GEOTRANSMD

Géolocalisation des Transports de Matières Dangereuses

Telematic Working Group

Bordeaux

03.06.2014

Agenda

- Context
- Project reminder
- Survey
- TP1 profiles
- TP2 Services
- Security – Availability
- Charges
- Information collected in case of accident – Problem of the casual observer

CONTEXT

Historical Context

- Mandate ECE/TRANS/WP.15/AC.1/108/Add.3 (24 October 2007) 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
- 2010 Final version of the « who does what » table (INF.11 of September 2010 of the Join Meeting)

TERMS OF REFERENCE OF THE INFORMAL WORKING GROUP ON THE USE OF TELEMATICS FOR THE CARRIAGE OF DANGEROUS GOODS

1. Consider what information provided by telematics enhances the safety and security of the transport of dangerous goods and facilitates such transport. In particular, consider who might benefit from the provision of such information and in what way, having regard, inter alia, to: consignors, transport operators, emergency responders, enforcers, regulators;
2. Consider necessary parameters for telematics systems, and examine if existing systems meet these parameters and what further developments might be necessary;
3. Consider the cost/benefit analysis of utilising telematics for the purposes identified above;
4. Consider what procedures/responsibilities might be necessary to monitor the information captured by telematics and how access to data should be controlled; and
5. Consider interfaces and synergy with other systems

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;

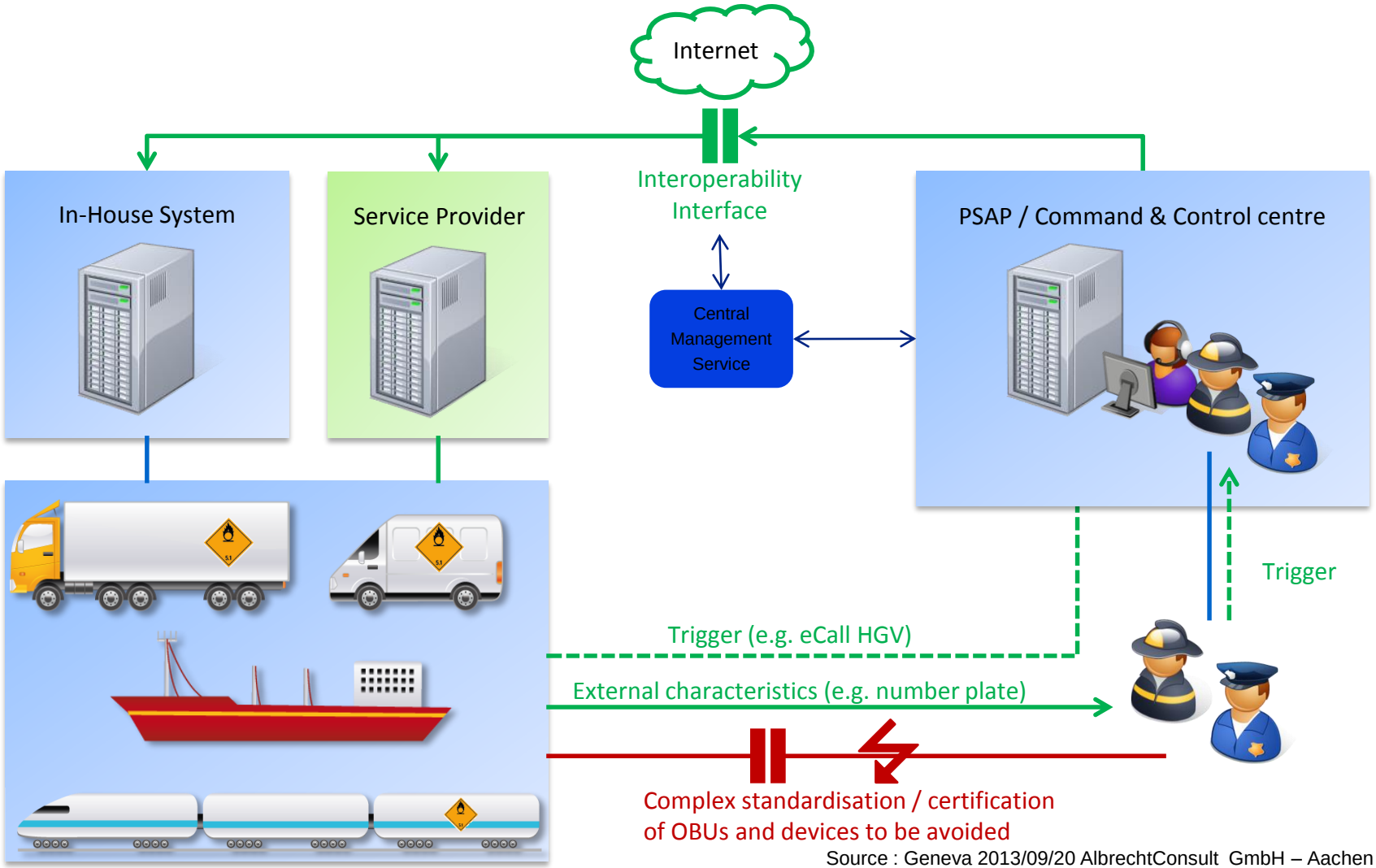
Work programme of the informal Working Group (2)

- 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.

Telematics System – Overview and Basic Considerations



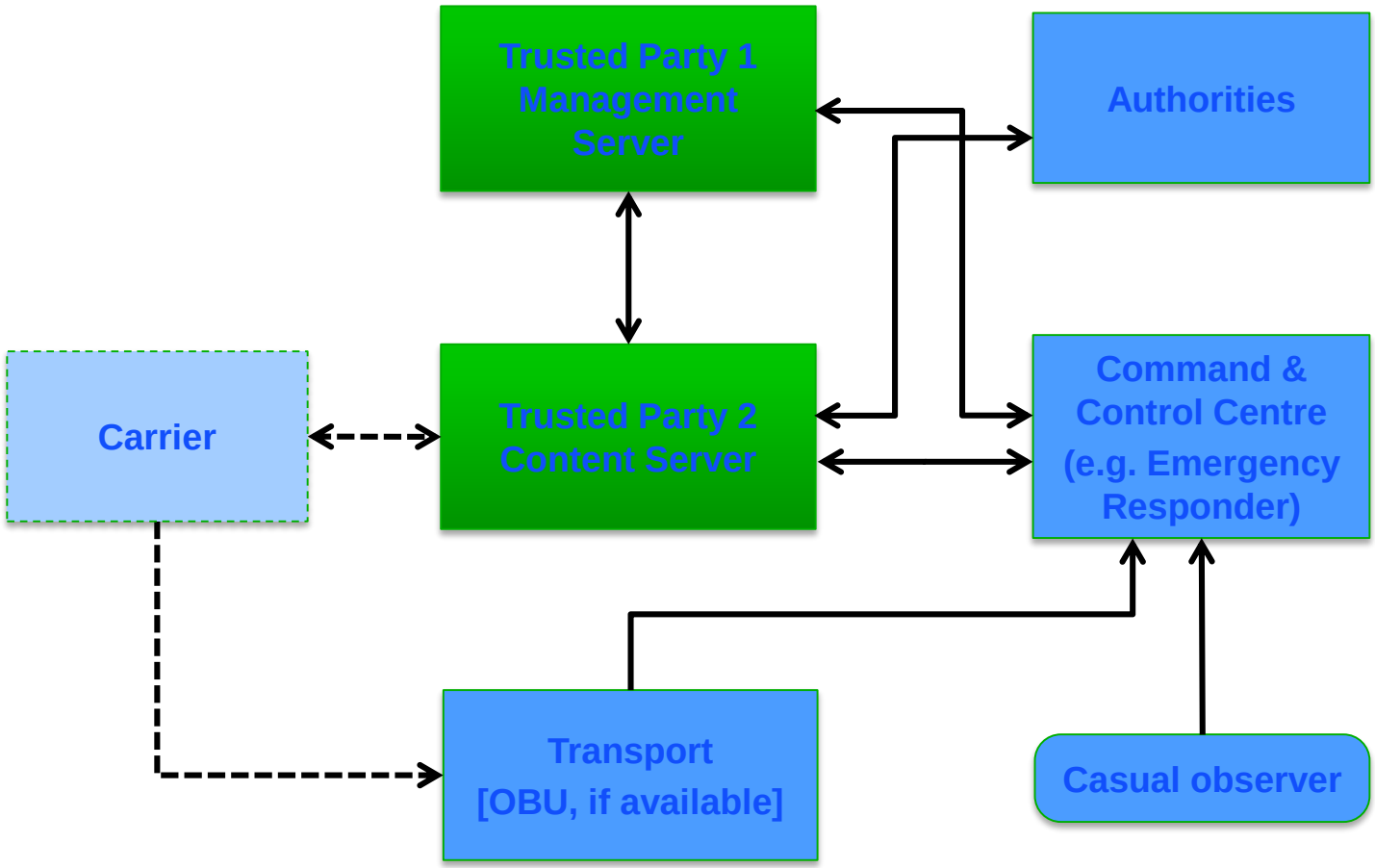
Source : Geneva 2013/09/20 AlbrechtConsult GmbH – Aachen – Viersen

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
- 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
  for vehicle initiated emergency notification (e.g. eCall HGV)
- There needs to be further central 'lookup' service to retrieve access credentials in case of access based on external observations
- Access must be controlled and data protection must be ensured
  ⇒ up-to-date cryptographic technology needed
- The interface should easily integrate into the existing landscape of Freight & Logistics IT services ⇒ use of widely accepted IT standards (e.g. web services & XML)

Source : Geneva 2013/09/20 AlbrechtConsult GmbH – Aachen – Viersen

Telematics system high-level architecture



Source : Geneva 2013/09/20 AlbrechtConsult GmbH – Aachen – Viersen

PROJECT REMINDER

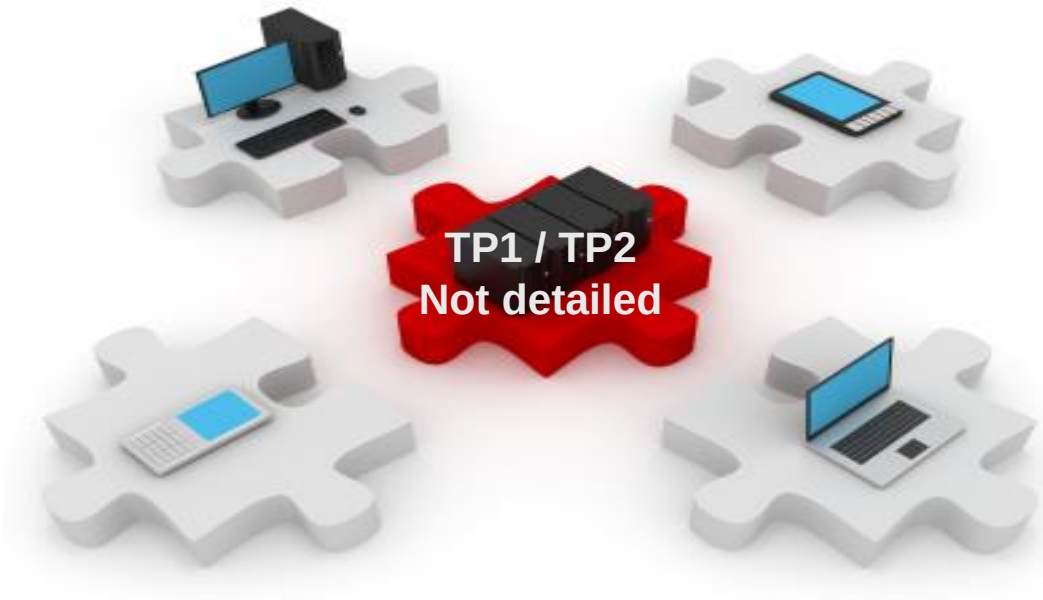
Partenaires

	Partner	Effort R&D	Financement
Leader	Novacom (ETI)	105 HM	25%
SMEs	FDC	11 HM	30%
	M3Systems	30 HM	45%
	Geoloc Systems	90 HM	45%
	E.RE.CA	43 HM	45%
	MD Service	34 H,M	45%
University	LNE	12 HM	40%
	Université de Grenoble	45 HM	100%
	CEA LIST	72 HM	40%
Public Body	CEREMA Dter Sud-Ouest	76 HM	3%
	CEREMA Dter Centre-Est	5 HM	13%

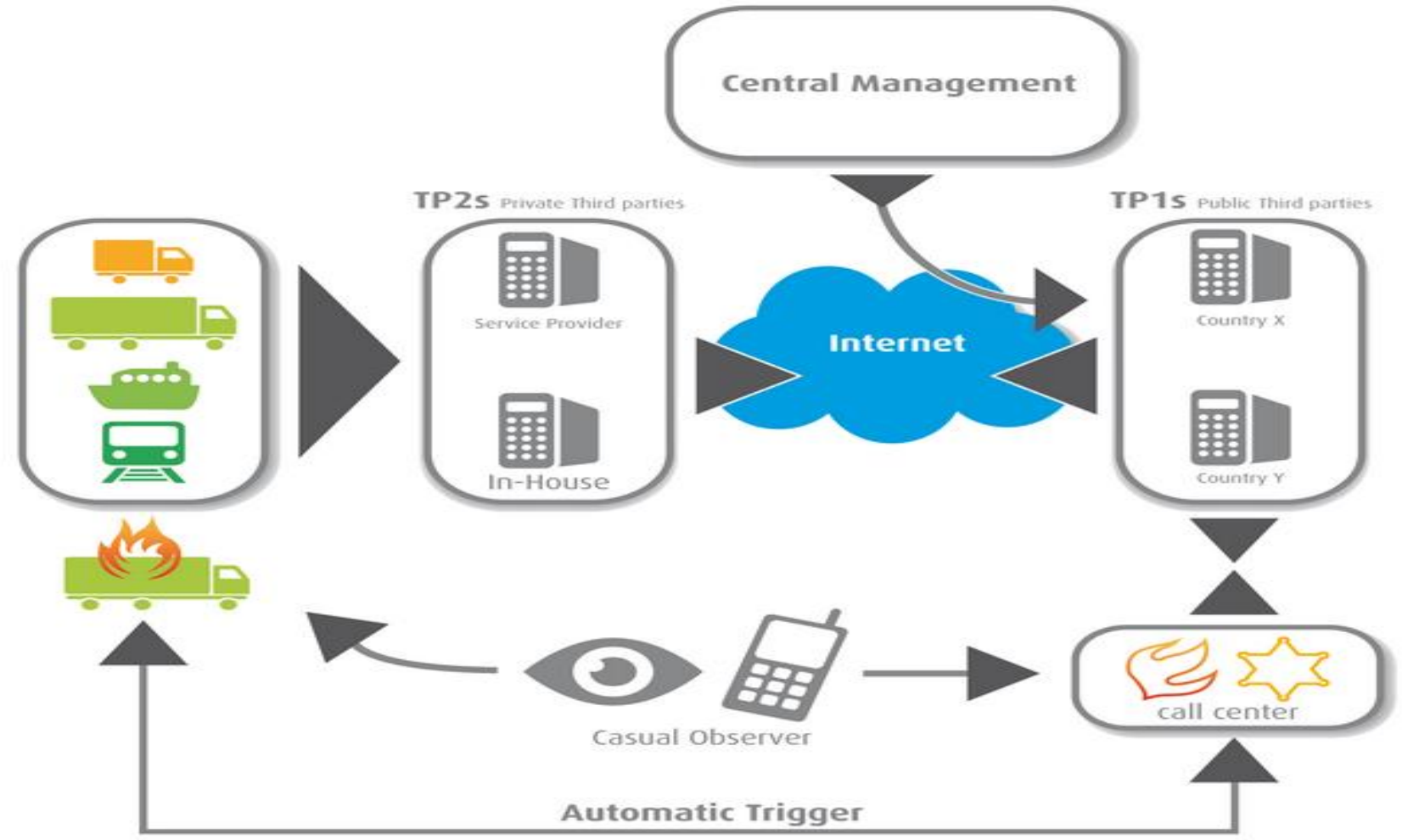
- **Total budget**: 5,9 M€, funding 1,9 M€ (33%)
  - 20 % ETI
  - 33 % SME
  - 29 % R&D
  - 17 % other
- **3 regions :**
  65 % Sud-Ouest
  22 % Paris
  13 % Lyon

