EU-MIDT

Card Issuing and Networking Committee

EU-MIDT/CINC/030-2005

TACHOnet Business Global Analyse

PREPARED BY: Yves HARDY
DATE: 31/01/2006
EU-MIDT CINC – 030-2005

REF : EU-MIDT/CINC/030-2005

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	Yves HARDY	European Commission	31/01/2006
CHECKED BY	Thierry GRANTURCO	Granturco & Partners – MIDT	31/01/2006
APPROVED BY	Marie-Christine BONNAMOUR	Cybele – MIDT Secretariat	31/01/2006
ISSUED BY	Secretariat	MIDT	31/01/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

EUROPEAN COMMISSION
Energy & Transport Directorate General

Unit : ITS Galileo

DG TREN

TACHOnet

Global Business Analysis

01_30

30.01.2006

Document Approval

	NAME	DATE	SIGNATURE
Prepared by:	F. Silvestre	22.01.2003	
Checked by:	F. Dugardin	18.03.2003	
Quality control by:	Ch. Timmermans	18.03.2003	
Approved by:	Y. Hardy	21.03.2003	

Distribution List

COMPANY	NAME	FUNCTION	FOR INFO / APPROVAL
DG TREN	Y. Hardy	Project Manager	Approval
DG TREN	L. Huberts	Porject Owner	Info

Change Control History

VERSION	DATE	AUTHOR	DESCRIPTION	PARAGRAPHS
00_01	23.01.2001	F. Silvestre	1st internal draft	
01_00	26.09.2001	F. Silvestre	1st external version	
01_01	17.05.2002	F. Silvestre	Official version – Feasibility Study	
01_10	10.11.2002	F. Silvestre	TCN 2nd Phase – 1st draft	
01_11	22.01.2003	F. Silvestre	TCN 2nd Phase – 2nd draft	
01_20	21.03.2003	F. Silvestre	TCN 2nd Phase – Official release	
01_30	30.01.2006	Y. Hardy	Insertion of the TACHOnet management procedure	See Annex

Document information

CREATION DATE:	22.01.2003
FILENAME:	TCN-GBA_01-30_EN.doc
LOCATION:	
NUMBER OF PAGES:	119

TABLE OF CONTENTS

Introduction

Purpose of the Global Business Analysis

In order to be able to suggest a system to a customer, one should understand the customer's business by performing a Global Business Analysis. This activity aims at formalizing the user requirements at both of functional and non-functional level, and will allow to verify the understanding of the business and to identify what is expected from Getronics (i.e. detail the scope of intervention).

By formally establishing the business by means of a modelling approach, one is compelled to think about business concepts and precisely define them. One is automatically confronted with inconsistencies in the understanding of the issue and differences in interpretation between domain experts and IT staff. The analysis documents the existing business situation and the target environment, including the requirements for a transition path and defines the set of use cases that describe the business situation. Modelling the business helps discovering the business tasks that an application would support. Use cases will then be derived from this business model.

The Global Business Analysis outputs two models: the Business Object Model and the (Enhanced) Use Case Model. These models represent what the customer expects from the application. Therefore it is very important to use a customer oriented vocabulary when naming and describing objects.

Scope of the Project

The current phase of the TACHOnet project aims at carrying out a detailed analysis & design which will :

- Take into account the legal and operational framework applicable for such interchange system (business needs, application features, security aspects, network infrastructure)
- Take into account the user requirements which current list is given below ("requirements" chapter) but obviously subject to be extended during the study in close collaboration with DG TREN and Member States Representatives (Task Force 2 from Card Issuing Working Group).
- Take into account the results of the feasibility study.

References

The present document makes references to the following documents:

- [1] TACHOnet Analysis & Design: Technical Annex
- [2] Council Regulation (EC) N° 2135/98
- [3] Annex IB – Chapter IV – Constructions and Functional Requirements for Tachograph Cards
- [4] TACHOnet Software Architecture Document
- [5] Card Issuing Working Group – General Report – URBA 2000
- [6] Access to some data through Tachonet by the enforcement officers during road side checks - SNRA/WG1/TF1/005 – Th. Granturco – 18-Oct-02
- [7] TACHOnet XML Messaging Reference Guide – Version 1.0
- [8] Note of the meeting to discuss TACHOnet/Card issuing – 25-Feb-03

Continued on next page

Introduction, Continued

Structure of the document

The first chapter describes the legal framework and the context of work. The second chapter identifies the different functional and non-functional requirements. A third chapter analyses the business processes related to card issuing in order to find out which TACHOnet functionalities are needed, how, when and where. The fourth chapter describes the Business Object Model in terms of class diagrams and classes description. The fifth chapter describes the Use-Case model by listing and explaining the different actors and use cases identified from the requirements and the business processes.

Chapter 1: Context

Overview

Introduction

This chapter sums up the legal framework and context of work surrounding the TACHOnet project.

Contents

This chapter contains the following topics.

Legal framework

Council Regulations

Council Regulation (EEC) n° 3821/85 provides for the installation and use of in vehicle recording equipment (the so-called « tachograph ») for the enforcement of driving hours of professional drivers in the field of road transport (goods and passengers).

The aim of that regulation is twofold :

- to ensure fair competition between drivers, hauliers and also with the other transport modes
- to enhance road safety by avoiding driver's fatigue and by controlling compliance with the legislation on speed limiters

The regulation has been amended by Council Regulation (EC) n° 2135/98 which introduced a new digital recording equipment and personal smart cards for drivers. The driver card allows for the identification of the drivers when they start their journey and for the recording of their activities.

A key element of the new regulation is to make sure that a driver holds only one card.

The issue of cards is the competence of the individual Member State where drivers have their normal residence.

The competent national authority should be able to check the uniqueness of issue by its own administration of a card to a particular driver, but such a check should also take place with the authorities of the other Member States to avoid a driver holding cards from several Member States.

In practice, this would be difficult, time consuming and bureaucratic without an appropriate telematic network between the national authorities.

Continued on next page

Legal framework, Continued

Legal requirements for exchanging information

• Council Regulation n°3821/85 Art. 19.2§3 :

- « Member States shall assist each other in applying this Regulation and in checking compliance therewith.

- Within the framework of this mutual assistance the competent authorities of the Member States shall regularly send one another all available information concerning :

. breaches of this regulation committed by non-residents and any penalties imposed for such breaches,

. penalties imposed by a Member State on its residents for such breaches committed in other Member States. »

• Council Regulation n°2135/98 Art. 1 :

- « The competent authorities of the issuing Member State shall, as far as this can be done, ensure that the applicant does not already hold a valid driver card ; » Art .1.7.b).(d)

- « … The authority issuing the card shall maintain a register of lost, stolen or defective cards » Art.1.5.a) 3rd §

- « Loss of the driver card must be reported … to the competent authorities of the State that issued it and to the competent authorities of the Member State of normal residence where they are different. » Art.1.9.b)2nd §

- « Where the authorities of the Member State in which the driver has his normal residence are different from those which issued his card and where the latter are requested to renew, replace or exchange the driver card, they shall inform the authorities which issued the old card of the precise reasons for its renewal, replacement or exchange; » Art.1.9.last §

Context of Work

Important characteristics

- Decision No 1720/1999/EC of the European Parliament and of the Council of 12 July 1999 adopted a series of actions and measures in order to ensure interoperability of and access to trans-European networks for the electronic interchange of data between administration (IDA).
- The TESTA-II action of IDA programme is currently interconnecting a network between the National administrations of the Member States and the European Institutions. This network facilities will be used as a mandatory service for the future application.
- The future application will be based on an interconnection/message process between the Member States. No central european database being the consolidation of the Member State data will exist. A potential central application will not be necessarily hosted by the European Commission Data Centre. It could be hosted by complementary services available on TESTA-II network.
- A certain number of already available commercial software products could probably perform the tasks requested with some limited adaptation. This kind of option should be evaluated in priority.
- Most of the data transmitted contain personal information. Despite the fact that the TESTA-II network is a private network not connected to the Internet, strong and reliable measures have to be taken at application level to ensure the confidentiality, security and integrity of the data transmitted.

Chapter 2: Requirements

Overview

Introduction

This chapter describes the different requirements (functional and non-functional).

Contents

This chapter contains the following topics.

Types of Requirements

Definition

A **requirement** is defined as "a condition or capability to which a system must conform".

Functional requirements specify actions that a system must be able to perform, without taking physical constraints into consideration. These are often best described in a use-case model and in use cases. Functional requirements thus specify the input and output behaviour of a system.

Requirements that are not functional are sometimes called **non-functional requirements**. Many requirements are non-functional, and describe only attributes of the system or attributes of the system environment.

FURPS+

There are a many different kinds of requirements. One way of categorizing them is described as the **FURPS+** model [GRA92], using the acronym FURPS to describe the major categories of requirements with subcategories as shown below.

- **F**unctionality,
- **U**sability,
- **R**eliability,
- **P**erformance and
- **S**upportability

The "+" in FURPS+ helps you to also remember to also include such requirements as

- design constraints,
- implementation requirements,
- interface requirements and
- physical requirements.

Functionality (FUN)

Functional requirements may include:

- feature sets,
- capabilities, and
- security.

Usability (USA)

Usability requirements may include such sub-categories as:

- human factors,
- aesthetics,
- consistency in the user interface,
- online and context-sensitive help,
- wizards and agents,
- user documentation, and
- training materials.

Continued on next page

Types of Requirements, Continued

Reliability (REL)

Reliability requirements to be considered are:

- frequency / severity of failure,
- recoverability,
- predictability,
- accuracy, and
- mean time between failure (MTBF).

Performance (PER)

A performance requirement imposes conditions on functional requirements. For example, for a given action, it may specify performance parameters for:

- speed,
- efficiency,
- availability,
- accuracy,
- throughput,
- response time,
- recovery time, or
- resource usage.

Supportability (SUP)

Supportability requirements may include:

- testability,
- extensibility,
- adaptability,
- maintainability,
- compatibility,
- configurability,
- serviceability,
- installability, or
- localizability (internationalization).

Design Requirement (DES)

A design requirement, often called a **design constraint**, specifies or constrains the design of a system.

Implementation Requirement (IMP)

An implementation requirement specifies or constrains the coding or construction of a system. Examples are:

- required standards,
- implementation languages,
- policies for database integrity,
- resource limits, and
- operation environments.

Continued on next page

Types of Requirements, Continued

Interface Requirement (INT)

An interface requirement specifies

- an external item with which a system must interact, or
- constraints on formats, timings, or other factors used by such an interaction.

Physical Requirement (HAR)

A physical requirement specifies a physical characteristic that a system must possess; for example,

- material,
- shape,
- size, and
- weight.

This type of requirement can be used to represent hardware requirements, such as

- the physical network configurations required

List of Functional Requirements

Introduction

Functional requirements specify actions that a system must be able to perform, without taking physical constraints into consideration. Functional requirements thus specify the input and output behaviour of a system.

A list of these functional requirements is given below with an identification and a short description for each of them.

These functional requirements are best described once translated into use cases (see Use Case Model chapter).

List of functional requirements

Each identified functional requirement is assigned a unique key "**FUN-*nn***" where ***nn*** is a sequence number identifying the functional requirement. The table hereafter lists all the functional requirements :

Functional Requirement Id	Description
FUN-01	The system must allow a member of the network to send requests to a particular or all the other members about possible delivery of a driver's smart card to a similar person.
FUN-02	The system must allow a member of the network to send a bulk request on all or a large part of its driver's smart card holders to a particular or all members of the network.
FUN-03	The system must allow a member to do statistics on messages issued and received from/to his system.
FUN-04	The system must provide automatic reply to the sender of the request through the use of a standard interface to the Members systems.
FUN-05	The system must track the workflow between senders and related replies.
FUN-06	The system must be able, in accordance with the rules on delays for each transaction, to automatically transmit alert messages to senders/replier/administrator when, f.i. a constraint on delay for reply is not fulfilled.
FUN-07	The system must allow the administrator to extract statistics of use, standard delay of reply by member/period, percentage of unsuccessful transaction,... .
FUN-08	The system must provide the management of user rights and permissions.
FUN-09	The system must be able to define and manage various type of messages already in the driver's smart card holder like pre-delivery check, stolen/lost cards, renewals, exchanges and duplicates.
FUN-10	The system must be able to include new members in the network through simple administrative tasks.

Continued on next page

List of Functional Requirements, Continued

List of functional requirements (continued)

Functional Requirement Id	Description
FUN-11	The system must be highly automatic to relieve the users of as many repetitive and tedious tasks as possible.
FUN-12	The system must provide at application level a full security (~~including non repudiation~~) and encryption policy compatible with the level of security required in such situation.
FUN-13	~~The system must guarantee that none of the Member of the network , including the administrator , is technically able to re-construct a consolidated European database through the use of the messages exchanged~~. The system must be such that none of the Member States of the network, including the administrator, re-construct a consolidated European database.
FUN-14	The system must allow a Member State (through its Card Issuing Authority) to ask for the status of card (lost, stolen,…) to the corresponding Card Issuing Authority of the Member State having issued the card.
FUN-15	The system must allow a Member State (through its Card Issuing Authority) to send card status modification requests (lost, stolen,…) to the corresponding Card Issuing Authority of the Member State having issued the card.
FUN-16	The system must allow enforcement authorities (through its Card Issuing Authority) to ask for driver's card status (based on either card number + issuing Member State code or driver's surname, first names, date of birth and issuing Member State code) to the corresponding Card Issuing Authority of the Member State having issued the card.
FUN-17	The system must allow enforcement authorities (through its Card Issuing Authority) to ask for workshop card status (based on workshop card number + issuing Member State code) to the corresponding Card Issuing Authority of the Member State having issued the card.

List of Non-functional Requirements

Introduction

Non-functional requirements describe only attributes of the system or attributes of the system environment.

Each identified non-functional requirement is assigned a unique key "**XXX-*nn***" where ***XXX*** identifies the type of requirement (e.g. PER for performance requirement) and ***nn*** is a sequence number identifying the non-functional requirement.

Usability requirements

The table hereafter lists all the non-functional "usability" requirements :

Usability Requirement Id	Description
USA-01	The system must guide users through an interface based on end user concepts.
USA-02	The system must be easy to learn and does not obstruct the thematic understanding of the users.
USA-03	The system must make it easy to correct mistakes.

Reliability requirements

The table hereafter lists all the non-functional "reliability" requirements:

Reliability Requirement Id	Description
REL-01	The system is to be designed as a robust and dependable operational system which is tolerant to operator errors and which will recover cleanly from power cuts or other disasters.
REL-02	The system must function reliably, with few or no interruptions in its first operational year and fewer still thereafter.
REL-03	The system must give stable and reproducible results.

Continued on next page

List of Non-functional Requirements, Continued

Performance requirements

The table hereafter lists all the non-functional "performance" requirements:

Performance Requirement Id	Description
PER-01	~~The system should be able to cover more than one contact point per country depending on the administrative organisation adopted by each country and able to work in a multi hierarchical environment~~. This is no longer the case since everybody agrees upon having a single point of contact per Member State (even though the Member State is organized with several Card Issuing Authorities – up to the Member State to manage its own organisation).
PER-02	There will be no restriction in time or place for the use of the software built from the specifications produced under this contract.
PER-03	The system must be able to establish and keep the dialog with the Members systems despite the various technical environments and technologies used on their sites.
PER-04	The system will be designed so that background tasks can continue while the user performs foreground tasks.
PER-05	The system will be used 24x7 by operators under pressure to produce results rapidly. The system must respond rapidly to user requests irrespective of any background tasks. Such high-availability (24x7) is also required from the Member States systems to ensure acceptable response time (less than 1 minute) to enforcement authorities requests.

