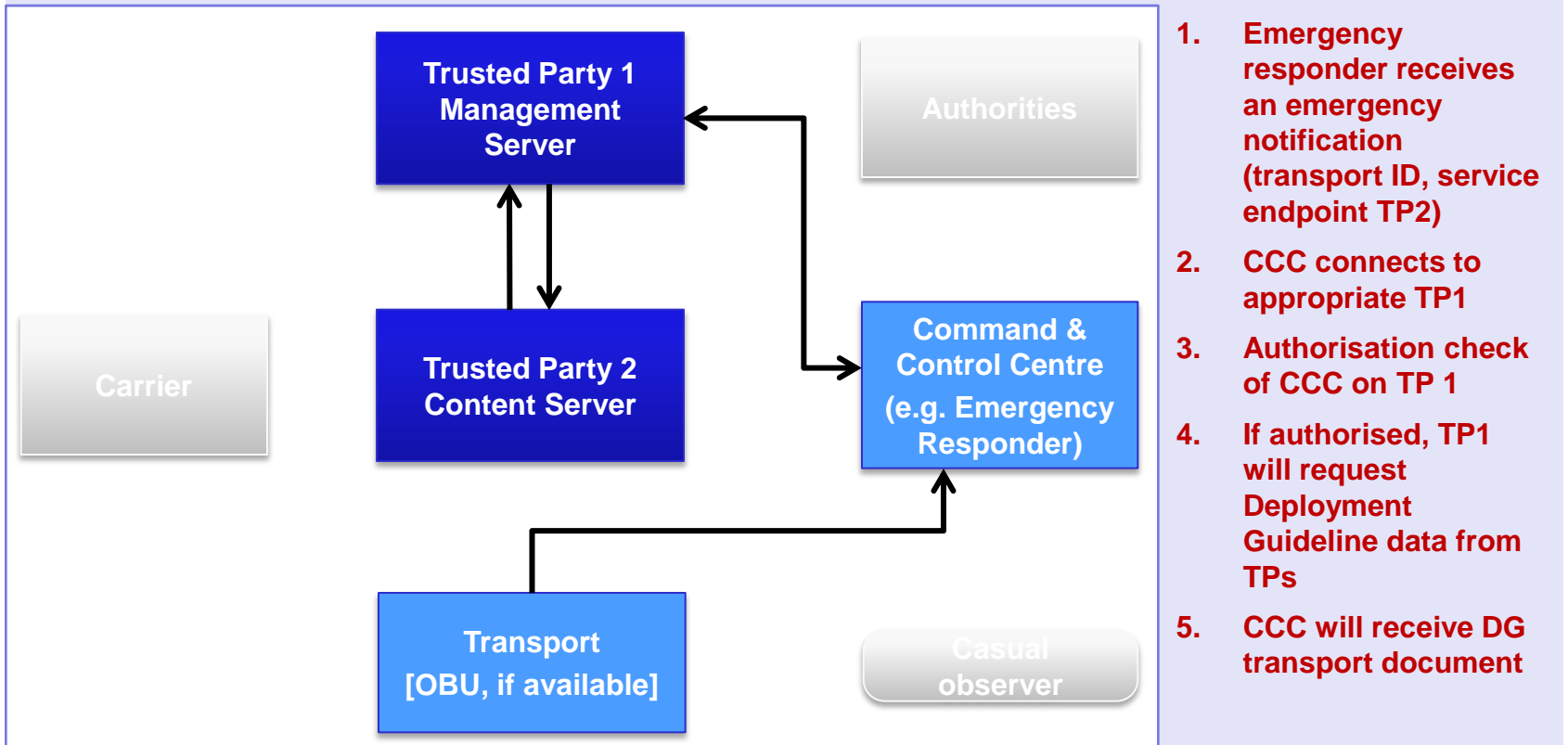


1. **Emergency responder receives an emergency notification (transport ID, service endpoint TP2)**
2. **CCC connects to appropriate TP2**
3. **Authorisation check of CCC on TP 1**
4. **If authorised, CCC will receive DG transport document**

## Telematics system architecture

### IV. Emergency situation with vehicle initiated emergency call (e.g. eCall HGV)

- Vehicle initiated emergency call is available and able to carry access credentials
- CCC has restricted access to the internet (proxy mode must be used)

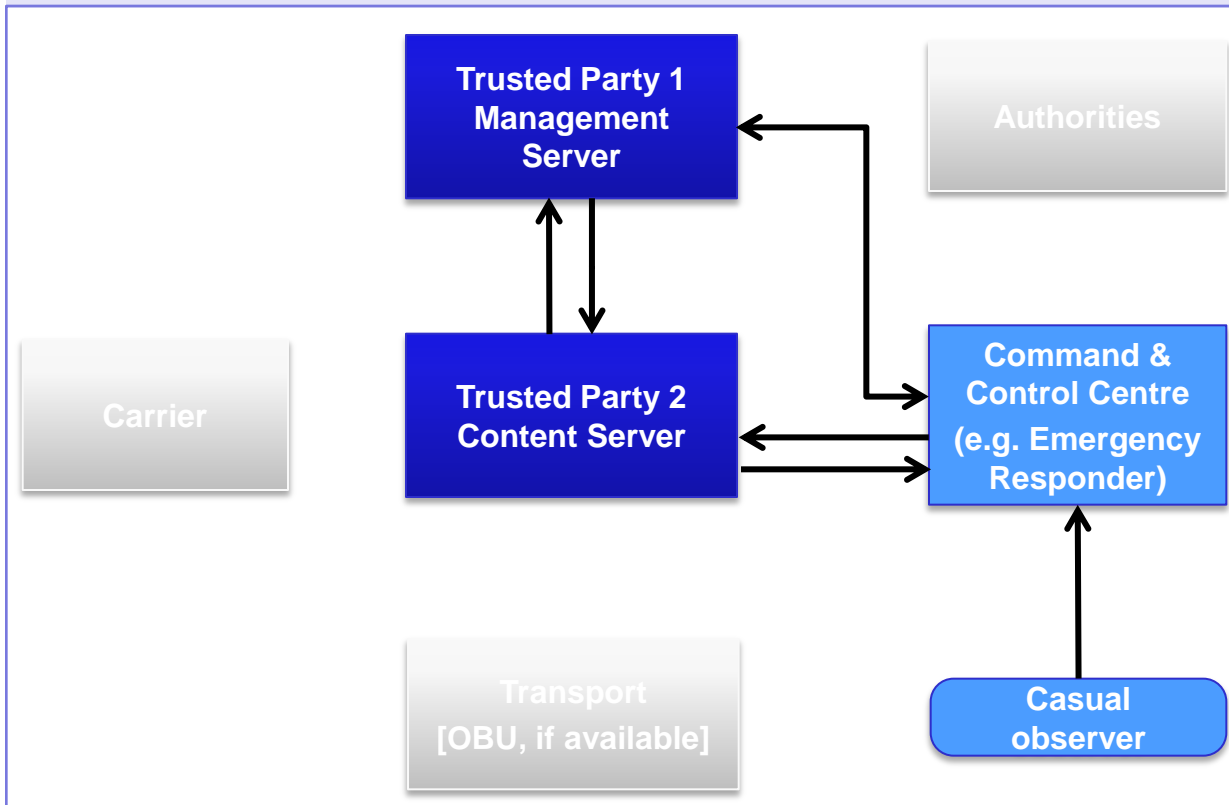


1. **Emergency responder receives an emergency notification (transport ID, service endpoint TP2)**
2. **CCC connects to appropriate TP1**
3. **Authorisation check of CCC on TP 1**
4. **If authorised, TP1 will request Deployment Guideline data from TPs**
5. **CCC will receive DG transport document**

# Telematics system architecture

## IV. Emergency situation reported by casual observer

- No automatic emergency call by the vehicle
- CCC has full access to the internet (redirect mode would be used)



1. **Emergency responder receives a call from an observer with observable criteria**
2. **CCC connects with appropriate TP1 and performs lookup; if authorised it receives credentials**
3. **CCC connects to appropriate TP2**
4. **Authorisation check of CCC on TP 1**
5. **If authorised, CCC will receive DG transport document**

## Issues

- ▶ **Legal basis (e.g. regarding digital signatures) not necessarily aligned in the ADR/AND/RID signatory countries**
- ▶ **Although the central storage ('national database') is no longer mandatory (but still feasible!), there are a couple of central ("national"/"European"?) responsibilities in the concept (TP1 ACL / certificate registry / revocation / proxy mode...) that need to be addressed and options / commitment to provide these central services need to be considered**
- ▶ **Service certification must be considered (avoid demanding new, dedicated structures with prohibitive cost)**

## Mock-up demo of system processes



## Conclusions / Recommendations

- ▶ **The architecture has been transformed into a technical specification that can be used for pilot implementation**
- ▶ **The specification is not final as it would be needed for inclusion into the regulatory framework**
  - Some parts require policy decision (e.g. federated TP1 vs. central TP1)
  - Some parts require feedback from the field (e.g. self-inspection and logging)
  - Data model of transport document  
(although much feedback has already been processed)
- ▶ **The full specification (after including feedback from WG Telematics and Transport Logistics WS) will be made available end of July**
- ▶ **It would be preferred to accompany local / regional / national pilot projects with a European umbrella led / accompanied by WG Telematics**
- ▶ **Regulation would require steps beyond successful pilots, namely agreements on standardisation and compliance assessments**

**Thank you!**

**Josef Kaltwasser  
AlbrechtConsult GmbH**



**direct contact  
Tel: +49 1520 877 04 02  
Fax: +49 241 500 718  
[Josef.Kaltwasser@albrechtconsult.com](mailto:Josef.Kaltwasser@albrechtconsult.com)**

# Project of the Federal Ministry of Transport, Building and Urban Development

“Telematics system architecture to allow electronic  
transport documents and improve emergency  
response in dangerous goods transport”

## AP220 – Relevant Standards



**Jonathan Harrod Booth**  
**Harrod Booth Consulting Limited**

**Working Group Telematics Meeting**  
**Tegernsee 03/04 June 2013**



## Outline

### ▶ **Scope and framework conditions**

- Need to understand the context of this work as it has developed over the last couple of years

### ▶ **Results from the previous R&D project**

- Summary of main conclusions / recommendations from the German national study carried out 2010/11

### ▶ **Assessment of relevant current telematics Standardisation**

- Review of relevant Standards across main surface transport modes
- Suitability of existing standards and trigger mechanisms for linkage to proposed back-office solution

### ▶ **Recommendations**

## Scope and framework conditions



## Scope and framework conditions

- ▶ The “Joint Meeting” is maintaining the DGT regulations for inland transport (rail, road & inland waterways) on a Europe+ scope
- ▶ The regulations are substantial and technically detailed when it comes to physical, material, etc. requirements – they do so far NOT mention Telematics
- ▶ What is mentioned is the optional electronic representation of the data requirements on the transport document – but this is based on “functional equivalence” which in itself is not specified
- ▶ DGT actors have so far drawn the conclusion that paperless transport is practically impossible and increasingly complain about this fact incurring unnecessary cost to their business
- ▶ The “Joint Meeting” has mandated an informal WG on Telematics (rotating chair DE/FR) – this group has created a tabular description of relevant data, including references to stakeholder roles and use cases
- ▶ Germany has launched a study in 2010 to consider the role that Telematics could potentially play in DGT
- ▶ The results of this study have been reported to WG Telematics – they are the basis of the current work

## Scope and framework conditions

### ► **The scope of Workpackage 220 is:**

- an analysis of the telematics standards to be used for the communication between the back-office systems.
- Furthermore, the operations should be determined (trigger), which can cause access to the back office interface.
- Standards, such as eCall and TARV, are examined and checked with regard to their suitability.

## Results from the previous R&D project





Freight / Commercial

- E-documentation
- E-clearances
- Smart container management
- Fleet management



Monitoring & Enforcement

- Track & Trace
- Enforcement
- Required Authority documents



Incident & Emergency Response

- Remote notification
- Incident scene data access
- Incident management
- Additional information sourcing
- Information dissemination

Architecture/Framework

Common terminology/ Common concepts

Classification

Identification

Location

Payload description

Load Status

Event /Status description

Communications

Processes

Security

## Previous Study – WP200 Conclusions

- ▶ **Many relevant existing and developing standards exist**
- ▶ **Regulation of Telematics in Dangerous Goods Transport needs to consider which domains & application areas are priorities & its approach to engagement with Standards bodies**
- ▶ **Establish a common data centric terminology for promotion into a number of these initiatives (i.e. provide views on appropriate data to support different DG applications for reuse by other initiatives):**
  - Raise awareness in Freight Single Framework and Regulated Vehicle initiatives
  - Engage with eCall HGV PWI activity in HeERO/CEN TC278 WG15 to ensure appropriate data set adopted, and business operational model appropriate
  - Consider review and input into existing standards (e.g. ISO 17687) to ensure alignment.
- ▶ **Consider support for establishment of open framework to support DG applications in future**

## **Assessment of relevant current telematics Standardisation**





## Extending the review of Standards

- ▶ **With a better understanding of the proposed back-office solution and services review relevant standards to examine ability for the standard to carry relevant data and expected trigger mechanisms**
- ▶ **Extend the review to road, rail and inland waterways**
  
- ▶ **Request/disclaimer: As this is involving areas beyond personal experience and expertise therefore there will be people present who will know some details in greater detail... comments are welcome**

## In each case....

### ▶ **This presentation provides:**

- A brief description of the intended use of the Standard(s)
- The scope of applicability
- Current status
- Ability to carry relevant data
- Triggers
- Recommendations

## For Roads – Relevant Telematics Standards

Common Name	Domain of Application	Region	Short Description
<b>eCall HG</b> V CEN TR 16405	Standards specifying vehicle initiated emergency notification	Europe	Developing appendix to eCall standards to support notification from HGVs/Dangerous Good Vehicles
<b>TARV</b> - ISO 15638 – multipart standard: ITS Framework for cooperative telematics applications for regulated commercial freight vehicles	A range of regulated telematics applications for commercial vehicles	International	Includes an emergency call application (Part 10) and a Dangerous Goods Monitoring application (Part 18)
<b>DATEX II</b>	Standard for traffic centre to centre communications	Europe	
<b>IS 17687</b> : 2007	Vehicle to centre dangerous goods messaging standard	International	ITS – Data Dictionary and Message Sets for electronic identification and monitoring of hazardous materials/dangerous goods transportation (ISO Standard – unknown usage)

# For Roads – eCall HGV

## ► Description

- Road-centric suite of protocols, high-level procedures and communications standards to support emergency incident notification from vehicle to emergency response (Public Service Answering Point - PSAP) and subsequent immediate communication

## ► Scope

- Europe + (CEN & ETSI) Standards, but wider uptake including Russian Federation

## ► Current status

- Core eCall standards adopted; EC promoting EU resolution for mandatory deployment in new private cars in EU in 2015.
- eCall HGV (including Dangerous Goods information), adopted as a CEN Technical Report (CEN TR 16405)
- Large-scale pre-deployment trials on-going HEERO and HEERO 2 – which have observations to be fed back into eCall HGV standard.

## ► Ability to carry relevant data

- eCall HGV Technical Report has an initial design to support some data for a remote call-out but as we do not have a definite definition of the required data elements for call-out. Further alignment and conformance check required. Note the eCall HGV Technical Report is subject to some revisions shortly as a result of feedback from the HEERO2 project - the HeERO team suggest that instead of having one data concept that provides the option to link to an IPv6 address AND provide the possibility for on-board data, there should be 2 data concepts, one simply providing a link and one simply providing data.