Expected Results

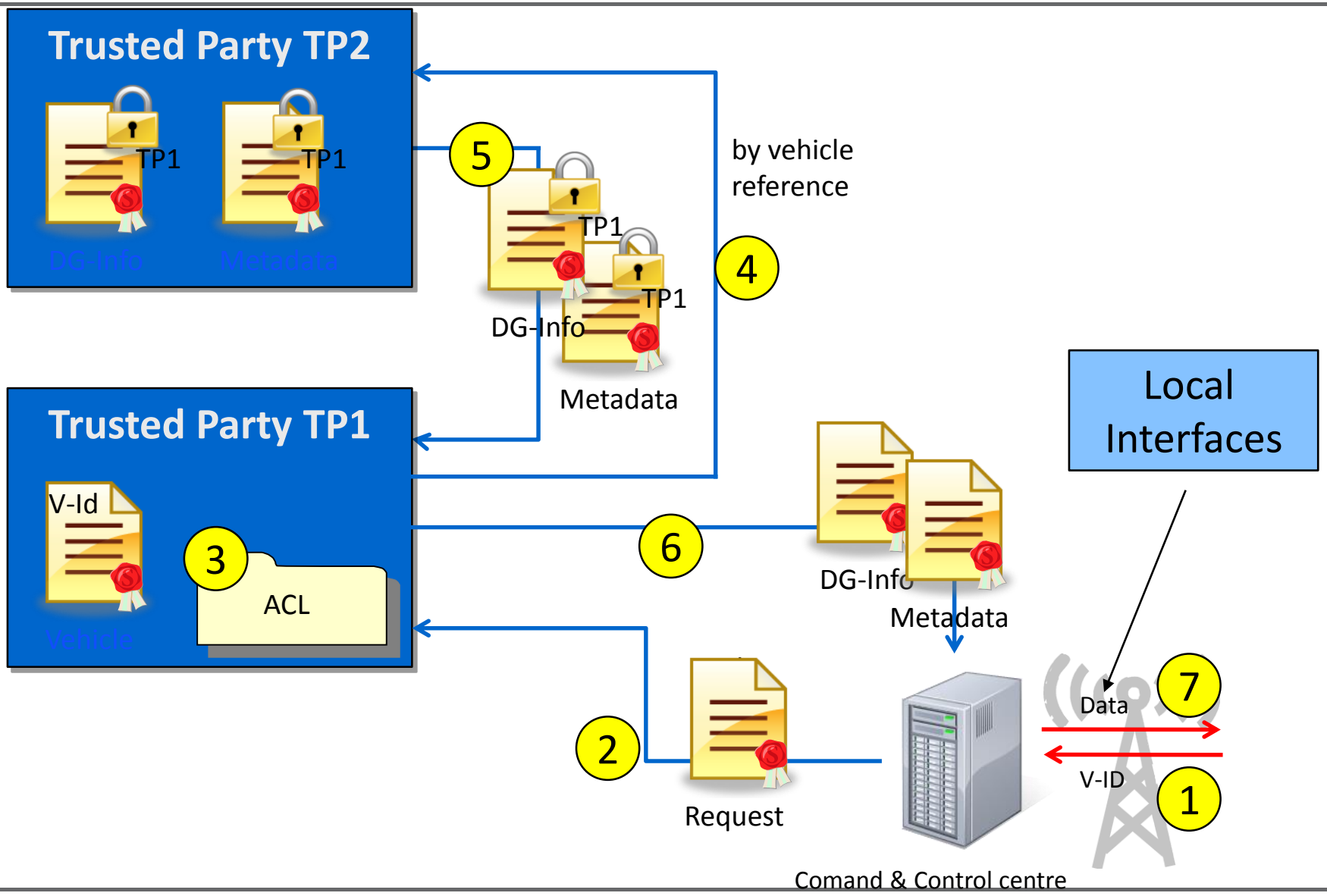
- Common modular architecture for all players of Transportation MD with a standardized exchange format that will ensure the independence of each module
- Application Modules
  - Supply chain actors modules
  - Operators Fleet Tracking
  - Local, national and international authorities
  - Emergency Services
  - Infrastructure operators
  - Statistical applications
  - Embedded Modules
  - Devices for road vehicles
  - Terminals for container and trailers
  - 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



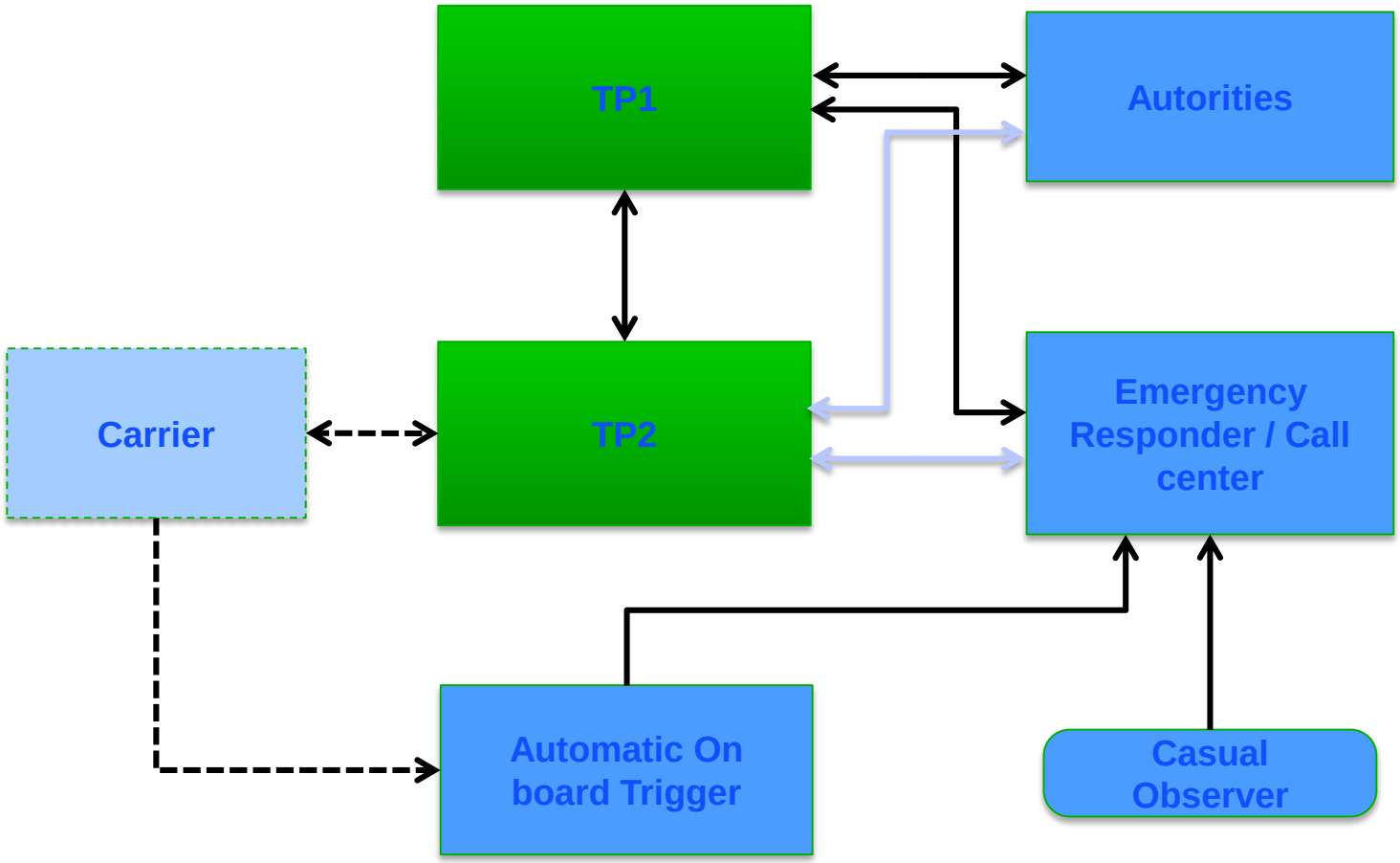
General schema



Security principle



Possible processus



Planning

- 3 years project with a demonstration at the 22nd ITS World Congress in Bordeaux 5 to 9 October 2015

WP1: Gestion de projet
36hm – 1 Juin'2013 -> 31 Mai'2016

WP2: Ananyse fonctionnelle
65hm – Juin'13 -> Juin'14

WP3: Architecture
76hm – Mar'14 -> Nov'14

WP4: Implementations
192hm – Dec'14 -> Sep'15

WP5: Demonstration
39hm – Sep'15 ->Mar'16

WP6: Certification/Securité
82hm – Juin'13 -> Mai'16

WP7: Communication
16hm – Juin'13 -> Mai'16

WP8: Evaluation
17hm – Jan16->Mai16

Partners

	Partner	Main activity	Roles
Leader	Novacom (ETI)	Fleet Management	TP1 and Fleet management TP2
SMEs	FDC	GNSS	Guarantee on position
	M3Systems	GNSS/OBU	Guarantee on position
	Geoloc Systems	Software	Low Cost TP2
	E.RE.CA	OBU	OBU provider and Low Cost TP2
	MD Service	DG Services	DG TP2
University	LNE	Certification	Certification
	Université de Grenoble	Risk Assement	Risk evaluation
	CEA LIST	Methodology	Security
Public Body	CEREMA Dter Sud-Ouest	Public policy	TP1 for Ministry
	CEREMA Dter Centre-Est	Public policy	State of the art

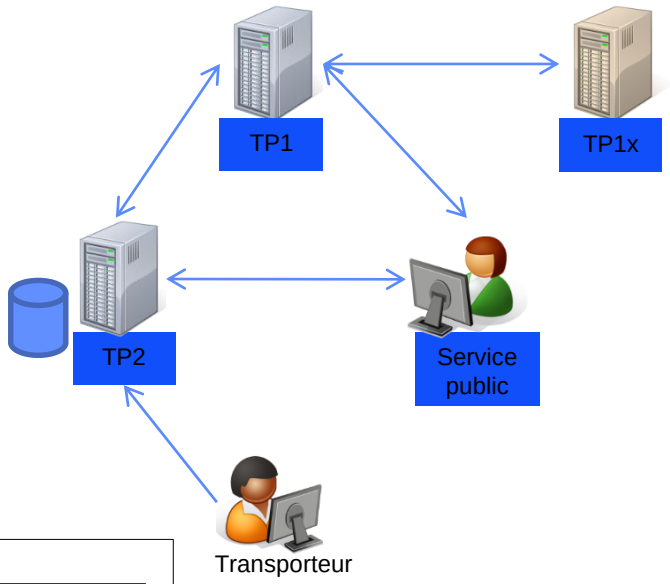
2 types of behavior are in place the proposed architecture:

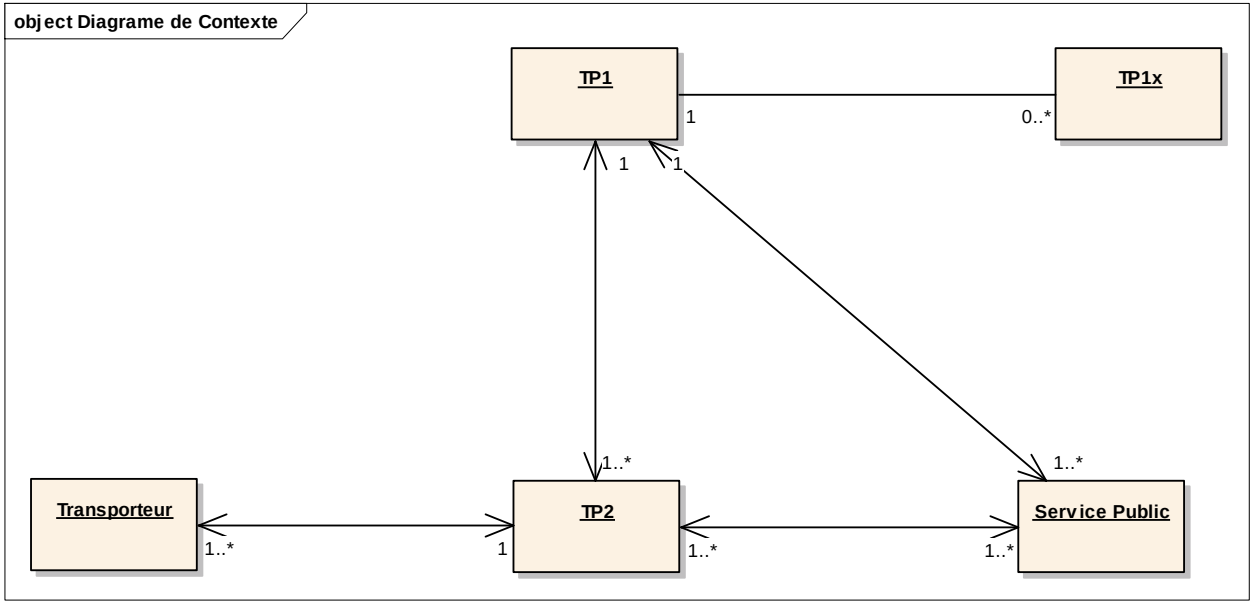
- Is it needed or could it possible to have just one?
- What impact will be expected?

TP1 PROXY VERSUS REDIRECT

Analysis: Registration TP1, TP2, Authorities, TU

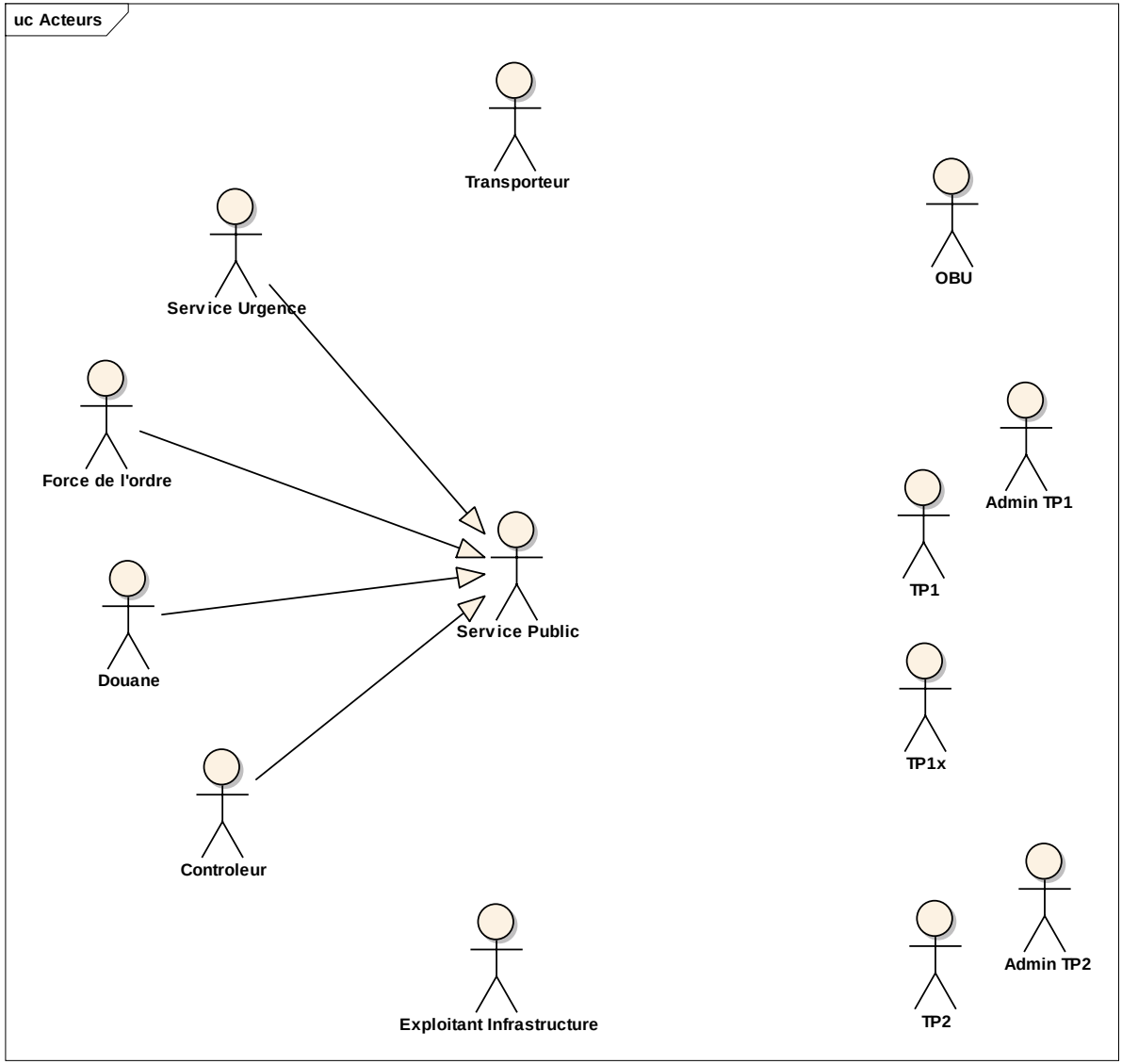
- Each TP1 knows all other TP1
- Each TP2 is registered to one TP1 in the country where it is registered and certificated
- Public services (authorities) is registered to one TP1 in its country
- Each carrier or more precisely each transport unit is registered to one TP2 at a time