Supportability requirements

The table hereafter lists all the non-functional "supportability" requirements:

Supportability Requirement Id	Description
SUP-01	The system should be able to support other types of message structure to cover f.i. a future driving licence network and correlated activities.
SUP-02	The system must be maintainable and extensible.
SUP-03	The system must be designed so that it can migrate to upgraded hardware or new versions of the operating systems involved.
SUP-04	The system must be able to migrate to other type of network than the one proposed by TESTA-II.
SUP-05	The system must provide solutions/rules regarding data encoding problems such as supporting different character sets, name truncation rules, name matching in case of misspelling,...

Continued on next page

List of Non-functional Requirements, Continued

Design requirements

The table hereafter lists all the non-functional "design" requirements:

Design Requirement Id	Description
DES-01	The system must be designed and documented with the expectation that its operational lifetime will be many years.
DES-02	Each Member of this network will organise its data about smart card holders with no constraints or recommendations on operating system and/or technology used. The system will be able to dialog with these environments or specify a generic interface to dialog with the Member's applications.

Implementation requirements

The table hereafter lists all the non-functional "implementation" requirements:

Implementation Requirement Id	Description
IMP-01	-

Interface requirements

The table hereafter lists all the non-functional "interface" requirements:

Interface Requirement Id	Description
INT-01	The system must use the network facilities supplied by the TESTA-II network.
INT-02	The algorithms in the software will be based on existing techniques and no research will be required to develop new algorithms under this contract.
INT-03	Most of the functionality of the new software shall depend on pre-existing or commercially available software.

Physical requirements

The table hereafter lists all the non-functional "physical" requirements:

Physical Requirement Id	Description
HAR-01	-

Chapter 3: Analysis of the Business Processes

Overview

Introduction

In order to be able to suggest a system to a customer, one should understand the customer's business. Modelling the business helps discovering the business tasks that an application would support. Use cases will then be derived from this business model.

However, the goal of this chapter is not to describe in details the different processes related to the card issuing and the enforcers checks (this is not in the scope of the TACHOnet project anyway) but to identify which TACHOnet functionalities are needed and when within these processes.

Therefore, the outlined processes are to be read as examples and does not dictate how the Member States should handle tachograph card issuing.

Important:

The following decisions have been taken (and agreed) during the feasibility study:

- TACHOnet will consider the Member State as having a SPOC CIA (Single Point Of Contact Card Issuing Authority), even though the Member State is organized through multiple CIAs managing their tachograph cards data in a common central data store (it's up to the Member State to manage the one-to-many relationship).
- For performance reasons (to reduce the amount of messages exchanged), a request message (and its corresponding response message) could contain several ('n') requests (for several card ids/drivers) instead of a single one.
- Enforcement Authorities may have access to some TACHOnet services through their National Card Issuing Authority (it's under the Member State's responsibility to grant enforcers access to the TACHOnet system). From the TACHOnet point of view, enforcers are seen as a Member State (SPOC CIA).

Contents

This chapter contains the following topics.

Section 3.1 - Card Issuing & Enforcers Process Hierarchy

Introduction

Card issuing can be modelled as process groups, including processes, carried out by a Card Issuing Authority.

The enforcers needs will be modelled as process carried out by Enforcement Authorities.

Card Issuing Authority

A Card Issuing Authority (CIA) is an official organism competent for issuing and managing tachograph cards. A card Issuing Authority may issue and manage tachograph cards for the Member State it depends on but also for other Member States not willing to set up such organisation in their own country but willing to have it "outsourced" by another Member State.

A Member State may also have a single or several Card Issuing Authorities managing card issuing for his resident drivers. Nevertheless, it has been agreed that TACHOnet will consider the Member State as having a SPOC CIA (Single Point Of Contact Card Issuing Authority), even though the Member State is organized through multiple CIAs managing their tachograph cards data in a common central data store (it's up to the Member State to manage the one-to-many relationship).

Enforcement Authority

During road-side checks, the enforcers want to use TACHOnet to check either the status of a card (driver or workshop card) or whether a driver does hold a valid card (when the driver is unable to show his card because it has been presumably lost or stolen). In both cases, the enforcers want to get the same level of information, i.e. some card details (card number, status, address where it has been issued, issuing date, expiry date, last modification date), some driver/workshop details (surname, first names, birth date, place of birth, driving licence number). Please refer to [6] for more details.

Beside these functional requirements, high-availability (24x7) is also required from the central TACHOnet system and the Member States systems (e.g. to process a TACHOnet request asking for checking against their local database the valididty and status of a card) to ensure acceptable response time (less than 1 minute) to enforcement authorities requests.

It has been agreed that enforcers might have access to TACHOnet but through their local Card Issuing Authority, i.e. TACHOnet consider the Member State Card Issuing Authority as the SPOC (Single Point Of Contact). Therefore, it's the Member State responsibility to grant enforcers access to TACHOnet.

Continued on next page

Overview, Continued

Process Hierarchy Diagram

The different processes related to card issuing can be modelled as follows:

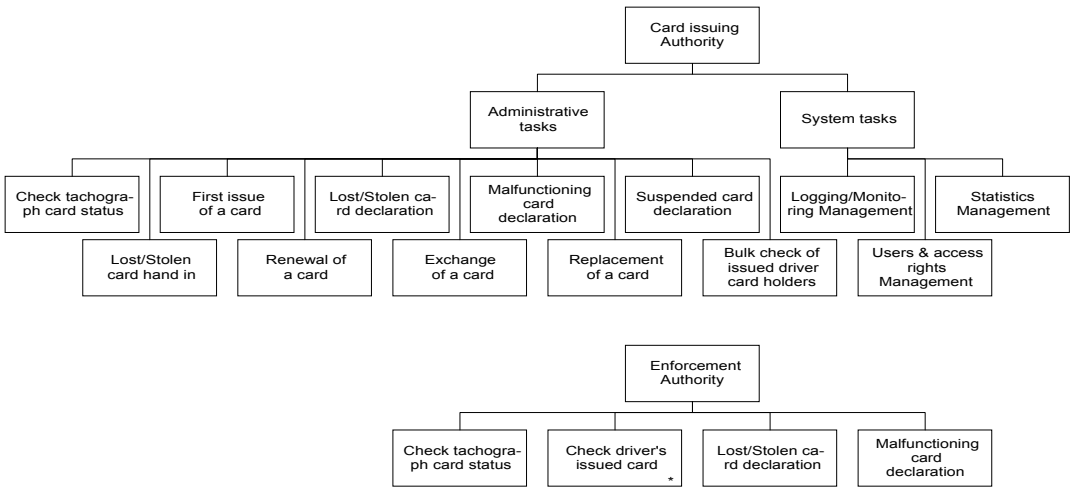


Figure 1 – Card Issuing Process Hierarchy

Administrative tasks

This process group gathers the different processes related to the administrative tasks carried out by an authorized clerk of the Card Issuing Authority. These can be summarized as follows:

Administrative tasks	Description
First issue of a card	This process deals with the issuing of a driver card to a new driver
Lost/stolen card declaration	This process deals with the declaration of a lost/stolen card
Malfunctioning card declaration	This process deals with the declaration of a malfunctioning card
Suspended card declaration	This process deals with the declaration of a suspended card
Lost/stolen card hand in	This process deals with the handing over of a found lost/stolen card
Renewal of a card	This process deals with the issue of a new tachograph card when an existing card reaches its expiry date, or is malfunctioning and has been returned to the issuing authority. Renewal always implies the certainty that two valid cards do not co-exist.

Continued on next page

Overview, Continued

Administrative tasks (continued)

Administrative tasks	Description
Exchange of a card	This process deals with the exchange of an existing valid driver card for an equivalent driver card for administrative reasons (e.g. the holder of the valid driver card has established his normal place of residence in another Member State).
Replacement of a card	This process deals with the issue of a tachograph card in replacement of an existing card, which has been declared lost, stolen or malfunctioning and has not been returned to the issuing authority. Replacement always implies a risk that two valid cards may co-exist.
Check tachograph card status	This process deals with the verification of the status of a tachograph card (driver or workshop) based on its card number.
Check driver's issued card	This process deals with the verification of whether a particular driver (based on his name, first names, date of birth,…) does actually hold a valid card. Such process will be carried out by the enforcers to check, during road-checks, when a driver is unable to show his card (pretending it's lost or stolen), that a driver does actually hold a valid card issued by a Member State.
Bulk check of issued cards	This process deals with the verification asked by a Member State that all or a large part of its driver card holders are not yet holder of another card in another country.

System tasks

This process group gathers the different processes related to the system tasks provided by the TACHOnet project. These tasks, carried out by authorized administrators, can be summarized as follows:

System tasks	Description
Users & access rights management	This process deals with the definition of the users having access to the TACHOnet functionalities along as their access rights to these functionalities.
Statistics Management	This process deals with the management of different statistics (e.g. usage,...) around TACHOnet activities.
Logging/Monitoring Management	This process deals with the management of different loggings around TACHOnet activities as long as the monitoring of the central system.

Section 3.2 - Administrative tasks

Overview

Introduction

This section analyses the different processes related to the administrative tasks carried out by an authorized clerk of the Card Issuing Authority.

Contents

This section contains the following topics.

First issue a card

Introduction

This process deals with the issuing of a driver card to a new driver, i.e. a driver who never asked yet for a driver card (and therefore doesn't hold any driver card).

Council Regulation (EC) N° 2135/98 mentions:

- *Art.14 §3(a)*: "The driver card shall be issued, at the request of the driver, by the competent authority of the Member State where the driver has his normal residence."
- *Art.14 §3(b)*: "Drivers shall give proof of their place of normal residence by any appropriate means, such as identity card or any other valid document."
- *Art.14 §3(c)*: "The competent authorities of the Member State issuing the driver card [...] may request any additional information or evidence."
- *Art.14 §3(d)*: "The competent authorities of the issuing Member State shall, as far as this can be done, ensure that the applicant does not already hold a valid driver card."
- *Art.14 §4(a)*: "[...]The driver card may not be valid for more than five years. The driver may hold one valid driver card only."
- *Art.14 §4(d)*: "Driver cards issued by Member States shall be mutually recognized.[...]"

Luxemburg agreement

During CIWG phase I, Member States have come to an agreement about the use of the driving license number. This agreement, called the "Luxemburg agreement", is described in the CIWG final report [5]. For what TACHOnet is concerns, it has been decided that a Member State issuing a card for a driver with a foreign driving license, should warn the Member State having issued the driving license that a tachograph card (giving its card number) has been issued using the corresponding driving license number.

Process description

As shown in Figure 2below, the issuing of a new card triggers processes and events among 3 different "entities":

- The *Card Issuing Authority* (CIA) issuing the card and asking for driver's issued cards verification,
- *TACHOnet* (providing central secure & reliable services for such verification),
- The different *Member States* performing the verification against their own data stores.

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Card Issuing Authorities* and *Member States* exchange information about tachograph cards. Therefore, the processes described for the *Card Issuing Authorities* and *Member States* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

Continued on next page

First issue a card, Continued

Process diagram

The issuing of a new card can be modelled as follows:

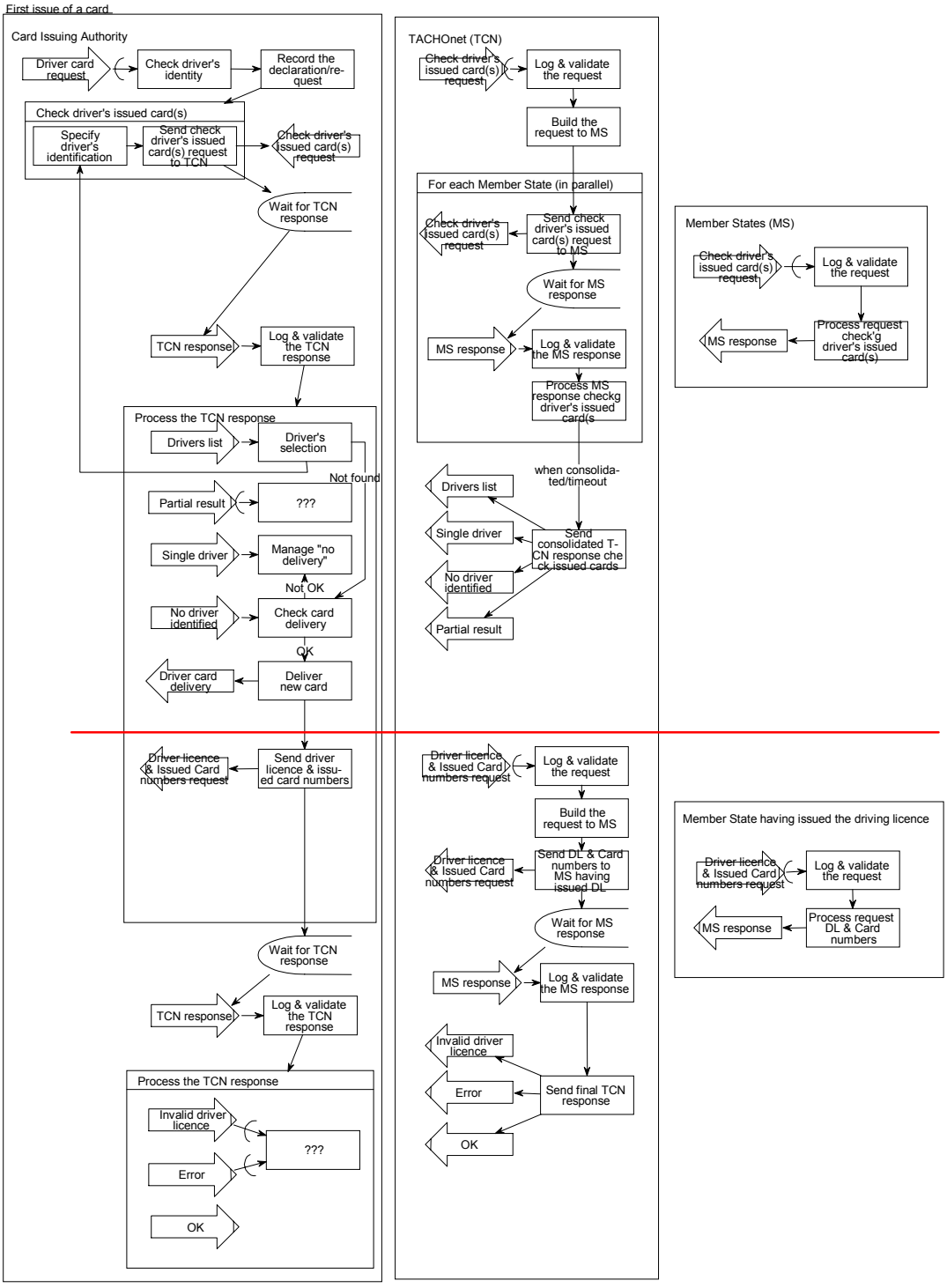


Figure 2 – "Issuing of a new card" process

Continued on next page

First issue a card, Continued

Process steps The issuing of a new card should follow more or less the following steps:

Step	Action
1	The CIA's clerk should first ask and verify the driver's identity by any appropriate means. The driver's driving license will be used.
2	When the driver is identified, the clerk should record the driver's request to prevent a driver from asking a driver card more than once in the same country or even in different countries at the same time.
3a	The clerk should then verify, via *TACHOnet*, that the driver doesn't hold yet any driver card or doesn't have any card request pending in any Member State connected to *TACHOnet* (including the one where the driver introduces his request) by sending a request to *TACHOnet* and waiting for its response (asynchronous).
3b	*TACHOnet* should then log and validate (syntactically) the request, send in parallel an equivalent request to the different *Member States*, wait for the response (asynchronous) from each of these *Member States*, process the responses and send a consolidated response back to the initiator of the request.
3c	The different *Member States* should be ready to receive a request for checking driver's issued cards against their own data stores. They should process the request, send back the response to *TACHOnet*.
4a	If the TACHOnet result is a single driver (matching the given driver identification criterias) holding yet a card or having a request pending, the clerk should refuse the request (and follow the procedure for fraud attempt). Procedure to be discussed by TF1 [8].
4b	If the TACHOnet result mentions the driver has not been identified in any Member States connected to TACHOnet, the clerk may decide to accept and deliver the card (or perform a new check based on the driver's driving license number – step 3a ?)
4c	If the TACHOnet result is a partial result, meaning at least one Member State didn't answer in time (for any reason such as network problem, system unavailable,...), **what should the clerk do? [8]**
5a	If the card is delivered to the driver AND if the driving license used to apply for the card is a foreign one, the CIA's clerk should then, via TACHOnet, warn the Member State having issued the driving license that a tachograph card (giving its number) has been delivered using the driving license number, by sending a request to *TACHOnet* and waiting for its response (asynchronous).
5b	*TACHOnet* should then log and validate (syntactically) the request, send an equivalent request to the *Member State* having issued the driving license number, wait for the response (asynchronous) from this *Member State*, process the response and send the response back to the initiator of the request.