## ► Triggers

- Note: eCall is limited to “life threatening situations” therefore can only be used for incident notification & response purposes
- eCall does not address what onward actions a PSAP must do on receipt of an eCall message, i.e. there is no international standardisation of the solution between PSAP and 2<sup>nd</sup> line emergency response entities. However having standardised data to request DGT information could lead to deployment of a standardised solution.

## ► Recommendations

- Provide firm guidance to CEN TC278 WG15 on form of data to be carried to support access to back-office solutions

# For Roads – TARV HGV

## ► Description

- Road-centric suite of communication and application specifications for regulated commercial vehicle operations – ISO 15638 multi-part standard. Many applications such as mass monitoring and driver hours. These include an emergency call application [similar to eCall] (Part 10) and a Dangerous Goods Monitoring application (Part 18). The underlying communications framework is the same as used for Cooperative ITS/CVHS. The scope of TARV is communications between the vehicle and recipients.

## ► Scope

- ISO international Standards , with wide international interest

## ► Current status

- Many parts of the multi-part Standard are already adopted as full ISO Standard.
- Part 18 (ADR) will progress no further until UNECE is satisfied that it meets their needs

## ► Ability to carry relevant data

- Part 10 has been build on similar lines to eCall HGV with potential ability to carry suitable data elements but as we do not have a definite definition of the required data elements for call-out. Further alignment and conformance check required.
- Part 18 (DG Monitoring) needs to be validated by this Working Group (or the Joint Meeting) before further standardisation can proceed. Review and comment by TWG required.

## ► Triggers

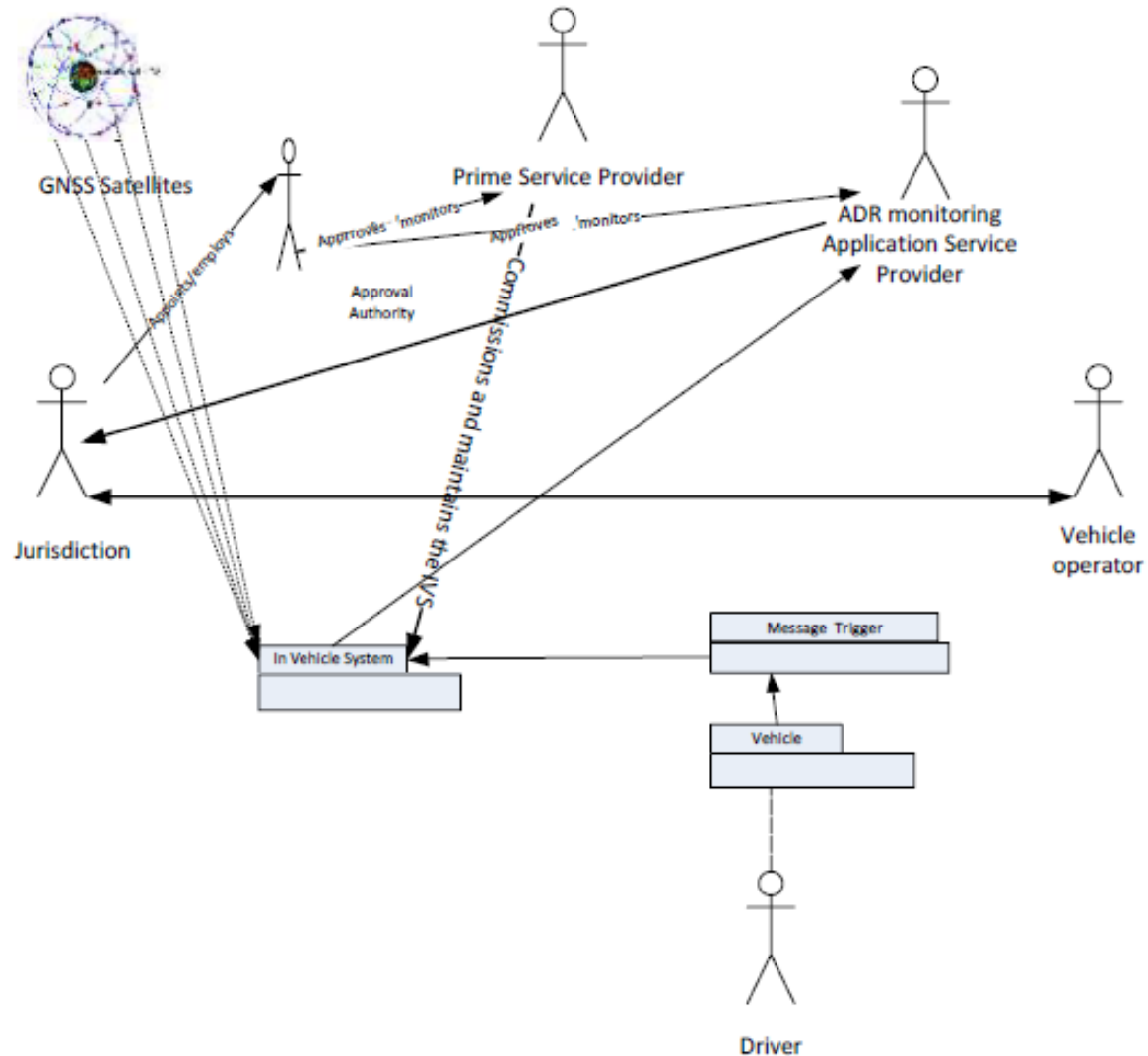
- TARV supports the concept of multiple service providers. Under Part 10, when a TARV eCall message is issue from a vehicle the first recipient is the application service provider, who is expected to pass the data and call to a PSAP. Receipt of the eCall message by the PSAP can trigger a call-out to the back office solution for DGT information.
- Part 18 (ADR) again uses the concept of an application service provider who receives data from the vehicle and passes this to a competent authority (regulator). Receipt of the ADR information by the authority can trigger a call-out to the back office solution for DGT information.

## ► Recommendations

- Provide firm guidance to ISO TC204 WG7 on form of data to be carried to support access to back-office solutions for Part 10 and Part 18, and the nature of application use that it would consider acceptable for Part 18.

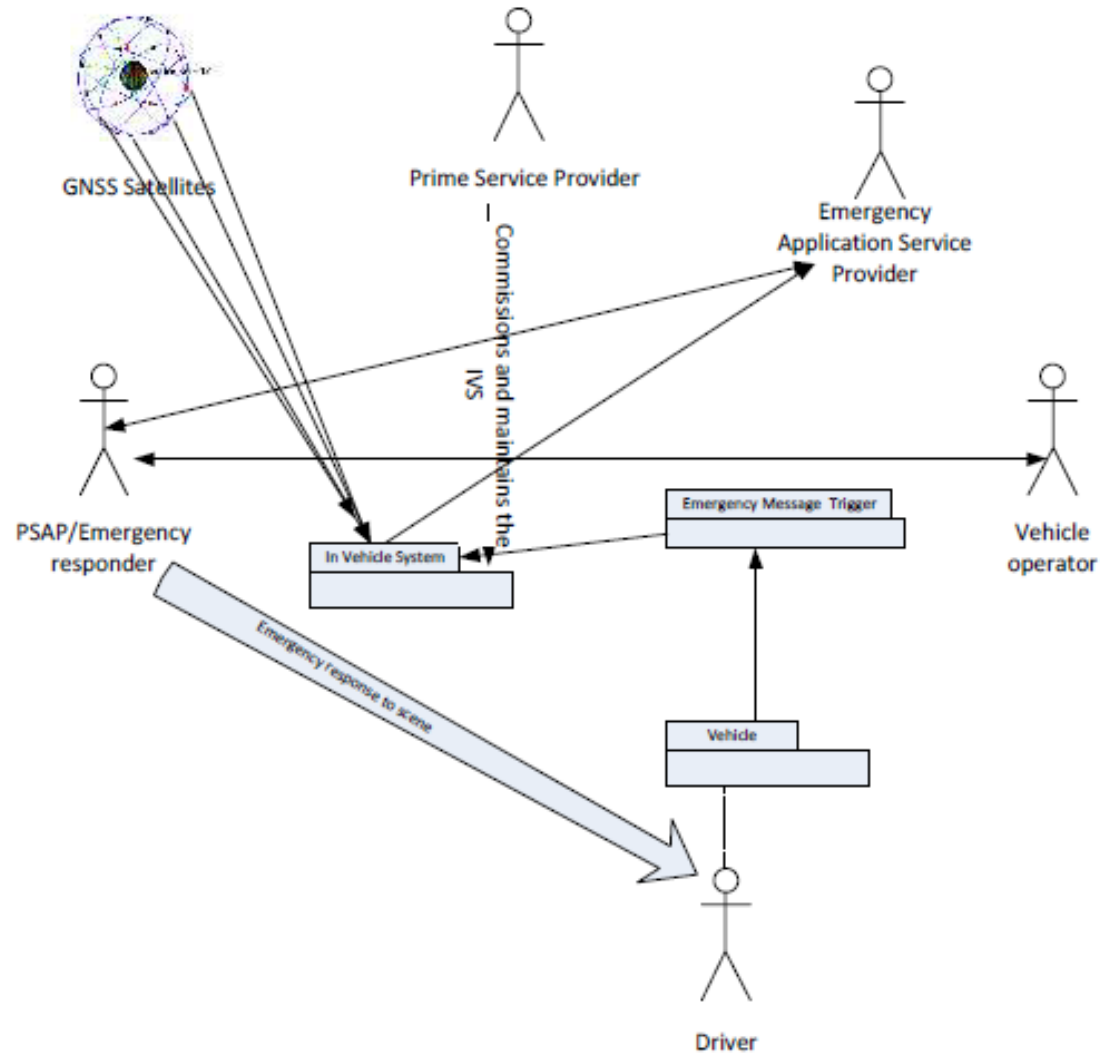
# For Roads – TARV HGV

## ADR Use Case (Part 18)



# For Roads – TARV HGV

## TARV eCall/Emergency Message Use Case (Part 10)



## For Roads – DATEX II

### ▶ **Description**

- Road-centric suite of information exchange protocols for information exchange between traffic centres.

### ▶ **Scope**

- Europe - CEN Standards, widely used by traffic centres in Europe

### ▶ **Current status**

- Parts 1-3 CEN 16157 are adopted Technical Specifications; Part 4-6 are in production.
- Part 3 (Situation Publication) contains some DG information elements – it is proposed to align this model more fully to the TWG DG data model during next period review
- As stated previously the modelling methodology used within the previous study and this one uses the DATEX II methodology to create a platform independent data model for Dangerous Goods Transportation

### ▶ **Ability to carry relevant data**

- As designed at present Part 3 does not explicitly define data elements to support call-out to a back-office DG information solution. However, the DATEX II model and process, is by design extensible and a change management process can enable these elements to be introduced into later revisions of Part 3.

### ▶ **Triggers**

- No specific triggers identified, as DATEX II is not a call and request transaction based service.

### ▶ **Recommendations**

- Encourage CEN TC278 WG8 to adopt the defined data structure to carry call-out information within the DATEX II data model and exchanges.



# For Roads – IS 17687

## ▶ Description

- Road-centric protocol and message set definition for remote identification and monitoring of dangerous goods IS 17687 – Intelligent transport systems – Data dictionary and message sets for electronic identification and monitoring of hazardous materials/dangerous goods transportation

## ▶ Scope

- ISO international full Standard. Usage unknown

## ▶ Current status

- As per all full standards under ISO (or CEN) this product is now due for a periodic review, which can reconfirm/refresh/remove content.

## ▶ Ability to carry relevant data

- Back-office call-out data – None – it was not part of the original design.

## ▶ Triggers

- No specific triggers identified. Any office based solution would have to have processes to address inbound information appropriately.

## ▶ Recommendations

- Suggest modifications to be considered in the periodic review.

## For Rail

- ▶ **On consultation with UK rail DG experts they identified that at present there is no internationally adopted system specification for the management of DGT, however TAF-TSI has been under-development for some time to address these issues and enable interoperability and harmonisation of approach**
- ▶ **The European Railways Agency (ERA) has recently proposed a CR to the existing TAF parameters in order to incorporate dangerous goods information into the consignment note – this is not aligned with the emerging requirements from TWG/studies for back office solutions access**
- ▶ **However, ERA has assured the TAF community that this proposal to include dangerous goods information in TAF consignment notes is in parallel to the RID information and is there to meet the legal requirement for consignment notes to carry complete information.**
- ▶ **Of course ERA colleagues are better placed to report progress on this topic**

# For European Inland Waterways

## ► Description

- Commission Regulation (EU) 164/2010 dictates the use of River Information Service (RIS) specifications on inland waterways in the Community

## ► Scope

- Europe

## ► Current status

- The RIS specifications are in widespread use.

## ► Ability to carry relevant data

- River Information Service (RIS) Electronic message specification support DGT information exchange, such as the ERINOT message, and others, but these messages do not currently support the likely data elements required for access to a back office solution.
- The ERI notification message (ERINOT) must be used for the reporting of dangerous and non dangerous cargo carried by inland waterway vessels. But there appears to be no direct functionality for incident notification.

## ► Triggers













- None currently included

## ► Recommendations

- Discuss with the RIS specifiers:
  - processes for change to support message content structure modification to support data elements for access to back office solutions
  - The experiences from eCall and approaches that can be used for incident notification within the RIS environment

# Summary – Relevant Telematics Standards

## Dangerous Goods Transport

Mode	Common Name	Domain of Application	Region	DGT content in messaging?	Support DGT back-office call-out?	Existing key identifier
Road	eCall HGV CEN TR 16405	Vehicle emergency notification comms.	Europe			VIN
	TARV - ISO 15638 Parts 10/18	Multipart standard: ITS Framework for cooperative telematics applications for regulated commercial freight vehicles	International			VIN, Vehicle Registration?
	DATEX II CEN 16157	Standard for traffic centre to centre communications	Europe			VIN?, Vehicle Registration?
	IS 17687: 2007	Vehicle to centre dangerous goods messaging standard	International			VIN?, Vehicle Registration?
Rail	TAF-TSI	ERA-led Telematics Application Framework	Europe			UIC Wagon Number
Inland Waterway	RIS – River Information System	Messaging system for inland waterways	Europe			Name; ENI number or IMO number?