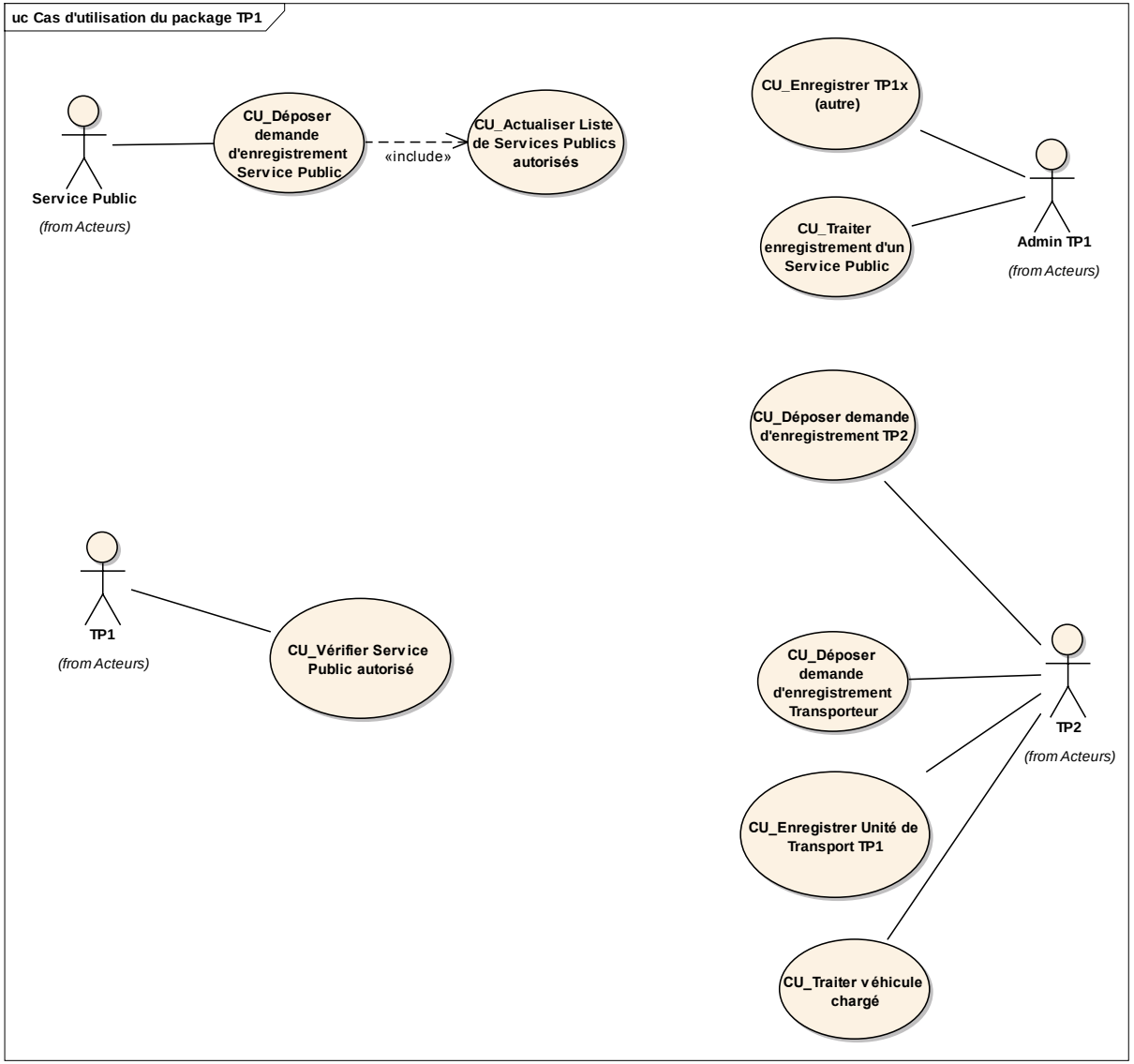


Identification of the actors

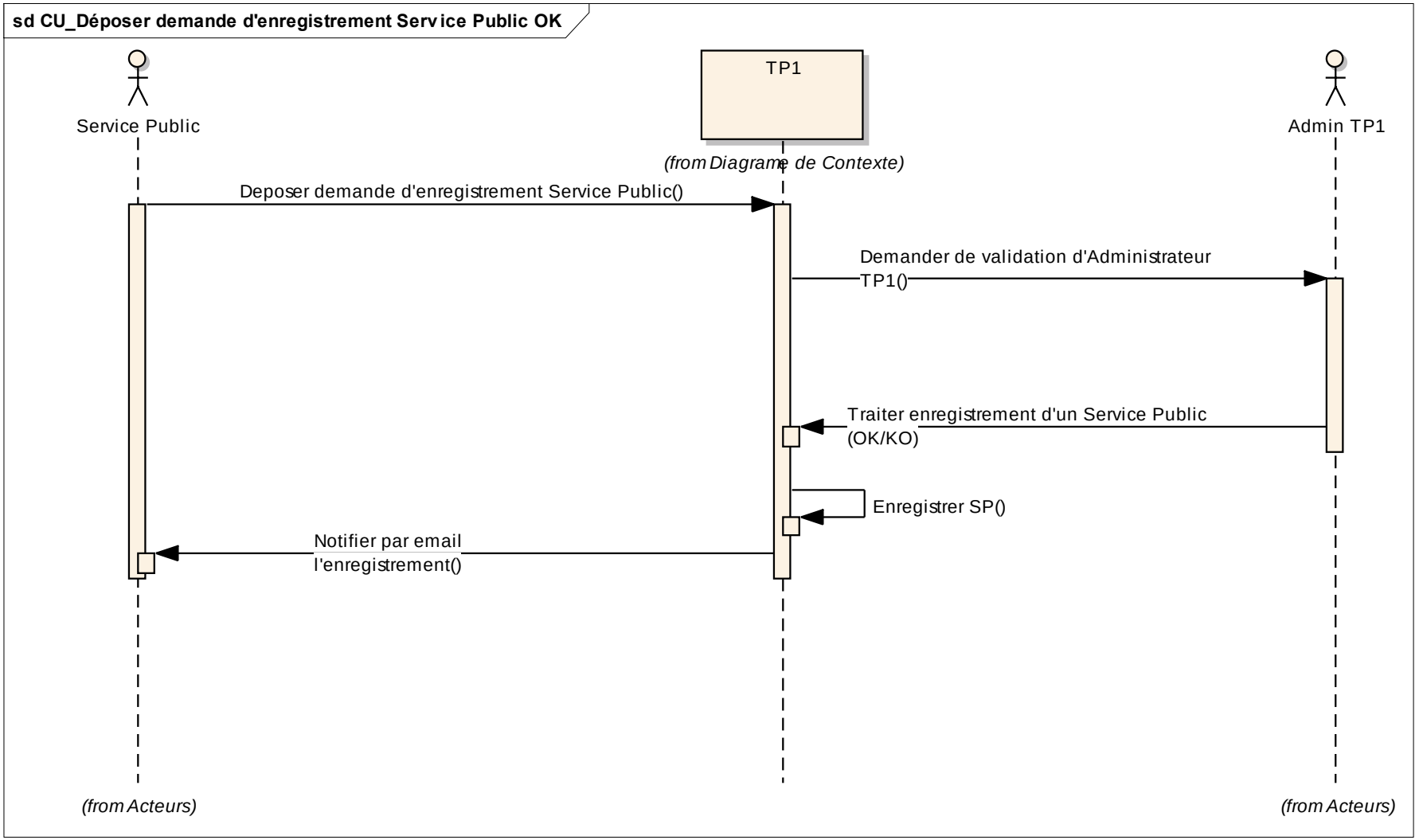
- Actors have been identified
- When possible « families » are identified



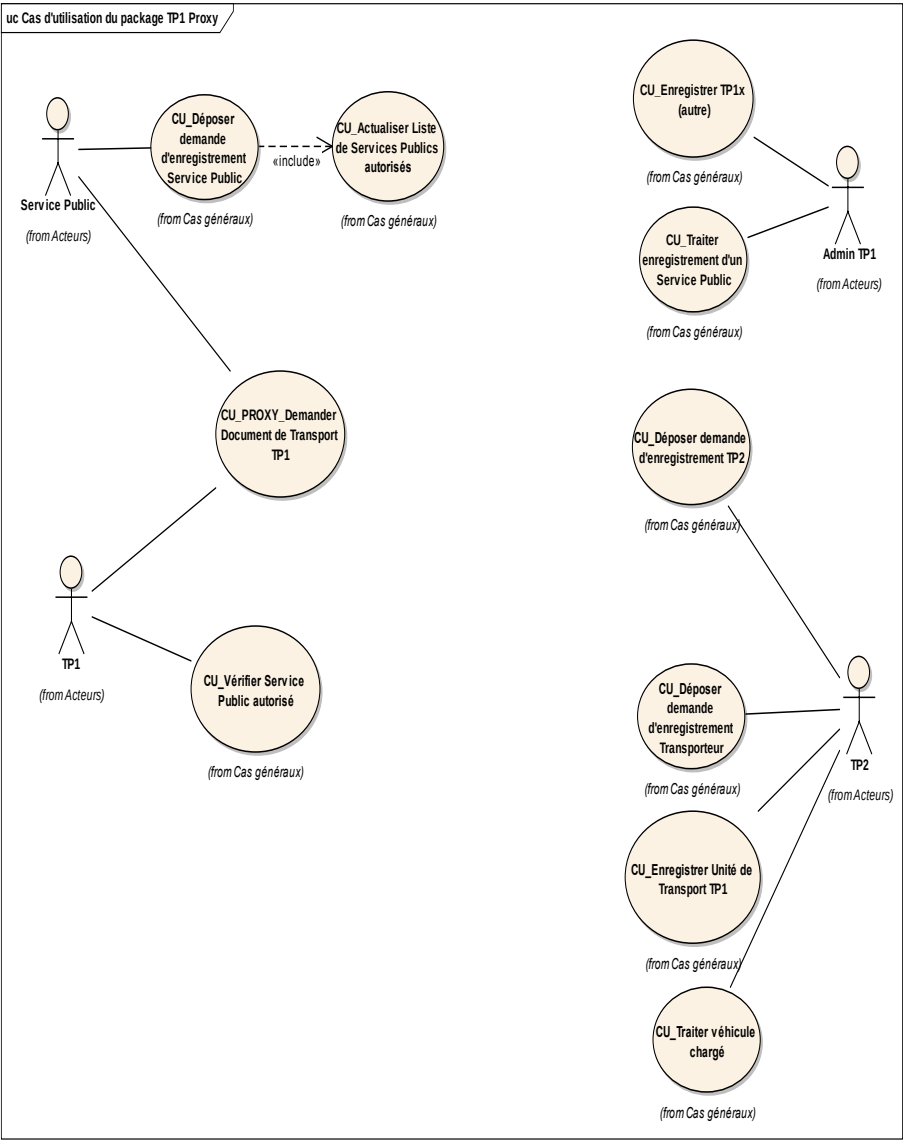
Identification of the work to do by actors

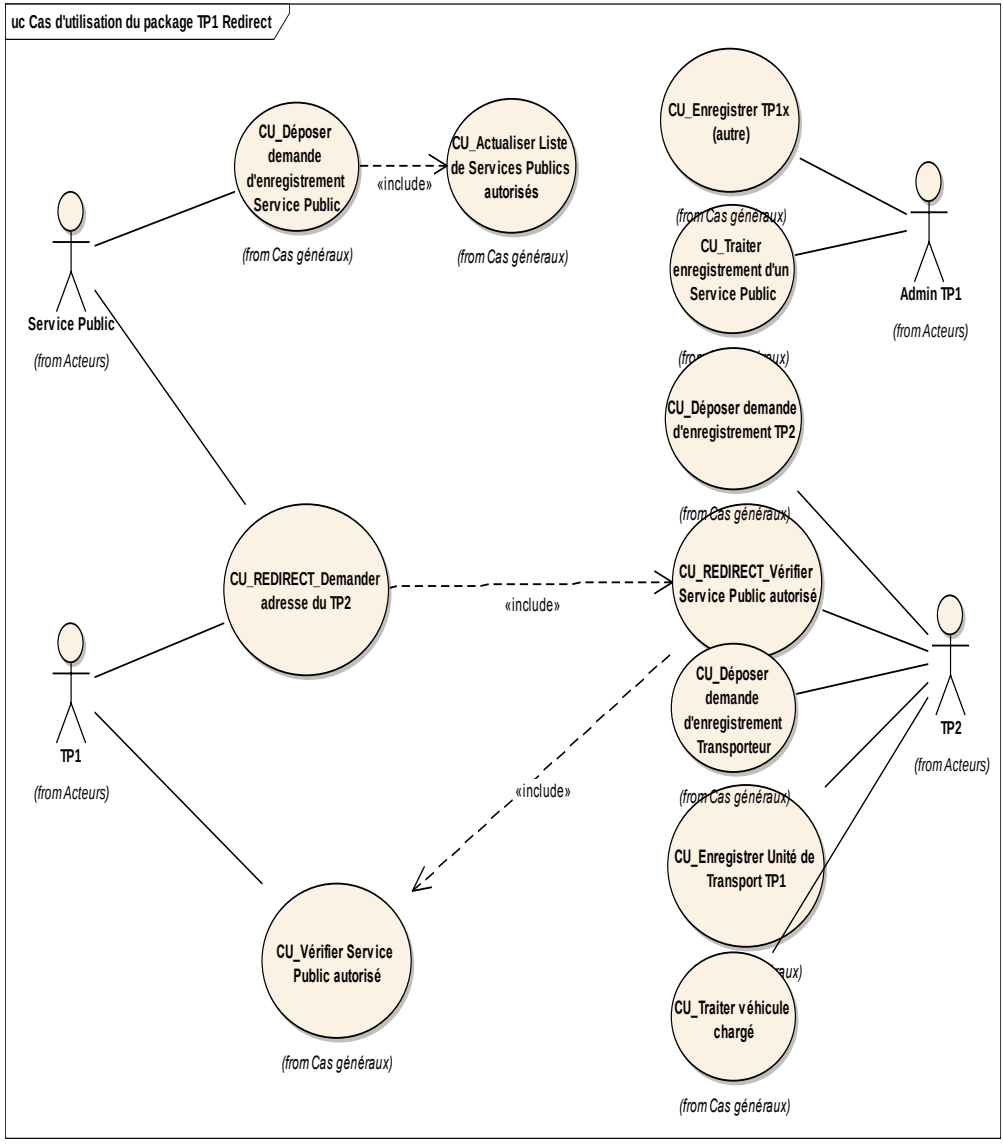


Identification of the behavior for each « work » to do



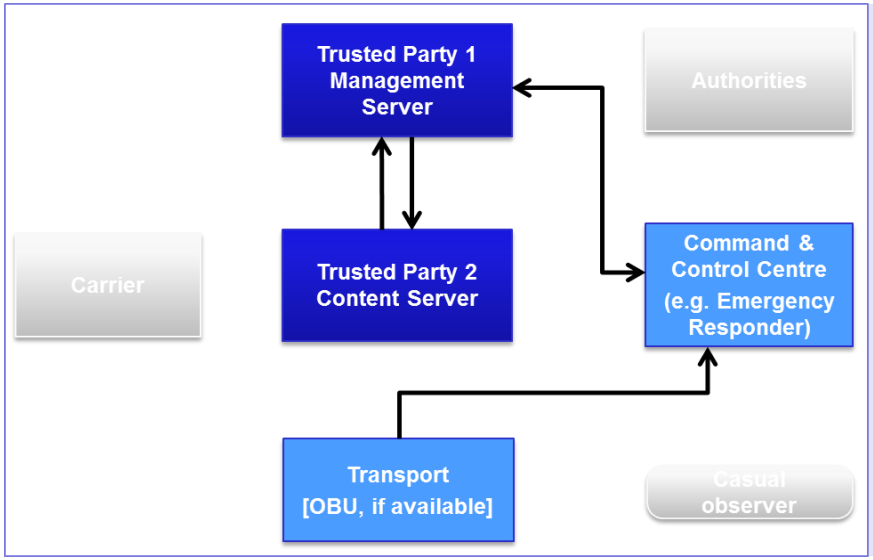
Package for TP1 « Proxy mode » versus « Redirect »