Continued on next page

First issue a card, Continued

Process steps (continued)

Step	Action
6	If the TACHOnet result (in fact the response from the Member State having issued the driving license) mentions the driving license number doesn't exist or that an error occurred (timeout,…), **what should the clerk do? [8]**

Anyway, the clerk's the judge: if he has any doubt about the validity of a request, he should proceed to a manual intervention (e.g. sending a fax,...).

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for checking whether a driver (based on driver's identification criteria's – to be defined later) does already hold a card or have a request pending somewhere.
2	Sending (and logging) an equivalent request to the different Member States connected to TACHOnet
3	Receiving, logging and validating responses from these Member States
4	Consolidating the different responses into a single one
5	Sending (and logging) the consolidated response to the initiator of the request
6	Receiving, logging, validating a request for warning the Member State having issued a driving license used for issuing a card that a card (giving its number) has been issued using that driving license number.
7	Sending (and logging) an equivalent request to the Member State having issued the driving license number.
8	Receiving, logging and validating response from this Member State.
9	Sending (and logging) the received response to the initiator of the request.
10	Receiving, logging and validating a receipt (ACK or NAK) from the initiator of the request

These identified services (along as requests, responses and receipts data structures) will be described in more details when translated into use cases in the Use-Case Model.

Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Continued on next page

First issue a card, Continued

Card request status

The card request (managed by *Card Issuing Authority*) should be encoded immediately after receipt by the administration in charge of processing the request and delivery. The request may have 2 status [8]:

- Application received
- Processed

From a TACHOnet point of view, what is important to know , when checking whether a driver does already hold a card, is whether a card has already been delivered to the driver or whether the driver is in the process of getting one (application has been submitted and is in progress).

Driver's identification in "check driver's issued cards" request message

The driver's identification criteria for checking driver's issued cards should be the following:

- Driver's surname,
- Driver's first names,
- Driver's birth date
- Driver's place of birth (optional)
- Driver's driving license number (optional for enforcers)

The driving license will be used as the official document to read the driver's details from. Unfortunately, the driver's driving license number cannot be used as reliable unique identification (even though it's required and stored when issuing a card) since a driver could hold more than one driving license (in different countries), driving licenses have an expiration date in some countries (and should then be renewed with no guarantee of keeping the same number),... . Nevertheless, the driver's driving license number might be sent (optional) so that Member States willing to check the validity of the driving license number could do so.

Technical issues such as data encoding, name encoding rules, name matching algorithm will be analysed in details in [4].

Driver's identification in "check driver's issued cards" response message

The responses sent by the different *Member States* to the driver's issued cards request should include the following information (the returned information is the same one as in the "Check driver's issued card" process carried out by the enforcers) about the matched drivers (i.e. yet holding a driver card or having applied for it):

- Code of Member State having issued the card
- Driver's surname
- Driver's first names
- Driver's birth date
- Driver's birthplace (optional)
- Driver's driving license number + issued date + status (all optional)

First issue a card, Continued

Driver's identification in "check driver's issued cards" response message (continued)

- Card number
- Card status (valid, stolen, lost,…)
- Address where the card has been issued
- Issue date (date of 1st validity)
- Expiry date
- Last status modification date

The search against local data stores performed by the Member States must deal with potential driver name misspelling, truncation,... . Technical issues such as data encoding, name encoding rules, name matching algorithm will be analysed in details in [4].

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. These questions should be addressed at the beginning of the next phase (detailed analysis) of the TACHOnet project.

Id	Question	Addressed to
1	Should TACHOnet also deal with the verification of other tachograph cards than the driver card (company, control, workshop)? If so, how can we identify the card holder (company, control authority, workshop)? What kind of information should be returned (company info + list of issued cards,...)? **Answer**: Only the driver card and the workshop card.	CIWG TF1
2	In how many days max. should the card issuing authority deliver the card to the applicant driver? What's the timeout value (minutes, hours,…) for processing this request? **Answer**: To be discussed by TF1	CIWG TF1
3	What's the estimation of the number of to-be-delivered tachograph cards (per type) per Member State? **Answer**: A rough estimation gives about 1600000 issued cards per year. That gives around 7000 to 15000 driver cards per day (all Member States included).	CIWG TF2

Continued on next page

First issue a card, Continued

Pending questions (continued)

Id	Question	Addressed to
4	What's the estimation of the number of transactions per day per Member State (taking into account peak period at the beginning)? **Answer**: A rough estimation gives about 1600000 issued cards per year. That gives around 7000 to 15000 driver cards per day (all Member States included).	CIWG TF2
5	Should TACHOnet be able to deal with MPOC CIAs within a Member State or could it assume to deal with a SPOC CIA per Member State? **Answer**: A SPOC CIA could be assumed.	DG-TREN
6	What should we do if the driving license used for card issuing has been issued by a foreign country not linked to TACHOnet? **Answer**: To be discussed by TF1	CIWG TF1
7	What if the Member State having issued the driving license answers the driving license is unknown? **Answer**: To be discussed by TF1	CIWG
8	Should TACHOnet provide a basic default "user interface" (e.g. web-based application) helping Member States (CIA or enforcers) to send requests to TACHOnet (e.g. fill in a web form) and view the results (e.g. a web form displaying the final results)? **Answer**: No. Only web services for computing the Phonex search keys and for US/ascii transliteration will be provided by TACHOnet.	Getronics

Continued on next page

First issue a card, Continued

Pending questions (continued)

Id	Question	Addressed to
9	Should TACHOnet perform latin-2-greek transliteration when sending the final response to the Greek CIA (from Latin-encoded responses)? Should TACHOnet perform greek-2-latin transliteration when sending the final response to a Latin CIA (from Greek-encoded response)? **Answer**: No. Only web services for computing the Phonex search keys and for Latin/Greek to US/ascii transliteration will be provided by TACHOnet. Up to the CIA to use it	CIWG TF1 Getronics

Lost/Stolen card declaration

Introduction

This process deals with the declaration of a lost or stolen card.

Council Regulation (EC) N° 2135/98 mentions:

- *Art.12 §1*: "If a card issued to an approved workshop or fitter [...] is stolen or lost, the authority shall supply a replacement card within five working days of receiving a detailed request to that effect."
- *Art.14 §4(a)*: "[...] The issuing authority shall keep records of issued, stolen, lost or defective cards for a period at least equivalent to their period of validity."
- *Art.14 §4(a)*: "[...] If the driver card is [...] lost or stolen, the authority shall supply a replacement card within five working days of receiving a detailed request to that effect."
- *Art.15 §1*: "[...] If the driver card is [...] lost or stolen, the driver shall apply within seven calendar days for its replacement to the competent authorities of the Member State in which he has his normal residence."
- *Art.16 §3*: "[...] Theft of the driver card shall be the subject of a formal declaration to the competent authorities of the State where the theft occurred. Loss of the driver card must be reported in a formal declaration to the competent authorities of the State that issued it and to the competent authorities of the Member State of normal residence where they are different."

Process description

As shown in Figure 3 below, the lost/stolen card declaration triggers processes and events among 3 different "entities":

- The *Member State where theft/loss occured* (declaring the theft/loss of the card),
- *TACHOnet* (providing central secure & reliable services for such declaration),
- The *Member State having issued the card* (recording the theft/loss of the card).

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Member State where theft/loss occured* and *Member State having issued the card* exchange information about tachograph cards. Therefore, the processes described for the *Member State where theft/loss occured* and *Member State having issued the card* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

According to [8], only theft should be notified via TACHOnet.

Continued on next page

Lost/Stolen card declaration, Continued

Process diagram

The declaration of a lost/stolen card can be modelled as follows:

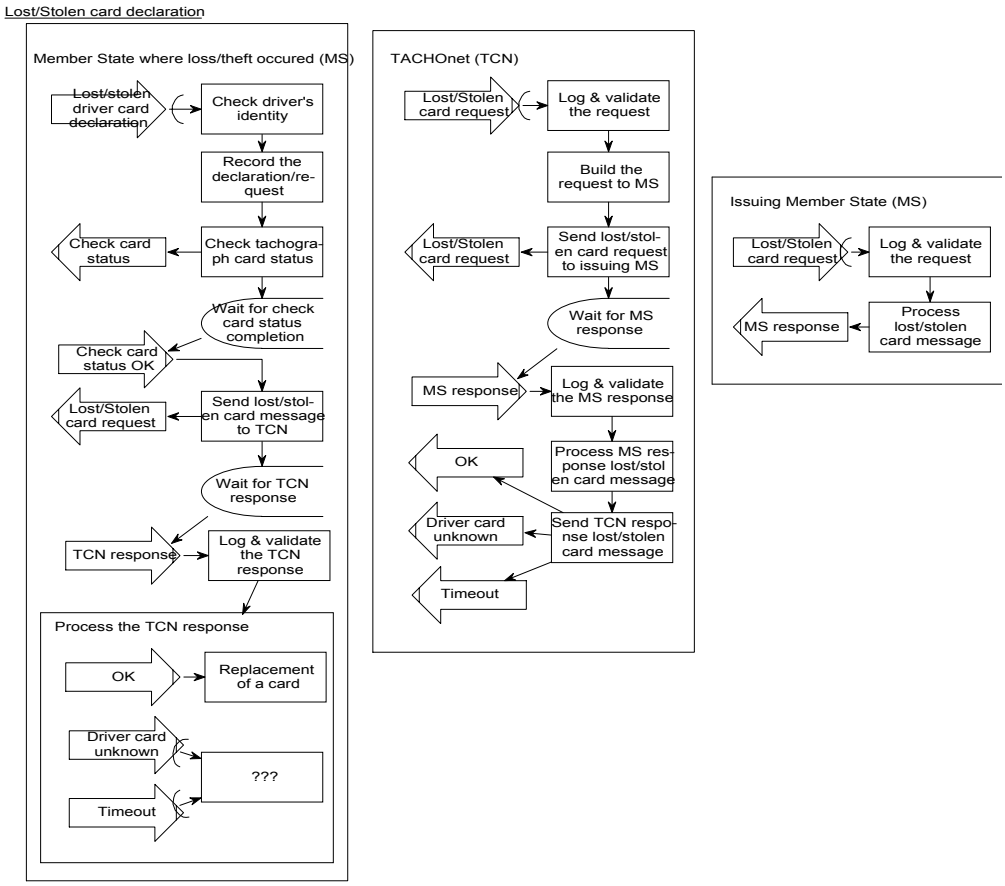


Figure 3 – "Lost/stolen card declaration" process

Process steps

The declaration of a lost/stolen card should follow more or less the following steps:

Step	Action
1	The clerk(or the enforcer) should first ask and verify the driver's identity by any appropriate means.
2	When the driver is identified, the clerk should record the details of the declaration (driver's identity, driver's card id, Member State having issued the card,...).
3	The clerk (or the enforcer) should then, via TACHOnet, check the status of the lost/stolen card by keying in its card number (see "Check tachograph card status" on page 56 for more details). This is required to allow the clerk visually check the details of the lost/stolen card prior to declaring it actually lost/stolen and then to avoid from mistakenly (e.g. typing error in card number) declaring lost/stolen another card.

Continued on next page

Lost/Stolen card declaration, Continued

Process steps (continued)

Step	Action
4a	The clerk should then, via *TACHOnet*, warn the Member State having issued the card that one of its issued card has been lost/stolen (so that the issuing authority shall keep records of it) by sending a request to *TACHOnet* and waiting for its response (asynchronous).
4b	*TACHOnet* should then log and validate (syntactically) the request, send an equivalent request to the *Member State having issued the card*, wait for the response (asynchronous) from the *Member State having issued the card*, process the response and send a consolidated response back to the initiator of the request.
4c	The *Member State having issued the card* should be ready to receive a request for processing lost/stolen card declaration against his own data store(s). It should process the request, send back the response to *TACHOnet*.
5a	If the result is positive, the driver should then proceed to the replacement of his driver's card (see "Replacement of a card" on page 55 for more details)
5b	If the result is negative (timeout or driver card unknown), **what should the clerk do?**

Identified TACHOnet service(s)

This process identifies several services that should be supplied by the TACHOnet network :

#	Services/Functions
1	Receiving, logging, validating a request for declaring a lost/stolen card
2	Sending (and logging) an equivalent request to the Member State having issued the card
3	Receiving, logging and validating response from the Member State having issued the card
4	Sending (and logging) the consolidated response to the initiator of the request

These identified services (along as requests and responses data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Continued on next page

Lost/Stolen card declaration, Continued

Request message

The message used for declaring lost/stolen cards should at least contain the following information:

- Code of the Member State having issued the card
- Lost/stolen card number
- Reason for declaring status modification

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF1 [8].

Id	Question	Addressed to
1	How should the clerk handle a “driver card id unknown” response?	CIWG TF1
2	How should the clerk handle a “timeout” (no response within time limit)?	CIWG TF1
3	What are the other types of response such a message could generate (e.g. driver card already mentioned as stolen,...)?	CIWG TF1
4	What if the driver does not remember his lost/stolen driver card number?	CIWG TF1
5	How to protect against “false” declarations (e.g. an ill-disposed person might abusively declare some drivers having lost their cards to be harmful to a company)?	CIWG TF1

Malfunctioning card declaration

Introduction

This process deals with the declaration of a malfunctioning card.

Council Regulation (EC) N° 2135/98 mentions:

- *Art.12 §1*: "If a card issued to an approved workshop or fitter [...] is damaged, malfunctions [...] , the authority shall supply a replacement card within five working days of receiving a detailed request to that effect."
- *Art.14 §4(a)*: "[...] The issuing authority shall keep records of issued, stolen, lost or defective cards for a period at least equivalent to their period of validity."
- *Art.14 §4(a)*: "[...] If the driver card is damaged, malfunctions [...], the authority shall supply a replacement card within five working days of receiving a detailed request to that effect."
- *Art.15 §1*: "[...] If the driver card is damaged, malfunctions [...], the driver shall apply within seven calendar days for its replacement to the competent authorities of the Member State in which he has his normal residence."
- *Art.16 §3*: "[...] If a driver card is damaged or if it malfunctions, the driver shall return it to the competent authority of the Member State in which he has his normal residence."

Process description

As shown in Figure 4 below, the malfunctioning card declaration triggers processes and events among 3 different "entities":

- The *Member State of driver's normal residence* (where the malfunctioning card declaration is made),
- *TACHOnet* (providing central secure & reliable services for such declaration),
- The *Member State having issued the card* (recording the malfunctioning card declaration).