## Emergency Notification Use Case

- ▶ **Aforementioned standards/specifications do all support different Dangerous Goods Transport information content**
- ▶ **They do not currently support data to enable call-out to a back-office solution.**
- ▶ **However, changes could be encouraged to support the back-office solution across the 3 modes for emergency notification and other use cases**



## For Remote (Road-side) Inspection/Monitoring

- ▶ **Competent authorities have a responsibility under European Directives 90/50/EC and the later 2008/54/EC to undertake uniform procedures to check the transport of Dangerous Goods by road**
- ▶ **These Directives provide a proforma of information to be gathered during a road-side check, which assumes access to the paper DG Transport Document.**
- ▶ **Discussions with officials at the UK's Vehicle and Operator Services Agency (VOSA) indicates that access to the proposed back office solution, although not a pre-requisite, has the potential to introduce operational efficiencies into the check process. This still assumes that the vehicle under scrutiny is stopped and key access details to the back office solution are provided to the checking official.**



## For Remote Inspection/Monitoring

- ▶ **Initiation of checks for loading details for a moving vehicle requires a different approach using the vehicle's unique visible identifiers/registration plates. The back-office solution needs to support an authorised user querying for Dangerous Goods Transport load information for an identified 'vehicle'**
  - ROAD: registration plate of lorry, tractor or trailer + Nationality; VIN?
  - INLAND WATERWAYS: Ship name and Nationality, ENI number ("European number of identification") or IMO number (for sea ships travelling inland waterways)
  - RAIL: UIC wagon number
  
- ▶ **Requires "directory services" for searching federated back-office solutions**
- ▶ **And guidance on what identification data shall be registered in the back-office (visible "vehicle" identifiers)**

## Recommendations





## Recommendations

- ▶ **Specify a clear technical approach to the back office solution – to identify capabilities and the specific data elements required to access the service for emergency response and off-vehicle monitoring purposes**
- ▶ **Disseminate the agreed data element information for back office solution access to the Standards and Specifications creators mentioned earlier**
- ▶ **Technical solutions must support concept of federated back-office systems and authorised search facilities supporting remote observer services**
- ▶ **Registration requirements, to be tested during trials, must clarify what identification data must be registered (regulation)**

Albore

**Thank you!**

**Jonathan Harrod Booth  
Harrod Booth Consulting Limited**



**direct contact  
Tel: +44 7990 520 404  
[jon@harrodbooth.com](mailto:jon@harrodbooth.com)**

## IT security mechanisms



## Overall approach: what needs to be protected

### ▶ **Privacy of DGT Document Data**

- DGT Document Data must be kept private during the entire process and may be revealed only to authorized organisations

### ▶ **Integrity of DGT Document Data**

- DGT Document Data must have integrity
- Changes of DGTdocument contents must be detectable
- The document must be linked to the originator

### ▶ **Access Control**

- Access to DGT Document Data must be granted only to authorized organisations
- Organisations have to be registered in advance
- Authorization must be based on a strong and reliable authentication mechanismen

# IT security mechanisms: Basic technologies

## Encryption, Digital Signatures and Certificates

### ► Main requirements in IT security can be grouped in categories

- Confidentiality: Data has to be kept private; only the intended recipient is able to read the content
- Integrity: Data is secured against non observable changes, that means modification of data is detectable
- Authenticity: The sender of a message can be verified
- Non-Repudiation: The sender of a message cannot deny the origin and the content of sent data

### ► Three basic mechanisms are available to fulfill the requirements

- Encryption: Data is encrypted with some key by the sender and will be decrypted with a corresponding key by the recipient (establishes confidentiality)
- Digital Signatures: Data is enriched by additional information ('Digital Signature') that the sender has added to the payload (establishes integrity)
- Certificates: A Certificate is a piece of information (analogous to a passport) that identifies a participant. A certificate is issued (and revoked) by a certification authority (establishes authenticity and non-repudiation)

## **Basic concepts like certificate, digital signature, CA, revocation**

## IT security basics: Public Key Cryptography and Public Key Infrastructures (PKI)

- ▶ **The most common implementations method for these IT security mechanisms are based on Public Key Cryptography and Public Key Infrastructures**
- ▶ **Public Key Cryptography means**
  - Each participant holds a **secret key** and a **public key**. The keys correspond to each other, based a sound mathematical foundation that ensures that information encrypted with one key can only be deciphered with access to the other key.
  - Each participant publishes its **public key**. It is used by senders for encryption and by receivers to validate digital signatures.
  - Each participant uses its **secret key** to produce digital signatures and to decrypt received data.
- ▶ **Public Key Infrastructure means**
  - A **Certification Authority** (sometimes called Trust Center) affirms that a **public key** belongs to a dedicated participant. This electronic affirmation is called **Digital Certificate**.
  - The **Certification Authority** publishes all certificates in a public directory
  - Whenever a certificate becomes invalid (e. g. due to fraud) the **Certification Authority** **revokes** the certificate. Revocations are also published.

## Example: Certification Authority

### ▶ Main functions of a Certification Authority

- **Registration of participants**, that means identification of the requester for a digital certificate
  - this task is sometimes delegated to a so called Registration Authority
- Secure **generation of a key pair** (public and private key for the requester)
- Secure **generation of a certificate** for the public key
  - Unique tie between the identifying properties of the requester and the generated public key
- Secure transmission of the private key to the requester
- Secure **publication of generated certificates** and public keys (as a part of the certificate)
- Revocation of certificates, publication of revocation list

### ▶ Main advantage of a Certification Authority

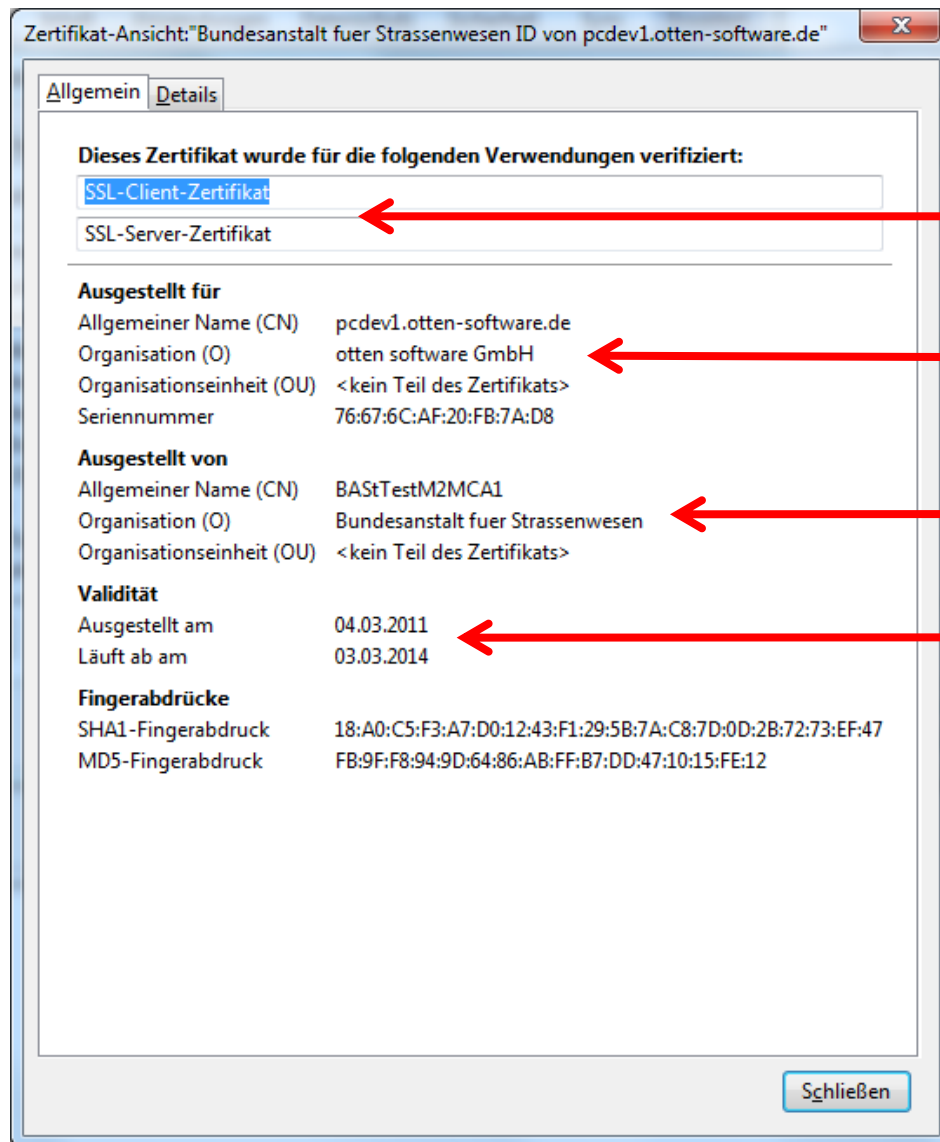
- **Delegation of Trust** (Issuer of digital identity Cards)
- Avoidance of the need for mutual identification of the communication partners



## Types of Certificates

- ▶ **The „quality“ of a certificate is determined by the following parameters**
  - The precision of the registration process, mainly the identification of the requester
  - The Safety and Security of the production and distribution processes for keys and certificates, mainly the technical and organizational processes to keep private keys really private
  - The response time for a certificate revocation request
- ▶ **Machine Certificates**
  - Usage:
    - Authentication during TSL/SSL connection setup
    - Signing Requests for DGT documents
  - Strength
    - Advanced certificate and digital signature
- ▶ **Personal Certificates**
  - Usage
    - Signing DGT documents
  - Strength
    - Qualified certificate and digital signature, DS is equivalent to manual signature