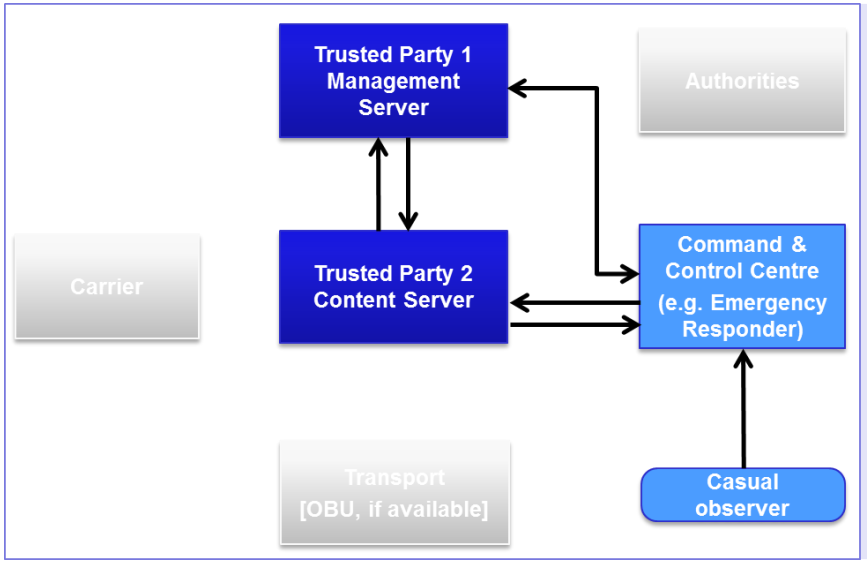
Reminder of German study

- Mode Proxy



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

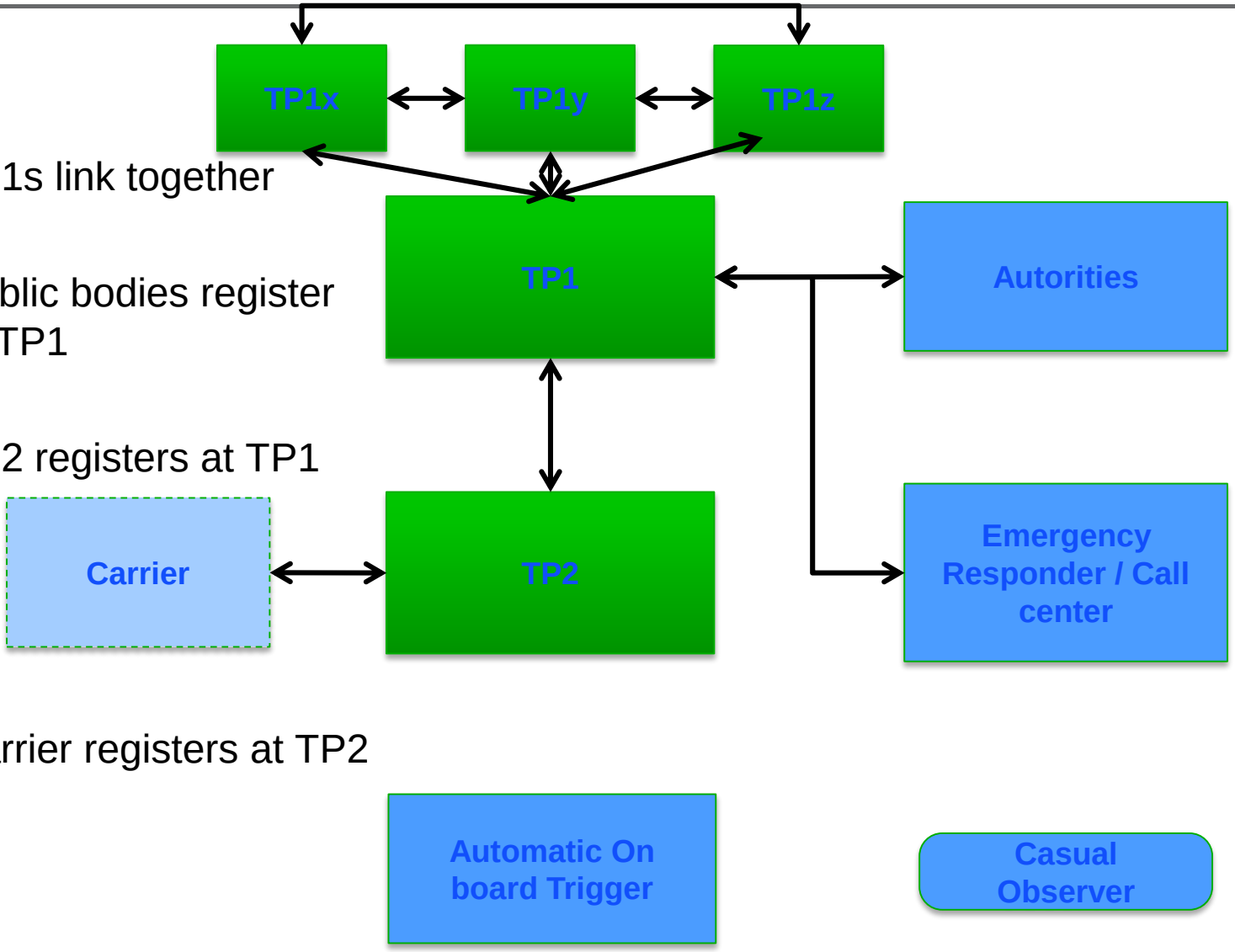
- Mode Redirect



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

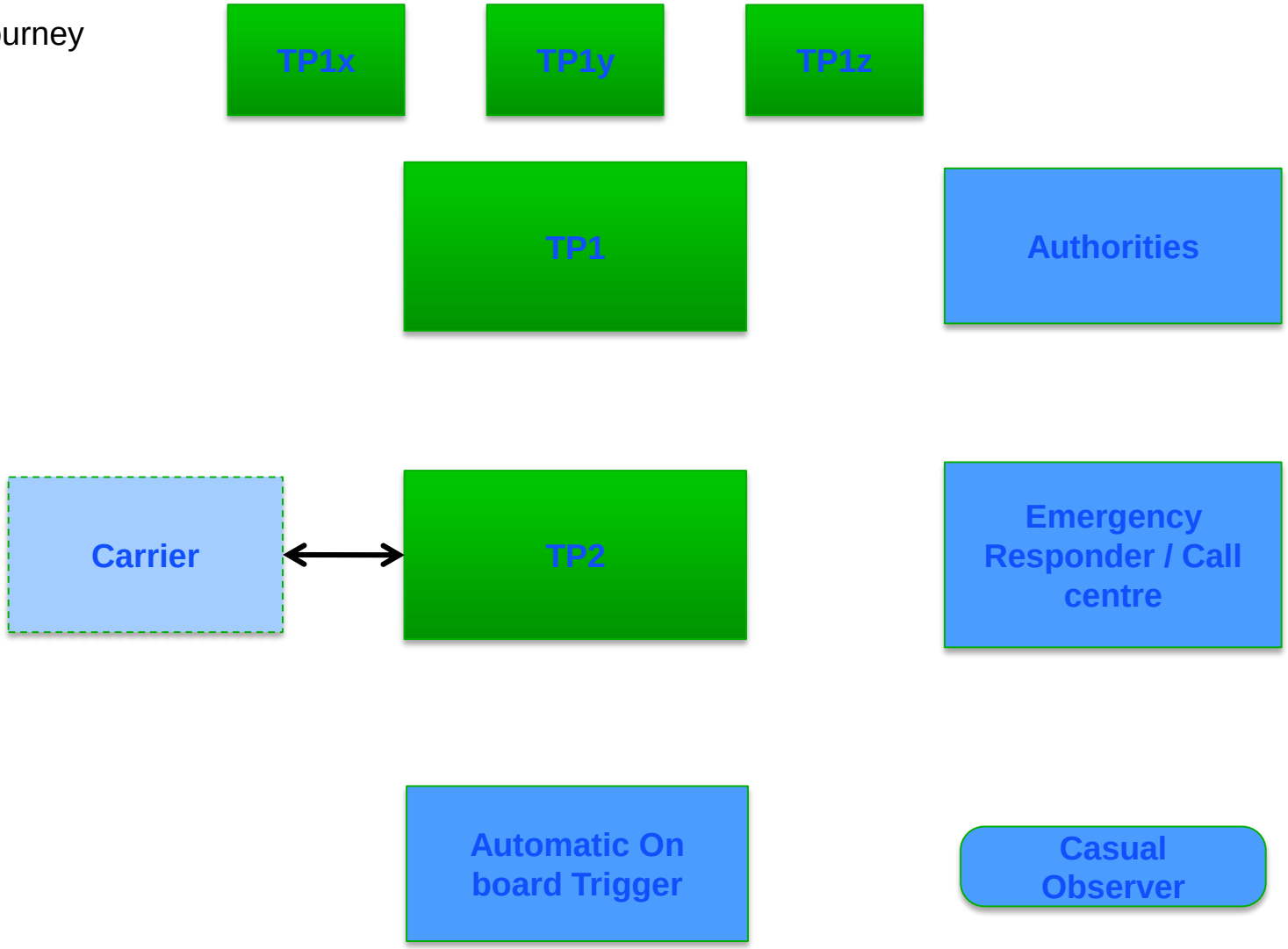
Common part – Link to be installed

- TP1s link together
- Public bodies register at TP1
- TP2 registers at TP1
- Carrier registers at TP2



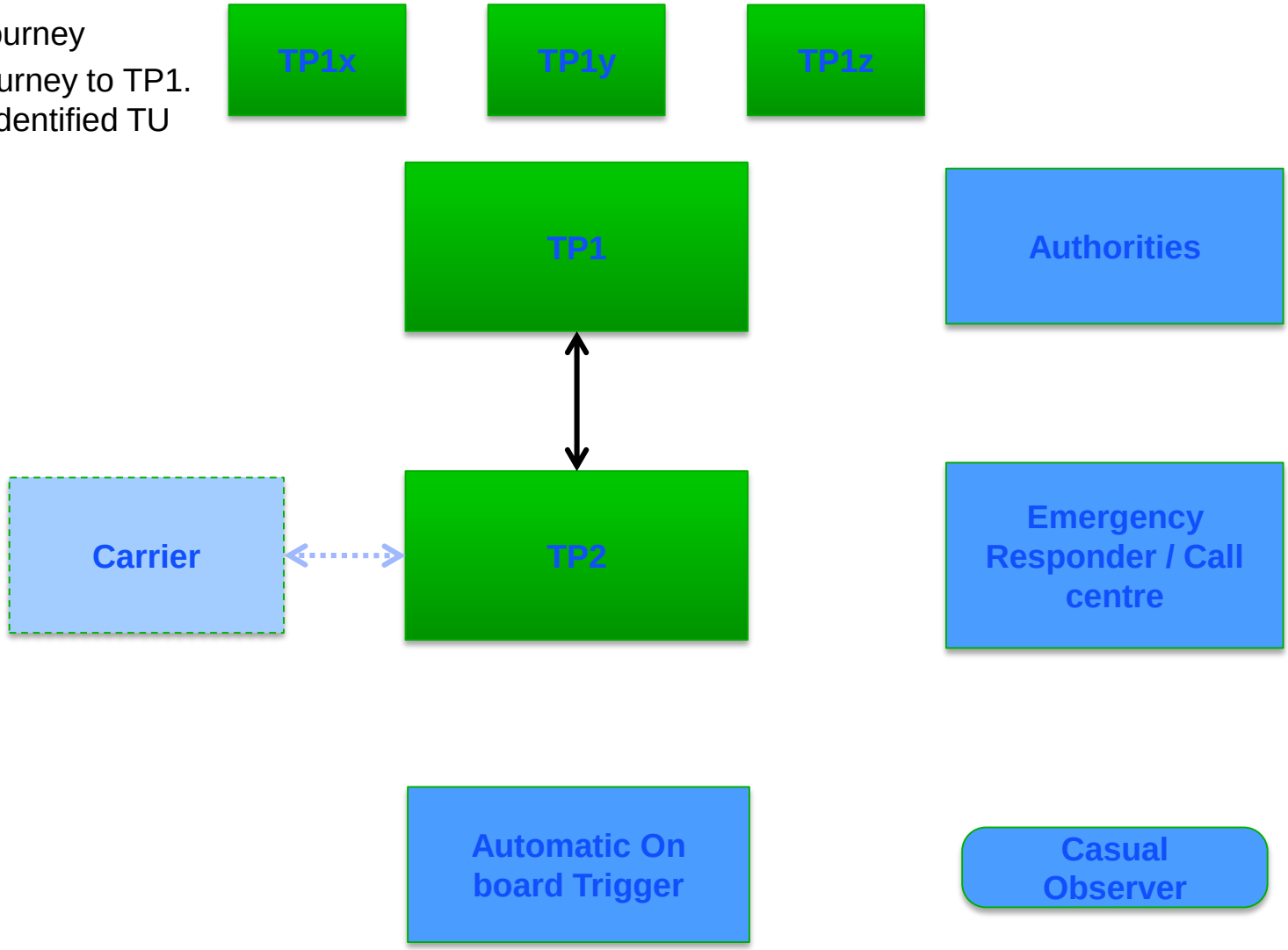
Dynamic behavior in proxy mode

1. Carrier registers a journey



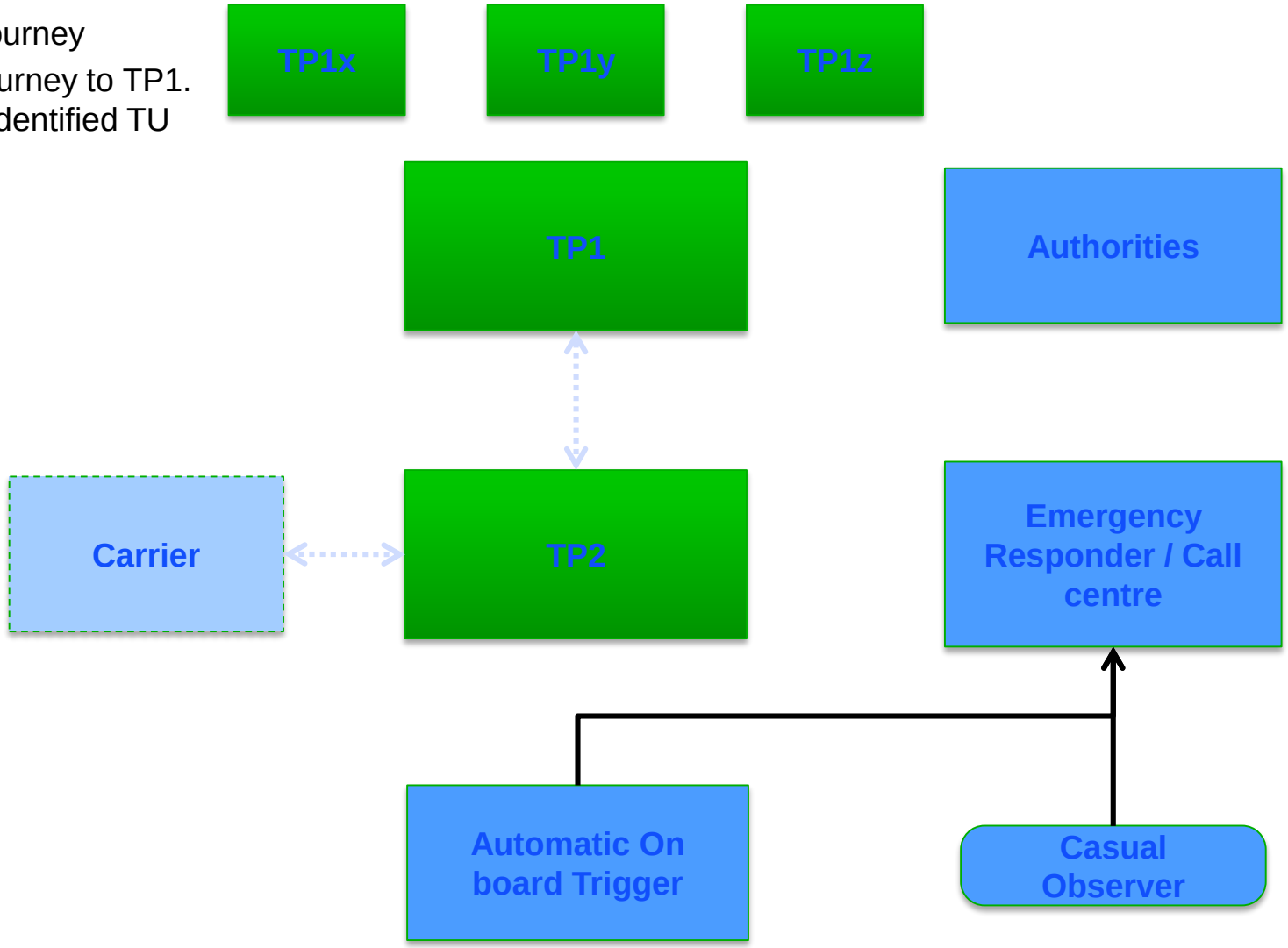
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip



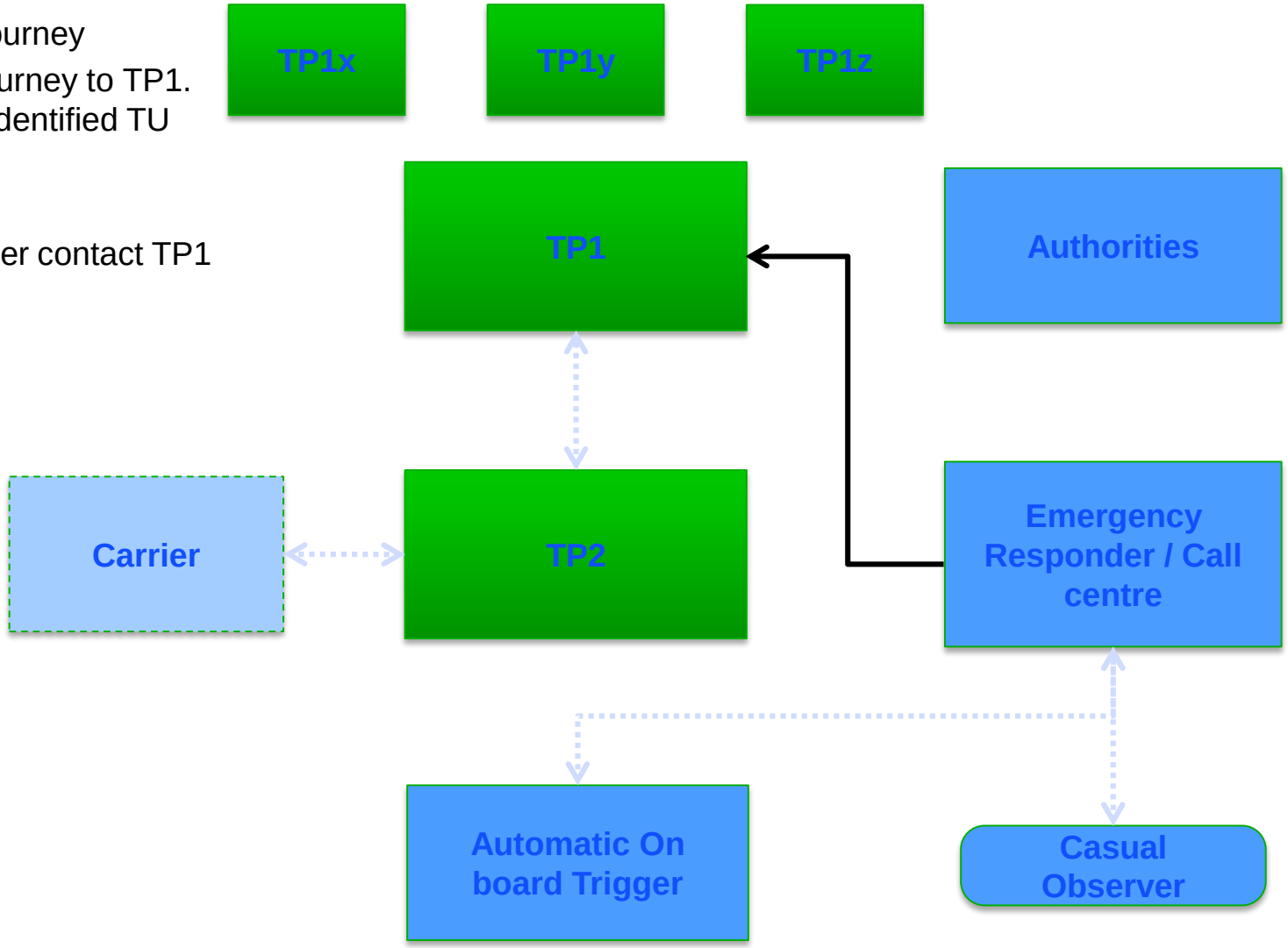
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs



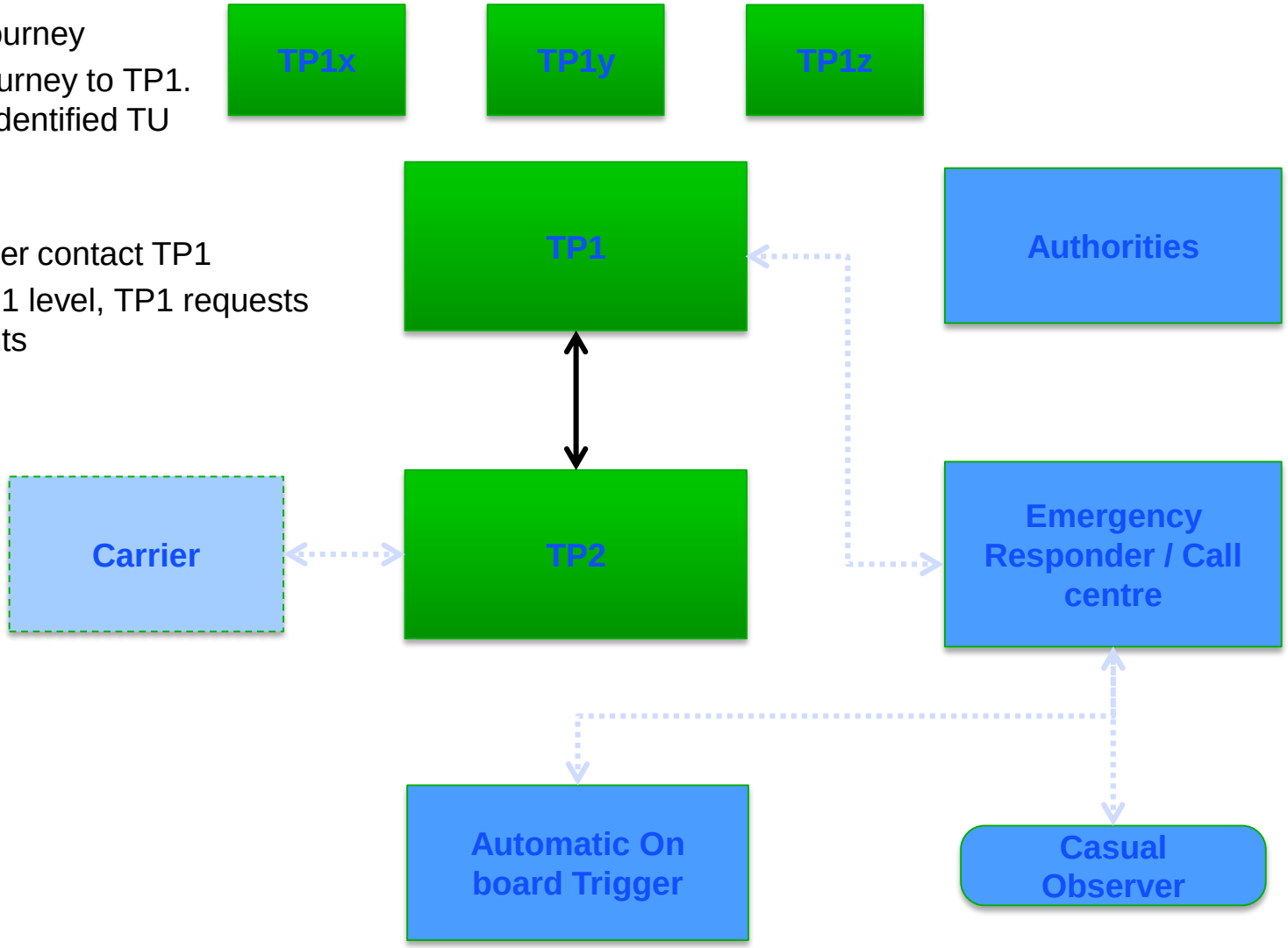
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP1



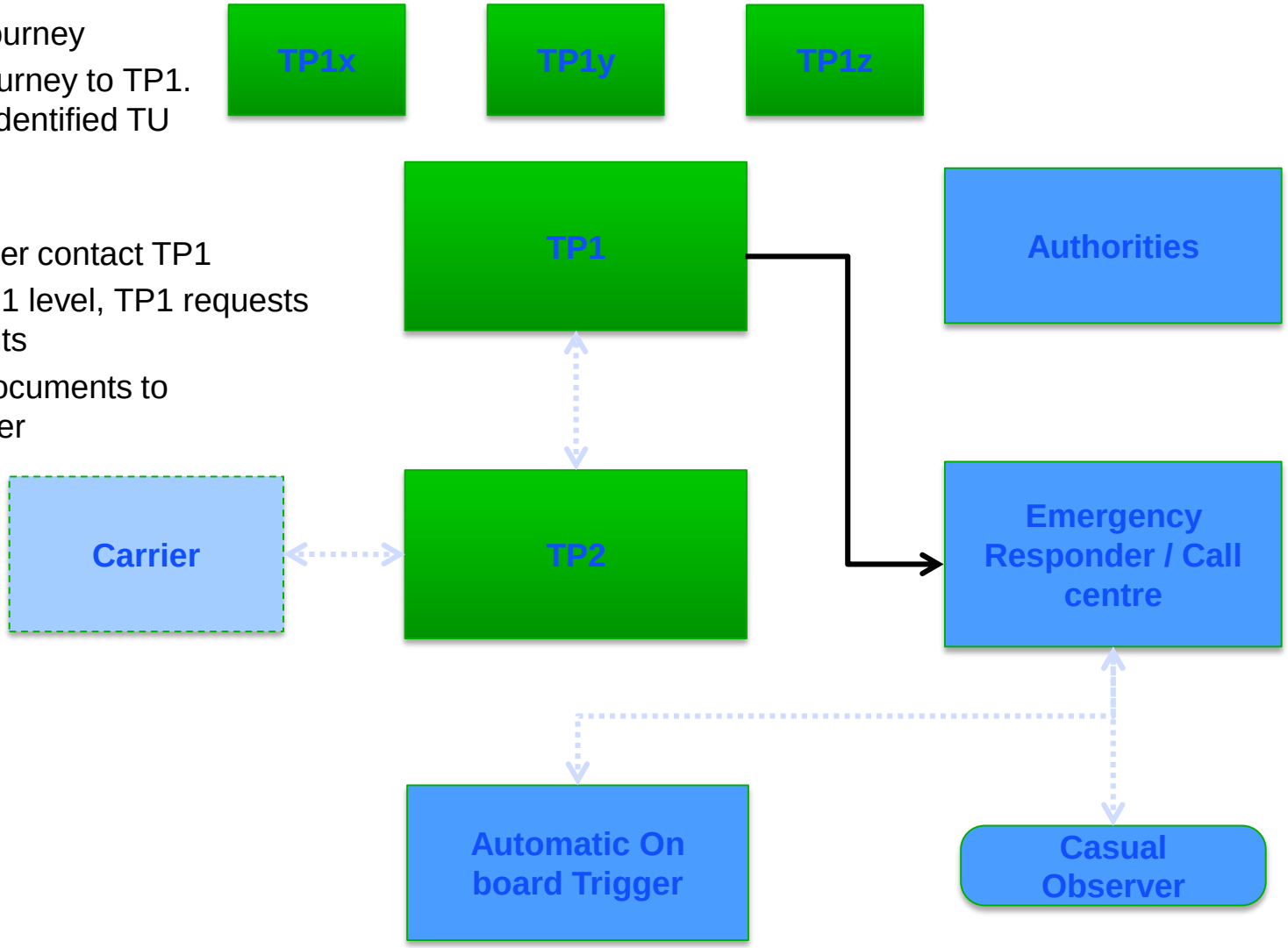
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP1
5. If TU is known at TP1 level, TP1 requests to TP2 the documents



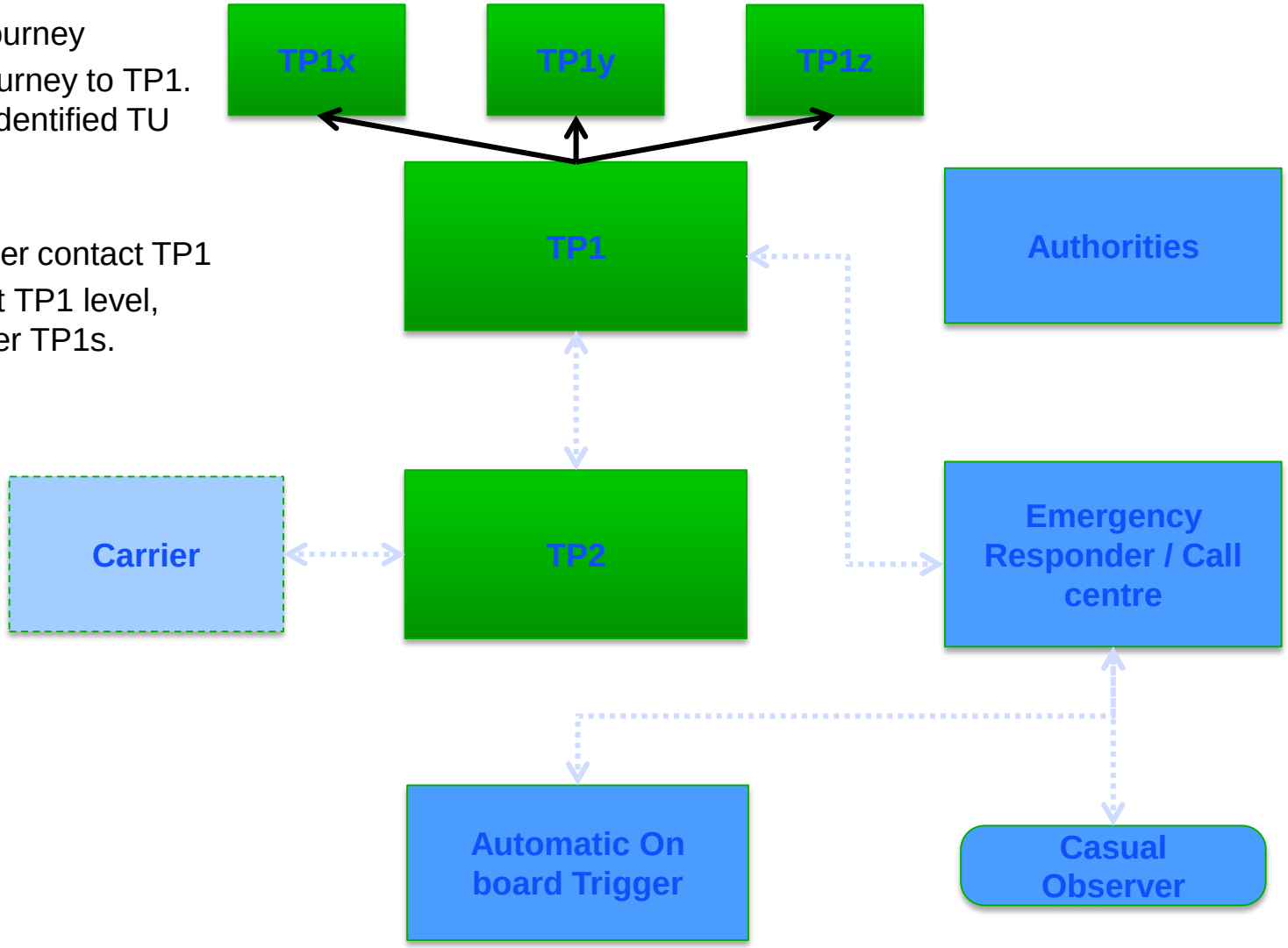
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP1
5. If TU is known at TP1 level, TP1 requests to TP2 the documents
6. TP1 transmits the documents to emergency responder



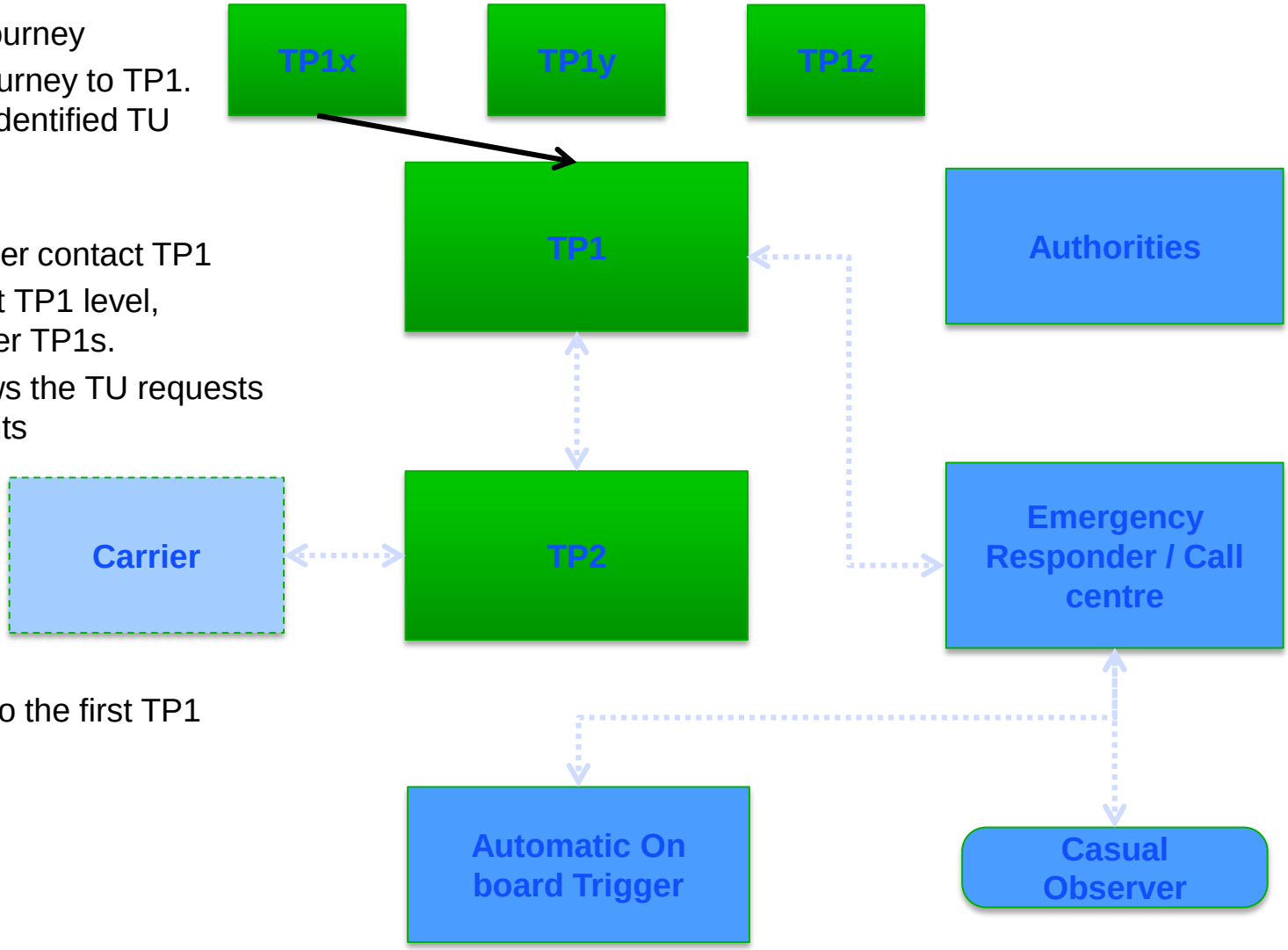
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP1
5. If TU is not known at TP1 level, TP1 requests to other TP1s.