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Member State of driver's normal residence* and *Member State having issued the card* exchange information about tachograph cards. Therefore, the processes described for the *Member State of driver's normal residence* and *Member State having issued the card* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

Malfunctioning card declaration, Continued

Process diagram

The declaration of a Malfunctioning card can be modelled as follows:

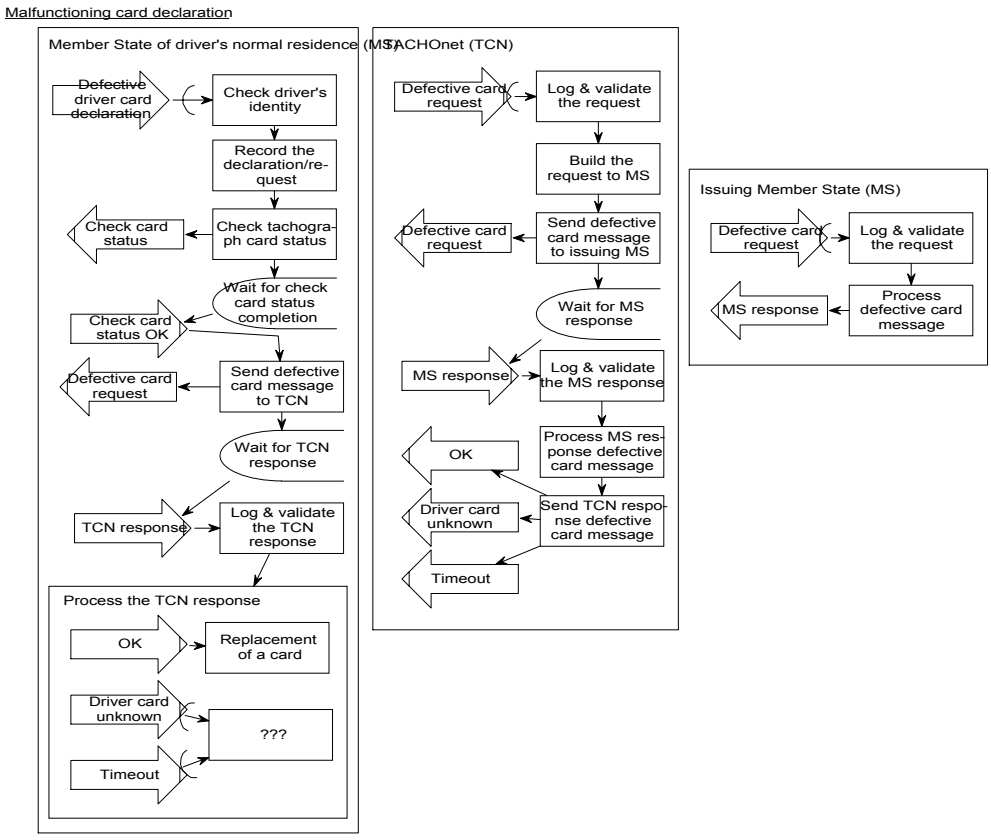


Figure 4 – "Malfunctioning card declaration" process

Process steps

The declaration of a Malfunctioning card should follow more or less the following steps:

Step	Action
1	The clerk (or the enforcer) should first ask and verify the driver's identity by any appropriate means.
2	When the driver is identified, the clerk (or the enforcer) should record the details of the declaration (driver's identity, driver's card id, Member State having issued the card,...). The driver should also hand in his malfunctioning card to the clerk.

Continued on next page

Malfunctioning card declaration, Continued

Process steps (continued)

Step	Action
3	The clerk (or the enforcer) should then, via TACHOnet, check the status of the malfunctioning card by keying in its card number (see "Check tachograph card status" on page 56 for more details). This is required to allow the clerk (or the enforcer) visually check the details of the malfunctioning card prior to declaring it actually malfunctioning and then to avoid from mistakenly (e.g. typing error in card number) declaring malfunctioning another card. Moreover, such request will return the internal TACHOnet reference of the actual CIA having issued the card, which will be passed on in the next request to speed up the process.
4a	The clerk (or the enforcer) should then, via *TACHOnet*, warn the Member State having issued the card that one of its issued card has been identified as malfunctioning and returned (so that the issuing authority shall keep records of it) by sending a request to *TACHOnet* and waiting for its response (asynchronous).
4b	*TACHOnet* should then log and validate (syntactically) the request, send an equivalent request to the *Member State having issued the card*, wait for the response (asynchronous) from the *Member State having issued the card*, process the response and send a consolidated response back to the initiator of the request.
4c	The *Member State having issued the card* should be ready to receive a request for processing malfunctioning card declaration against his own data store(s). It should process the request, send back the response to *TACHOnet*.
5a	If the result is positive, the driver should then proceed to the replacement of his driver's card (see "Replacement of a card" on page 55 for more details)
5b	If the result is negative (timeout or driver card unknown), **what should the clerk do?**

Continued on next page

Malfunctioning card declaration, Continued

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for declaring a malfunctioning card
2	Sending (and logging) an equivalent request to the Member State having issued the card
3	Receiving, logging and validating response from the Member State having issued the card
4	Sending (and logging) the consolidated response to the initiator of the request

These identified services (along as requests and responses data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Request message

The message used for declaring malfunctioning cards should at least contain the following information:

- Code of the Member State having issued the card
- Malfunctioning card number
- Reason for declaring card status modification

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF1 [8].

Id	Question	Addressed to
1	How should the clerk handle a “driver card id unknown” response ?	CIWG TF1
2	How should the clerk handle a “timeout” (no response within time limit) ?	CIWG TF1
3	What are the other types of response such a message could generate (e.g. driver card already mentioned as stolen,...) ?	CIWG TF1
4	Should the driver proceed to a renewal or replacement?	CIWG TF1

Suspended card declaration

Introduction

This process deals with the declaration of a suspended card.

Council Regulation (EC) N° 2135/98 mentions:

- *Art.14 §4(c)*: "The driver card [...] may not be withdrawn or suspended [...] unless the competent authority of a Member State finds that the card has been falsified, or the driver is using a card of which he is not the holder, or that the card held has been obtained on the basis of false declarations and/or forged documents. If such a suspension or withdrawal measures are taken by a Member State other than the Member State of issue, the former shall return the card to the authorities of the Member State which issued it and shall indicate the reasons for returning it."

Process diagram

The declaration of a suspended card can be modelled as follows:

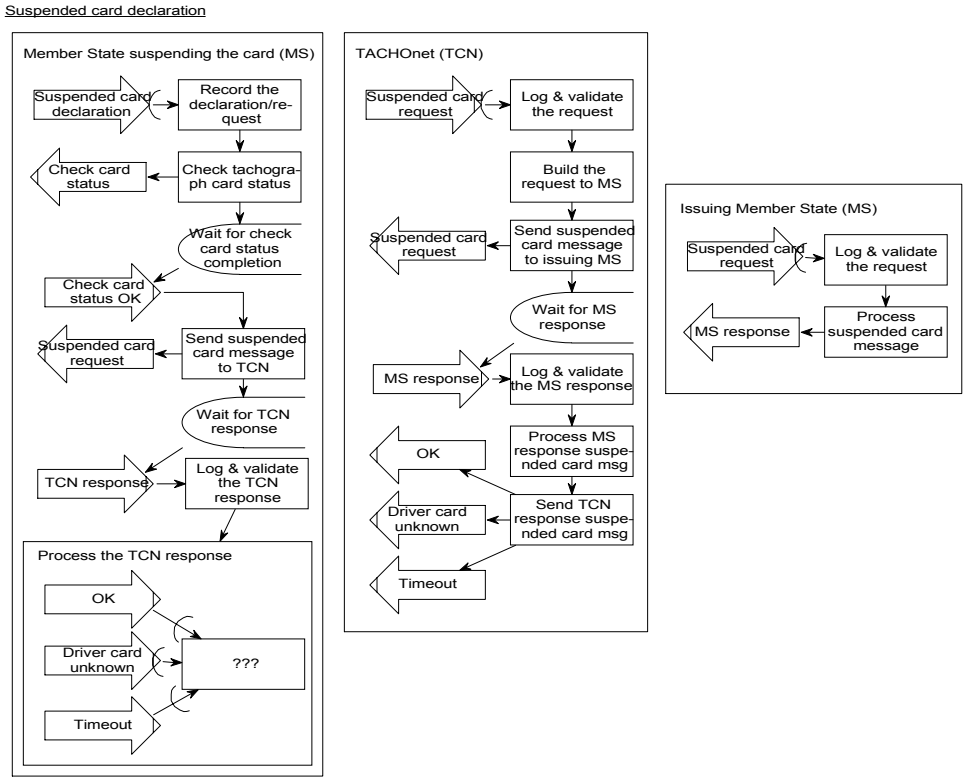


Figure 5 – "Suspended card declaration" process

Continued on next page

Suspended card declaration, Continued

Process description

As shown in Figure 5 above, the suspended card declaration triggers processes and events among 3 different "entities":

- The *Member State suspending the card* (where the suspended card declaration is made),
- *TACHOnet* (providing central secure & reliable services for such declaration),
- The *Member State having issued the card* (recording the suspended card declaration).

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Member State suspending the card* and *Member State having issued the card* exchange information about tachograph cards. Therefore, the processes described for the *Member State suspending the card* and *Member State having issued the card* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

According to [8], 'suspend' is when the card is temporarily taken from the driver e.g. whilst an investigation takes place, it could later be handed back to the driver. 'withdraw' is when the card is not returned to the driver, when the investigation is complete.

Process steps

The declaration of a suspended card should follow more or less the following steps:

Step	Action
1	A representative of the authority suspending the card (e.g. police officer,...) sends his driver card suspension request to the card issuing authority of his Member State. Then, the clerk should record the details of the declaration (requestor's identity, driver's identity, driver's card id, Member State having issued the card,...). The driver should also have handed in his driver card to the representative of the authority suspending it who, in turn, will hand it over to the clerk at the time of this declaration.
2	The clerk should then, via TACHOnet, check the status of the suspended card by keying in its card number (see "Check tachograph card status" on page 56 for more details). This is required to allow the clerk visually check the details of the suspended card prior to declaring it actually suspended and then to avoid from mistakenly (e.g. typing error in card number) declaring suspended another card. Moreover, such request will return the internal TACHOnet reference of the actual CIA having issued the card, which will be passed on in the next request to speed up the process.
3a	The clerk should then, via *TACHOnet*, warn the Member State having issued the card that one of its issued card has been suspended and for which reason (so that the issuing authority shall keep records of it) by sending a request to *TACHOnet* and waiting its response (asynchronous).

Continued on next page

Suspended card declaration, Continued

Process steps (continued)

Step	Action
3b	*TACHOnet* should then log and validate (syntactically) the request, send an equivalent request to the *Member State having issued the card*, wait for the response (asynchronous) from the *Member State having issued the card*, process the response and send a consolidated response back to the initiator of the request.
3c	The *Member State having issued the card* should be ready to receive a request for processing suspended card declaration against his own data store(s). It should process the request, send back the response to *TACHOnet*.
4a	If the result is positive, the clerk should archive the declaration.
4b	If the result is negative (timeout or driver card unknown), **what should the clerk do?**

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for declaring a suspended card
2	Sending (and logging) an equivalent request to the Member State having issued the card
3	Receiving, logging and validating response from the Member State having issued the card
4	Sending (and logging) the consolidated response to the initiator of the request

These identified services (along as requests and responses data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Continued on next page

Suspended card declaration, Continued

Request message

The message used for declaring suspended cards should at least contain the following information:

- Code of the Member State having issued the card
- Suspended card number
- Reason for declaring the suspension [see [8])

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF1 [8].

Id	Question	Addressed to
1	How should the clerk handle a “driver card id unknown” response ?	CIWG TF1
2	How should the clerk handle a “timeout” (no response within time limit) ?	CIWG TF1
3	What are the other types of response such a message could generate (e.g. driver card already mentioned as stolen,...) ?	CIWG TF1
4	Should the forger be recorded as such to avoid from issuing him a driver card later ?	CIWG TF1
5	Should the reason(s) of the suspension be listed in the message? If so, what’s the exhaustive list of suspension codes?	CIWG TF1

Lost/stolen card hand in

Introduction

This process deals with the handing over of a more likely lost/stolen card.

Process diagram

The handing over of a lost/stolen card can be modelled as follows:

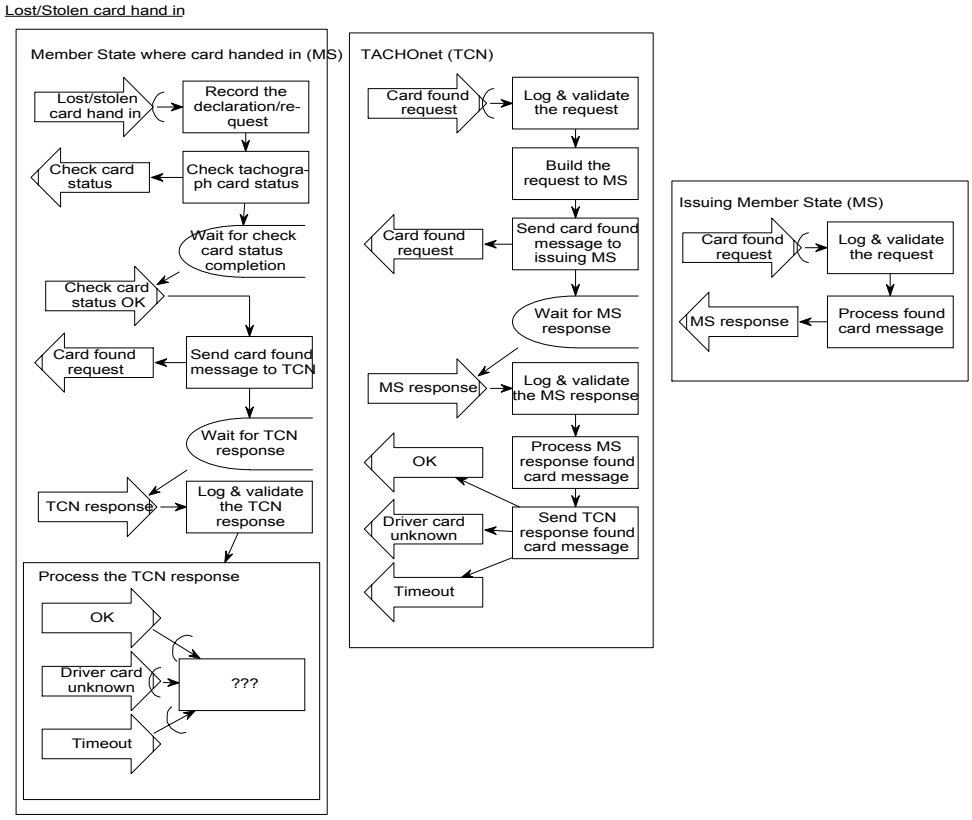


Figure 6 – "Lost/stolen card hand in" process

Continued on next page

Lost/stolen card hand in, Continued

Process description

As shown in Figure 6 above, the lost/stolen card hand in declaration triggers processes and events among 3 different "entities":

- The *Member State where the card's handed over* (where the suspended card declaration is made),
- *TACHOnet* (providing central secure & reliable services for such declaration),
- The *Member State having issued the card* (recording the lost/stolen card hand in declaration).

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Member State where the card's handed over* and *Member State having issued the card* exchange information about tachograph cards. Therefore, the processes described for the *Member State where the card's handed over* and *Member State having issued the card* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

According to [8], the status of the card will not change even though it has been handed in.

Process steps

The handing over of a lost/stolen card should follow more or less the following steps:

Step	Action
1	Someone brings back a driver card he found somewhere (more likely lost or stolen). The clerk should record the details of the declaration (driver's identity, driver's card id, Member State having issued the card,...). The clerk should also return the driver card to the Member State authority having issued the card.
2	The clerk should then, via TACHOnet, check the status of the card handed over by keying in its card number (see "Check tachograph card status" on page 56 for more details). This is required to allow the clerk visually check the details of the card prior to declaring it actually handed over and then to avoid from mistakenly (e.g. typing error in card number) declaring handed over another card. Moreover, such request will return the internal TACHOnet reference of the actual CIA having issued the card, which will be passed on in the next request to speed up the process.
3a	The clerk should then, via *TACHOnet*, warn the Member State having issued the card that one of its issued card has been found and for which reason (so that the issuing authority shall keep records of it) by sending a request to *TACHOnet* and waiting for its response (asynchronous).