## Example: Digital Certificates of TSL/SSL communication



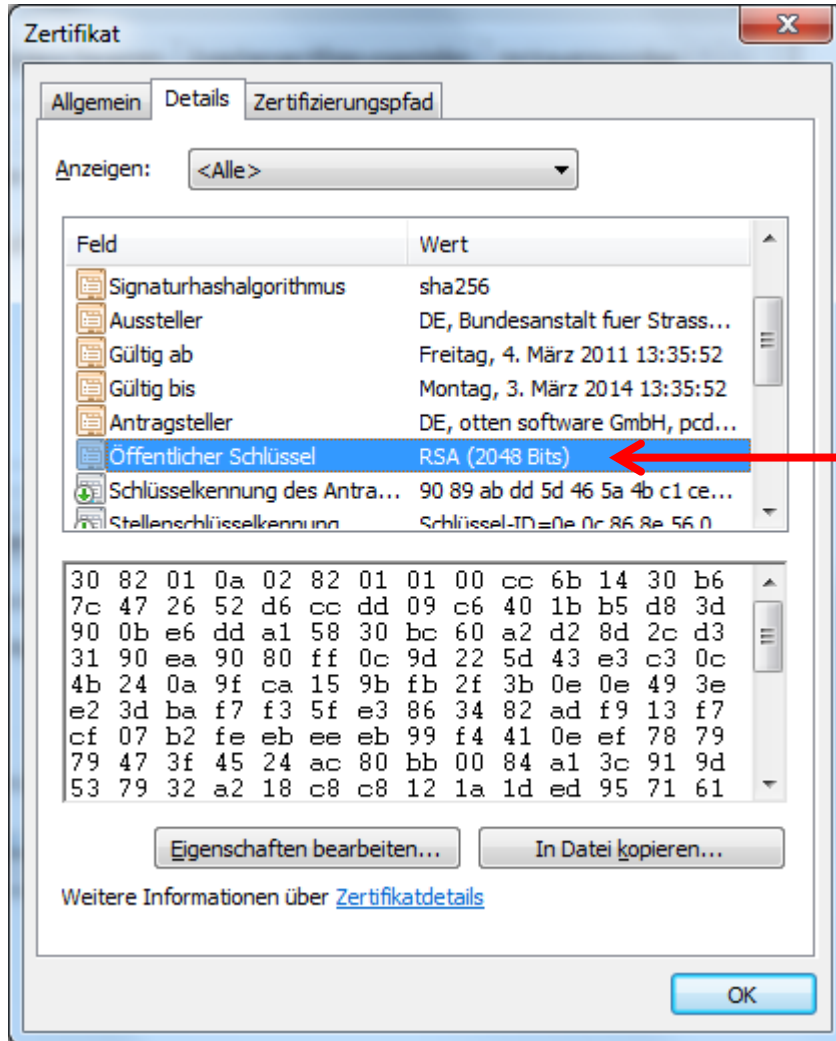
Key Usage

Machine Name / URI

Issuer / CA

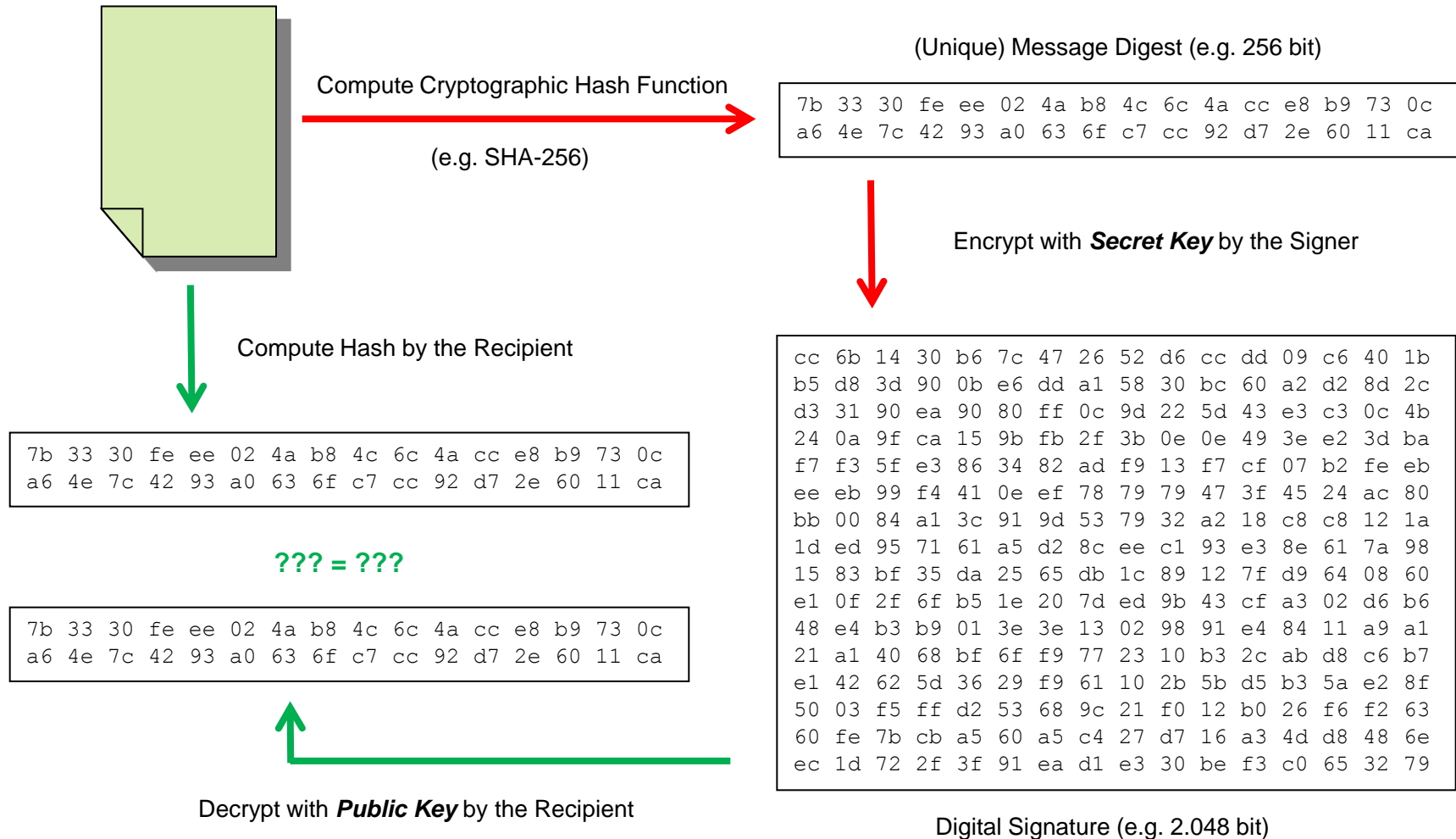
Validity

# Example: Digital Certificates

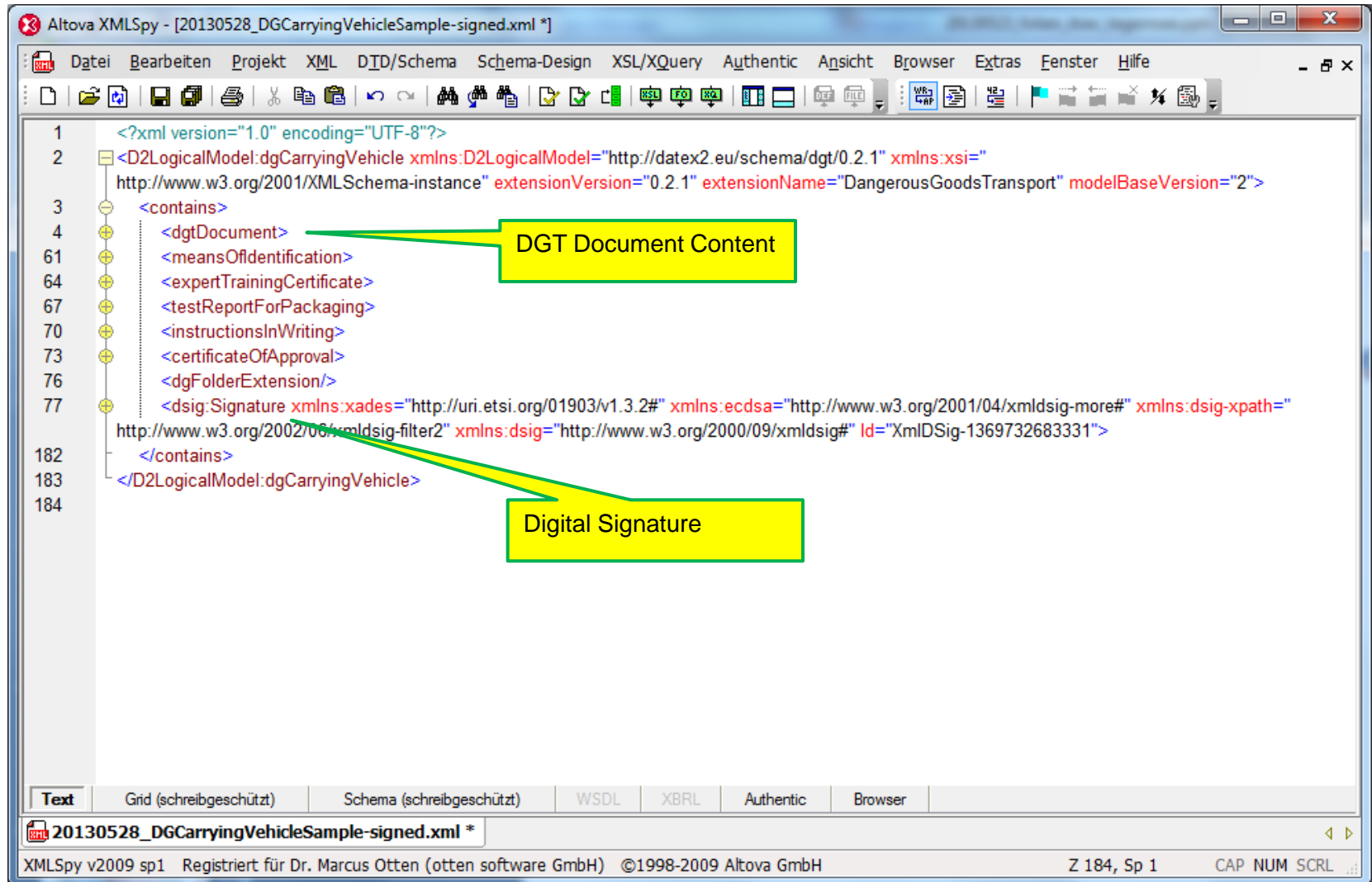


Public Key

# From messages to signed messages: How Digital Signatures are computed and checked



# XMLDSig: A W3C Standard for Signing XML documents



The screenshot shows the XMLSpy interface with the following XML content:

```

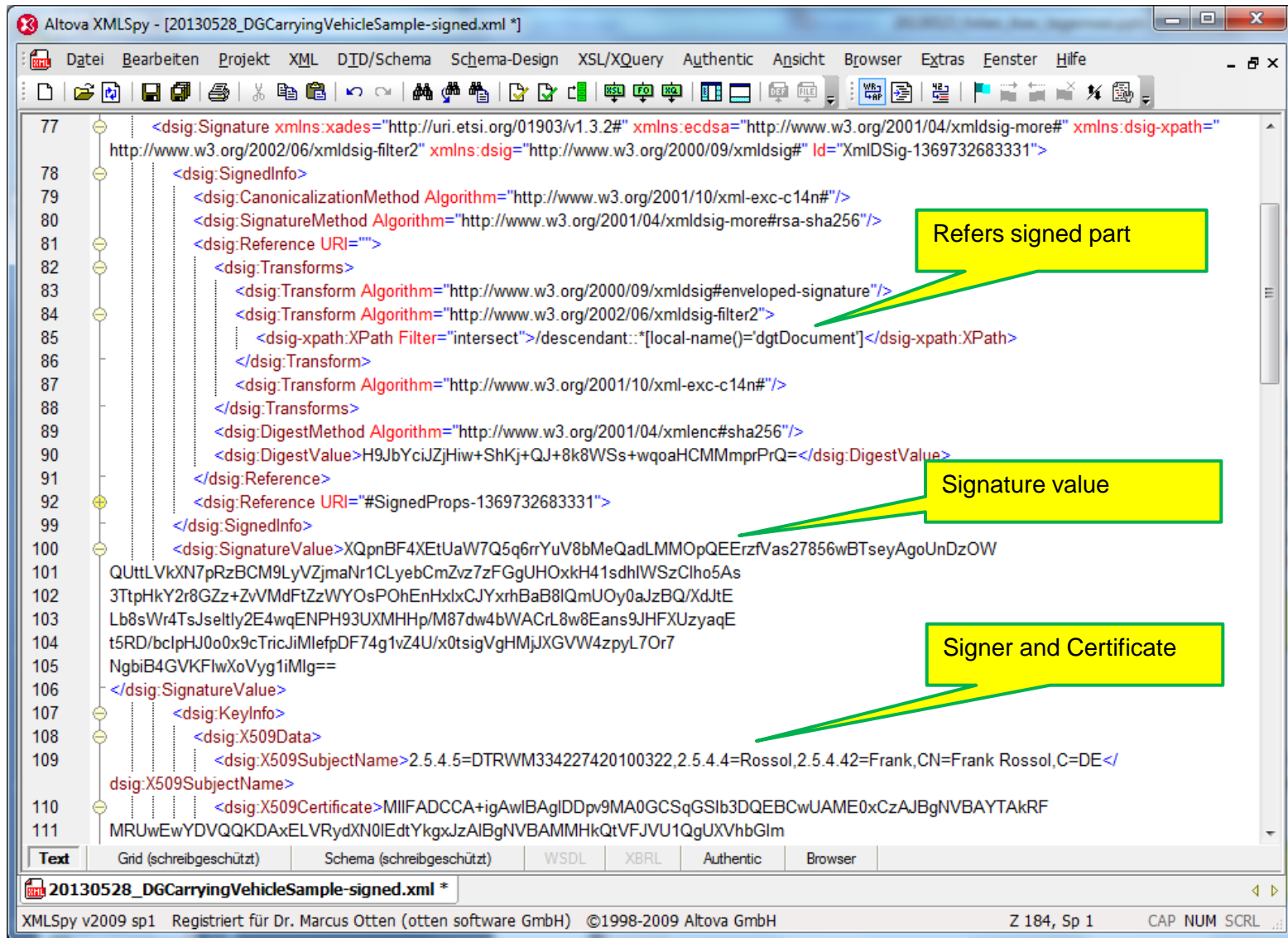
1 <?xml version="1.0" encoding="UTF-8"?>
2 <D2LogicalModel:dgCarryingVehicle xmlns:D2LogicalModel="http://datex2.eu/schema/dgt/0.2.1" xmlns:xsi="
  http://www.w3.org/2001/XMLSchema-instance" extensionVersion="0.2.1" extensionName="DangerousGoodsTransport" modelBaseVersion="2">
3   <contains>
4     <dgtDocument>
61     <meansOfIdentification>
64     <expertTrainingCertificate>
67     <testReportForPackaging>
70     <instructionsInWriting>
73     <certificateOfApproval>
76     <dgFolderExtension/>
77     <dsig:Signature xmlns:xades="http://uri.etsi.org/01903/v1.3.2#" xmlns:ecdsa="http://www.w3.org/2001/04/xmlsig-more#" xmlns:dsig-xpath="
  http://www.w3.org/2002/06/xmlsig-filter2" xmlns:dsig="http://www.w3.org/2000/09/xmlsig#" Id="XmlDSig-1369732683331">
182   </contains>
183 </D2LogicalModel:dgCarryingVehicle>
184
  
```

Two yellow callout boxes highlight specific parts of the XML:

- DGT Document Content**: Points to the `<contains>` element (line 3).
- Digital Signature**: Points to the `<dsig:Signature>` element (line 77).

The status bar at the bottom indicates: XMLSpy v2009 sp1, Registriert für Dr. Marcus Otten (otten software GmbH), ©1998-2009 Altova GmbH, Z 184, Sp 1, CAP NUM SCRL.

# XMLDSig: A W3C Standard for Signing XML documents



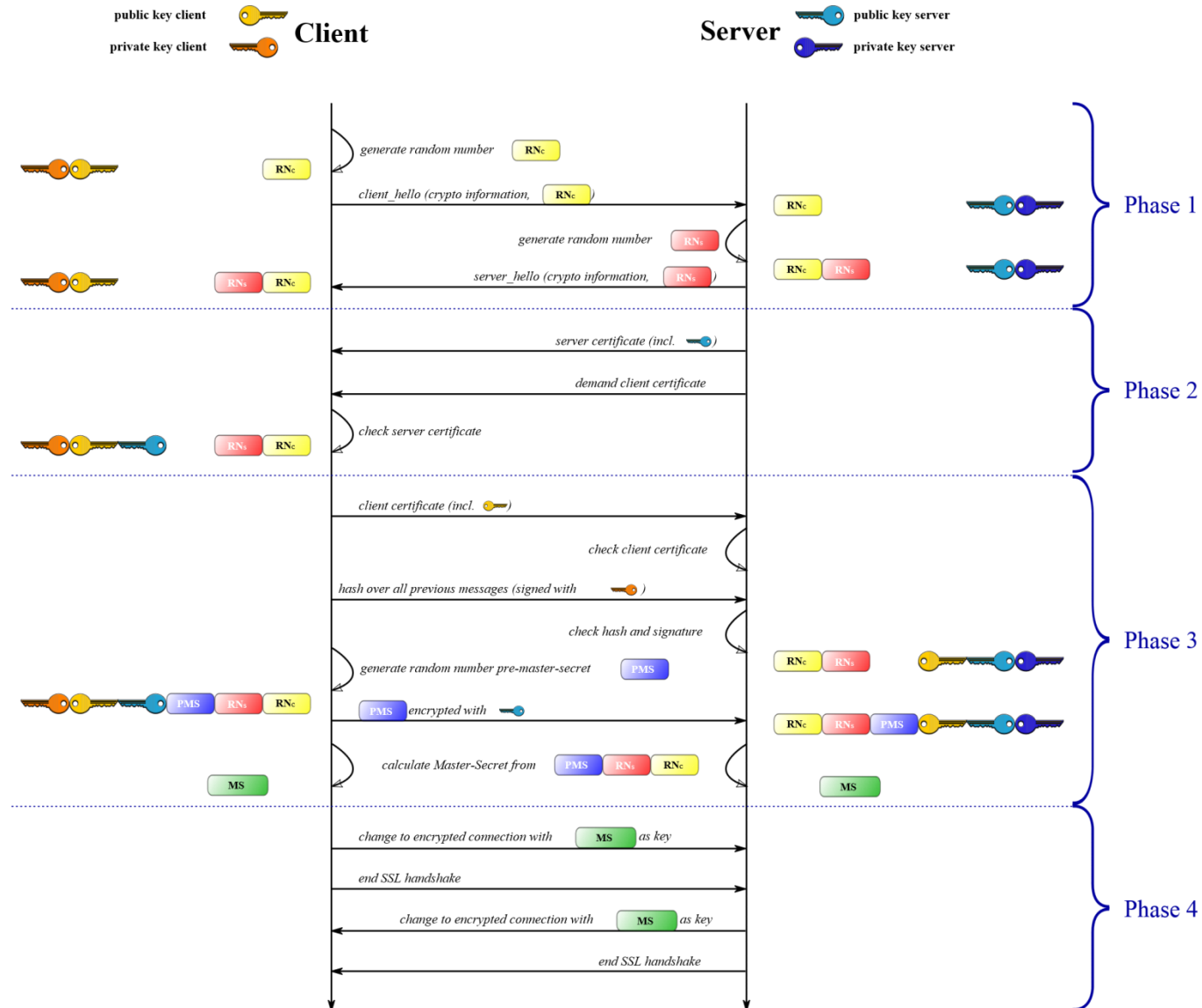
The screenshot displays the XML structure of a signed document in XMLSpy. The root element is `<dsig:Signature>` with various namespace attributes. It contains a `<dsig:SignedInfo>` block with the following elements:

- `<dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">`
- `<dsig:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmlenc-rsa-sha256#">`
- `<dsig:Reference URI="">`
  - `<dsig:Transforms>`
    - `<dsig:Transform Algorithm="http://www.w3.org/2000/09/xmlsig-enveloped-signature#">`
    - `<dsig:Transform Algorithm="http://www.w3.org/2002/06/xmlsig-filter2#">`
      - `<dsig-xpath:XPath Filter="intersect"/>/descendant::*[local-name()='dgtDocument']</dsig-xpath:XPath>`
    - `<dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">`
  - `<dsig:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc-sha256#">`
  - `<dsig:DigestValue>H9JbYciZJHw+ShKj+QJ+8k8WSs+wqoaHCMMmprPrQ=</dsig:DigestValue>`
  - `<dsig:Reference URI="#SignedProps-1369732683331">`
- `<dsig:SignatureValue>XQpnBF4XEtUaW7Q5q6rYuV8bMeQadLMMOpQEErZfVas27856wBTseyAgoUnDzOW  
QUtLLVkXN7pRzBCM9LyVZjmaNr1CLyebCmZvz7zFGgUHOxkH41sdhIWSzClho5As  
3TtpHkY2r8GZz+ZvVmdFzZWYOsPOhEnHlxCJYxrhBaB8IQmUOy0aJzBQ/XdJtE  
Lb8sWr4TsJseltly2E4wqENPH93UXMHHp/M87dw4bWACrL8w8Eans9JHFXUzyaqE  
t5RD/bclpHJ0o0x9cTricJiMlefpDF74g1vZ4U/x0tsigVgHMjXGvVW4zpyL7Or7  
NgbiB4GVKFlwXoVyg1iMlg==`
- `<dsig:KeyInfo>`
  - `<dsig:X509Data>`
    - `<dsig:X509SubjectName>2.5.4.5=DTRWM334227420100322,2.5.4.4=Rossol,2.5.4.42=Frank,CN=Frank Rossol,C=DE</dsig:X509SubjectName>`
    - `<dsig:X509Certificate>MIIFADCCA+igAwIBAgIDDp9MA0GCSqGSIb3DQEBCwUAME0xCzAJBgNVBAYTAkRFMRUwEwYDVQQKDAxELVRydXN0IEdtYkxjZAlBgnVBAMMHkQtVFJVU1QgUXVhbGlm`

Annotations in the image point to specific parts of the XML:

- Refers signed part:** Points to the `<dsig:Reference URI="">` element.
- Signature value:** Points to the `<dsig:SignatureValue>` element.
- Signer and Certificate:** Points to the `<dsig:X509Certificate>` element.