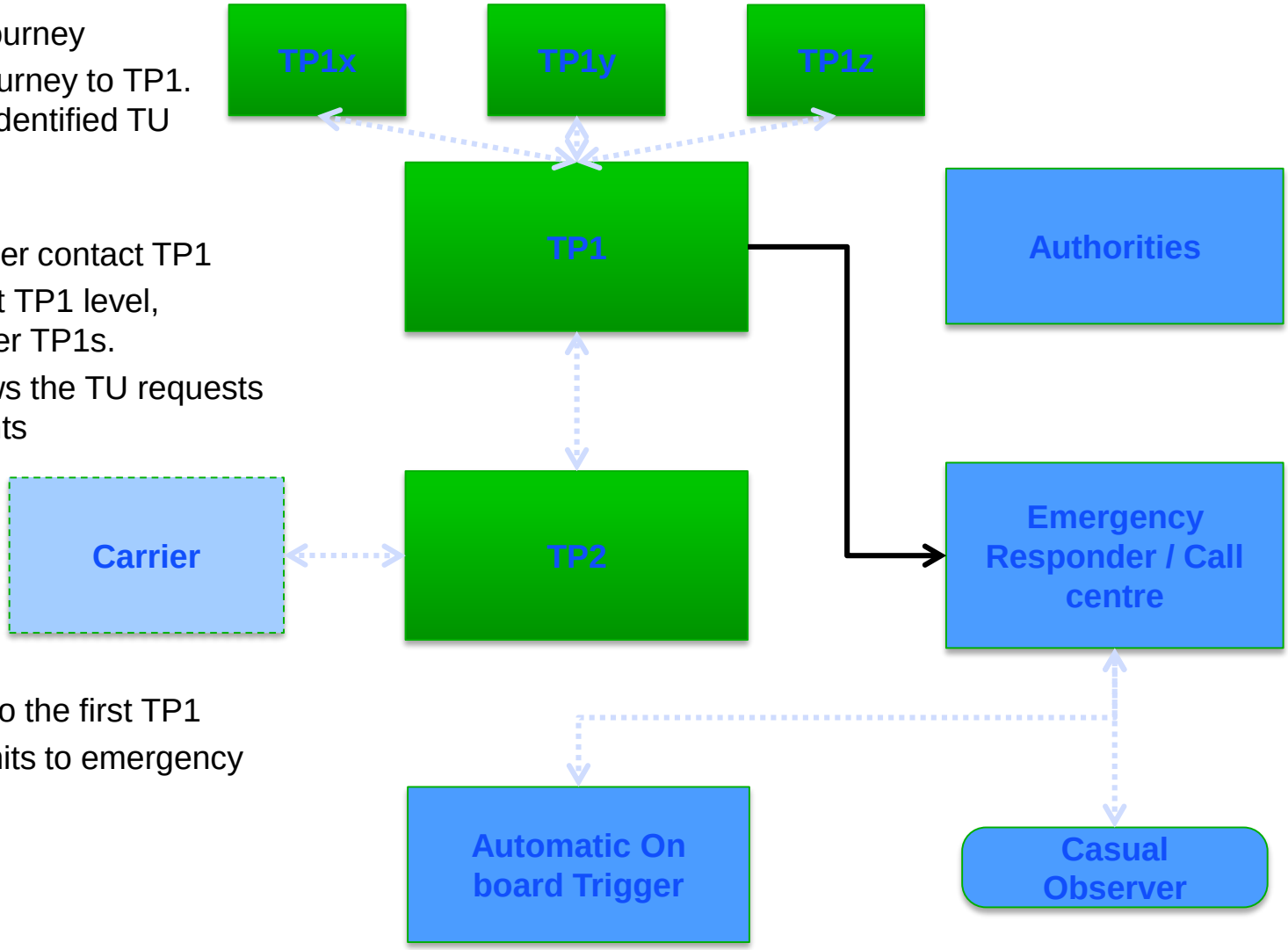
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP1
5. If TU is not known at TP1 level, TP1 requests to other TP1s.
6. The one which knows the TU requests to TP2 the documents
7. This TP1 transmits to the first TP1



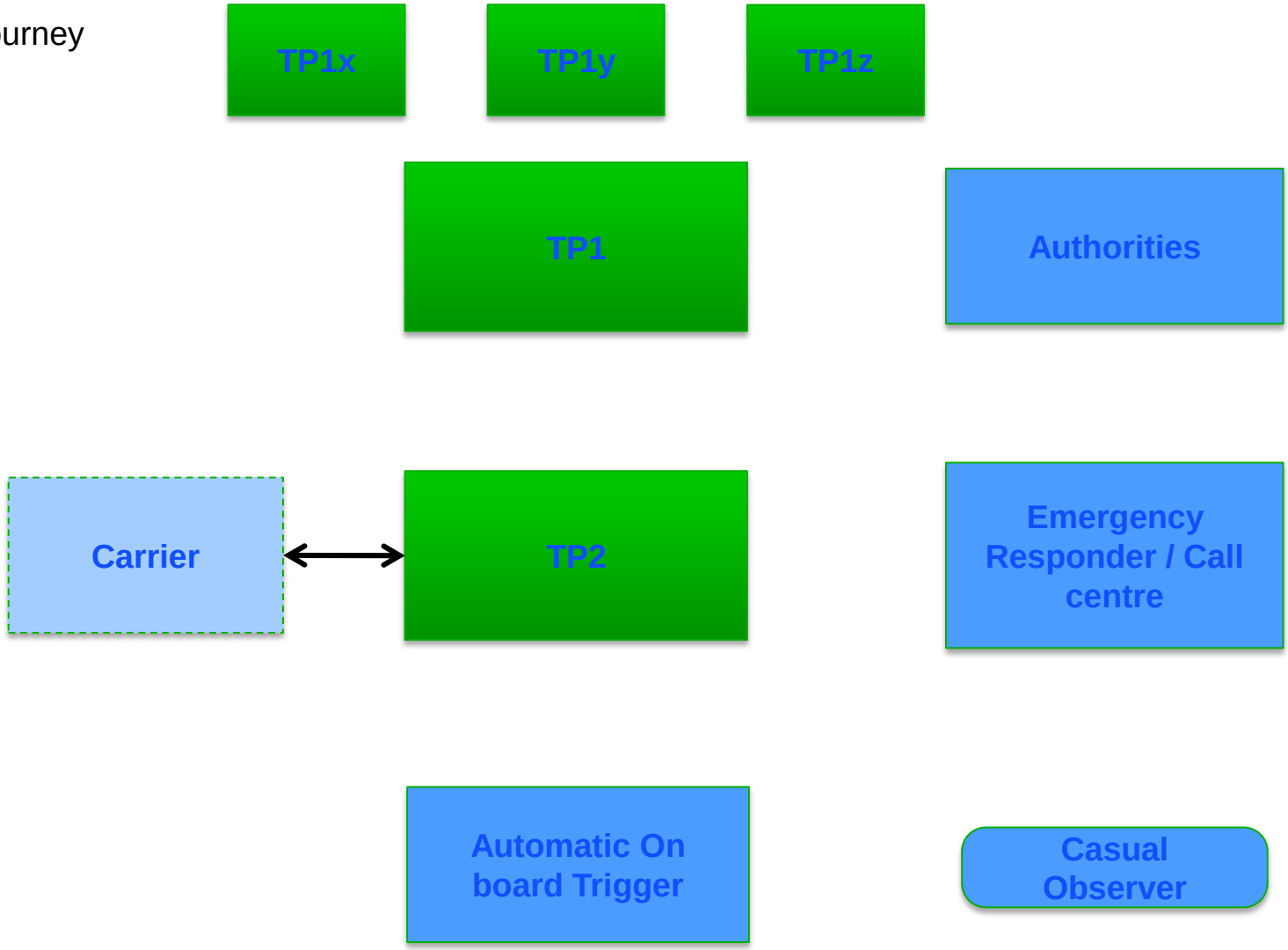
Dynamic behavior in proxy mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP1
5. If TU is not known at TP1 level, TP1 requests to other TP1s.
6. The one which knows the TU requests to TP2 the documents
7. This TP1 transmits to the first TP1
8. The first TP1 transmits to emergency responder



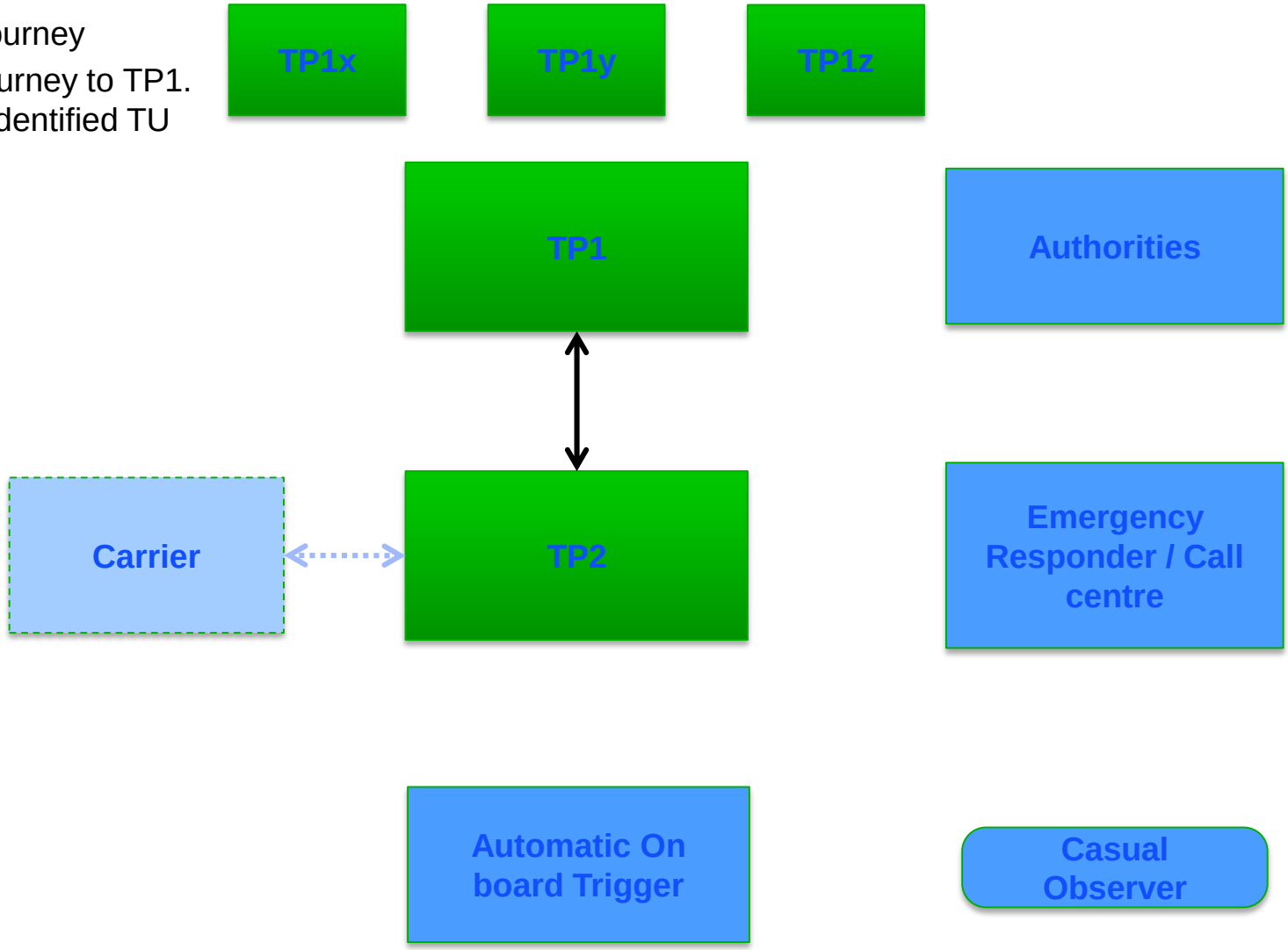
Dynamic behavior in redirect mode

1. Carrier registers a journey



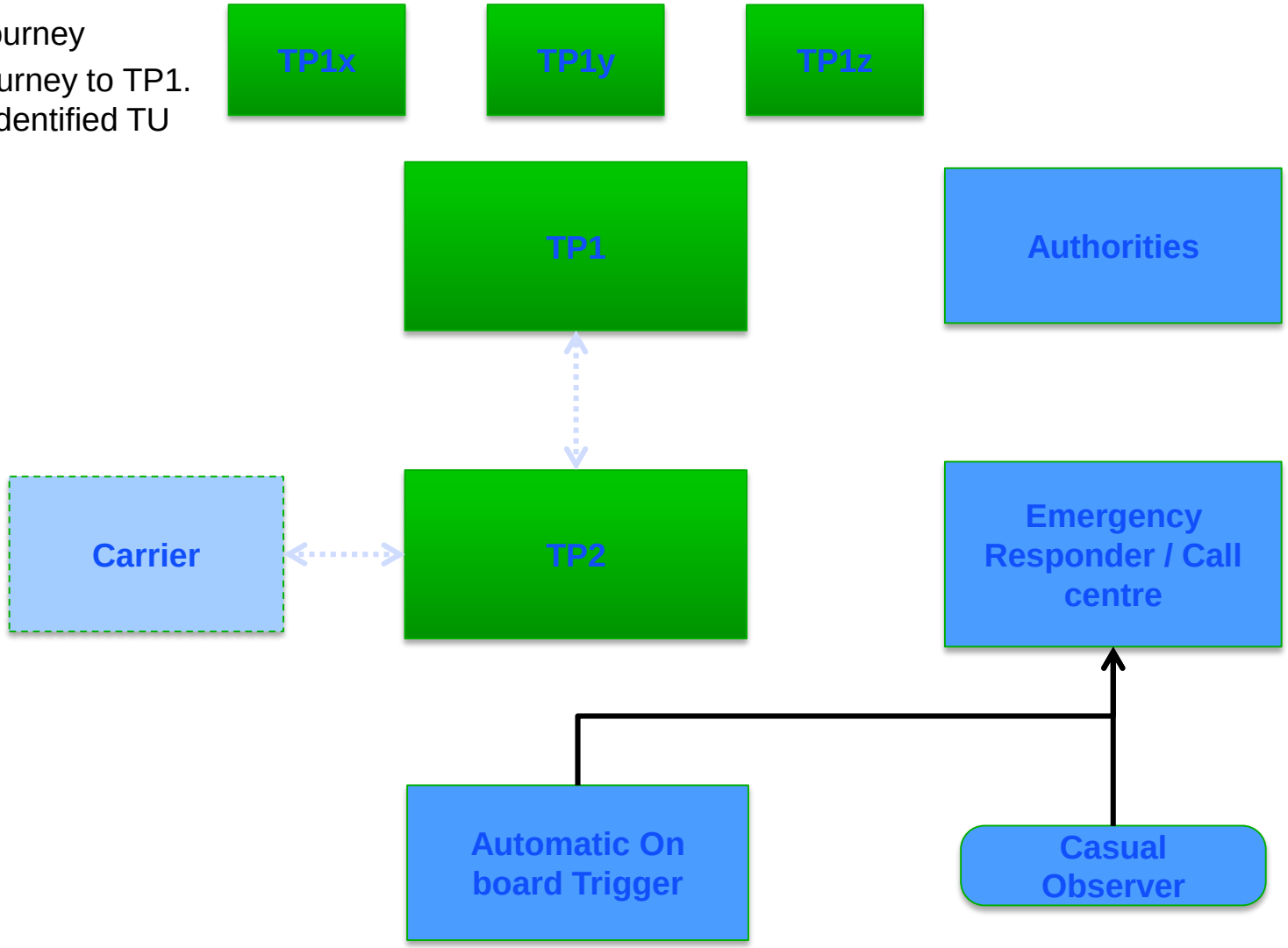
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip



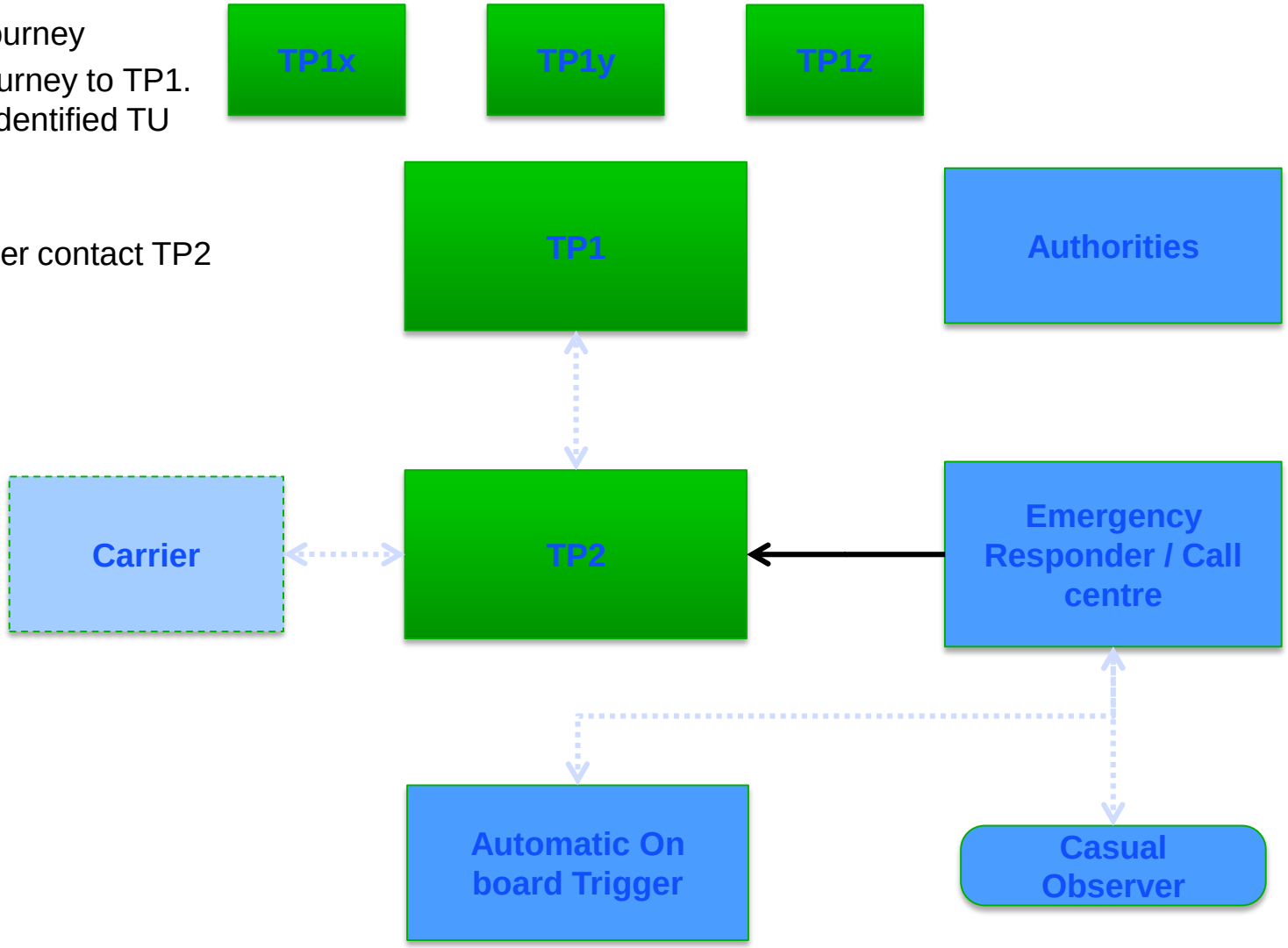
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs



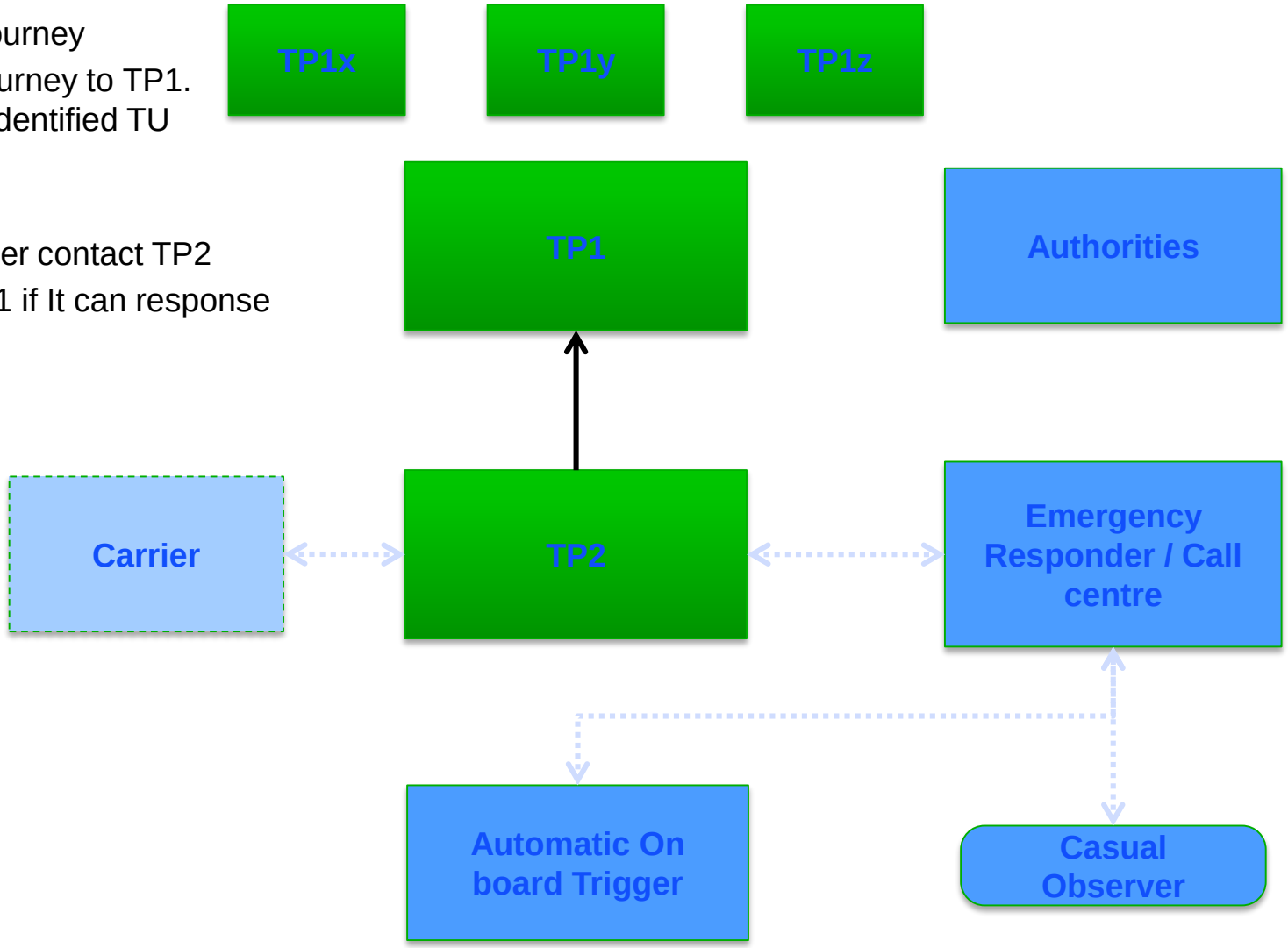
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2



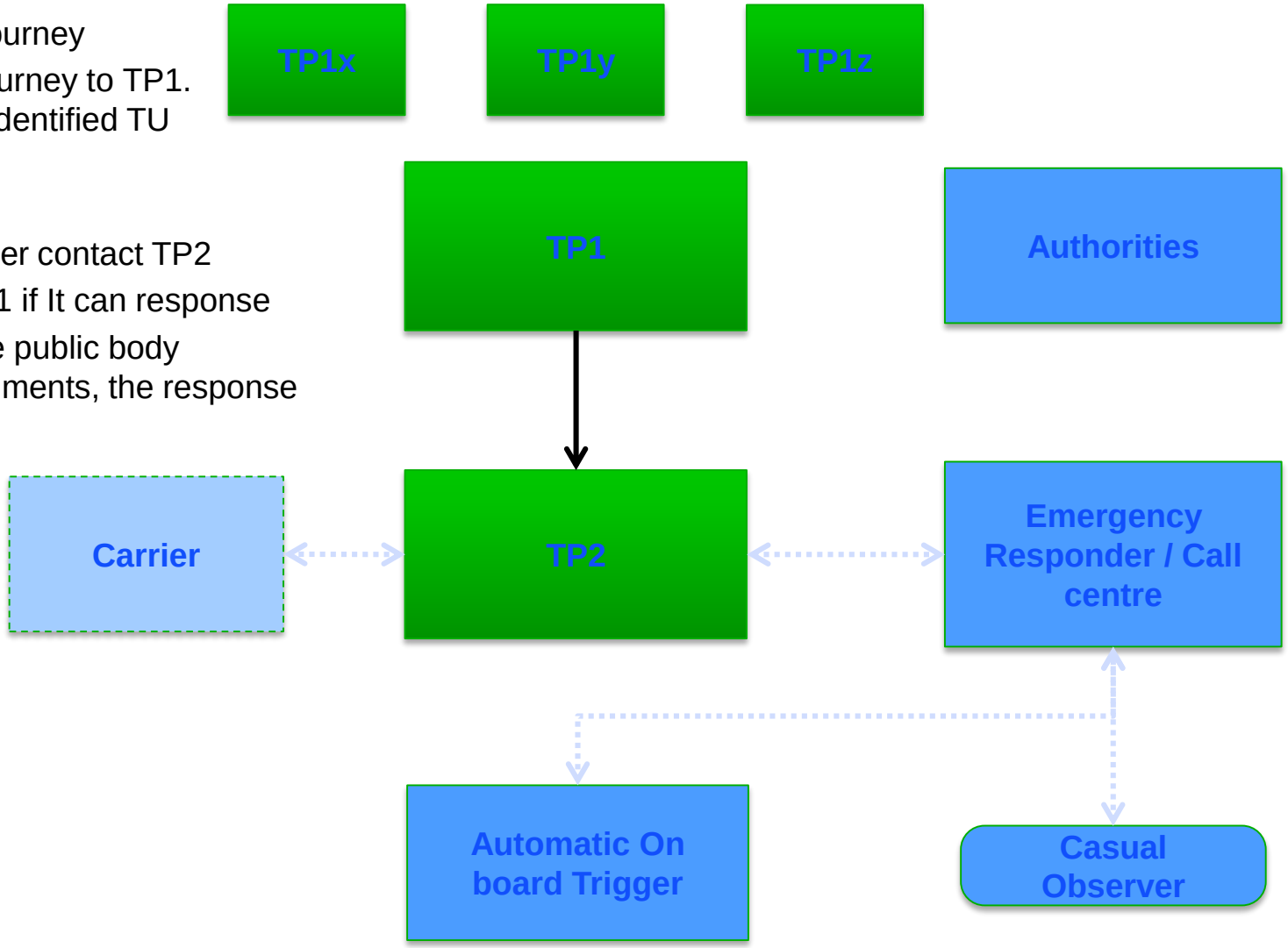
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response



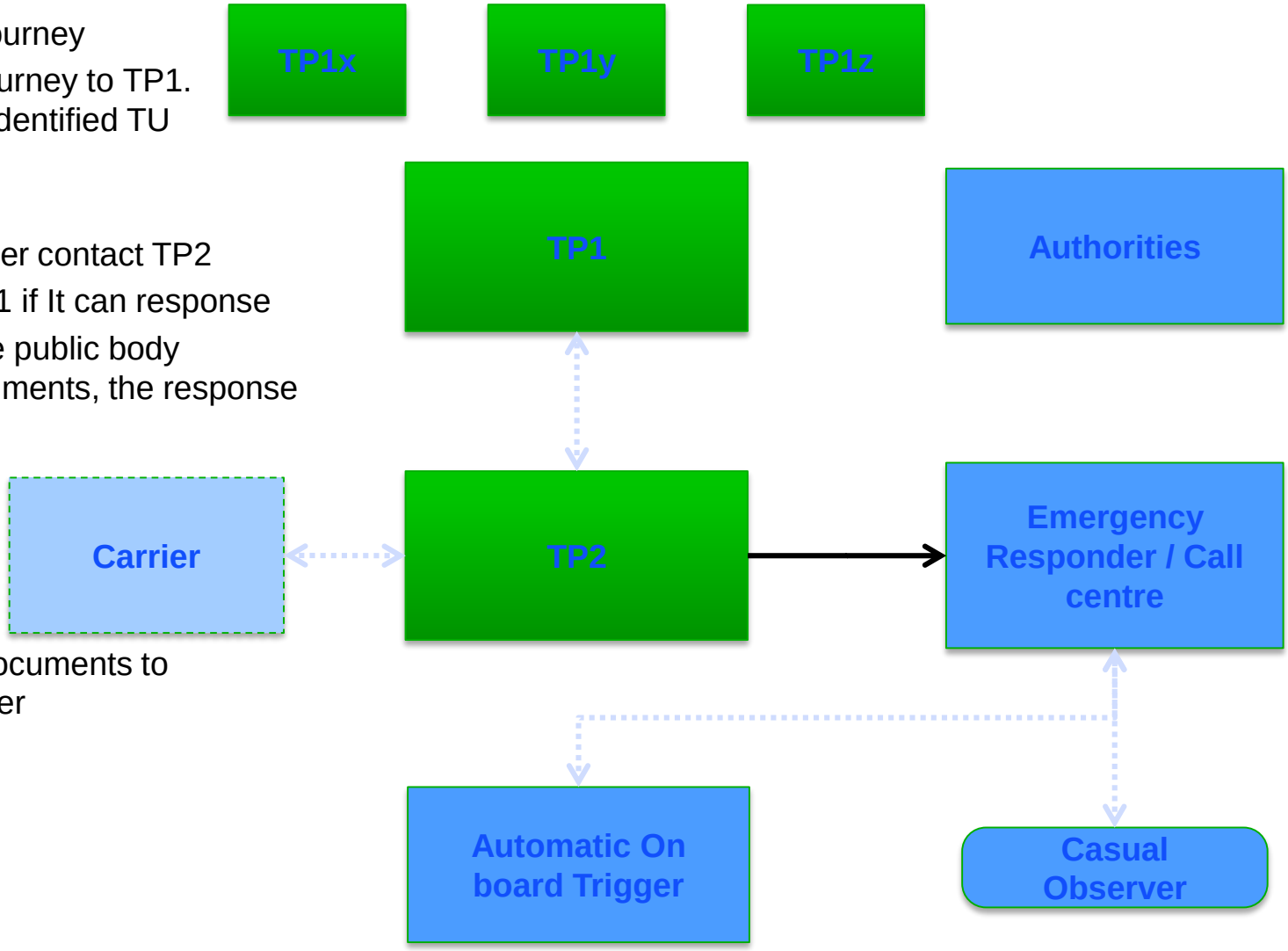
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response
6. If the TP1 knows the public body which asks the documents, the response is Yes



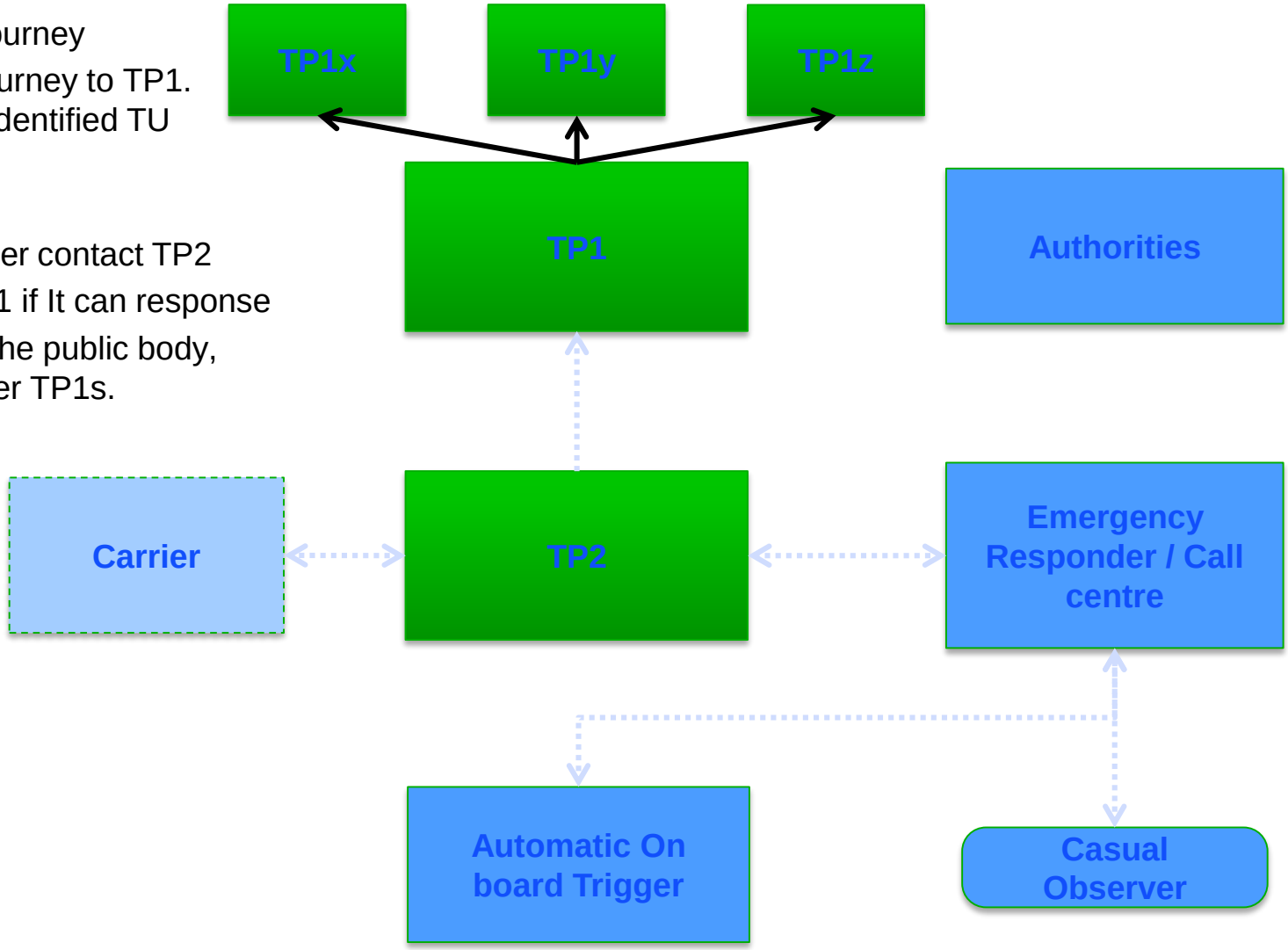
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response
6. If the TP1 knows the public body which asks the documents, the response is Yes
7. TP2 transmits the documents to emergency responder