Continued on next page

Lost/stolen card hand in, Continued

Process steps (continued)

Step	Action
3b	*TACHOnet* should then log and validate (syntactically) the request, send in parallel an equivalent request to the *Member State having issued the card*, wait for the response (asynchronous) from the *Member State having issued the card*, process the response and send a consolidated response back to the initiator of the request.
3c	The *Member State having issued the card* should be ready to receive a request for processing lost/stolen card hand in declaration against his own data store(s). It should process the request, send back the response to *TACHOnet*.
4a	If the result is positive, the clerk should archive the declaration.
4b	If the result is negative (timeout or driver card unknown), **what should the clerk do?**

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for declaring a lost/stolen card hand-in
2	Sending (and logging) an equivalent request to the Member State having issued the card
3	Receiving, logging and validating response from the Member State having issued the card
4	Sending (and logging) the consolidated response to the initiator of the request

These identified services (along as requests and responses data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Request message

The message used for declaring lost/stolen card hand in should at least contain the following information:

- Code of the Member State having issued the card
- found card number
- Reason for declaring card status modification

Continued on next page

Lost/stolen card hand in, Continued

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF1 [8].

Id	Question	Addressed to
1	How should the clerk handle a “driver card id unknown” response?	CIWG TF1
2	How should the clerk handle a “timeout” (no response within time limit)?	CIWG TF1
3	What are the other types of response such a message could generate (e.g. driver card already mentioned as stolen,...)?	CIWG TF1

Renewal of a card

Introduction

This process deals with the issue of a new tachograph card when an existing card reaches its expiry date, or is malfunctioning and has been returned to the issuing authority. Renewal always implies the certainty that two valid cards do not co-exist. Council Regulation (EC) N° 2135/98 mentions:

- *Art.14 §4(a)*: "[...] In the event of a request for the renewal of a card whose expiry date is approaching, the authority shall supply a new card before the expiry date provided that the request was sent to it within the time limits [...]"
- *Art.14 §4(e)*: "When a Member State replaces or exchanges a driver card, the replacement or exchange, and any subsequent replacement or renewal, shall be registered in that Member State."
- *Art.15 §1*: "[...] Where a driver wishes to renew his driver card, he shall apply to the competent authorities of the Member State in which he has his normal residence not later than 15 working days before the expiry date of the card."

Process description

According to [8] and since the renewal should always be processed by the Member State where the driver has his normal residence, which is also the same Member State having issued the card (otherwise it's not a renewal but an exchange), the renewal of a card doesn't need to be handled via TACHOnet.

Exchange of a card

Introduction

This process deals with the exchange of an existing valid driver card for an equivalent driver card for administrative reasons (e.g. the holder of the valid driver card has established his normal place of residence in another Member State).

Council Regulation (EC) N° 2135/98 mentions:

- *Art.14 §4(d)*: "[...] Where the holder of a valid driver card issued by a Member State has established his normal place of residence in another Member State, he may ask for his card to be exchanged for an equivalent driver card; [...] responsibility of the Member State which carries out the exchange to verify if necessary whether the card produced is actually still valid. Member States carrying out an exchange shall return the old card to the authorities of the Member State of issue and indicate the reasons for so doing."
- *Art.14 §4(e)*: "When a Member State replaces or exchanges a driver card, the replacement or exchange, and any subsequent replacement or renewal, shall be registered in that Member State."

Process description

As shown in Figure 7 below, the exchange of a card triggers processes and events among 3 different "entities":

- The *Member State of driver's normal residence* (where the exchange of card declaration is made),
- *TACHOnet* (providing central secure & reliable services for such declaration),
- The *Member State having issued the card* (recording the exchange of a card).

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Member State of driver's normal residence* and *Member State having issued the card* exchange information about tachograph cards. Therefore, the processes described for the *Member State of driver's normal residence* and *Member State having issued the card* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

Continued on next page

Exchange of a card, Continued

Process diagram

The exchange of a card can be modelled as follows:

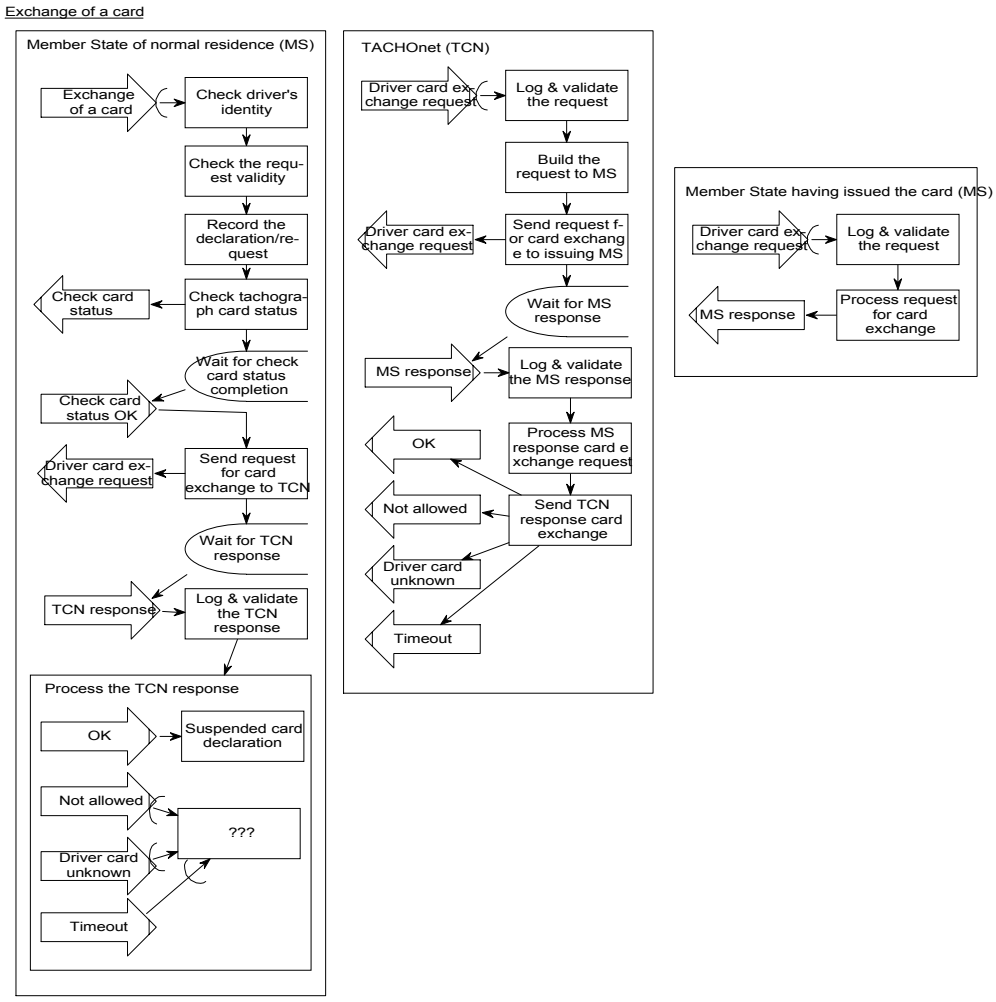


Figure 7 – "Exchange of a card" process

Process steps

The exchange of a card should follow more or less the following steps:

Step	Action
1	The clerk should first ask and verify the driver's identity by any appropriate means.
2	When the driver is identified, the clerk should record the details of the request (driver's identity, driver's card id, Member State having issued the card,...).

Continued on next page

Exchange of a card, Continued

Process steps (continued)

Step	Action
3	The clerk should then, via TACHOnet, check the status of the card by keying in its card number (see "Check tachograph card status" on page 56 for more details). This is required to allow the clerk visually check the details of the card prior to exchanging it and then to avoid from mistakenly (e.g. typing error in card number) exchanging another card. Moreover, such request will return the internal TACHOnet reference of the actual CIA having issued the card, which will be passed on in the next request to speed up the process.
3a	The clerk should then, via *TACHOnet*, warn the Member State having issued the card (should be different than the one of normal residence) that one of its issued card is in the process of being exchanged (so that the issuing authority shall keep records of it) by sending a request to *TACHOnet* and waiting for its response (asynchronous).
3b	*TACHOnet* should then log and validate (syntactically) the request, send an equivalent request to the *Member State having issued the card*, wait for the response (asynchronous) from the *Member State having issued the card*, process the response and send a consolidated response back to the initiator of the request.
3c	The *Member State having issued the card* should be ready to receive a request for processing the declaration of the exchange of a card against its own data store(s). It should process the request, send back the response to *TACHOnet*.
4a	If the result is positive, the clerk should proceed to the exchange of the card. At delivery time, the driver should hand in his old card. The clerk should proceed to the suspension of this card (reason: card exchanged) via the "Suspended card declaration" process. According to [8], this doesn't apply to all countries as some countries will request return of the old card before issuing the exchanged card. Some countries will have an over the counter service.
4b	If the result is negative (not allowed, timeout or driver card unknown), **what should the clerk do?**

Continued on next page

Exchange of a card, Continued

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for an exchange of a card
2	Sending (and logging) an equivalent request to the Member State having issued the card
3	Receiving, logging and validating response from the Member State having issued the card
4	Sending (and logging) the consolidated response to the initiator of the request

These identified services (along as requests and responses data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Request message

The message used for card exchange should at least contain the following information:

- Code of the Member State having issued the card
- Number of the card to exchange
- Reason for declaring card status modification.

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF1 [8].

Id	Question	Addressed to
1	How should the clerk handle a “request not allowed” response (e.g. stolen card,...)?	CIWG TF1
2	How should the clerk handle a “driver card id unknown” response?	CIWG TF1
3	How should the clerk handle a “timeout” (no response within time limit)?	CIWG TF1
4	What are the other types of response such a request could generate?	CIWG TF1

Continued on next page

Exchange of a card, Continued

Pending questions (continued)

Id	Question	Addressed to
5	Should a malfunctioning card be replaced or renewed?	CIWG TF1
6	Is the card exchange process the same for each type of tachograph card (driver, company, control, workshop)?	CIWG TF1
7	Are the card replacement index and renewal index unchanged in case of exchange?	CIWG TF1

Replacement of a card

Introduction

This process deals with the issue of a tachograph card in replacement of an existing card, which has been declared lost, stolen or malfunctioning and has not been returned to the issuing authority. Replacement always implies a risk that two valid cards may co-exist.

Council Regulation (EC) N° 2135/98 mentions:

- *Art.12 §1*: "If a card issued to an approved workshop or fitter [...] is damaged, malfunctions [...] , the authority shall supply a replacement card within five working days of receiving a detailed request to that effect."
- *Art.14 §4(a)*: "[...] If the driver card is damaged, malfunctions [...], the authority shall supply a replacement card within five working days of receiving a detailed request to that effect."
- *Art.14 §4(e)*: "When a Member State replaces or exchanges a driver card, the replacement or exchange, and any subsequent replacement or renewal, shall be registered in that Member State."
- *Art.15 §1*: "[...] If the driver card is damaged, malfunctions [...], the driver shall apply within seven calendar days for its replacement to the competent authorities of the Member State in which he has his normal residence."

Process description

According to [8] and since the replacement should always be processed by the Member State where the driver has his normal residence, which is also the same Member State having issued the card (otherwise it's not a replacement but an exchange), the replacement of a card doesn't need to be handled via TACHOnet.

Check tachograph card status

Introduction

This process deals with the verification of the state of a tachograph card based on its card number. This process is very useful for enforcement authorities to detect any theft or forgery. Therefore, such a process should ideally be available 24x7. Enforcers should be able to check driver cards and workshop cards [6].

This process should also be carried out by CIA to check the owner of a card (based on its number) prior to declaring it lost or stolen or malfunctioning.

Process diagram

The verification of a tachograph card can be modelled as follows:

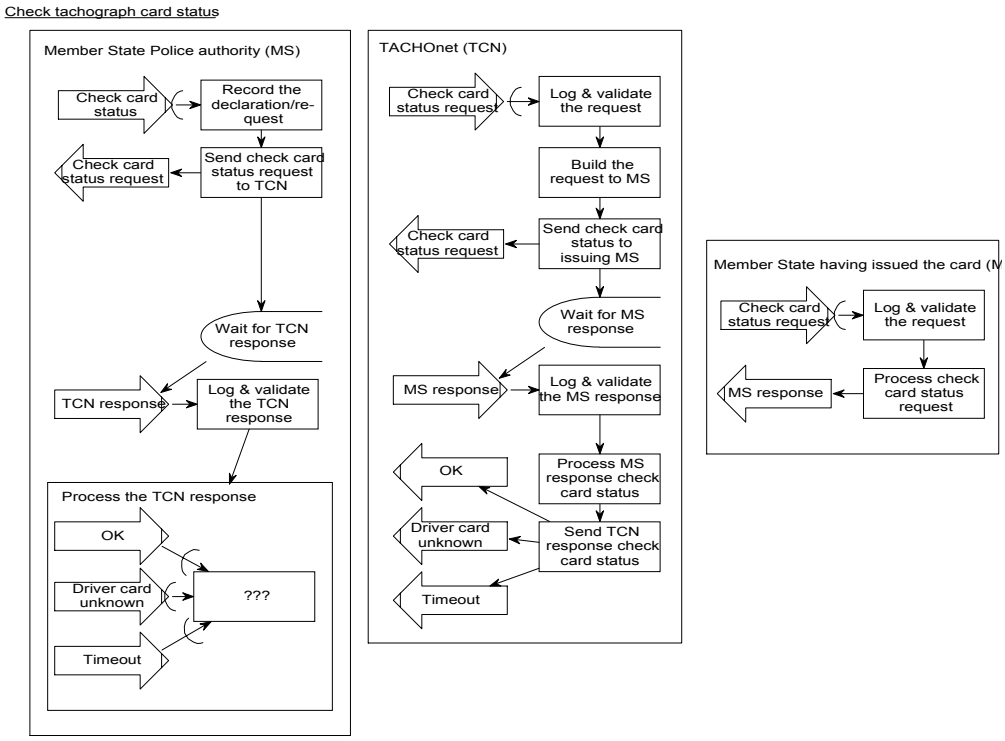


Figure 8 – "Check tachograph card" process

Continued on next page

Check tachograph card status, Continued

Process description

As shown in Figure 8 above, the verification of a tachograph card triggers processes and events among 3 different "entities":

- The *Member State Enforcement Authority* (willing to perform the verification of a tachograph card). Granting *Enforcement* Authorities access to TACHOnet is under the responsibility of each Member State and has to be managed by them accordingly (should impersonate a Member State's CIA as only CIAs are managed as authorized entities),
- *TACHOnet* (providing central secure & reliable services for such verification),
- The *Member State having issued the card* (performing the verification against its own data store).

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Member State of driver's normal residence* and *Member State having issued the card* exchange information about tachograph cards. Therefore, the processes described for the *Member State of driver's normal residence* and *Member State having issued the card* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

Process steps

The verification of a tachograph card should follow more or less the following steps:

Step	Action
1	The authorized enforcer gets connected to the "check tachograph card" application (typing in his user name and password) and types in the card number and the issuing member state code (identifying uniquely a tachograph card) of the tachograph card he'd like to check. Note that the so-called "check tachograph card" application is the kind of application a Member State needs to provide to grant *Enforcement* Authorities access to *TACHOnet* (by impersonating a CIA).
2	The application sends, via *TACHOnet*, the request for checking the given card to the Member State having issued the card (based on the issuing member state sign)
3a	*TACHOnet* should then log and validate (syntactically) the request, send in parallel an equivalent request to the *Member State having issued the card* (SPOC), wait for the response (asynchronous) from the *Member State having issued the card*, process the response and send a consolidated response back to the initiator of the request.
3b	The *Member State having issued the card* should be ready to receive a request for checking the status of a card against its own data store(s). It should process the request, send back the response to *TACHOnet*.

