



# Network architecture of the SCOOP project for road operators

---

## Deliverable 2.4.1.5

### Activity 2: Studies

### Sub-activity 2.4 > Specifications

Version 2.00

Publication date: 12/05/2017



Co-financed by the Connecting Europe Facility of the European Union

## Information on the document

Document: Network architecture of the Scoop@F project for road operators

Date of publication: 12/05/2017

Responsible, Entity: Erwan BROQUAIRE, Guilhem AUTRET, Jean-Marc TISSIER, Cerema SO

Status: Version 2.00 – Approved

## Publication history

Version	Date	Contributor(s)	Main updates & changes	Diffusion
2.00	12/05/2017	E. BROQUAIRE MC. ESPOSITO	New deliverable	Release 2

### Reference to the version administration

Version number to be composed of 3 digits > vR.XY

- **R** corresponds to the release number : it is upgraded each time SC Studies validates the diffusion of a new release,
- **X** is the major version number: it is upgraded each time SC Studies validates the deliverable,
- **Y** is the minor version number: it is upgraded each time a contributor changes anything.

Once the deliverable is approved, its version number is upgraded from vR.XY to vR.(X+1)0

Once the deliverable is release, its version number is upgraded from vR.XY to v(R+1).00

As illustration :

- 0.03 > Work in progress version
- 0.10 > Del. Approved by SC Studies but not released
- 2.00 > Del. approved & released (in release 2)
- 2.05 > Del. Updated - in progress version

# Table of Contents

1.	Context .....	5
2.	General architecture of the scoop@F project .....	5
2.1	Physical architecture .....	5
2.2	IP architecture (level 3 of the OSI module) .....	5
2.3	Protocols used.....	6
3.	Typical architecture of a TMS .....	9
4.	Integration of Scoop equipment in the architecture of a TMS .....	11
4.1	Case of the DIR A.....	11
4.2	Case of the DIR Ouest .....	12
4.3	Case of the DIR IF.....	13
4.4	Case of the department of Isère .....	14
4.5	Case of Sanef.....	15
5.	Network architecture retained to upload PKI queries, the logs and operating information...	16
5.1	Data exchanges.....	16
5.2	TLS tunnel set up .....	16
5.3	Positioning of firewalls in the architecture.....	16
5.4	Configuration of road-side equipment.....	17
5.5	Configuration of vehicles .....	17
5.6	Recap of exchanges for IPv6 .....	18
5.7	Additional securing .....	18
5.8	Acquisition .....	18
6.	Implementation of TLS tunnels .....	19
6.1	Principle.....	19
6.2	Filtering.....	19
6.3	Sizing.....	19
6.4	Positioning of the tunnel's termination .....	19
7.	Conclusions .....	20
7.1	Choice between IPv4 and IPv6 .....	20
7.2	Positioning of the tunnel's termination .....	20
7.3	Operational rollout .....	20

## Table of Illustrations

Illustration 1: Summary schema of exchanges .....	8
Illustration 2: Typical architecture of a TMS .....	9
Illustration 3: general integration schema .....	10
Illustration 4: Integration of equipment in the DIR A architecture .....	11
Illustration 5: Integration of equipment in the DIR O architecture .....	12
Illustration 6: Integration of equipment in the DIR IF architecture .....	13
Illustration 7: Integration of equipment in the LD 38 architecture .....	14
Illustration 8: Integration of equipment in the SANEF architecture .....	15
Illustration 9: Schematic diagram of the tunnel's termination .....	19

# 1. Context

Initially intended for road operators to describe Scoop's internal network, this document presents more generally the network architecture of the scoop project and its integration in the road operators' networks.

## 2. General architecture of the scoop@F project

### 2.1 Physical architecture

To operate, the scoop project needs the following servers and equipment:

- PKI servers, to manage the different certificates:
  - RCA, to manage and initialise the chain of confidence
  - LTCA, to deliver the long-term certificates for the ITS equipment (ITSS-R and OBU)
  - PCA, to deliver the short-term certificates or pseudonym certificates
  - DC, to distribute the lists of confidence and lists of revocation
- road operator servers
  - Scoop platform, to manage the DatexII messages
  - an ITSS-R server (created by each road operator, in conjunction with its ITSS-R supplier): to control the ITSS-Rs, configure the ITSS-Rs, update the ITSS-Rs and for the T-logs
  - an OBU server (created by each road operator, in conjunction with its OBU supplier): to control the OBUs, configure the OBUs, update the OBUs and for the T-logs
  - a SCOOP application server (supplied by DiRIF) to operate the SCOOP application on a tablet, in the road operators' vehicles (authentication, updating, uploading application logs and configuration)
  - a mapping server (supplied by the DiRIF): with which the OBU can have a complete map in real time
  - a storage space to store the different U-logs (different directories to separate log accesses from their different recipients according to the type of logs: OBUu, OBUo, ITSS-R)
- The Road Side Units (ITSS-R)
- The On-Board Units (OBU)
  - The OBU-U for the general public
  - Road Operator OBU-RO with special rights

### 2.2 IP architecture (level 3 of the OSI module)

The communications between ITSS-R and OBU are in:

- GeoNetworking for exchanges of CAM and DENM messages
- IPv6 for OBU exchanges with the PKI
- IPv4 for ITSS-R exchanges with the PKI

The OBU-RO have a 3G IPv4 connection to dialogue with the scoop application server and the OBU server.

The road operator network is in IPv4 and the communications flowing through this network must therefore be either IPv4 or an IPv6 machine to an IPv6 machine encapsulated in the IPv4 (TLS tunnel).