# TSL/SSL connection setup using Digitale Certificates



**How are similar requirements met and similar questions handled in other relevant business areas (eCommerce, health, ...)**



## Public Key Infrastructure (PKI) is widely used and “of the shelf” technology

### ▶ **TLS/SSL encryption of Websites**

- Websites present a Digital Certificate to prove their validity; certificates are issued by different Trust Centers (e. g. VeriSign)

### ▶ **EUCARIS - European CAR and driving license Information System**

- Communication of EUCARIS servers is secured by SSL
- (XML-)Messages are signed using certificates

### ▶ **German Mobility Data Marketplace ([service.mdm-portal.de](http://service.mdm-portal.de))**

- Authentication at marketplace information portal is based on enduser certificates (instead of username/password)
- Machine-2-Machine-communication is secured by TSL/SSL with certificate based mutual authentication of sender and recipient

### ▶ **German Fiscal Authorities**

- In B2G communication taxpayers have to sign their tax announcements digitally

### ▶ **Germany eANV Electronic record procedure for waste recovery and disposal**

- Communication is secured by OSCI eGovernment Framework based on certificates
- (XML-)Messages are digitally signed using certificates

## IT security mechanisms in our DGT Framework proposal

### ▶ **Our Dangerous Goods Framework proposal**

- TSL/SSL encryption of communication processes with mutual authentication (sender and recipient)
- Digital signatures for dangerous goods data and data requests

### ▶ **authentication of communication channels**

- machine-2-machine communication after mutual authentication based on certificates

### ▶ **encryption of communication channels**

- TSL/SSL encryption of communication channels

### ▶ **Authentication and authorization mechanisms**

- The identification of participants is without any exception based on digital certificates

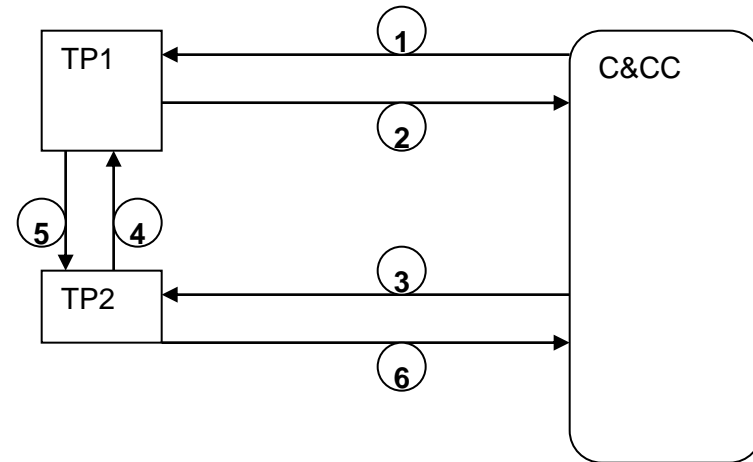
### ▶ **Signed Data**

- DGT document is secured by a (qualified) digital signature
- Data Request message for DGT informations is secured by a (qualified or non-qualified) digital signature

## Examples for the use of PKI for DS and Authentication

### ► C&CC determines URI for TP2 (Step 1 and 2)

- TSL/SLL-Channel using Certs from C&CC and TP1
- XMLDSig SOAP Request , Signature from C&CC (automatically generated)



### ► C&CC gets DGT-Document from TP2 (Direct Mode, Step 3 to 6):

- TSL/SLL-Channel using Certs from C&CC and TP2
- TSL/SLL-Channel using Certs from TP2 and TP1
- XMLDSig SOAP Request, Signature from C&CC (automatically generated)
- SOAP Response with XMLDSig DGT Document (qualified signature from carrier)

## **Organisational, financial and technical impacts**

## Impacts of our DGT Model

- ▶ **No need for a dedicated Public Key Infrastructure**
  - Due to the usage of standardized Algorithms and Certificate Structures the system can be based on existing Public Key Infrastructure
- ▶ **How can users obtain certificates**
  - For both personal and machine certificates national and international certification authorities are available
  - Machine certificates are issued by a variety of companies, e.g. verisign, baltimore, digicert, RSA security, Twathe
  - Qualified personal certificates can be obtained from trustcenters according to DIRECTIVE 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures
- ▶ **Carriers and C&CCs IT systems**
  - must be able to build, sign and verify XML documents
  - must implement SOAP interfaces to TP1 and TP2 with IT standard mechanisms including certificate based TSL/SSL connections



Bundesministerium  
für Verkehr, Bau  
und Stadtentwicklung

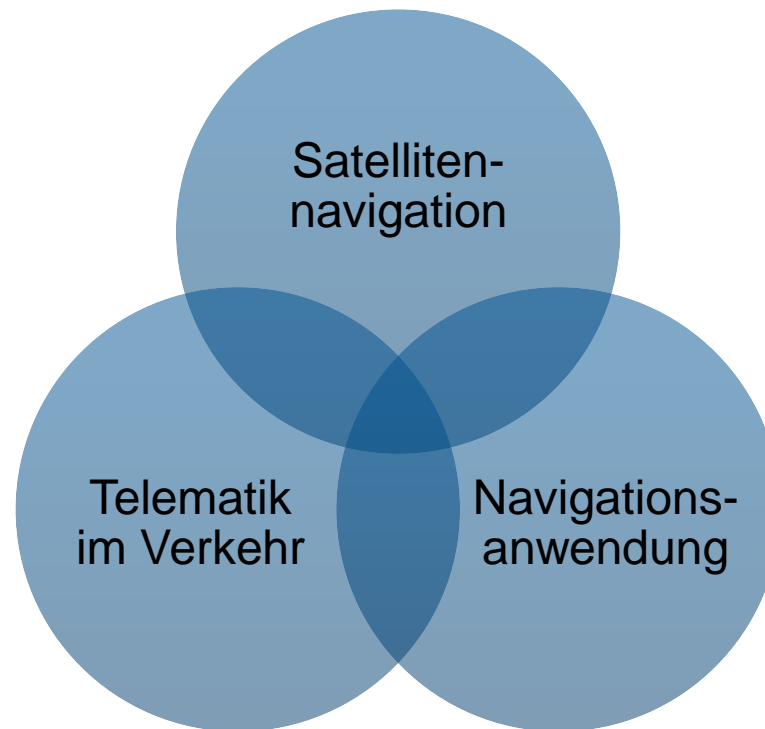
# Telematik im Verkehr

11. Sitzung der Arbeitsgruppe „Telematik“ der  
Gemeinsamen Sitzung  
03. – 04.06.2013 in Tegernsee

BMVBS – UI 35

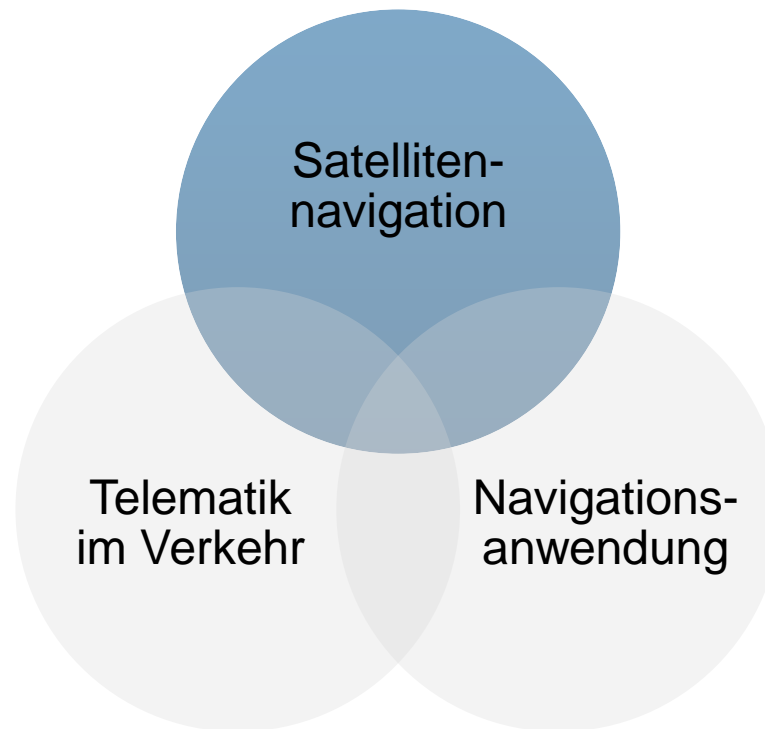


## Das Tätigkeitsfeld von Referat UI 35





## Satellitenavigation - Anwendungen - Telematik



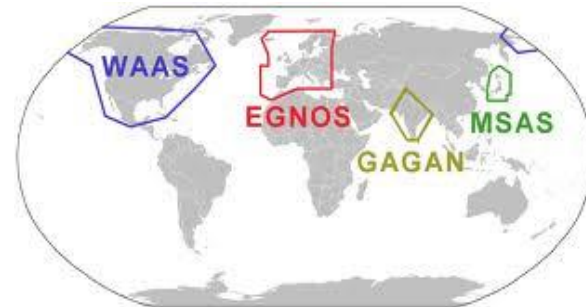




## Satellitenavigation - Anwendungen - Telematik

### Satellitenavigation leistet weltweit entscheidende Unterstützung bei Ortung und Positionierung

- Bestehende Globale Satellitenavigationssysteme (GNSS)
  - GPS (USA)
  - GLONASS (RUS)
- regionale Ergänzungssysteme
  - WAAS (Nordamerika)
  - EGNOS (Europa)
  - MSAS (Japan / Asien)
  - GAGAN (Indien)





## Satellitenavigation - Anwendungen - Telematik

### Die Europäische Union entwickelt mit Galileo und EGNOS einen eigenständigen Zugang zur Satellitenavigation

- politische Entscheidung
- sichert Unabhängigkeit  
(*strategisch & wirtschaftlich*)
- sichert Technologiekompetenz  
(*Empfängerentwicklung*)





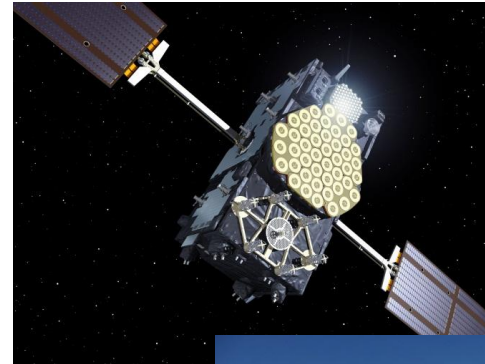
## Satellitennavigation - Anwendungen - Telematik

### Galileo Weltrauminfrastruktur

- 30 Satelliten
- auf drei Umlaufbahnen
- in 23 260 km Höhe

### Galileo Bodeninfrastruktur

- Zwei Kontrollzentren steuern Satelliten und Signale
- Zwei Sicherheitszentren (GSMC) für PRS
- Ein GNSS Servicezentrum für OS, CS und SoL
- Weltweites Netz von mehr als 20 Bodenstationen





## Satellitenavigation - Anwendungen - Telematik

- **Offener Dienst (OS)**  
Offenes, kostenloses Basissignal
- **„Public Regulated Service“ (PRS)**  
robuster verschlüsselter Dienst  
*(vor allem für Behörden mit  
Sicherheitsaufgaben)*
- **„Search and Rescue“ Dienst (SaR)**  
Verbesserung internationaler Hilfssysteme
- **Kommerzieller Dienst (CS)**  
Kommerzielles Signal  
mit kostenpflichtiger Zusatzinformation
- **„Safety of Life“ Dienst (SoL)**  
über EGNOS auf Basis Galileo + GPS  
Integritätsmeldung *(alle 10 Sek.)*





## Satellitennavigation - Anwendungen - Telematik

### Entwicklungsphase (bis 2013)

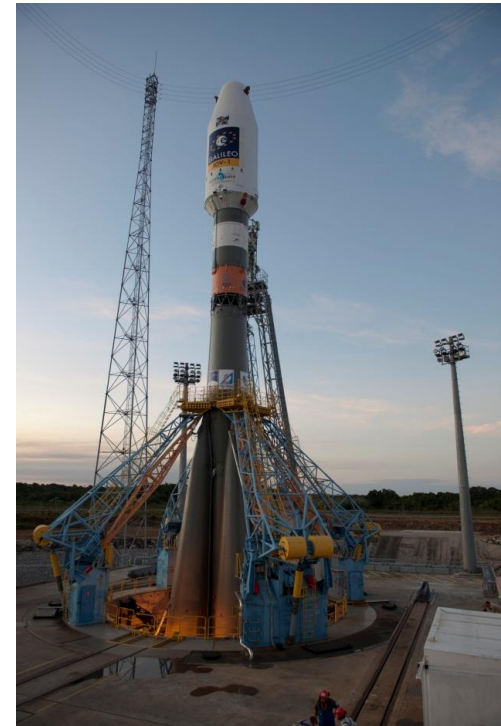
- seit Oktober 2012 vier Satelliten im All
- Aufbau der zentralen Bodeninfrastruktur
- Validierung der Systemfunktionen

### Erste Betriebsbereitschaft (ab 2014/15)

- ‚Initial Operational Capability‘ - IOC
- erste Galileo-Dienste verfügbar
- Spürbare Verbesserung beim Offenen Dienst durch GPS + Galileo
- PRS zunächst eingeschränkt nutzbar

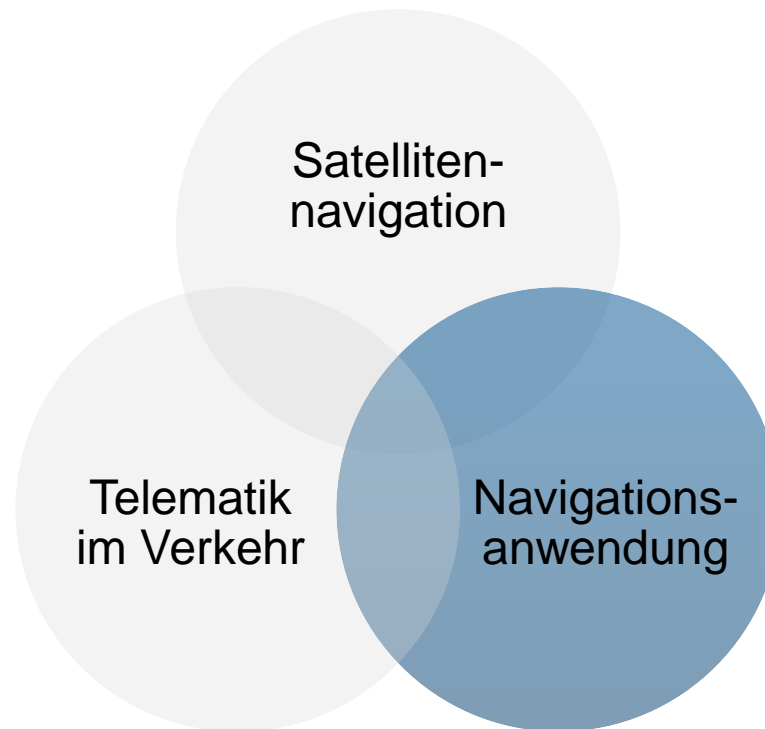
### Vollausbau (bis etwa 2018)

- Konstellation aus 30 Satelliten im All
- Vollausbau der Bodeninfrastruktur
- eigenständige Verfügbarkeit aller Dienste