Continued on next page

Check tachograph card status, Continued

Process steps (continued)

Step	Action
4a	If the result is positive (card detected), the status of the card is returned and handled accordingly by the police officer.
4b	If the result is negative (not allowed, timeout or driver card unknown), **what should the police officer do?**

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for a checking the status of a card
2	Sending (and logging) an equivalent request to the Member State having issued the card (SPOC)
3	Receiving, logging and validating response(s) from the Member State having issued the card
4	Building the final response
5	Sending (and logging) the final response to the initiator of the request

These identified services (along as requests, responses and receipts data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Request message

The message used for checking a card should at least contain the following information:

- Code of the Member State having issued the card
- Number of the card to check

Continued on next page

Check tachograph card status, Continued

Response message

The response message to checking a driver card should return the same information as the one for checking driver's issued card (see Driver's identification in "check driver's issued cards" response message at page 29).

For a workshop card, the information is more or less similar:

- Card number
- Card status (valid, stolen, lost,…)
- Address where the card has been issued
- Issue date (date of 1st validity)
- Expiry date
- Last status modification date
- Workshop name
- Workshop address
- Surname, first names and date of birth of the individual to who the card was issued.

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. These questions should be addressed at the beginning of the next phase (detailed analysis) of the TACHOnet project.

Id	Question	Addressed to
1	Should TACHOnet provide a basic default "user interface" (e.g. web-based application) helping Member States (CIA or enforcers) to send requests to TACHOnet (e.g. fill in a web form) and view the results (e.g. a web form displaying the final results)? **Answer**: No. Up to the Member State (via CIA application?) to implement such application.	CIWG TF2

Check driver's issued card

Introduction

This process deals with the verification of whether a particular driver (based on his name, first names, date of birth,…) does actually hold a valid card.

Such process will be carried out by the enforcers during road-checks to check, when a driver is unable to show his card (pretending it's lost or stolen), that this driver does actually hold a valid card issued by a Member State. Therefore, such process should ideally be available 24x7 [6].

This process will also be carried out by CIA when issuing a new card (see description at page 25).

Process steps

The process steps are the same as the ones described for checking a tachograph card status (see page 57), except that the card number in the request is replaced by the driver's surname, first names, datye of birth,… .

Request message

The request message to checking driver's card should contain the same information as described in "Driver's identification in "check driver's issued cards" request message" at page 29).

The only difference between CIAs and enforcers usage is that the CIAs requests should target all Member States whereas the enforcers requests will only target the Member State having issued the driver's card (as the driver must prove he owns a valid card, he should at least tell the enforcers where he did get the card he couldn't show). Therefore, the request message should also contain an optional "Issuing Member State Code" indicating whether to target all Member States (if empty) or a particular one (if specified).

Response message

The response message to checking driver's card should return the same information as described in "Driver's identification in "check driver's issued cards" response message" at page 29).

Pending questions

See page 59.

Bulk check of issued driver card holders

Introduction

This process deals with the verification asked by a Member State that all or a large part of its driver card holders are not yet holder of another card in another country. This is for use by those countries that will not be joined to TACHOnet at go live and will need to carry out a check at a later date [8].

Basically, this process merely consists of performing the same verification as explained in the "First issue a card" process (check driver's issued card(s)) but not only for a single driver but for a bunch of drivers.

Therefore, several aspects such as the size of the request/response, the required processing time,... will have to be analysed deeper.

Process diagram

This process can be modelled as follows:

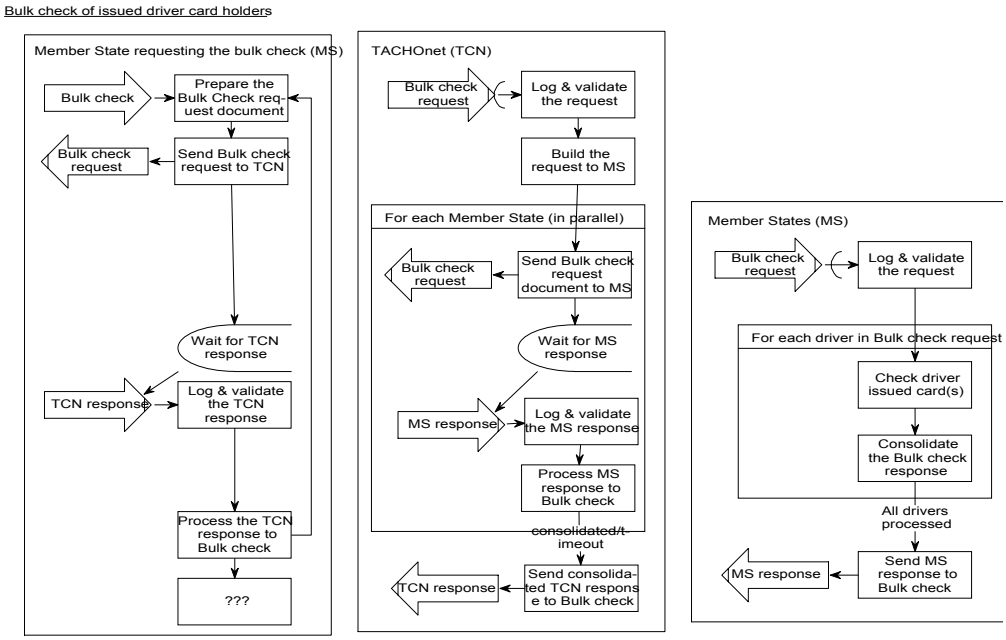


Figure 9 – "Bulk check of issued driver card holders" process

Continued on next page

Bulk check of issued driver card holders, Continued

Process description

As shown in Figure 9 above, the bulk check of issued driver card holders triggers processes and events among 3 different "entities":

- The *Member State issuing the bulk check* (CIA) issuing the card and asking for the bulk verification,
- *TACHOnet* (providing central secure & reliable services for such verification),
- The different *Member States* performing the verification against their own data stores.

As mentioned earlier, business process modelling aims only at identifying the different *TACHOnet* events and services needed to help *Card Issuing Authorities* and *Member States* exchange information about tachograph cards. Therefore, the processes described for the *Card Issuing Authorities* and *Member States* "entities" are just drawn as "helpers" to find out *TACHOnet* services. **Only** the processes of the *TACHOnet* entity are of interest for the scope of the TACHOnet project.

Process steps

The verification asked by a Member State that all or a large part of its driver card holders are not yet holder of another card in another country should follow more or less the following steps:

Step	Action
1	The clerk should ask for the generation of an input file (which structure will be defined later on) listing the driver card holders (driver surname, driver first name, driver's license number, driver's birthdate,...) to check.
2a	The clerk should then verify, via *TACHOnet*, that its CIA's drivers don't hold yet any driver card or don't have any card request pending in any Member State connected to *TACHOnet* by sending to *TACHOnet* the request for checking issued cards for the listed drivers and waiting for its receipt and then its response (asynchronous).
2b	*TACHOnet* should then log and validate (syntactically) the request, send in parallel an equivalent request to the different *Member States*, wait for the response (asynchronous) from each of these *Member States*, process the responses and send a consolidated response (listing each Member State result for each requested driver card holder) back to the initiator of the request.
2c	The different *Member States* should be ready to receive a request for checking drivers' issued cards against their own data stores. They should process the request, send back the response to *TACHOnet*.
3	The clerk should then analyse the consolidated result.

Continued on next page

Bulk check of issued driver card holders, Continued

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Receiving, logging, validating a request for checking whether drivers (based on drivers' identification criteria's – to be defined later) does hold yet a card or have a request pending somewhere.
2	Sending (and logging) an equivalent request to the different Member States connected to TACHOnet
3	Receiving, logging and validating responses from these Member States
4	Consolidating the different responses into a single one
5	Sending (and logging) the consolidated response to the initiator of the request

These identified services (along as requests and responses data structures) will be described in more details when translated into use cases in the Use-Case Model.

Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. These questions should be addressed at the beginning of the next phase (detailed analysis) of the TACHOnet project.

Id	Question	Addressed to
1	What's the estimation of the number of drivers that might be included in a bulk check request? **Answer**: Max. 1000	CIWG TF2
2	What's the timeout value for such a request (how long should TACHOnet wait for receiving responses from the Member States?)? **Answer**: Such requests are to be considered as *batch* requests (more than a single request) and should then be processed over night (with a timeout of several hours) to avoid from disturbing *online* requests.	CIWG TF2

Section 3.3 - System tasks

Overview

Introduction

This process group gathers the different processes related to the system tasks provided by the TACHOnet project and carried out by authorized administrators.

Contents

This section contains the following topics.

Users & access rights management

Introduction

This process deals with the definition of the users having access to the TACHOnet functionalities along as their access rights to these functionalities.

What's a TACHOnet user?

TACHOnet aims at providing Member States (through their Card Issuing Authorities – CIAs) with secure and reliable services for exchanging information about tachograph cards.

Figure 10 sums up the different types of users TACHOnet will manage. These are *CIA*, *CIA administrator* and *TCN administrator*.

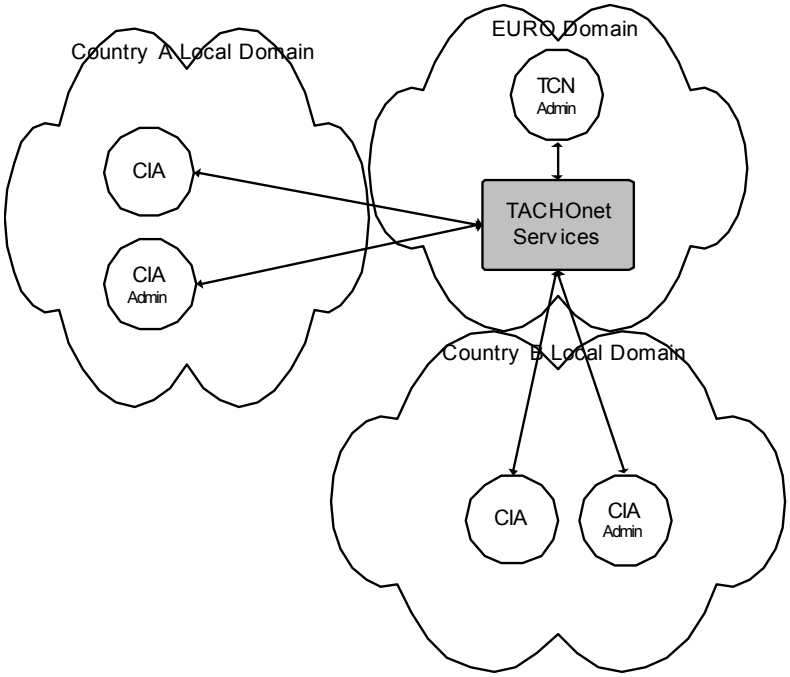


Figure 10 – TACHOnet users

Please refer to [4] for more technical details about architecture, security and network issues.

Continued on next page

Users & access rights management, Continued

What's a *CIA* user type?

As you might see in Figure 10, TACHOnet considers a whole CIA as a single user (the CIA administrator excepted). TACHOnet does not manage each CIA users (e.g. the clerks performing administrative tasks). These latter ones have to be managed accordingly by each Member State's CIA under their own responsibility. From the TACHOnet viewpoint, the *CIA* as a whole is a single user and will be defined accordingly (a single digital certificate will be delivered for a *CIA*,...). Therefore, enforcers are also considered as CIA users who should then be managed by each Member State (TACHOnet only have a SPOC CIA).

A *CIA*-typed user will be granted the rights for carrying out any of the administrative tasks (see Administrative tasks for more details).

As mentioned earlier (see "Card Issuing Authority" definition), a Member State may have a single or several Card Issuing Authorities managing card issuing for his resident drivers. Nevertheless, it has been agreed that TACHOnet will consider the Member State as having a SPOC CIA (Single Point Of Contact Card Issuing Authority), even though the Member State is organized through multiple CIAs managing their tachograph cards data in a common central data store (it's up to the Member State to manage the one-to-many relationship).

What's a *CIA Administrator* user type?

A *CIA Administrator* user type stands for the interface between TACHOnet and a *CIA* regarding system tasks (user management, statistics, logging,...). A *CIA Administrator* may only manage a single *CIA*. But a *CIA* may be managed by one or more *CIA Administrators* (but at least one).

From the TACHOnet viewpoint, the *CIA Administrator* is a single user and will be defined accordingly (a single digital certificate will be delivered for a *CIA Administrator*,...).

A *CIA Administrator*-typed user will be granted the rights for carrying out any of the system tasks (see System tasks for more details).

What's a *TCN Administrator* user type?

The *TCN (TACHOnet) Administrator* is in charge of administering the whole TACHOnet services in terms of configuration, performance, logging, tracking,... .

The *TCN Administrator* is not related to any *CIA* and works for the *Trusted Third Party* company hosting and managing the TACHOnet services.

Continued on next page

Users & access rights management, Continued

Process diagram

This process group can be modelled as follows:

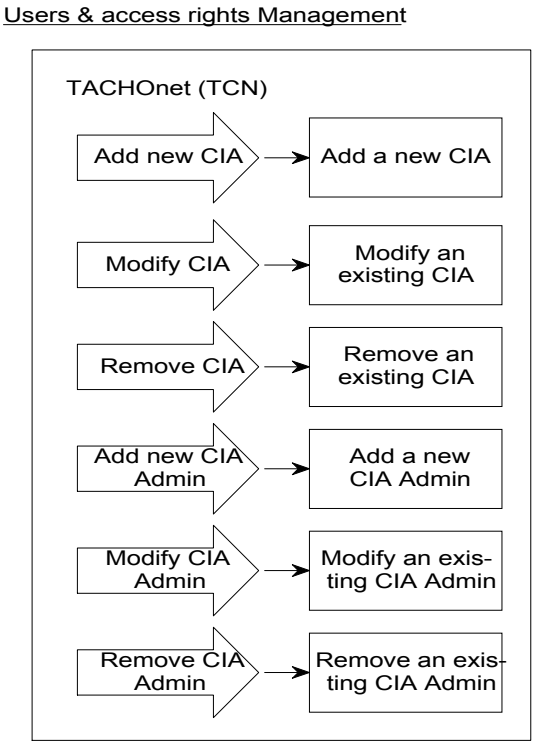


Figure 11 – "Users & access rights management" process

Process description

As shown in Figure 11 above, different processes have been identified for users & access rights management:

Process	Description
Add a new CIA	This process deals with the TACHOnet definition of a new Member State Card Issuing Authority *CIA*-typed user.
Modify CIA parameters	This process deals with the modification of some parameters (IP address,...) of an existing *CIA*-typed user.
Remove CIA	This process deals with the removal of an existing *CIA*-typed user.
Add CIA Admin	This process deals with the TACHOnet definition of a new *CIA Administrator*-typed user.
Modify CIA Admin	This process deals with the modification of some parameters of an existing *CIA Administrator* -typed user.

Continued on next page

Users & access rights management, Continued

Process description (continued)

Process	Description
Remove CIA Admin	This process deals with the removal of an existing *CIA Administrator* -typed user.

Important note:

These processes raise some important issues regarding procedures and policies (operational, audit, security,…) that should be put in place in order to address some questions like:

- How to join in?
- How to define an administrator?
- How to exclude a Member State?
- How to make the system evolve?
- …

Such processes will be carried out manually according sound procedures defined and approved by a kind of TACHOnet User Group (see below).

TACHOnet User Group

The TCN User Group (or Management Board) would consist of a representative of each Member State using the TACHOnet system and some representatives of the European Commission (ideally from the DG TREN's Inland Transport Directorate) in order to define and manage operational and security procedures (who may be in, how to join in,…) as well as the evolution of the system.

Defining the structure and the roles of such a group is beyond the scope of this document but its setup is of prime importance for the success of the whole project. Such a group (or board) should obviously be set up prior to deploying the TACHOnet system.

Users & access rights management, Continued

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF2 [8].

Id	Question	Addressed to
1	Which authority will be granted the rights for adding or removing a *CIA*-typed user? **Answer:** *The DG TREN Inland Transport Directorate*	DG TREN
2	What will be the procedure(s) for adding, modifying, removing a Member State (and its corresponding administrator)?	CIWG TF2
3	How long should TACHOnet keep logging and tracking info for a removed user?	CIWG TF2

Statistics management

Introduction

This process deals with the management of different statistics (e.g. usage,...) around TACHOnet activities.