Internet supports both versions: IPv4 and IPv6

- The road operator is interfaced with Internet IPv4 and IPv6
- The PKI servers will be interfaced with Internet IPv4 and/or IPv6

## 2.3 Protocols used

### Exchanges between an ITSS-R and the platform (PF):

- **webservice (http) (language: DATEX II)**
- the ITSS-R periodically transmits the DATEX II uploads from the CAM aggregations
- the ITSS-R transmits for each DENM received from a vehicle its translation in DATEXII upon receipt
- the ITSS-R, for the first logon and after each logoff, declares itself with the PF; at the same time and periodically (every 24 hr by default, but configurable) it requests snapshot of current situations concerning it
- for each DateX II received from the TMS, the PF transmits it to the ITSS-Rs concerned (and active)

### Exchanges between an OBU-RO and the PF:

- **webservice (http) (language: DATEX II):**
- the OBU transmits for each DENM received from a vehicle or created by itself the DENM's translation in DATEXII upon receipt
- each time the motor starts, the OBU performs the following steps:
  - logon: the OBU declares itself to the PF
  - the OBU transmits its position
  - the OBU requests a snapshot to obtain the current situations concerning it

### Exchanges between an ITSS-R and the ITSS-R server:

- **control:** the ITSS-R supplier supplies its control tool, which will be able to read the MIB produced by the ITSS-R; the control tool will interact with the ITSS-R in SNMP; this is the tool that transmits the SNMP queries
- **configuration:** a configuration file per ITSS-R is recorded in a space on this server; each ITSS-R scans this server periodically (e.g., every 24 hr) and downloads the file if necessary; protocol: https
- **software update:** a space on this server will be reserved to record an update; idem for configuration -> each ITSS-R scans this server periodically (e.g., every 24 hr); protocol: https
- **transmission of logs:** periodic push of logs from the ITSS-Rs; protocol: https

#### **Exchanges between the PF and the ITSS-R server:**

- the platform regularly queries the control tool to have the general state of the ITSS-R (nominal, minor error, major error)

#### **Exchanges between an OBU-RO and the OBU server:**

- control: the OBU supplier supplies its control tool, which will be able to read the MIB produced by the OBU; the control tool will interact with the IOBU in SNMP; this is the tool that transmits the SNMP queries
- configuration: a configuration file per OBU is recorded in a space on this server; each OBU scans this server at its startup and downloads the file; protocol: https
- software update: a space on this server will be reserved to record an update; idem for configuration; protocol: https
- transmission of logs: periodic push of logs (20s by default); protocol: https

#### **Exchanges between an OBU-RO and the SCOOP server:**

- configuration: the configuration is done via the administration interface of the SCOOP application server; the information is recovered at each startup of the OBU (see above)
- update: same operation as OBU
- authentication

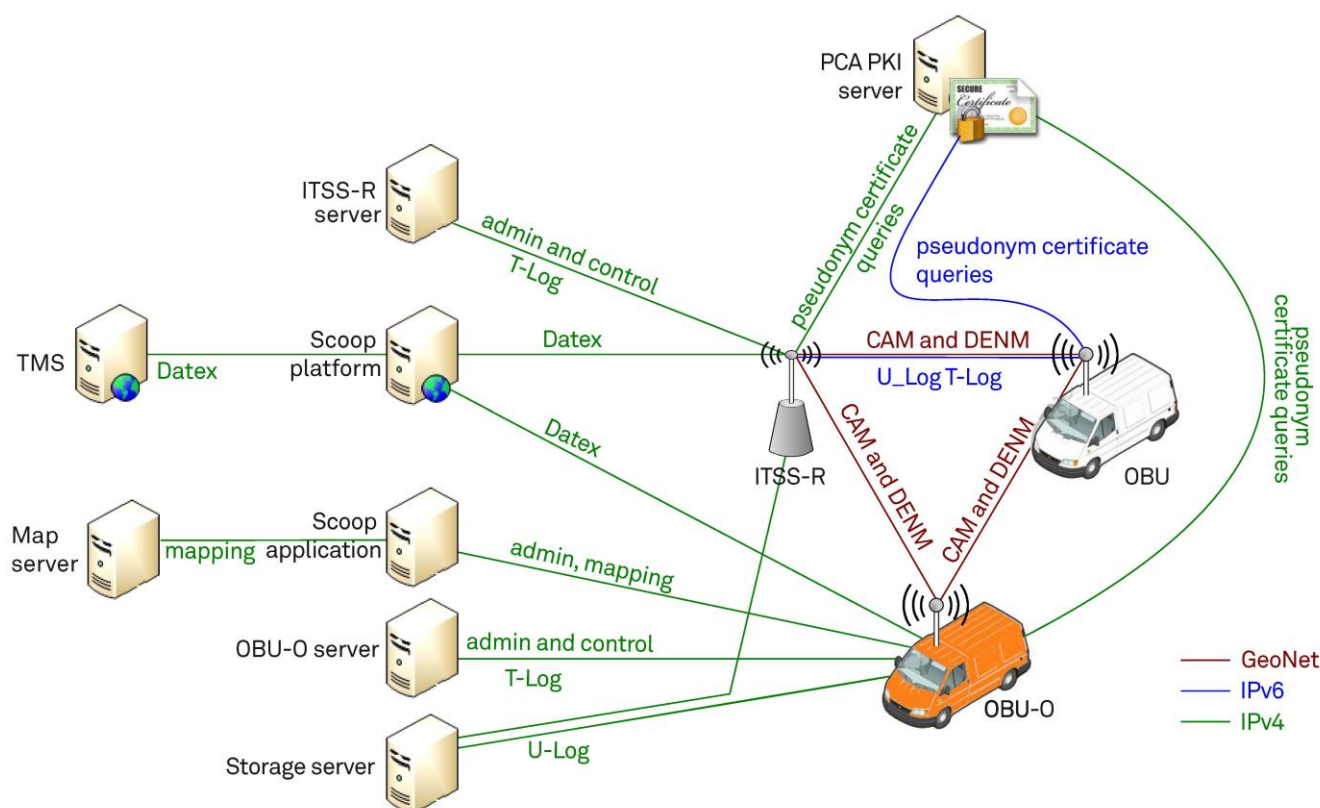
#### **Exchanges between an OBU-RO and the mapping server:**

- webservice

#### **Exchanges between an OBU/ITSS-R and the PKI server:**

- protocol: http

The OBUs and the ITSS-Rs transmit pings every 30 seconds to verify the connections with the different servers that they communicate with regularly.