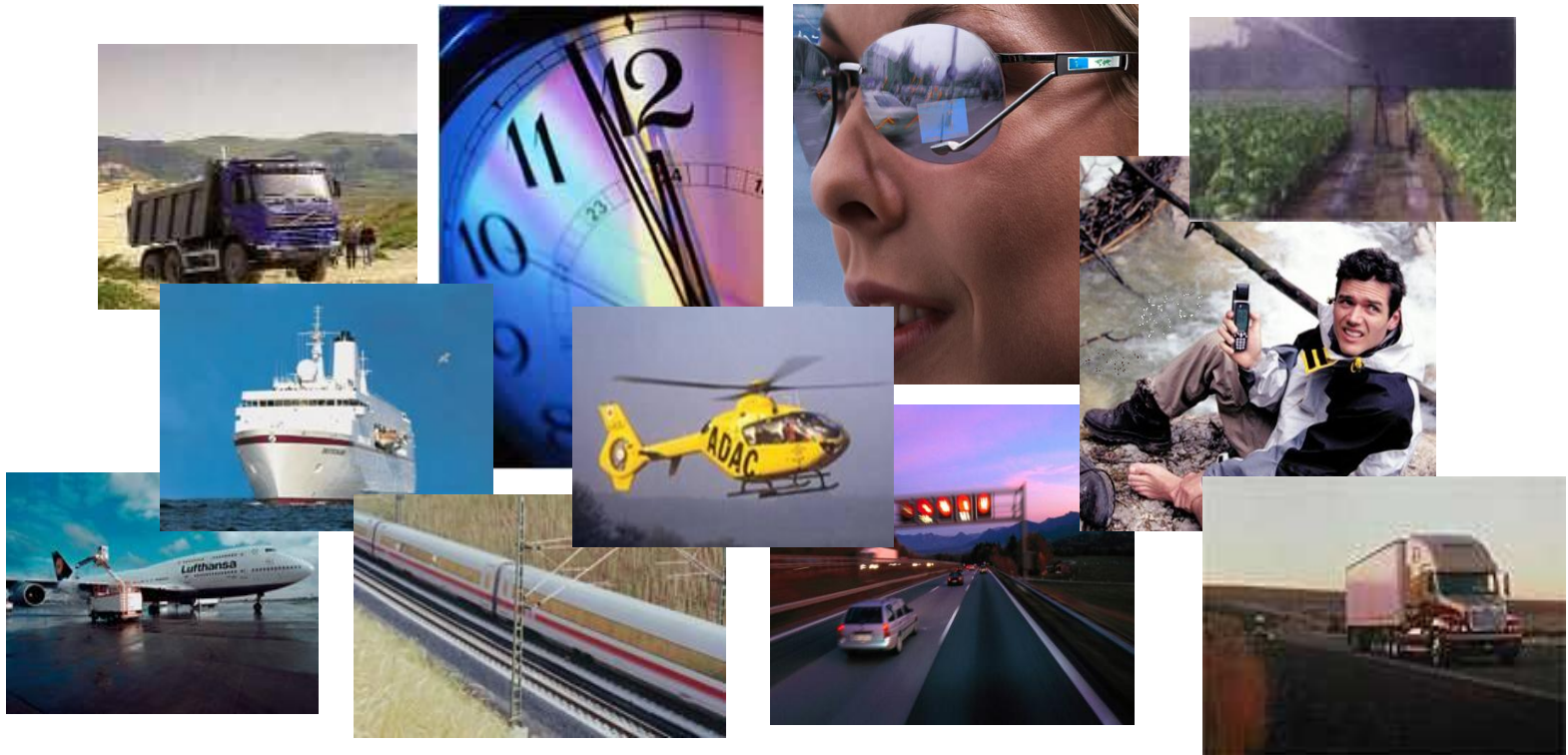
## Satellitenavigation - **Anwendungen** - Telematik





# Satellitennavigation - Anwendungen - Telematik

## Vielfältige Einsatzmöglichkeiten der Satellitennavigation





## Satellitennavigation - Anwendungen - Telematik

### Satellitennavigation auf der Straße – weit mehr als reine Navigation

- Mautsysteme für effizientere Nutzung der Infrastruktur
- Flottenmanagement für Logistik, ÖPNV, Taxi-Dienste
- Neue Mobilitätsangebote z.B. Flexible Autovermietung, Mitfahrgelegenheiten







## Satellitennavigation - Anwendungen - Telematik

### mehr Sicherheit durch präzise Ortung

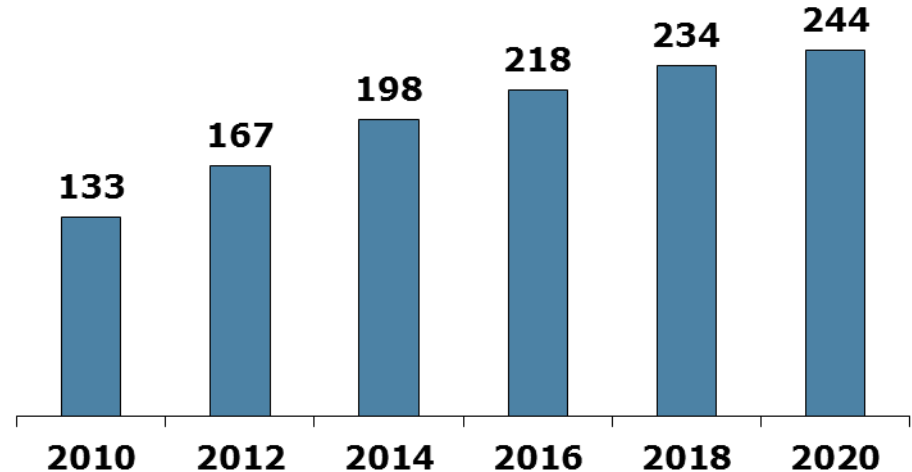
- eCall automatischer Notruf mit Positionsdaten
- Überwachung von Gefahrguttransporten
- Effizientere Rettung bei Gefahrgutunfällen
- Neue Möglichkeiten für Unfallrekonstruktion und Diebstahlsicherung





## Satellitennavigation - Anwendungen - Telematik

- Der weltweite Markt für Anwendungen der Satellitennavigation bietet deutliches Wachstumspotenzial
- Marktbericht der GSA prognostiziert stetiges Wachstum von jährlich 11 % bis 2020



**Markt für GNSS-taugliche Produkte in Mrd. €**

Quelle: „GNSS Marktbericht“, GSA Oktober 2010



## Satellitennavigation - **Anwendungen** - Telematik

### **Deutschland für Wettbewerb gut aufgestellt**

- Logistikdrehscheibe für Europa
- Forschungsstandort
- starker IT-Sektor
- international führende Automobilindustrie
- Kleine und mittlere Unternehmen sind das wirtschaftliche Rückgrat



Synergiepotenziale liegen zunehmend in der **Kooperation über Branchengrenzen** hinweg



## Satellitennavigation - Anwendungen - Telematik

### Bundesregierung unterstützt Entwicklung innovativer Navigationstechnologie

- Galileo Test- und Entwicklungsumgebungen
- Förderprogramme
- Raumfahrtstrategie der Bundesregierung





## Satellitennavigation - Anwendungen - Telematik



- Gemeinsames Netzwerk der regionalen Initiativen für Satellitennavigation
- Starkes Engagement der Bundesländer
- Schirmherrschaft und Moderation des BMVBS

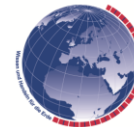




## Satellitennavigation - Anwendungen - Telematik

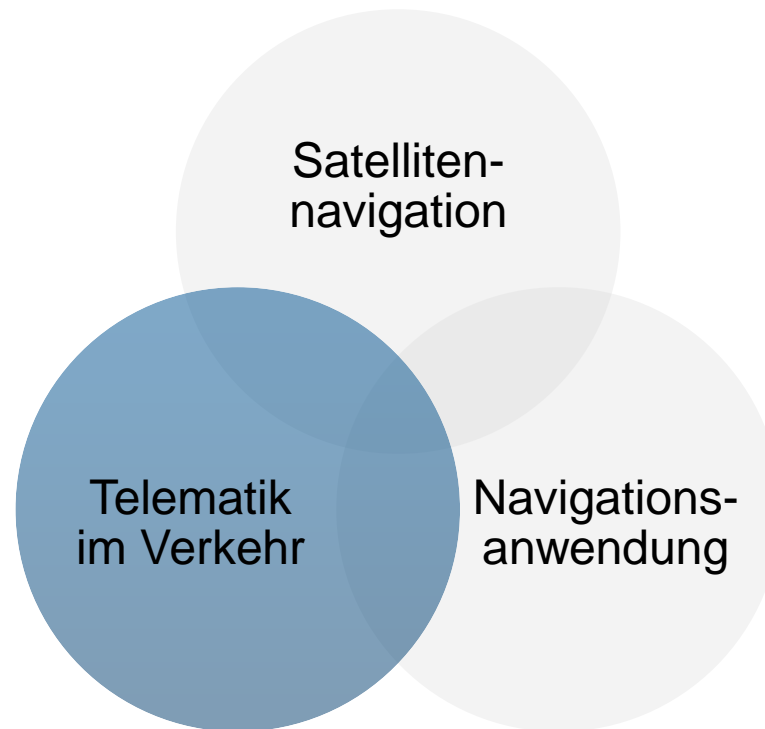
### Die Navigationskonferenz *Orientierung in der intelligenten Welt*

- jährliche Konferenz des BMVBS zu Navigationsanwendungen
- Nächster Termin 04.06.2013 im Rahmen der Fachmesse Transport Logistik München





## Satellitennavigation - Anwendungen - Telematik





## Satellitennavigation - Anwendungen - Telematik

### Verkehrstelematik für Sicherheit & Effizienz

- Telematiksysteme können Verkehr flüssiger machen und steigern Vernetzung der Verkehrssysteme
- in allen Verkehrsbereichen verbreitet
- privatwirtschaftliche Initiative gefragt
- ‚Kollektive Systeme‘ können staatlich betrieben werden  
(z.B. Beispiel Lenk- und Leitsysteme)



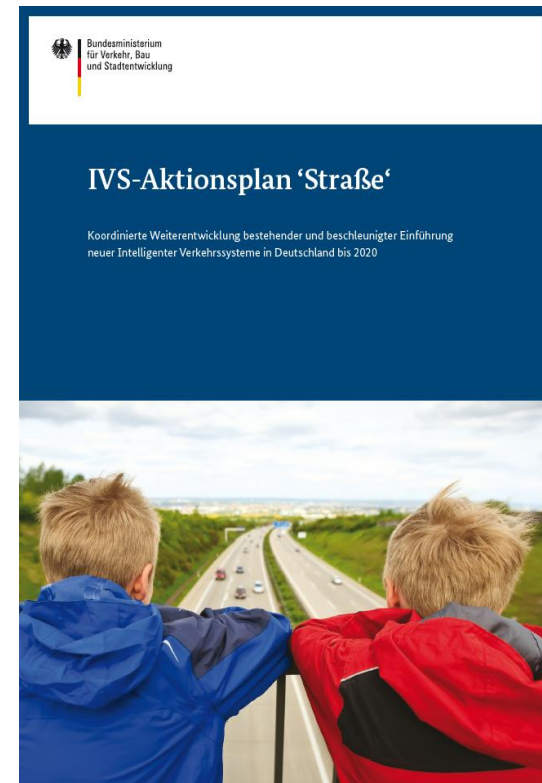




## Satellitennavigation - Anwendungen - Telematik

Europäische **IVS-Richtlinie** erfordert nationale Umsetzung mit Aktionsplänen

- Deutscher IVS-Aktionsplan „Straße“ von BMVBS unter Beteiligung der maßgeblichen nationalen Akteure erarbeitet (Fdf LA 20)
- Erste Vorstellung beim ITS-Weltkongress 22.-26.10.2012 in Wien
- IVS-Konferenz am 26.02.2013 im BMVBS hat Aktionsplan weiter bekannt gemacht und für Mitwirkung bei Umsetzung geworben



Vielen Dank für Ihre Aufmerksamkeit.

Bundesministerium für Verkehr,  
Bau und Stadtentwicklung (BMVBS)

Referat UI 35 - Verkehrsoptimierung, Telematik im Verkehr  
Invalidenstraße 44  
D-10115 Berlin

[www.bmvbs.de](http://www.bmvbs.de)



# **Developments in TAF TSI concerning Transport of Dangerous Goods by rail**

**Tegernsee – 3-4 June 2013**



- ❖ In RISC committee held in October 2012, ERA was requested to better align the data conveyed in the framework of the TAF TSI in regards existing RID requirements
- ❖ ERA analysed the current data catalogue of the TAF and prepared a change to the content of the current messages, these changes will be adopted soon.

The changes to the TAF data catalogue are discussed and validated through the Change Control Management chaired by ERA



- ❖ **Core objectives of the TAF TSI and UNECE Telematics WG are not the same**
- ❖ **TAF TSI aims at establishing an optimum level of interoperability of data exchanges related to rail freight business**
- ❖ **TAF TSI is not focussed on safety improvements**
- ❖ **TAF TSI developments are operated within a strict scope and agenda included in the Strategic European Deployment Plan**



- ❖ To date, the following information can be considered within the TAF TSI scope:
  - ◆ CIM/SMGS consignment note, including dangerous goods description (as required by Chapter 5.4 of RID)
  - ◆ Other RID requirements concerning legally binding exchange of information between RUs and IMs, for example section 1.4.3.6
  - ◆ ...
- ❖ The sector has prepared the corresponding data structures (messages) to be incorporated in the TAF TSI messages



### ❖ A combination of information sources:

-> **what train is where at what time?**

- ◆ TAF TSI 'train running information'

-> **what is carried in/on what wagon?**

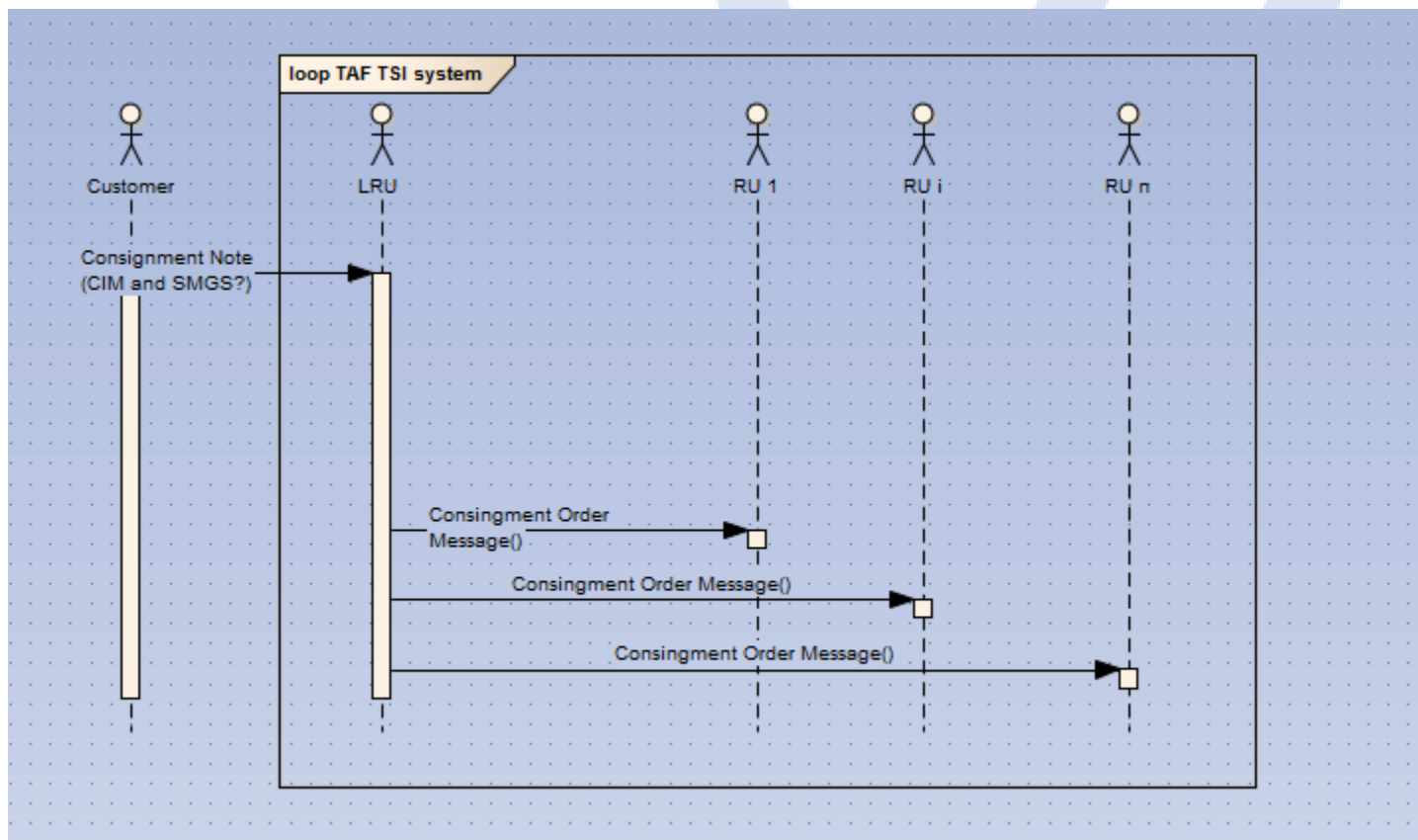
- ◆ TAF TSI 'train composition message' inc. wagon number