Statistics, what's in a word?

Statistics are valuable data for evaluating the usage of a system, its relative performance,... . Therefore, TACHOnet will automatically generate, on a weekly, monthly and/or yearly basis, two different types of statistics report depending on the target user(s):

Target user type	Statistics report type
CIA Administrator	A first report will be generated for each *CIA* (and sent to their corresponding *CIA Administrator*). It will contain info about: • Number of requests/receipts/responses sent by *CIA* to TACHOnet (globally + per type of request/response + per time slices) • Number of requests/receipts/responses sent by TACHOnet to *CIA* (globally + per type of request/response + per time slices) • Average time for sending receipt to request/response (+ slowest/fastest time) per type of request/response • Average time for sending response to request (+ slowest/fastest time) per type of request • Average size of requests/receipts/responses (+ smallest/highest) per type of request/response • % of fully completed requests sent by *CIA* to TACHOnet (per type of request) • % of fully completed requests sent by TACHOnet to *CIA* (per type of request) • % of failed requests sent by *CIA* to TACHOnet (per type of failure and request) • % of failed requests sent by TACHOnet to *CIA* (per type of failure and request) • Others needful info are welcome... **Important**: All the information provided to a *CIA* only deals with transactions involving that *CIA*.
TCN Administrator	A second report (DB-based) will be generated for TACHOnet internal purposes. It will contain info about: • More or less the same info as above but including all CIAs • Servers availability, performance,... • DB availability, performance, volume,... • Others needful info are welcome...

Continued on next page

Statistics management, Continued

Process diagram

This process group can be modelled as follows:

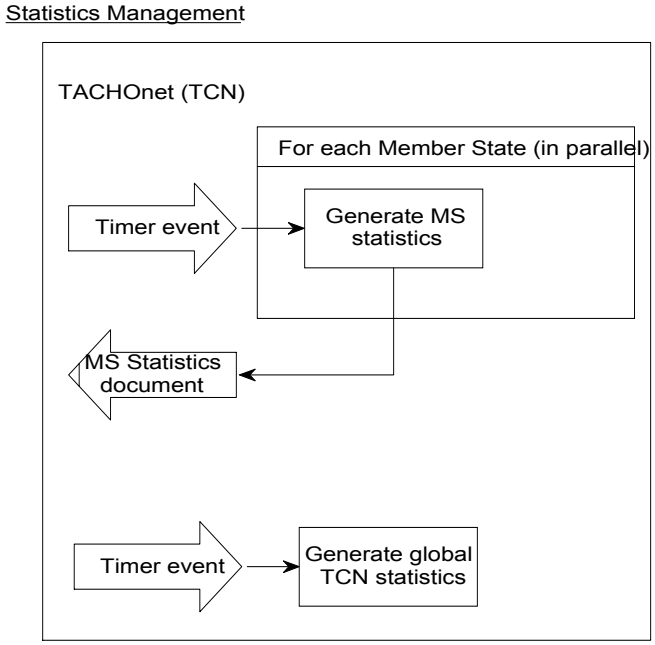


Figure 12 – "Statistics management" process

Process description

As shown in Figure 12, two different processes have been identified:

Process	Description
Generate CIA statistics	This process aims at generating usage statistics report (#requests, #responses, processing meantime,...) for each *CIA* user (only with its related data) defined in TACHOnet and to make this report available (for browsing via a secure Web interface) to the corresponding *CIA Administrator*.
Generate global TCN statistics	This process aims at generating some statistics info (usage per CIA, peak time, performance, failure rate,...) for TACHOnet internal purposes (for browsing via a secure Web interface), i.e. not aimed at being distributed to Member States

Continued on next page

Statistics management, Continued

Identified TACHOnet service(s)

This process clearly identifies several services that should be supplied by the TACHOnet network:

#	Services/Functions
1	Generate a statistics report for each Member State CIA on a weekly, monthly and yearly basis and make this report available (for browsing via a secure Web interface) to each corresponding CIA Administrator.
2	Generate global TACHOnet statistics info (for browsing via a secure Web interface) for TACHOnet internal purposes on a weekly, monthly and yearly basis

These identified services (along as requests, responses and receipts data structures) will be described in more details when translated into use cases in the Use-Case Model. Technical issues such as data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF2 [8].

Id	Question	Addressed to
1	What are the other types of statistics that should be generated (if any)?	CIWG TF2
2	How long should TACHOnet keep track of statistics info?	CIWG TF2

Logging & Monitoring management

Introduction

This process deals with the management of different loggings around TACHOnet activities. Logging information is of major importance to keep track of the different transactions carried out by TACHOnet and to be able to generate statistics about these transactions. This process deals also with the constant monitoring of the system.

Process diagram

This process group can be modelled as follows:

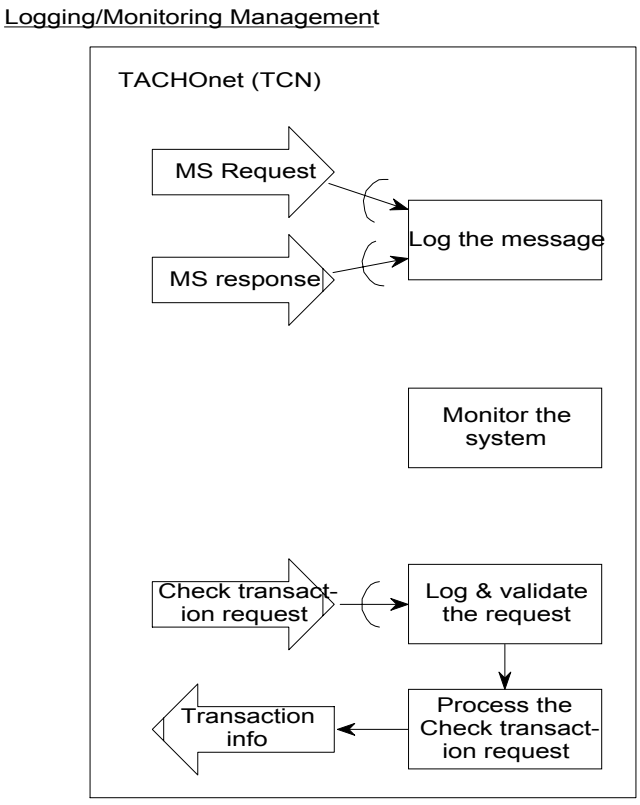


Figure 13 – "Logging management" process

Process description

As shown in Figure 13, different processes have been identified:

Process	Description
Log the message	This process aims at logging each sent/received message.
Monitor the system	This process aims at monitoring the TACHOnet system.

Continued on next page

Logging & Monitoring management, Continued

Process description (continued)

Process	Description
Process the "Check transaction" request	The "check transaction" request aims at checking (against the tracking database) whether a transaction has effectively been carried out by TACHOnet (when and with which result). This request is useful to provide evidence of the (non) execution of a transaction in case of disputation or impeachment. The "Check transaction" request will be handled manually through a procedure defined and approved by a kind of TCN User Group (or Management Board), as already explained in the frame of Users & access rights management.

Pending questions

Different questions come to mind when analysing the process and its interactions with TACHOnet. Most of these questions should be addressed by CIWG TF1 [8].

Id	Question	Addressed to
1	Is the full logging of every message still needful (non-repudiation is no longer a requirement)? Anyway, some logging are still foreseen for monitoring and statistics purposes.	CIWG TF2
2	If so, what are the procedures to put in place in order to provide someone with detailed info about logging activities?	CIWG TF2
3	What is the procedure to handle the "Check transaction" request?	CIWG TF2
4	How long should TACHOnet keep track of the transactions?	CIWG TF2

Chapter 4: Business Object Model

Overview

Introduction

The business object model aims at understanding the customer's language that is associated with his business. This model reflects the particular part of the user domain which is relevant for the project.

Contents

This chapter contains the following topics.

Section 4.1 - Class Diagrams

Overview

Introduction

This section lists all the class diagrams together with a textual description for each one of them stating their goal.

Contents

This section contains the following topics.

Local Business Object Model

Introduction

The Local Business Object Model diagram gives an overview of the different entities related to card issuing and their relationships between them. A more detailed description is given for each entity (class) in the Classes section.

Diagram

The different entities related to card issuing can be modelled as follows:

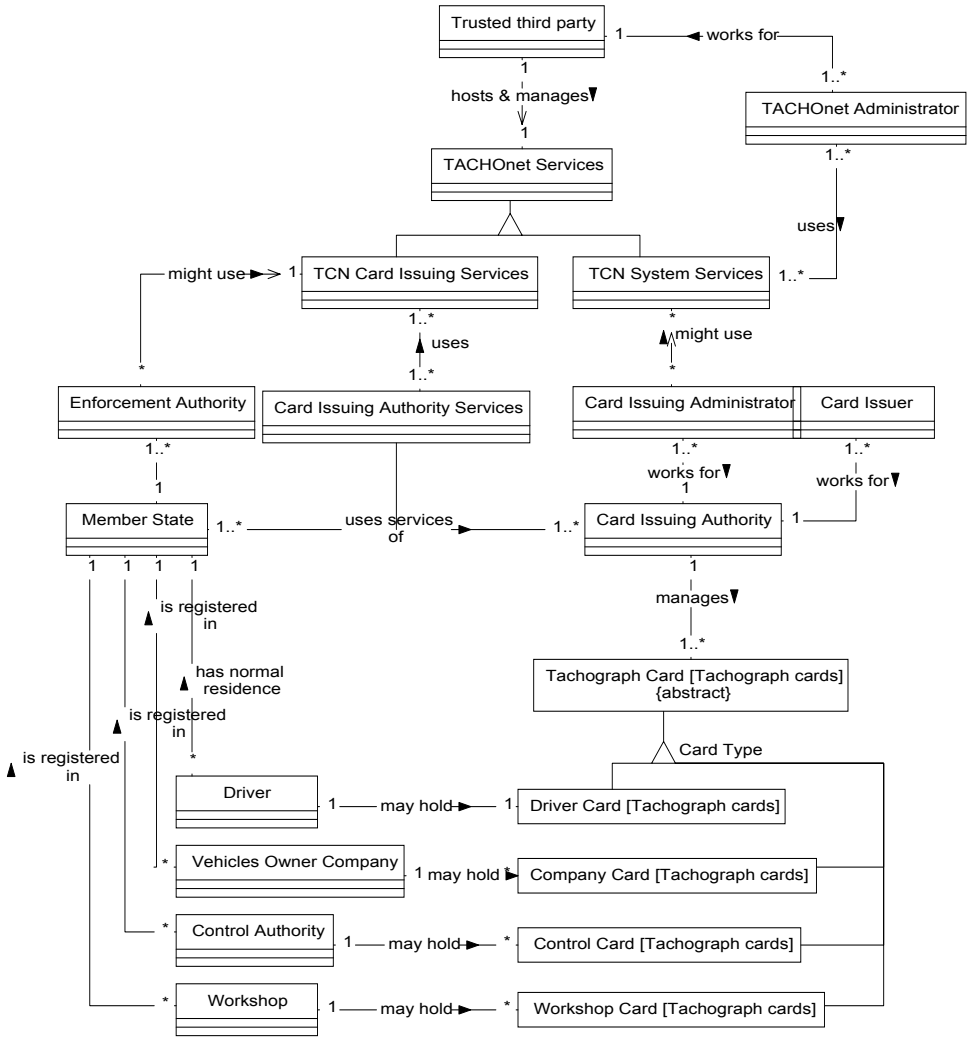


Figure 14 – Local Business Object Model

Continued on next page

Local Business Object Model, Continued

Description

TACHOnet Services represents the services that, for instance, Card Issuing Services will use to check card issuing information between Member States. **TCN Card Issuing Services** represents the administrative tasks as described on page 24. **TCN System Services** represents the system tasks as described on page 64.

Trusted Third Party stands for a company or organisation that will act as the trusted "manager" of the TACHOnet services in terms of hosting, configuration, administration,... .

TACHOnet Administrator represents someone working for the trusted third party and in charge of administering the TACHOnet services.

Card Issuing Services represents the services that a Card Issuing Authority provides to a Member State. A Card Issuing Authority may provide its services to several Member States. A Member State may use the services provided by one or several Card Issuing Authorities.

Card Issuing Authority represents an authority that's authorized to issue and manage tachograph cards (see Tachograph cards on page 79 for more details about types of cards).

Card Issuer represents someone working for a Card Issuing Authority and in charge of performing administrative tasks related to card issuing (TCN Card Issuing Services).

Card Issuing Administrator represents someone working for a Card Issuing Authority and in charge of performing system tasks related to TACHOnet (TCN System Services)

Member State represents a Member State that shall take the necessary measures to ensure they are able to issue driver cards. To do so, a Member State uses the services provided by a Card Issuing Authority.

Enforcement Authority stands for one or several authorities (like police authority) that might use some of the TCN Card Issuing Services (under the responsibility of the Member State to which the Enforcement Authority belongs).

Tachograph cards

Introduction

This map aims at defining what are tachograph cards.

Diagram

The different types of tachograph cards can be modelled as follows:

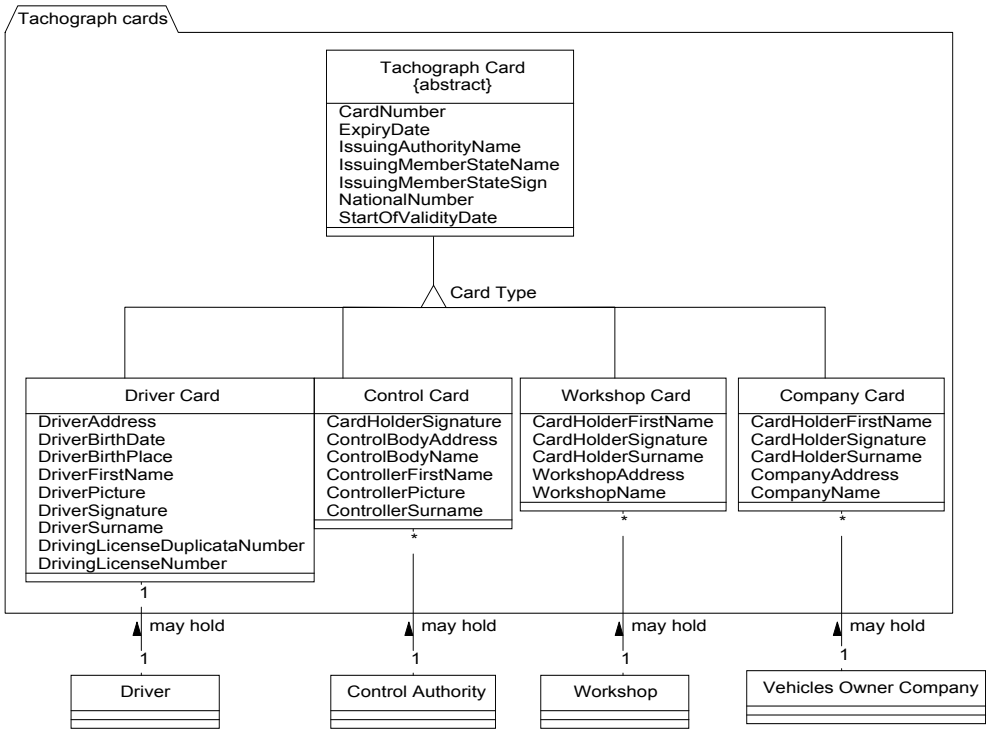


Figure 15 – Tachograph cards

Tachograph card

A tachograph card is a smart card intended for use with a recording equipment (total equipment intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers). Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage. Tachograph cards are of 4 different types which definition is given below.

Driver card

The driver card is a tachograph card issued by the authorities of a Member State to a particular driver. The driver card identifies the driver and allows for storage of driver activity data.