*Illustration 1: Summary schema of exchanges*

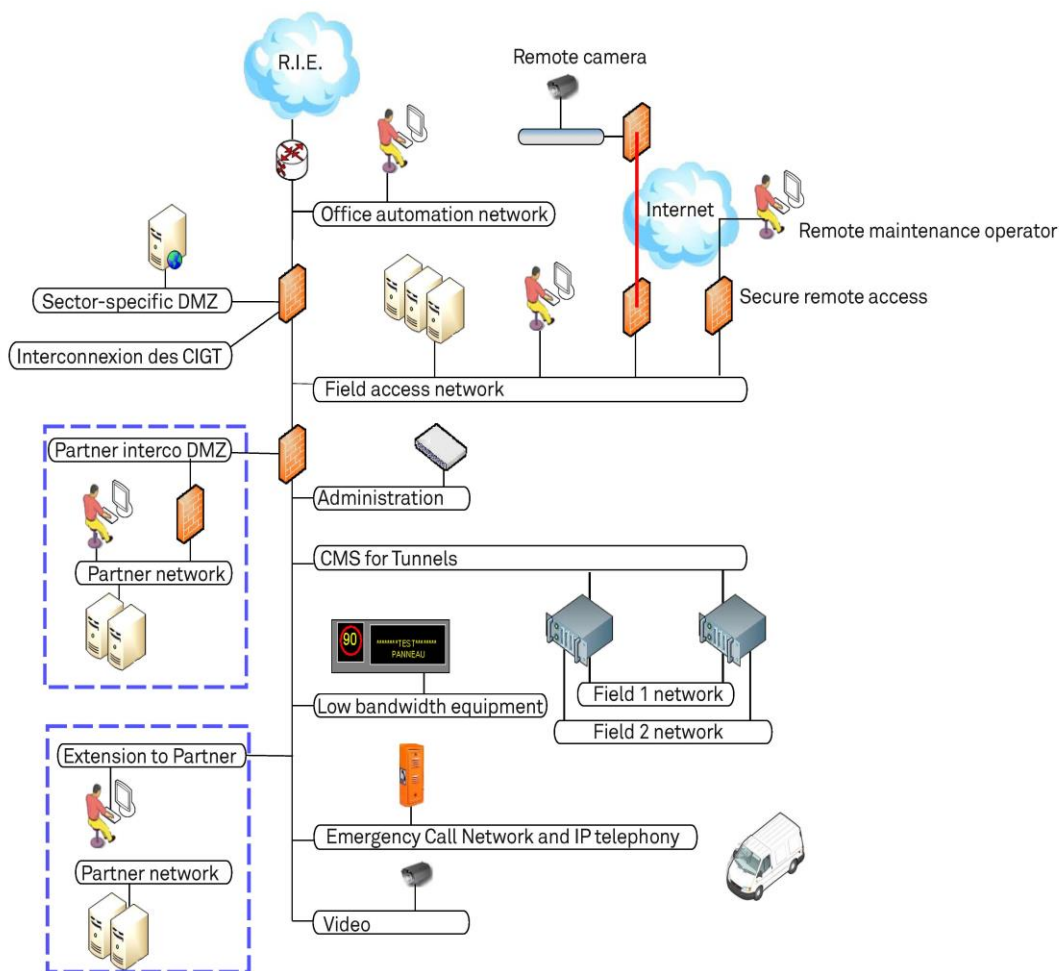
This is the equipment that has to be integrated in the road operators' architecture.



### 3. Typical architecture of a TMS

The [Scoop@F](#) project with its previously described architecture must fit into the existing networks of traffic operators.

The typical architecture of a TMS is represented below:

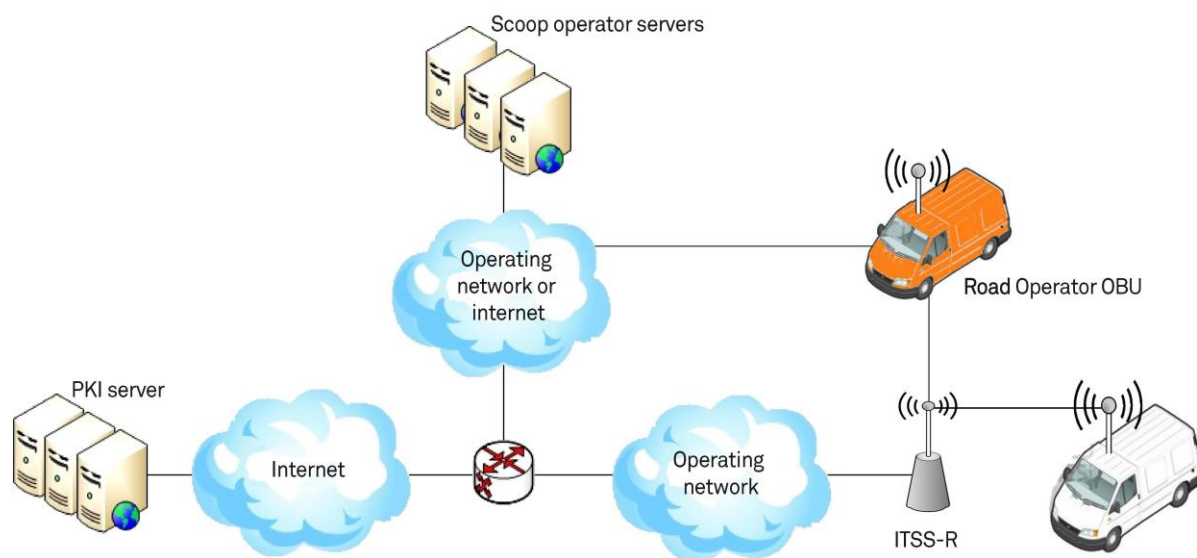


*Illustration 2: Typical architecture of a TMS*

**Note:** In the case of the DIR IF, the Sirius network does not correspond at present to the schema. The field equipment will be regrouped in the same LAN, which will include many routing points.