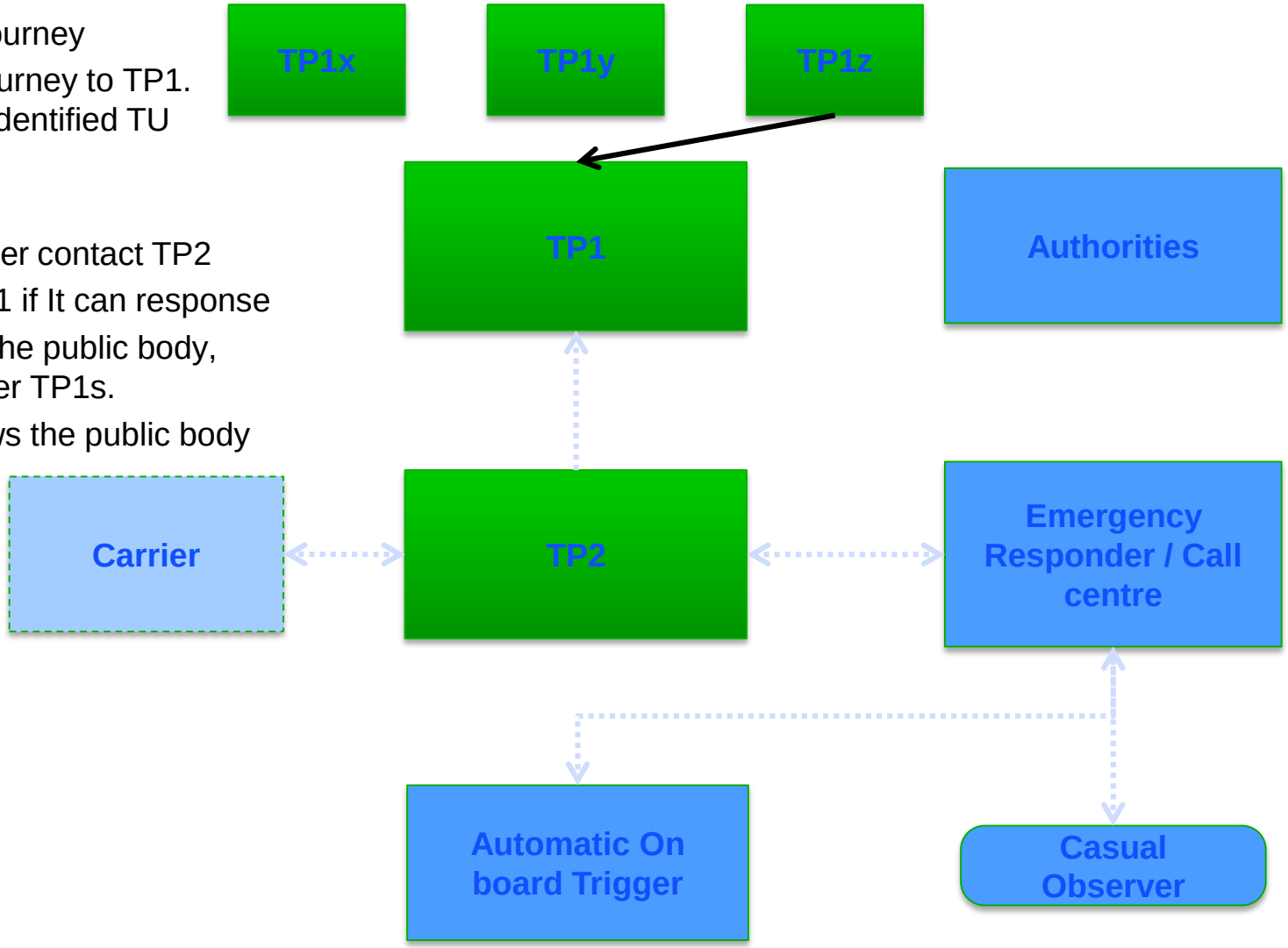
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response
6. If TP1 do not know the public body, TP1 requests to other TP1s.



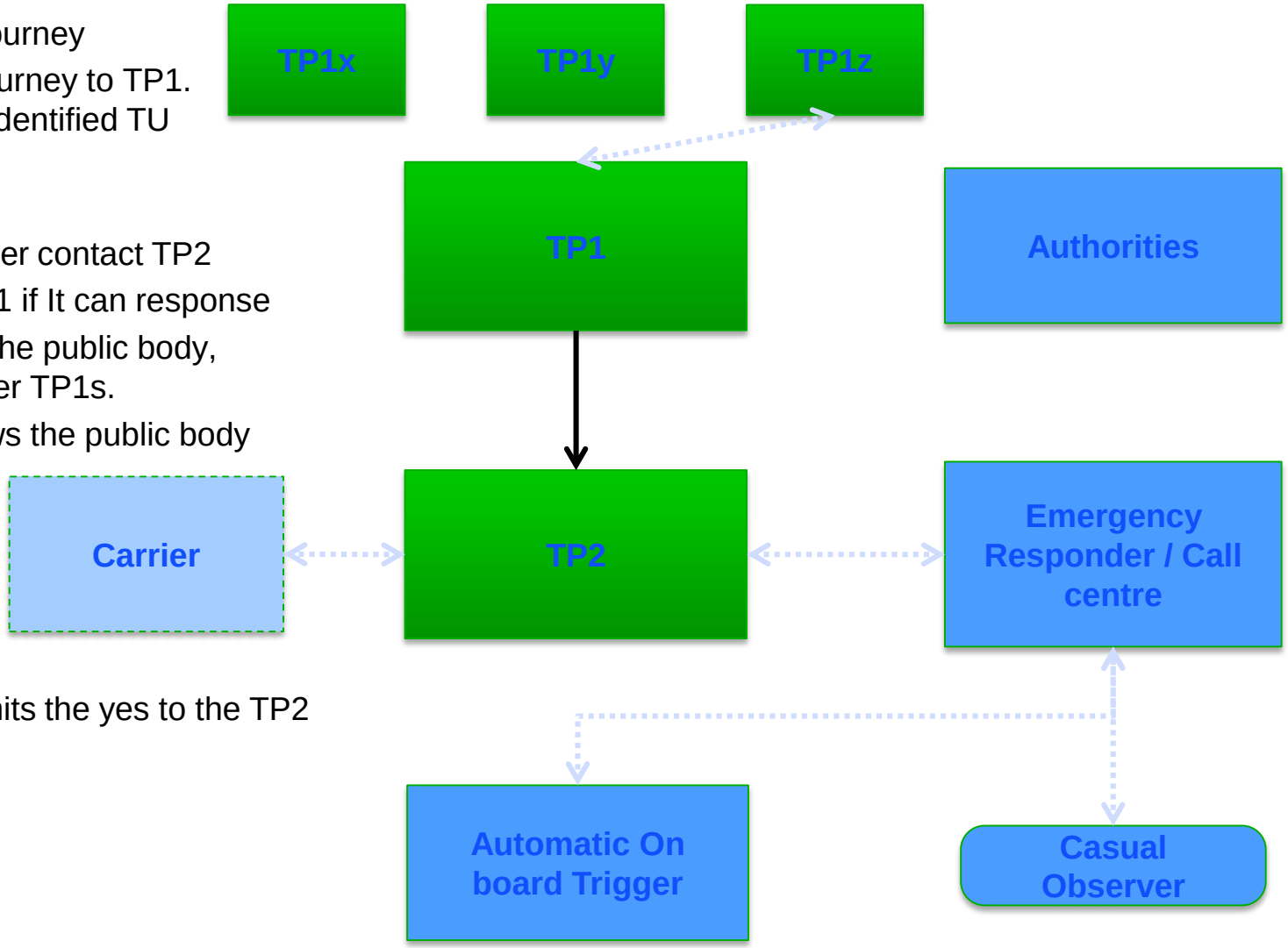
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response
6. If TP1 do not know the public body, TP1 requests to other TP1s.
7. The one which knows the public body responses Yes



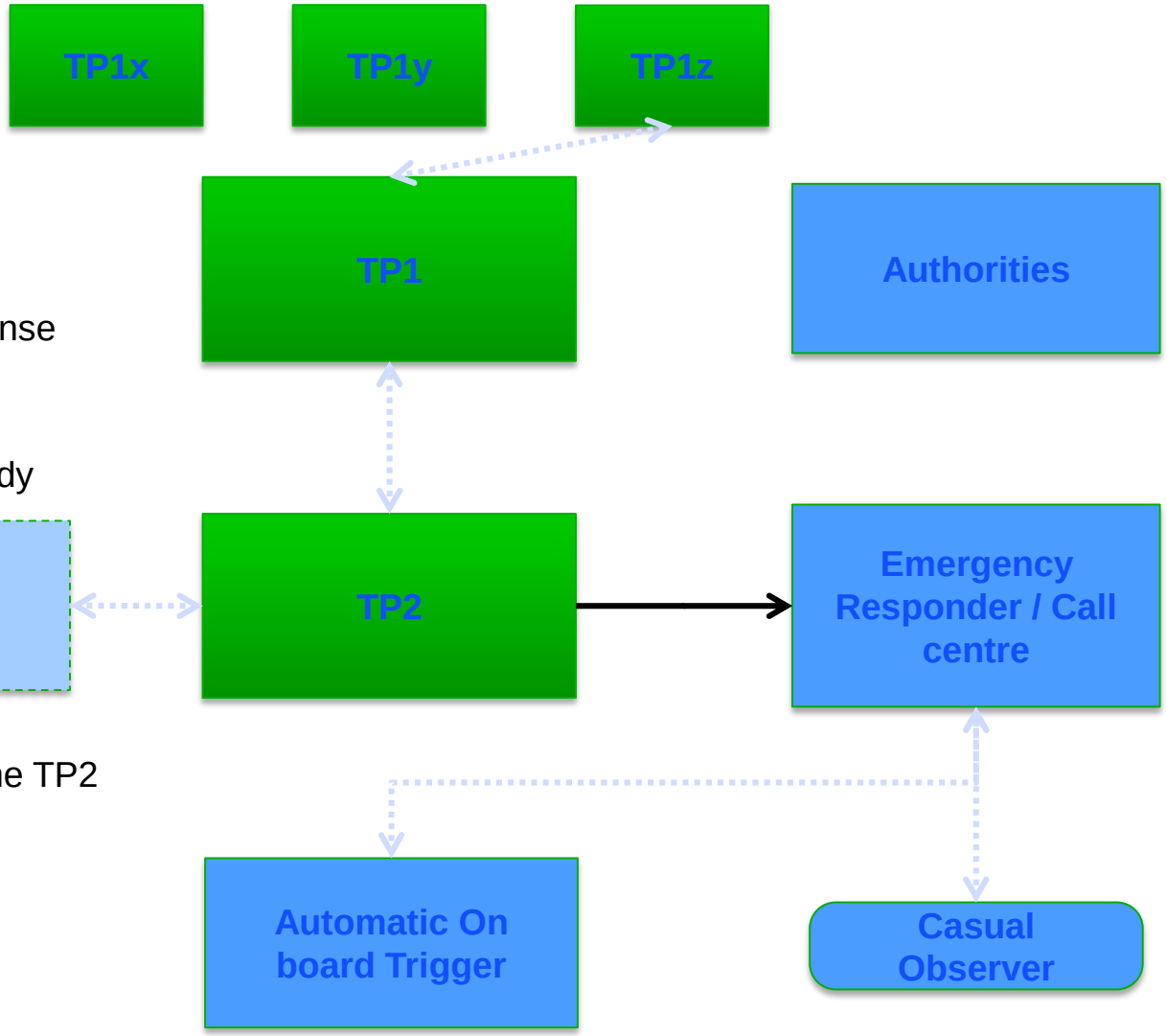
Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response
6. If TP1 do not know the public body, TP1 requests to other TP1s.
7. The one which knows the public body responses Yes
8. The first TP1 transmits the yes to the TP2



Dynamic behavior in redirect mode

1. Carrier registers a journey
2. TP2 registers this journey to TP1. TP1 knows that an identified TU is on trip
3. Alert occurs
4. Emergency responder contact TP2
5. TP2 requests its TP1 if It can response
6. If TP1 do not know the public body, TP1 requests to other TP1s.
7. The one which knows the public body responses Yes
8. The first TP1 transmits the yes to the TP2
9. TP2 transmits the documents to emergency responder



Analysis

If the two modes are implemented:

- Both modes need requests between TP1 and TP2:
  - ✓ Either to get the documents
  - ✓ Either to know if the request is addressed by a relevant public body
- Some public body (authority) have not the right to access directly on Internet and so will not be able to request directly to TP2
- TP2 must implement the response to the TP1 to transmit the documents on request of authorities which are not able to request directly
- TP2 must be able to request the TP1 or received the acknowledgment of the TP1 to control or deliver the documents to a public body

If only the proxy mode is implemented:

- TP2 do not need to implement part of the “work”
- TP1 will be the only access for public bodies
- The number of exchange will be less
- OBU or/and eCall do not have the Url of the TP2
  - ✓ No risk of error during input of the Url
  - ✓ Market will be more open because moving from one TP2 to another one will be easier

TP1 mode proxy can be the solution to implement without redirect solution?

DISCUSSION OR ADDITIONAL COMMENTS

The architecture is designed to be secure and data available in real time. It is a network based on Internet.

SECURITY AND AVAILABILITY

STRIDE : spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege

Type of threats	Description	Type of need associated
Spoofing or electronic identity theft	Impersonates equivalent to pretend to be someone else when access to the computer.	**Authentification**
Tampering or data falsification	Falsification involves malicious modification of data. It may be, by instance, unauthorized alteration of data exchanged between two computers over an open network such as the Internet.	**Integrity**
Repudiation	Non-repudiation is the concept of ensuring that a party in a dispute cannot repudiate, or refute the validity of a statement or contract. By instance, a party sends a message to achieve a specified receiver. The sender can not say he did not send it said message. In any case it can not "repudiate" this message.	**Non-repudiation**
Information disclosure	Threats of information disclosure involve the exposure of information to individuals who are not supposed to have access. It may be , for example, the ability of a user to read a file that is not authorized to access or the ability of an intruder to read data transmitted between two computers.	**Confidentiality**
Denial of service	The denial of service attacks cause impossible access to the system to valid users , for example , making a temporarily unavailable or unusable Web server.	**Availability**
Elevation of privilège	Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.	**Authorisation**

Level description

- Tier I - Basic site infrastructure (non-redundant)
  - ✓ Basic site (non-redundant) , a single power source . Tier 1 data centers have many SPOF, systems must be stopped during logistics operations maintenance.
- Tier II - Redundant capacity components site infrastructure (redundant)
  - ✓ Infrastructure with redundancy for certain components , but non-redundant power supply and air conditioning.
- Tier III - Concurrently maintainable site infrastructure
  - ✓ Infrastructure with all redundant components , all systems are dual power , coupled power but in active / passive mode , the balancing may have an impact on the availability of services.
- Tier IV - Fault tolerant site infrastructure
  - ✓ Infrastructure fully redundant , fault-tolerant , energy supply in active / active mode. This type of data center reaches and exceeds an availability rate of 99.99% (less than 24 minutes per year cumulative judgment). This type of data center does not require system shutdown , even for logistics operations maintenance and asset replacement equipment.

Data centre classification by the UPTIME INSTITUTE

Level	Charasteristics	Availability	Annual shutdown	Hot maintenance	Sensibility to breakdown
1	No redondancy	99,671%	28,8 hours	No	No
2	Partly redundant	99,749%	22,0 hours	No	No
3	Redundancy active/passive	99,982%	1,6 hours	Yes	No
4	Redundancy active/active	99,995%	0,4 hour_	Yes	Yes

The total availability of the foreseen architecture will the sum of the availability of couple (TP1/TP2).

What level would be relevant for TP1 and TP2 ?

Could it be possible to allow a low level to TP2 if TP1 ensures the availability of data ?

DISCUSSION OR ADDITIONAL COMMENTS

Claude.pfauvadel@developpement-durable.gouv.fr
jean-philippe.mechin@cerema.fr

THANK YOU FOR YOUR ATTENTION