-> **how can the information concerning Dangerous Goods be reached by third parties?**

- ◆ Several options need to be assessed



## ❖ Sequence diagram







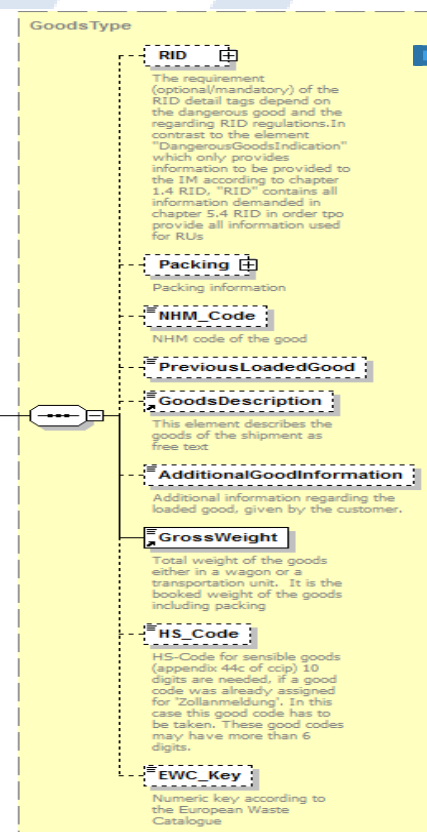
- ❖ Most of section A (WHO DOES WHAT RID table) elements will be integrated in the TAF TSI data catalogue

Consignment order message

Wagon

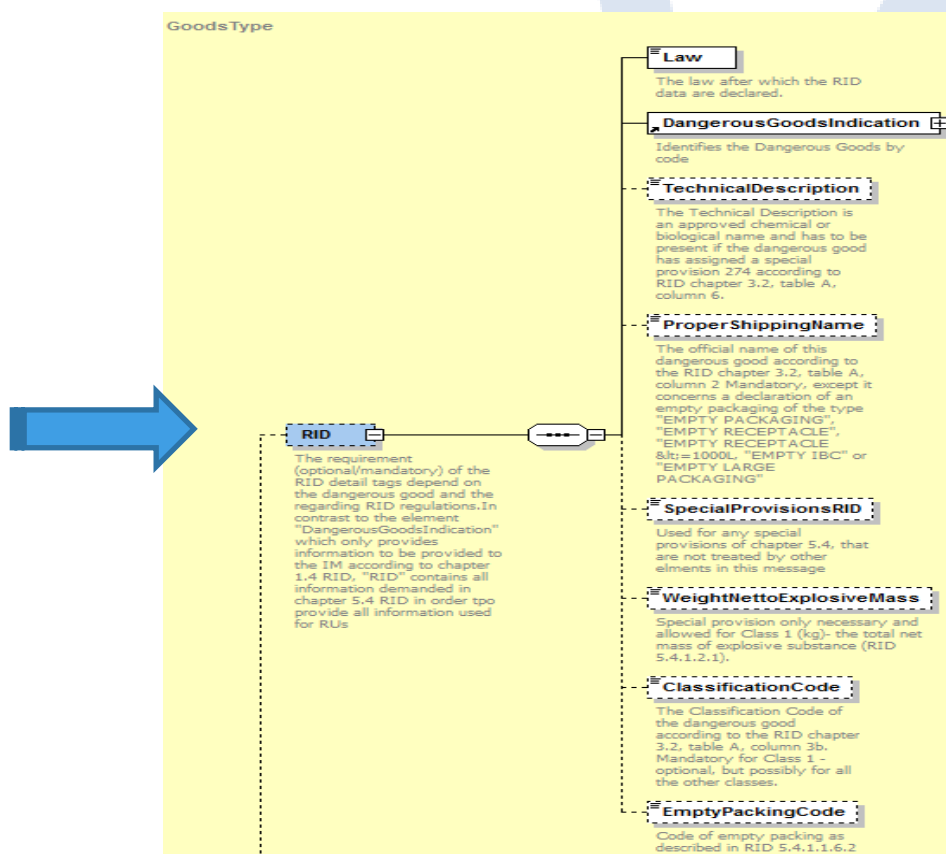
- Goods

Goods  
1..99  
Describes the good inside the mean of transport



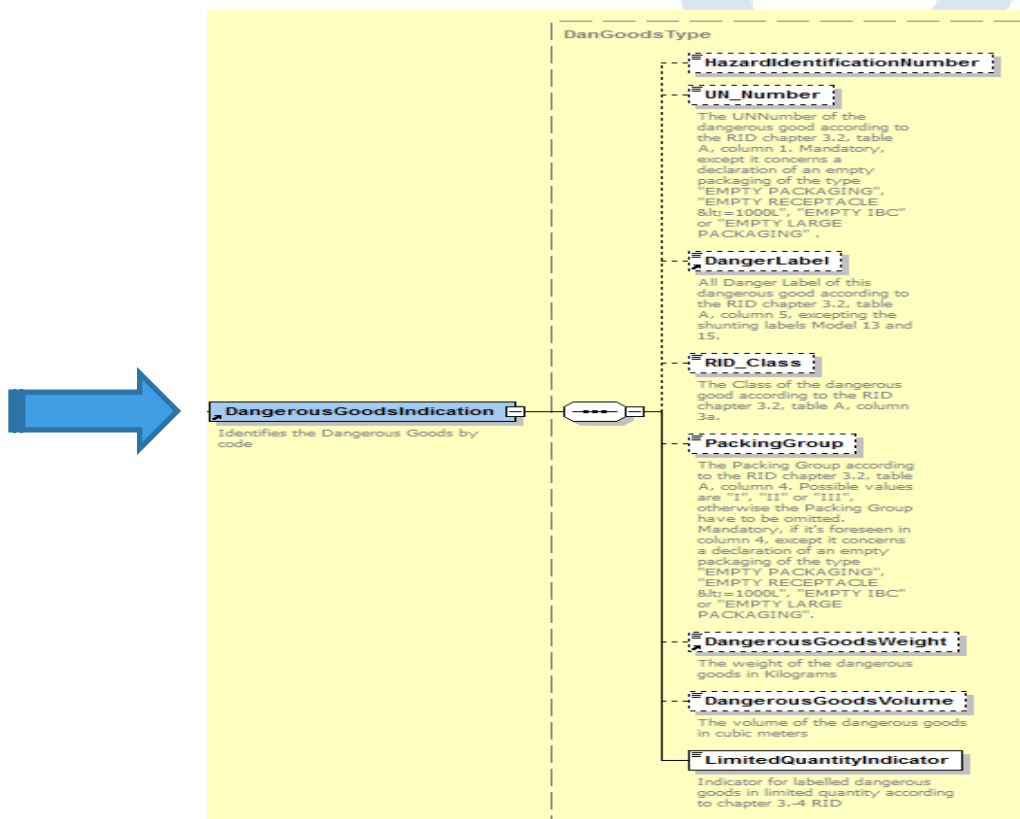


## ❖ Most of section A elements will be integrated in the TAF TSI data catalogue





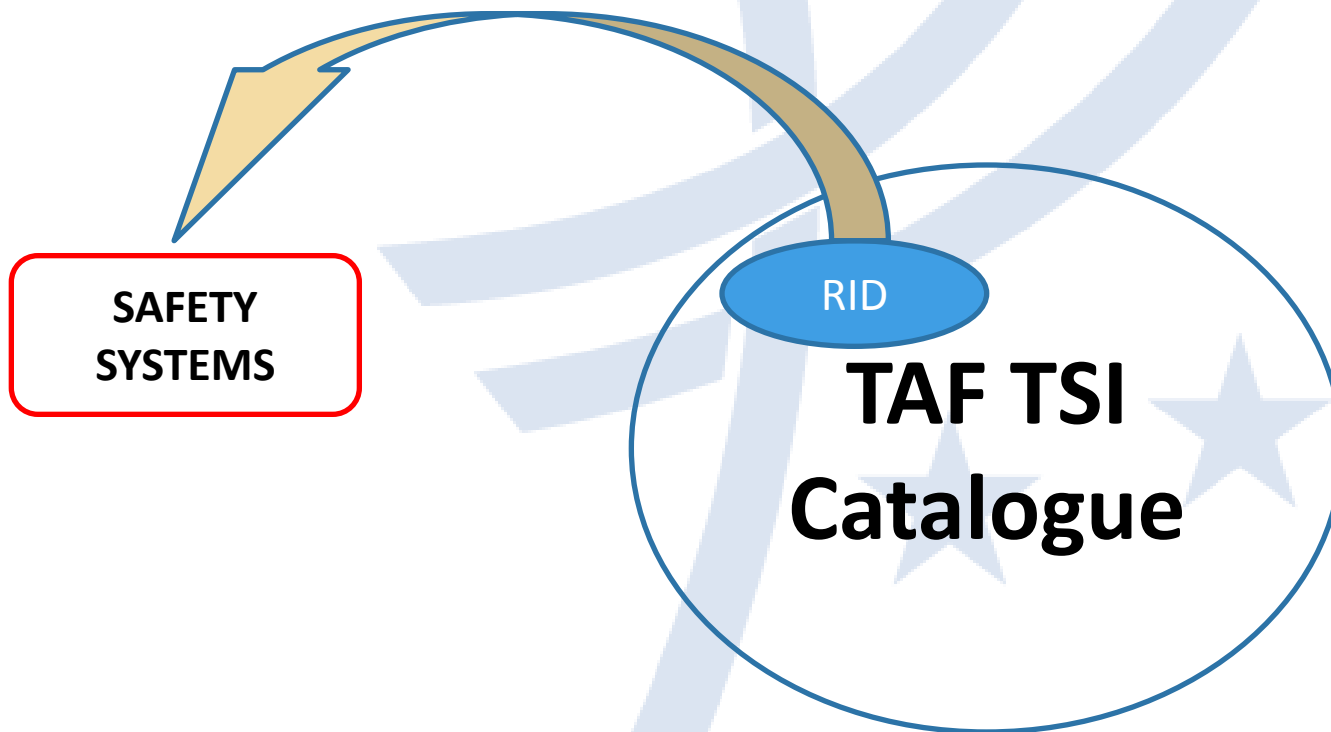
- ❖ Most of section A elements will be integrated in the TAF TSI data catalogue





# Added value for non-TAF and safety related systems.

- ❖ TAF catalogue will contain RID data, but this will not be used in TAF system:





# Thank you for your kind attention:

ERA Telematics Team

Project officers for Telematics Applications at European Railway Agency

E-mail: [Mickael.VARGA@era.europa.eu](mailto:Mickael.VARGA@era.europa.eu)  
[Stefan.Jugelt@era.europa.eu](mailto:Stefan.Jugelt@era.europa.eu) [Rodrigo.Gutierrez@era.europa.eu](mailto:Rodrigo.Gutierrez@era.europa.eu)  
[Rafael.garciamartinez@era.europa.eu](mailto:Rafael.garciamartinez@era.europa.eu)



# Further French Development

**Jean-Philippe MECHIN**  
**Cete du Sud-Ouest**  
**5 June 2013**



Ressources, territoires, habitats et logement  
Énergies et climat Développement durable  
Prévention des risques Infrastructures, transports et mer

Présent pour l'avenir



Centre d'Études Techniques de l'Équipement du Sud-Ouest

# Context

- 24 October 2007 Mandate including 2 parts :
  - I. TERMS OF REFERENCE OF THE INFORMAL WORKING GROUP ON THE USE OF TELEMATICS FOR THE CARRIAGE OF DANGEROUS GOODS
  - II. WORK PROGRAMME OF THE INFORMAL WORKING GROUP ON THE USE OF TELEMATICS FOR THE CARRIAGE OF DANGEROUS GOODS
- 31 August 2010 Final version of the « who does what » table

# Strong interest expressed in France

- Ministry of Ecology Sustainable Development and Energy
- Companies like :
  - Novacom
  - FDC
  - Geoloc Systems
  - M3 System
  - MD Service
  - Renault Trucks
- Telematic services already for freight and also DGT used by several operators



# Work programme of the informal Working Group (1)

- 1 & 2. Examine national research projects and EC feasibility study
- 3. Verify or examine in what kind of functions in dangerous goods transport telematics facilities might be desirable (also in addition to tracking & tracing) in a multimodal perspective, to improve transport safety or security, each to be examined separately if necessary;
- 4. Verify or examine in which additional, mode-specific functions telematics facilities might be desirable (such as derailment detection, control of Mobile Explosives Manufacturing Units (MEMU) vehicles), to improve transport safety or security, each to be examined separately if necessary;
- 5. Verify or examine who the users of the screened telematics facilities would be (public and private);
- 6. Verify or examine what data and communication and in which form the desired telematics facilities would be needed;

# Work programme of the informal Working Group (2)

- 7. Verify or examine to whom the data should be communicated (often several addressees);
- 8. Verify or examine whether, how and where the collected data should be stored and how it should be accessed;
- 9. Verify or examine what kind of regulations should be created and to whom they should be addressed in order to ensure that the necessary data is available for those who need it (e.g. obligation for transport companies to use on-board-units in vehicles);
- 10. Verify or examine if sufficient regulation can be provided in RID/ADR/ADN or if something more is needed in the European Union;
- 11. Verify or examine what kind of complementary standardisation would be needed to ensure interoperability of all regulated facilities and also of on-board-units with other tracking & tracing systems in other sectors;