**Note:** The term "partner" signifies another road operator or any other entity that has to exchange information with the TMS.

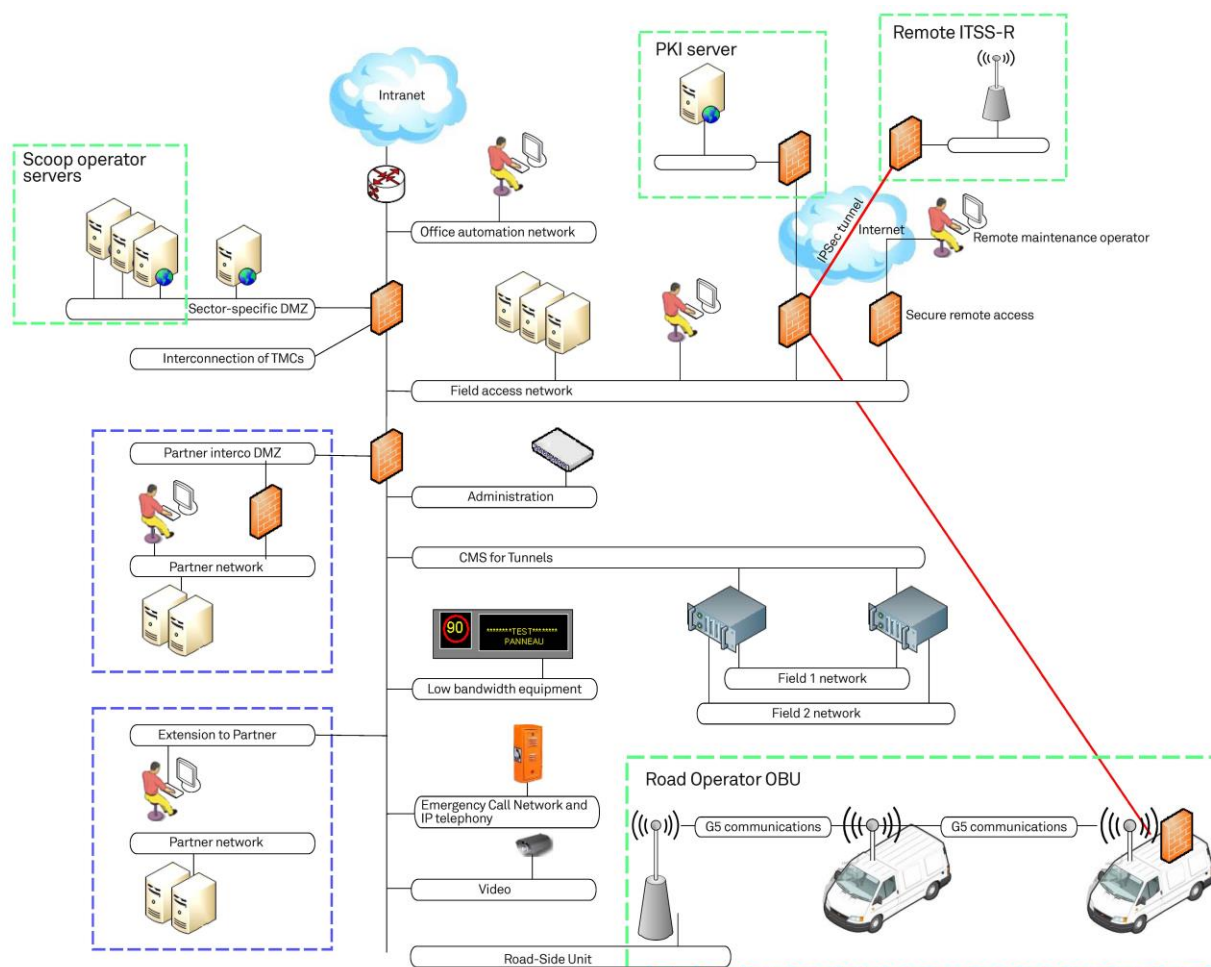
The integration of Scoop in the road operators' architecture is therefore done very schematically as follows:



*Illustration 3: general integration schema*

## 4. Integration of Scoop equipment in the architecture of a TMS

### 4.1 Case of the DIR A

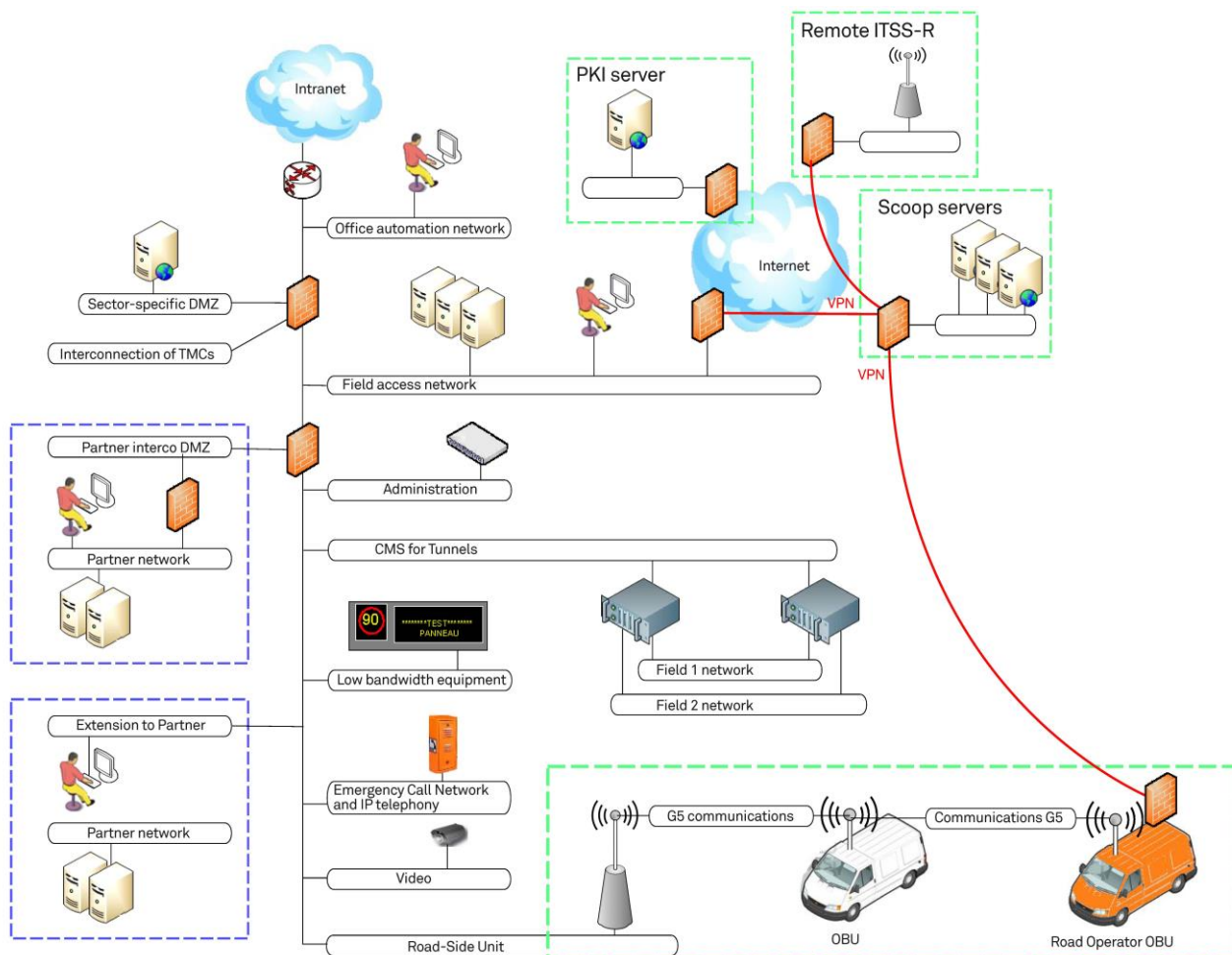


*Illustration 4: Integration of equipment in the DIR A architecture*

An ITSS-R VLAN is created. It is dedicated to the scoop@F project's road-side equipment. The remote ITSS-Rs are repatriated to the TMS according to the same schema as the existing remote equipment through TLS tunnels pursuant to the General Security Repository (GSR).

The Scoop servers are put on the sector-specific DMZ network or on a new DMZ dedicated to Scoop@F. It is comprised of several functional servers, as seen in paragraph 2.

## 4.2 Case of the DIR Ouest



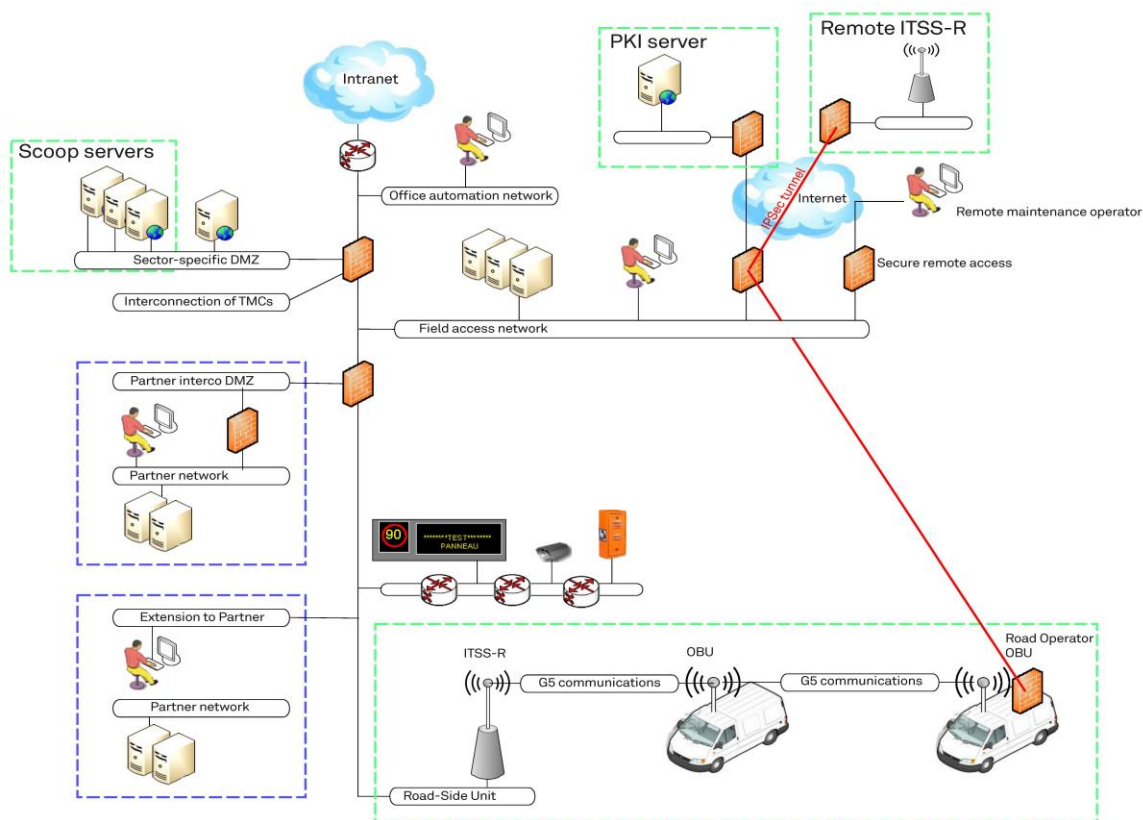
*Illustration 5: Integration of equipment in the DIR O architecture*

An ITSS-R VLAN is created. It is dedicated to the scoop@F project's road-side equipment. The remote ITSS-Rs and Road Operator OBUs are repatriated to the Scoop servers in 3G.