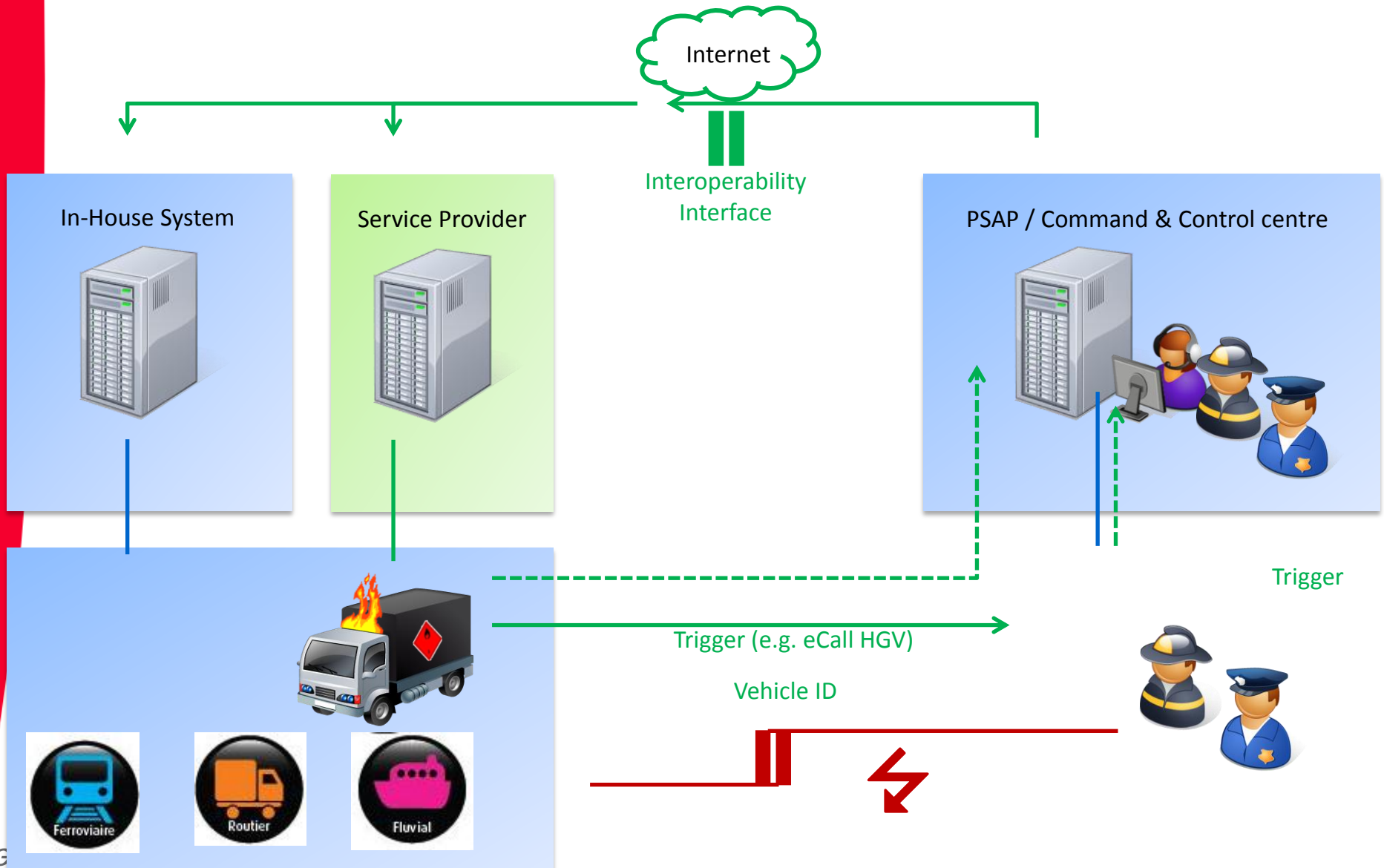
# Work programme of the informal Working Group (3)

- 12. On the basis of items 1-11 above, draft a preliminary concept of appropriate telematics facilities, including possible data centres and their organisation, and a preliminary scope of necessary regulations and standards;
- 13. Draw up a proposal to verify or assess the feasibility of the telematics facilities examined and their cost/benefit for the users;
- 14. Draw up the final description of the telematics facilities that are decided upon;
- 15. Draw up a proposal for the amendments to ADR/RID/ADN that will be required by the telematics facilities decided upon;
- 16. Draw up a summary description of necessary standards to complement the regulations.

# German proposal for §8 and 12

- 8. Verify or examine whether, how and where the collected data should be stored and how it should be accessed;
- 12. On the basis of items 1-11 above, draft a preliminary concept of appropriate telematics facilities, including possible data centres and their organisation, and a preliminary scope of necessary regulations and standards;
  - Security ensured with 2 levels of Trusted Parties (TP1, TP2)
  - Focus on procedure as regulated for transport documents :
    - Carrier
    - Competent authorities
    - Emergency responders
  - Possibility of automatic trigger or casual observers

# Basic application scenario with federated services



# GeoTrans MD Project

- National call for proposal for innovative projects with objectives to finalise a demonstrator
- Consortium must integrate private, university and public bodies
- Funding from 25% to 45% depending the status (SMEs, University, )
- Leader must be a private company
- Request for economic Impact with a business plan and working places to create
- The project must be technically and economically self standing (independently of the Joint Meeting decision)
- Link with International partners and bodies is seen as an add value

# Partners

	Partner	Effort R&D	Funding
<b>Leader</b>	Novacom (ETI)	105 HM	25%
<b>SME</b>	FDC	11 HM	30%
	M3Systems	30 HM	45%
	Geoloc Systems	90 HM	22%
	E.RE.CA	43 HM	45%
	MD Service	34 H,M	45%
<b>University</b>	LNE	12 HM	40%
	Université de Grenoble	45 HM	100%
	CEA LIST	72 HM	40%
<b>Public Body</b>	CETE SO	76 HM	3%
	CETE Lyon	5 HM	13%

- **Budget global : 5,9 M€, aide de 1,9 M€ (33%)**

- 20 % ETI
- 33 % PME
- 29 % Laboratoire
- 17 % autres

- **3 regions :**  
65 % South-Ouest  
22 % Paris  
13 % Lyon

# Various DGT actors related to project partners

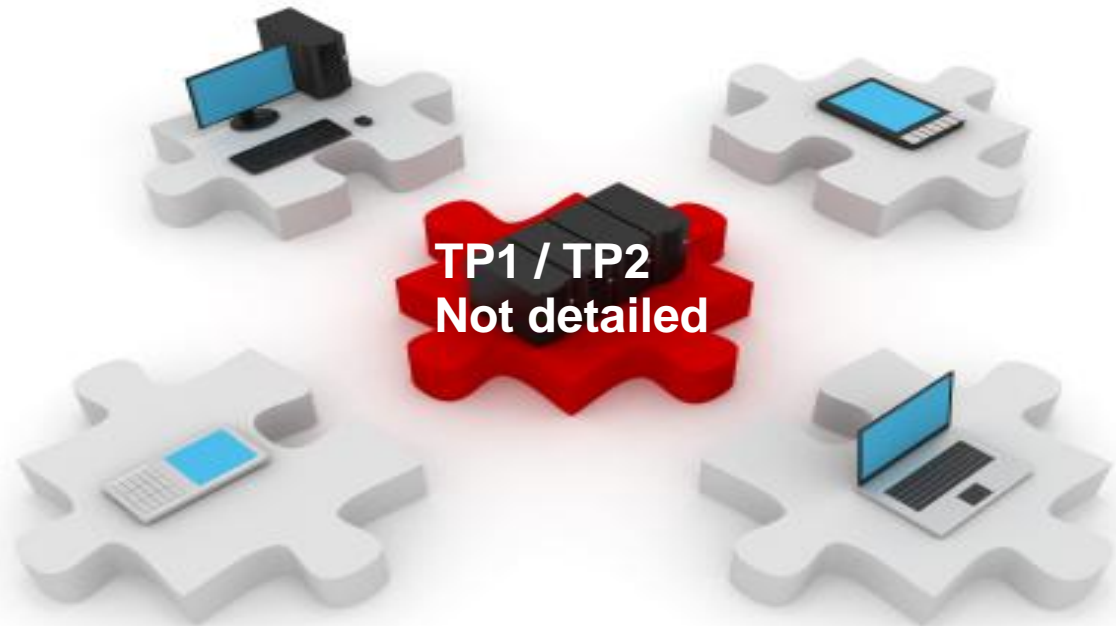
- AERAZUR
- AIR FRANCE
- AIRBUS
- AMBRUSTER
- BERNARD
- BIOLANDES
- BOURGEY MONTREUIL
- CANAVI BOTANICA
- CLARIANT
- COOPERATIVE DE BROONS
- DAHER
- DECATHLON
- DHL
- DGS Transports
- DRT
- EOLYS
- E3Cortex
- EXPRESSIONS PARFUMÉES
- BERNARD
- CLARIANT
- EADS Astrium
- FIRMINICH (CH)
- JEANNEAU-BENETEAU
- Groupe PHM
- Groupe Pierre LE GOFF
- Groupe SOUFFLET
- LOGITRANS
- MAIS ADOUR
- NIPPON EXPRESS
- PENA Environnement
- Transport QUIL
- RENAULT
- ROCHE
- SECURITE CIVILE
- TAKASAGO
- TRADIBEAUCE
- T-TRAM
- VIVADOUR...





# Expected Results

- Common modular architecture for all players of Transportation MD with a standardized exchange format that will ensure the independence of each module
- Application Modules
  - Supply chain actors modules
  - Operators Fleet Tracking
  - Local, national and international
  - Emergency Services
  - Infrastructure operators
  - Statistical applications
  - Embedded Modules
  - Devices for road vehicles
  - Terminals for container and traile...
  - Collection and onboard data processing
  - Data transmission
  - Access and control information for the crew
- More users will automatically decrease the cost of the System for each one



# Innovation

- Key technology to remove locks:
  - Federating and distributing in a selective and secure way, all data used in systems management and monitoring of hazardous materials.
  - Designing a distributed information system that can be certified by a safety assessment organization.
  - Designing an information system taking into account all regulatory and operational constraints, especially guaranteeing anonymity and data access control.
  - Developing and integrating embedded systems in a module location and GNSS navigation certified by implementing the principles of the CEN Workshop Agreement CWA 16390: 2012)
  - Managing the process of certification for the modules

The challenge of the project is related to the size of the system, the volume and the security of transactions, its European identity and to comply with regulatory (need to know, access control, ...) constraints.

Links to other projects: GEOFENCING MD (LUTB), SCUTUM (FP7)

# Planning compatible with Joint Meeting bi-annual agenda

- 3 years long project with a large demonstration at ITS World Congress in Bordeaux 5 to 9 October 2015

WP1: Project management

*36mm – 1 Juin'2013 -> 31 Mai'2016*

WP2: Functional analysis

*65mm – Juin'13 -> Juin'14*

WP3: Architecture

*76mm – Mar'14 -> Nov'14*

WP4: Implementations

*192mm – Dec'14 -> Sep'15*



22nd  
ITS World Congress  
Bordeaux, France  
5 to 9 October  
2015

WP5: Demonstration

*39mm – Sep'15 -> Mar'16*

WP6: Certification/Security

*82mm – Juin'13 -> Mai'16*

WP7: Dissemination

*16mm – Juin'13 -> Mai'16*

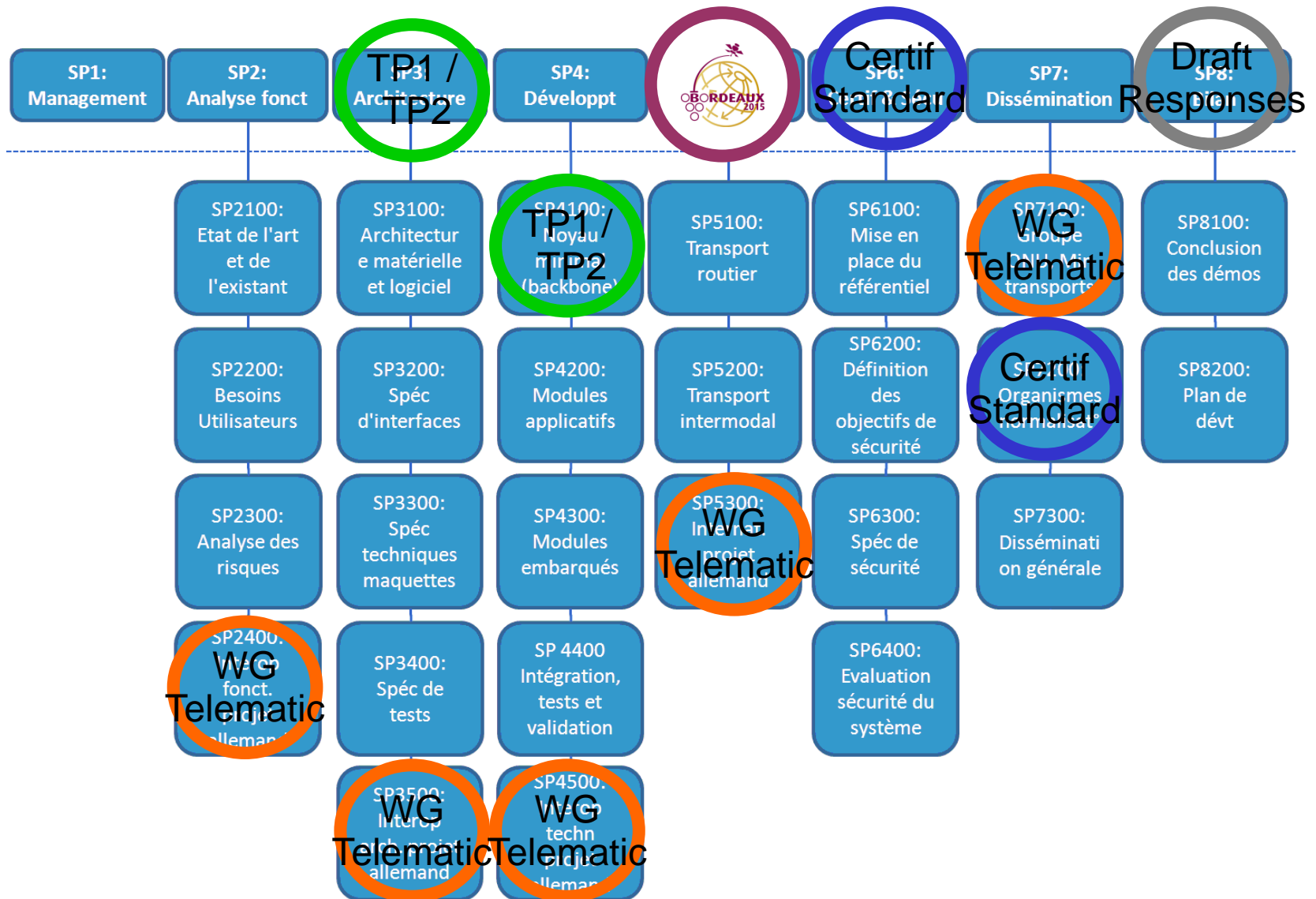
WP8: Results

*17mm – Jan'16->Mai'16*

# Partner Involvement

Partner	Domain of involvement
Novacom	Trusted Party 1, Trusted Party 2, Fleet operator services, Statistic
FDC	Trusted GNSS positioning and time stamp, Jamming and Spoofing detection
M3 Systems	GNSS positioning and hybridation
Geoloc Systems	Trusted Party 2, Road operator Services, Carrier services
E.RE.CA	On board equipment, Embedded services
MD Service	Trusted Party 2, Shipper, Consignor, Consignee, Carrier Services
LNE	Certification process
Grenoble Univ.	Real time environment risk evaluation
CEA List	Security and Specification validation
CETE SO & Lyon	Link with Telematic Working Group, Trusted Party 1, Link with local Road Operator, National road operator,

# GeoTrans MD organisation



# Points examined by the project in relation with the architecture

- Testing internet backoffice
- Verifying how much we depend on standard
- Testing security issues
- Experiment certification issues
- Look at optimizing the quantity of data
- Check implementation in practice and work on access control to the data

Depending on European Commission view

- Try to experiment TP1 issues centralized vs decentralized

# Response to the Work Programme

- GeoTransMD will use the architecture proposed by Germany as validated by the Telematic WG by implementing :
  - Back office (Real life functioning)
- GeoTransMD will give element to highlight response to :
  - § 3 in a multimodal perspective
  - § 4 depending on transport mode and willingness of the actors
  - § 5 in line with the needs expressed by actors
  - § 6 by declining from the German study an XML schema
  - § 7 by identifying the end users for private or public services
  - § 9 by showing the minimal equipment needed
  - § 11 with the certification rules proposal in line with the German study
  - § 13-16 by having a strong link with the Telematic WG to give some proposal for these items



# Thank you for your attention