The Scoop platform is hosted at an outside service provider so it can be accessed by the other members of the Ouest project. It is comprised of several functional servers, as seen in paragraph 2.

The PKI servers are also present at a partner.

## 4.3 Case of the DIR IF



*Illustration 6: Integration of equipment in the DIR IF architecture*

A Road-Side Unit VLAN is created on the RTHD and Sirius networks (progressively for Sirius). It will be dedicated to the scoop@F project's road-side equipment. The remote ITSS-Rs and the OBUOs are repatriated to the TMS according to the same schema as the existing remote equipment via TLS tunnels pursuant to the General Security Repository (GSR).

The Scoop servers are put on the sector-specific DMZ network or on a new DMZ dedicated to Scoop@F. It is comprised of several functional servers, as seen in paragraph 2.

## 4.4 Case of the department of Isère

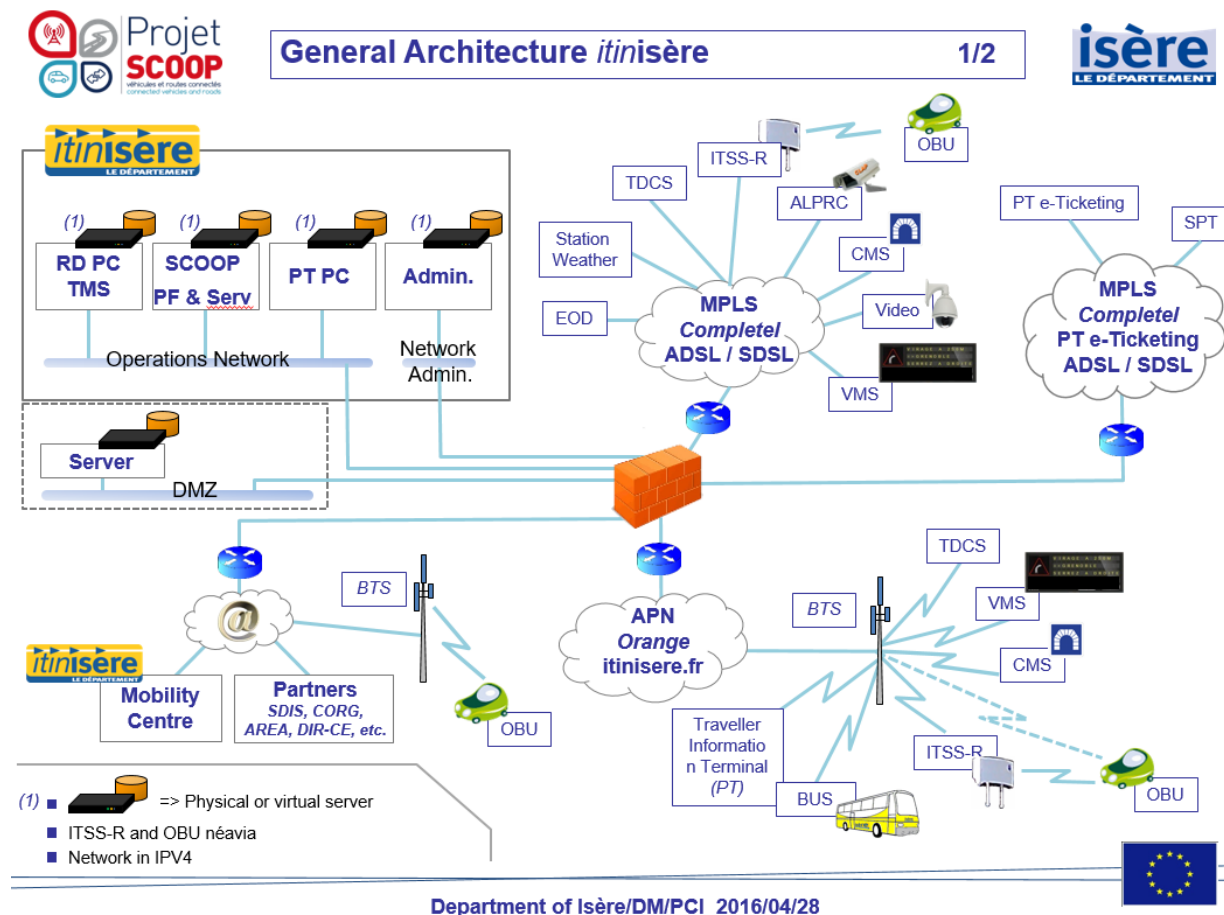


Illustration 7: Integration of equipment in the LD 38 architecture

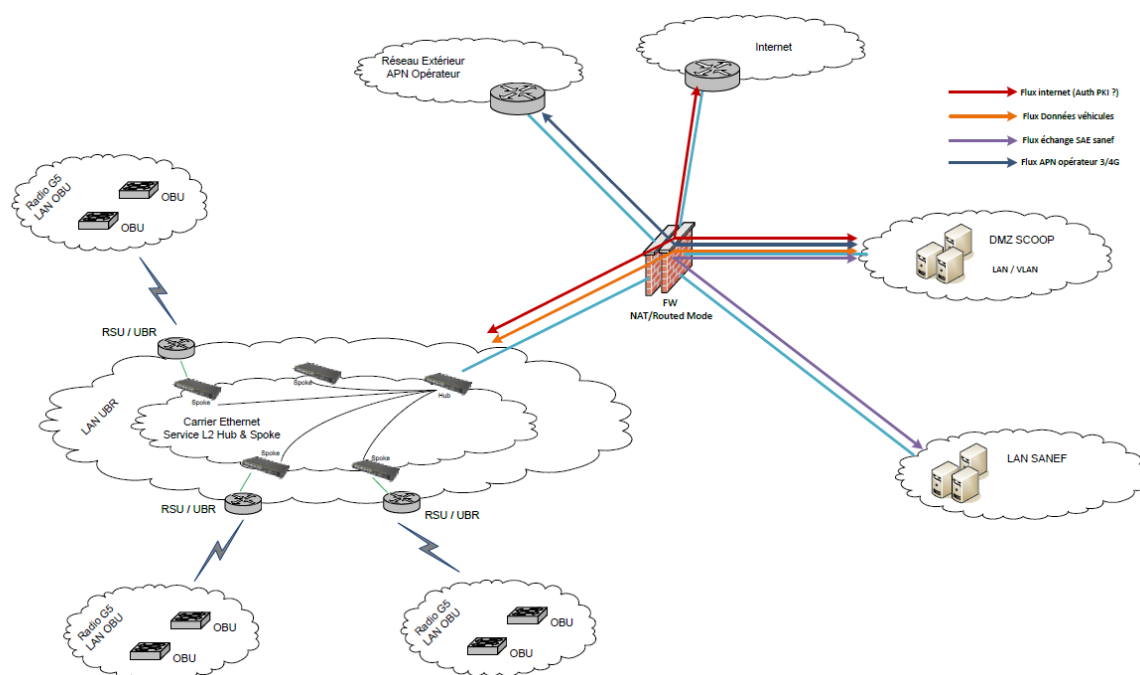
Links between the network architectures of LD38 and the DIRs.

- The DIRs' field access network is called operating network in Isère.
- The DIRs' field network is created in Isère by the operated networks (APN Orange and MPLS Completel)

The ITSS-Rs are positioned on the operated networks and the scoop@F servers on the operating network.



## 4.5 Case of Sanef



*Illustration 8: Integration of equipment in the SANEF architecture*

The ITSS-Rs are positioned on an ITSS-R LAN in a level 2 hub and spoke.  
The Scoop servers are positioned on a dedicated DMZ, independent of the Sanef network.

## 5. Network architecture retained to upload PKI queries, the logs and operating information

The following architecture seeks to minimise the IPv6 communications and tunnels encapsulating IPv6 and gives priority to IPv4 exchanges between systems when possible.

### 5.1 Data exchanges

The data flows are as follows:

- 1- between the ITSS-R and the Scoop platform, the ITSS-R server and the PKI - IPv4 server
- 2- between the ITSS-R and the OBU-U/OBU-RO – Geonetworking over G5
- 3- between the OBUs and the platform, the PKI server, the Scoop application and the OBU-RO server - IPv4 over 3G/4G
- 4- between the OBUs and the PKI – IPv6 server on G5, then in a tunnel to the broker tunnel

### 5.2 TLS tunnel set up

The OBUs can communicate with the PKI servers, either via a 3G/4G access or via an ITSS-R.

When the communications are routed by the ITSS-Rs, since the existing networks are in IPv4, tunnels must be set up so the IPv6 traffic can transit on the networks. IPv4. A TLS tunnel must be set up between the ITSS-Rs and a firewall with IPv6 connectivity, as indicated in paragraph 6.

The TLS tunnels must follow the recommendations specified in:

- The RFC 4492 of April 2016 : <https://tools.ietf.org/html/draft-ietf-tls-tls13-09>

When the OBUs have a 3G/4G access, they can communicate by directly addressing the IPv4 or IPv6 address of the PKI server.

### 5.3 Positioning of firewalls in the architecture

Traffic filtering must be implemented in the tunnel to prevent all IPv6 traffic from being authorised. The ITSS-R must not become an open access point to the Internet.

When there is no firewall between field access and the traffic operator's equipment, just a routing point, a firewall will have to be deployed in the scoop@F project.

This will be done in order to prevent road operator's equipments from being accessible from vehicles..



The ITSS-Rs have an IPv4 interface on the road operator's network, in a dedicated VLAN, just like the other equipment : VMS, cameras, etc. Only the flows between this equipment and the Scoop servers or to the broker tunnel are authorised in the firewall.

## 5.4 Configuration of road-side equipment

The road-side equipment implements at least the following services: TLS tunnel set up, dual stack IPv4/IPv6 and DNS.

The road-side equipment will be IPv6 routers for the OBUs. Their link-local address is found in the range fe80 ::/64.

As indicated in the deliverable 2.4.4.8 §5.2 IPv6 Address, the IPv6 address of road-side equipment will be done via EUI-64.

As indicated in the draft IETF [<https://tools.ietf.org/html/draft-petrescu-ipv6-over-80211p-03#section-5.5>] and pursuant to the RFC 6275, the routers will emit unsolicited multicast Router Advertisements every 0.1 seconds.

They will use the following flags:

- A=1: the vehicle can configure its IPv6 address alone
  - M=0: the vehicle does not solicit the DHCP server to obtain its IPv6 address
- and a global-unicast 2000::/3 type address range corresponding to the local network.

The RDNSS option is used to give the DNS' IPv6 address.

The DNSv6 server will be carried either by the ITSS-R or by a Scoop platform server. It will respond in particular to queries requesting the IPv6 address of the PKI servers.

The tunnels have only to be set up for the queries from OBUs to the PKI servers. The OBUs' logs are recovered by the ITSS-Rs in IPv6. The ITSS-R returns then in IPv4 to the log server.

## 5.5 Configuration of vehicles

The vehicle has a system to change the MAC address regularly in order to protect its anonymity. Therefore, it is possible to use EUI-64 to define its IPv6 address.

The equipment does not need to solicit the router too often, since the router will frequently emit "unsolicited multicast RAs."

It will use Optimistic DAD as authorised by the norm ISO 21210.

## 5.6 Recap of exchanges for IPv6

1. A vehicle appears in the range of the 802.11p radio field of an ITSS-R (road-side unit). It has already a link-local type IPv6 address on its interface;
2. It sends an RS (Router Solicitation) query or receives an "unsolicited multicast RA"
3. The road-side equipment responds by the RA query message described above and/or emits an "unsolicited multicast RA" frame;
4. The vehicle records the router's address as gateway and assigns itself an address from the IPv6 range given by the router and records the DNS' address;
5. It makes a DAD query (optimistic DAD);
6. If the DNSv6 server is in the vehicle's local network:
  1. The vehicle makes a Neighbour Solicitation query to know the MAC address of the DNSv6 server;
  2. The DNS server responds to it with a Neighbour Advertisement query;
  7. Otherwise the DNS query goes through the router.
8. The vehicle solicits the DNS service to know the PKI's IPv6 addresses.
9. The vehicle transmits the queries to the PKI server and transmits its logs in IPv6 to the ITSS-R.
10. The router recovers the network traffic and uses its TMS side dual stack IPv6-IPv4 to re-encapsulate the IPv6 traffic and make it transit on an IPv4 network. The TLS tunnels between the router and the firewall terminating the tunnel are set up permanently.

The ITSS-R only sets up the TLS tunnel for the OBUs' PKI queries. The logs are transmitted to the road operator's Scoop servers in IPv4.

## 5.7 Additional securing

The following system can be implemented by the road operators to improve the security:

- Implement a service that verifies that the Router Advertisement and/or Neighbour Advertisement queries are not emitted wrongfully to spoof the MAC and/or IPv6 addresses of the services present (routing, DHCP, DNS or other). In case of detection, an alert is uploaded to the PKI servers. The rafixd and the RFC6105 service can be used to protect oneself. Implementation of this service remains delicate as shown by CVE-2011-2395.

## 5.8 Acquisition

The Scoop project must purchase a block of IPv6 addresses for each ITSS-R. To ensure the future, 16 million blocks of IPv6 addresses should be reserved, namely one /40.

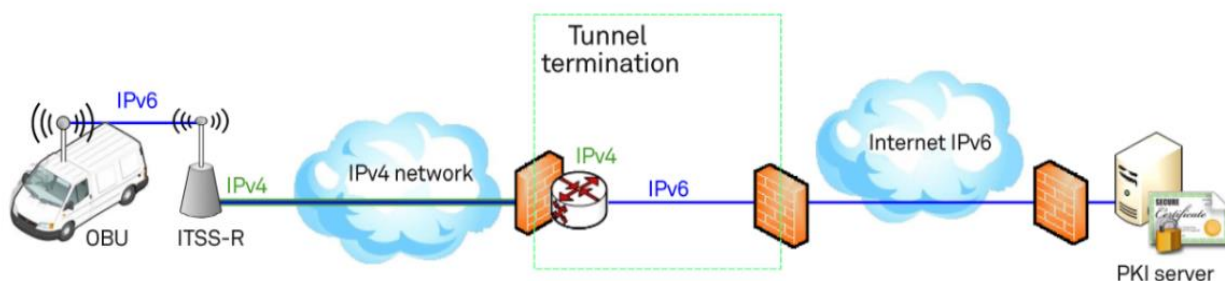
## 6. Implementation of TLS tunnels

### 6.1 Principle

TLS tunnels allow communications between IPv6 machines through an IPv4 network and the partitioning of this traffic from the rest of the road operator's network.

### 6.2 Filtering

Filtering must be implemented within a tunnel so the OBUs can exchange with the PKI without the ITSS-Rs becoming an open Internet access point:



*Illustration 9: Schematic diagram of the tunnel's termination*

The filtering rules must be the following:

- for the IPv4 firewall, the only flows authorised are those related to the TLS tunnel
- for the IPv6 firewall, the only flows authorised are: IPv6 from the OBUs to the PKI servers and for the necessary protocols to exchange certificates.

### 6.3 Sizing

The tunnel's termination will initially be sized for 300 tunnels.

### 6.4 Positioning of the tunnel's termination

The tunnel's termination will be positioned as a priority at a hosting company, or alternatively at a road operator.

## 7. Conclusions

### 7.1 Choice between IPv4 and IPv6

The following items have been taken into account in the choice between an architecture prioritising IPv4 or IPv6:

- IPv6 will in any case be necessary for the communications with the vehicles, because IPv4 is not specified for G5 communications.
- Prioritising IPv6 implies ramping up system administrators' competence on this protocol.
- Prioritising IPv6 will allow homogeneous IP addressing between the different Scoop@F systems and avoid having some machines in IPv4 and others in IPv6.
- IPv6 makes it possible to be free of existing IPv4 addressing plan constraints (already restricted for some road operators)

Ultimately, the choice is decided on the set up of TLS tunnels to cross through the IPv4 networks. The TLS technology has the advantage of already being mastered by the IPv4 network administrators, while the IPv6 technologies like 6rd or DSMip have the advantage of pushing the administrators towards the IPv6 world where the Scoop project is headed.

The architecture described gives priority to IPv4 within the road operators' networks for the 1st wave of Scoop. IPv6 will be reconsidered as part of the new architecture for the 2nd wave.

### 7.2 Positioning of the tunnel's termination

The TLS tunnel termination task will be provided by a hosting company.

### 7.3 Operational rollout

In the rollout, the road operators will ensure:

- That their equipments comply with the recommendations above
- That the general architecture schema is adapted to their network architecture
- The latency time of each phase