A driver may hold one and only one driver card.

Continued on next page

Tachograph cards, Continued

Company card

The Company card is a tachograph card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment.

The Company card identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company.

A Vehicles Owner Company may hold several company cards.

Control card

The Control card is a tachograph card issued by the authorities of a Member State to a national competent control authority.

The Control card identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading.

A Control Authority may hold several Control cards.

Workshop card

The Workshop card is a tachograph card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Member State.

The Workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the recoding equipment

A Workshop company may hold several Workshop cards.

Pending questions

The following questions come to mind:

Id	Question	Addressed to
1	Is the tachograph cards model (Figure 15) still valid?	CIWG

Continued on next page

Tachograph cards, Continued

Community Model Tachograph cards

Visual representation of the different types of tachograph cards is given below:

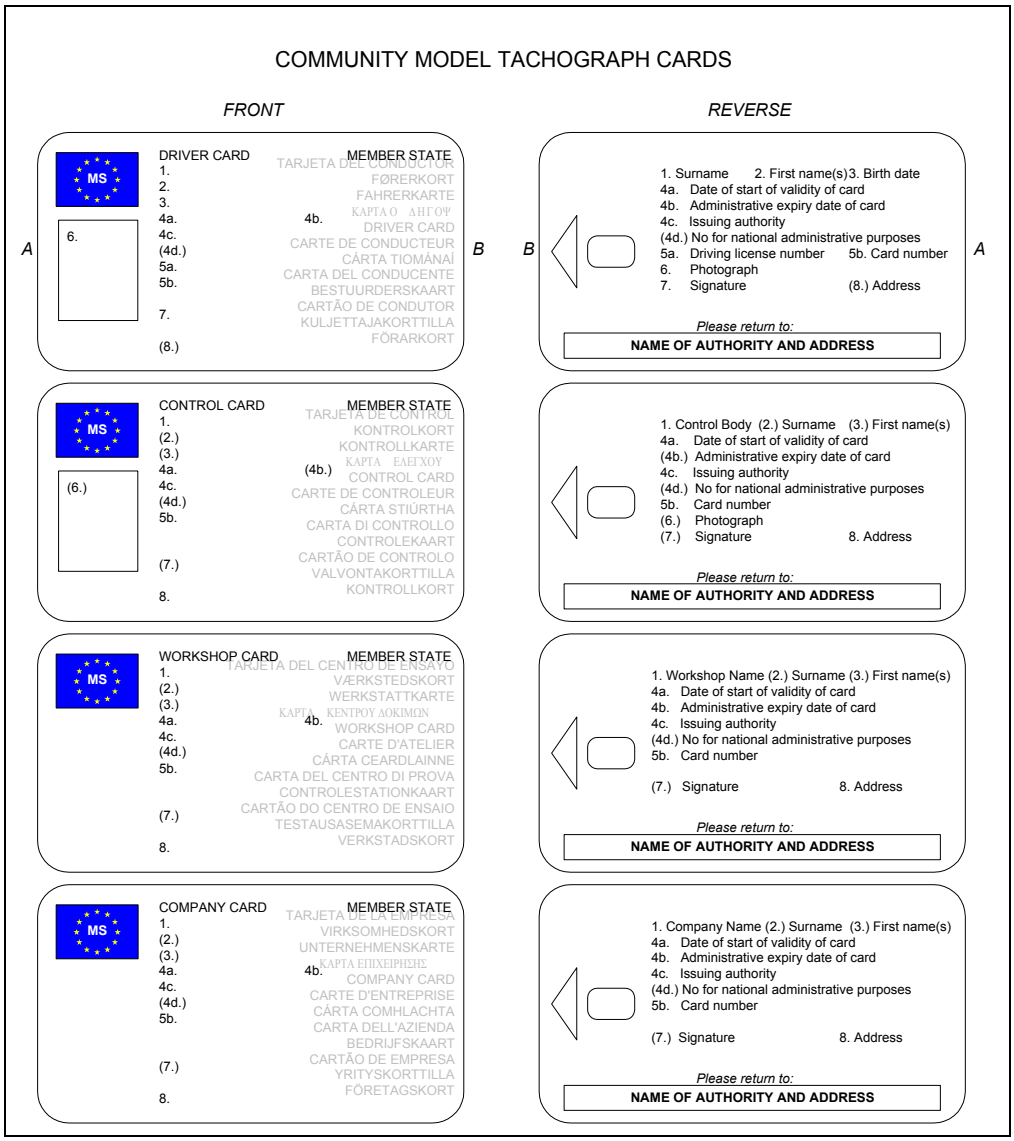


Figure 16 – Community Model Tachograph cards

Section 4.2 - Classes

Overview

Introduction

This section lists all classes of the Business Object Model by name. A textual description is provided for each class.

Contents

This section contains the following topics.

Class <Tachograph card>

Description

This abstract class models the tachograph card and all the information available on that card (mandatory or optional).

A tachograph card is a smart card intended for use with a recording equipment (total equipment intended for installation in road vehicles to show, record and store automatically or semi-automatically details of the movement of such vehicles and of certain work periods of their drivers). Tachograph cards allow for identification by the recording equipment of the identity (or identity group) of the cardholder and allow for data transfer and storage.

There are 4 different types of tachograph cards:

- driver card,
- control card,
- workshop card,
- company card.

Association statements

Each Tachograph Card:

- **manages** Is related to only one Card Issuing Authority.

Continued on next page

Class <Tachograph card>, Continued

Properties

The Tachograph card exposes the following properties:

Property	Description
CardNumber	The card number is a 16 alpha-numerical character that uniquely identifies a tachograph card within the Member State issuing it). A card is therefore uniquely identified by the code of the issuing Member State and the card number. The 14th alpha-numerical character of a card number (the card consecutive index) is used to differentiate the different cards issued to a company, a workshop or a control body entitled to be issued several tachograph cards. The company, workshop or control body is uniquely identified by the 13 first characters of the card number. Its original value (first card issuing) shall be 0. The 15th alpha-numerical character of a card number (the card replacement index) is incremented by 1 each time a tachograph card is replaced (in the order 0,...,9, A,...,Z). Its original value (first card issuing) shall be 0. In case of renewal, its value shall be reset to 0. The 16th alpha-numerical character of a card number (the card renewal index) is incremented by 1 each time a tachograph card is renewed (in the order 0,...,9, A,...,Z). Its original value (first card issuing) shall be 0.
ExpiryDate	Administrative expiry date of card in dd/mm/yyyy or dd.mm.yyyy format.
IssuingAuthorityName	Name of the issuing authority.
IssuingMemberStateName	The name of the Member State issuing the card (optional)
IssuingMemberStateSign	The distinguishing sign of the Member State issuing the card (B, K, D, GR, E, F, IRL, I, L, NL, A, P, FIN, S, UK). This is MANDATORY.
NationalNumber	National card number for administrative purposes (optional).
StartOfValidityDate	Date of start of validity of card in dd/mm/yyyy or dd.mm.yyyy format.

Class <Driver card>

Description

This class models the driver card which is a tachograph card issued by the authorities of a Member State to a particular driver.

The driver card identifies the driver and allows for storage of driver activity data.

The driver card is white

Association statements

Each Driver Card:

- Inherits from Tachograph Card
- **may hold** Is related to only one Driver.

Properties

The Driver card exposes the following properties (beside the ones exposed by his parent class):

Property	Description
DriverAddress	Normal place of residence or postal address of the card holder (optional)
DriverBirthDate	Birth date of the driver in dd/mm/yyyy or dd.mm.yyyy format
DriverBirthPlace	Place of birth of the driver
DriverFirstName	First name(s) of the driver
DriverPicture	Photograh of the driver
DriverSignature	Signature of the driver
DriverSurname	Surname of the driver
DrivingLicenseDuplicataNumber	Driving license duplicata number at the date of issue of the driver card (if any)
DrivingLicenseNumber	Driving license number at the date of issue of the driver card

Class <Company card>

Description

This class models the Company card which is a tachograph card issued by the authorities of a Member State to the owner or holder of vehicles fitted with recording equipment.

The Company card identifies the company and allows for displaying, downloading and printing of the data stored in the recording equipment which has been locked by this company.

The Company card is yellow.

Association statements

Each Company Card:

- Inherits from Tachograph Card
- **may hold** Is related to only one Vehicles Owner Company.

Properties

The Company card exposes the following properties (beside the ones exposed by his parent class):

Property	Description
CardHolderFirstName	First name(s) of the card holder (if applicable)
CardHolderSignature	Signature of the holder (optional)
CardHolderSurname	Card holder surname (if applicable)
CompanyAddress	Postal address of the company
CompanyName	Company name

Class <Control card>

Description

This class models the Control card which is a tachograph card issued by the authorities of a Member State to a national competent control authority.

The Control card identifies the control body and possibly the control officer and allows for getting access to the data stored in the data memory or in the driver cards for reading, printing and/or downloading.

The Company card is blue.

Association statements

Each Control Card:

- Inherits from Tachograph Card
- **may hold** Is related to only one Control Authority.

Properties

The Control card exposes the following properties (beside the ones exposed by his parent class):

Property	Description
CardHolderSignature	Signature of the holder (optional)
ControlBodyAddress	Postal address of control body
ControlBodyName	Control body name
ControllerFirstName	First name(s) of the controller (if applicable)
ControllerPicture	Photograph of the controller (if applicable)
ControllerSurname	Surname of the controller (if applicable)

Class <Workshop card>

Description

This class models the Workshop card which is a tachograph card issued by the authorities of a Member State to a recording equipment manufacturer, a fitter, a vehicle manufacturer or workshop, approved by that Member State.

The Workshop card identifies the cardholder and allows for testing, calibration and/or downloading of the recoding equipment.

The Workshop card is red

Association statements

Each Workshop Card:

- Inherits from Tachograph Card
- **may hold** Is related to only one Workshop.

Properties

The Workshop card exposes the following properties (beside the ones exposed by his parent class):

Property	Description
CardHolderFirstName	First name(s) of the card holder (if applicable)
CardHolderSignature	Signature of the holder (optional)
CardHolderSurname	Card holder surname (if applicable)
WorkshopAddress	Postal address of the workshop
WorkshopName	Workshop name

Chapter 5: Use-Case Model

Overview

Introduction

This chapter describes the use-case model comprehensively, in terms of how the model is structured into packages and what use cases and actors are in the model.

The proposed use case model only deals with the TACHOnet system and does not include use cases related to the Card Issuing Authority processes (beyond the scope of this study).

Important:

The following decisions have been taken (and agreed) during the feasibility study:

- TACHOnet will consider the Member State as having a SPOC CIA (Single Point Of Contact Card Issuing Authority), even though the Member State is organized through multiple CIAs managing their tachograph cards data in a common central data store (it's up to the Member State to manage the one-to-many relationship).
- For performance reasons (to reduce the amount of messages exchanged), a request message (and its corresponding response message) could contain several ('n') requests (for several card ids/drivers) instead of a single one.
- Enforcement Authorities may have access to some TACHOnet services through their National Card Issuing Authority (it's under the Member State's responsibility to grant enforcers access to the TACHOnet system). From the TACHOnet point of view, enforcers are seen as a Member State (SPOC CIA).

Contents

This chapter contains the following topics.

Introduction

What's a Use-Case Model ?

A use-case model is a model of the system's intended functions and its surroundings. It serves as a contract between the customer, the users and the system developers on the functionality of the system, which allows :

- Customers and users to validate that the system will become what they expected.
- System developers to build what is expected.

The same use-case model is used in system analysis, design, implementation, and testing.

The use-case model consists of **use cases** and **actors**.

What's an Actor ?

An **actor** defines a coherent set of roles that users of the system can play when interacting with it. A user can either be an individual or an external system.

What's a Use Case ?

A **use case** defines a set of use-case instances, where each instance is a sequence of actions a system performs that yields an observable result of value to a particular actor. Each use case in the model is described in detail, showing step-by-step how the system interacts with the actors, and what the system does in the use case. Use cases function as a unifying thread throughout the software lifecycle.

Actor Catalog

Introduction

This block describes the list of actors identified for the TACHOnet system.

List of actors

The table hereafter gives a description of the different actors of the TACHOnet system :

Actor	Description
CIA Application	A *CIA*-typed user (see page 66)
Enforcers	The enforcers managed as a *CIA*-typed user (see page 66)
CIA Administrator	A *CIA Administrator*-typed user (see page 66)
TACHOnet	The TACHOnet system
TCN Administrator	A *TCN Administrator*-typed user (see page 66)

Use Case Catalog

Introduction

This block describes the list of use cases identified for the TACHOnet system.

Use Cases Diagram for TCN Administrative Tasks

The following figure outlines the different use cases and actors related to the TACHOnet administrative tasks:

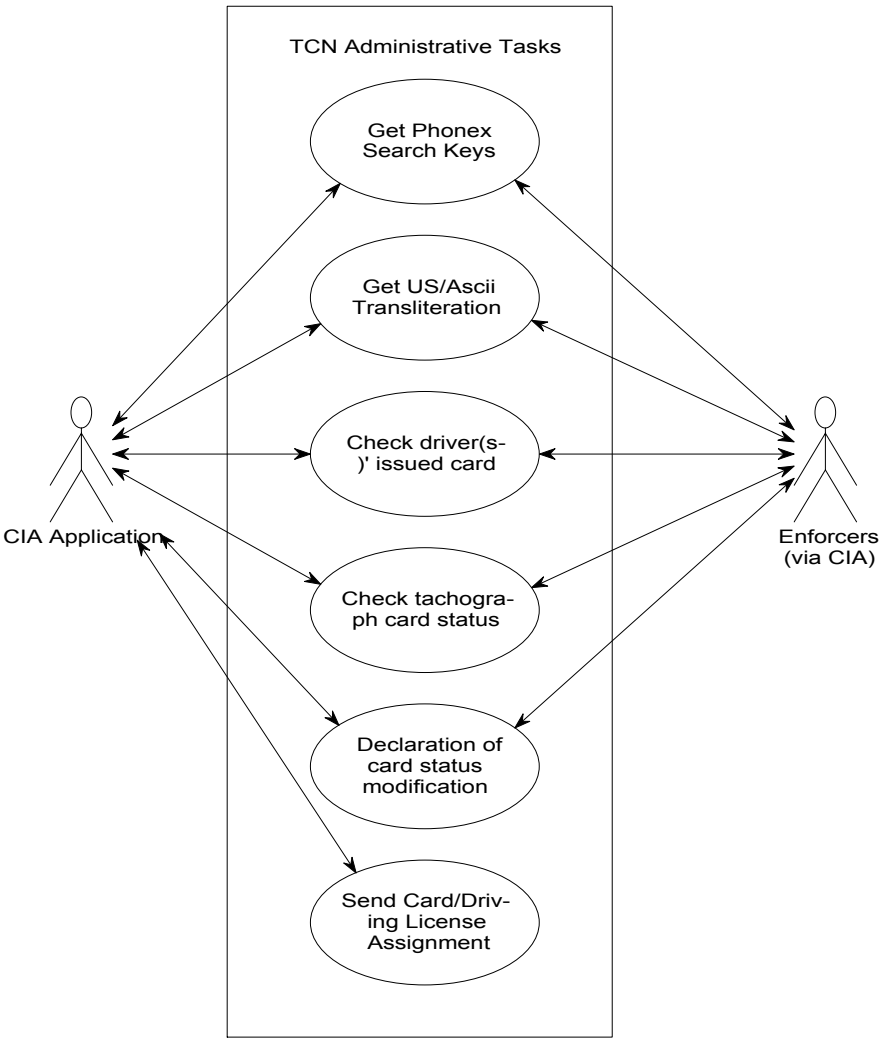


Figure 17 – Use Cases Diagram for TCN Administrative Tasks

Continued on next page

Use Case Catalog, Continued

Use Cases Diagram for TCN System Tasks

The following figure outlines the different use cases and actors related to the TACHOnet administrative tasks:

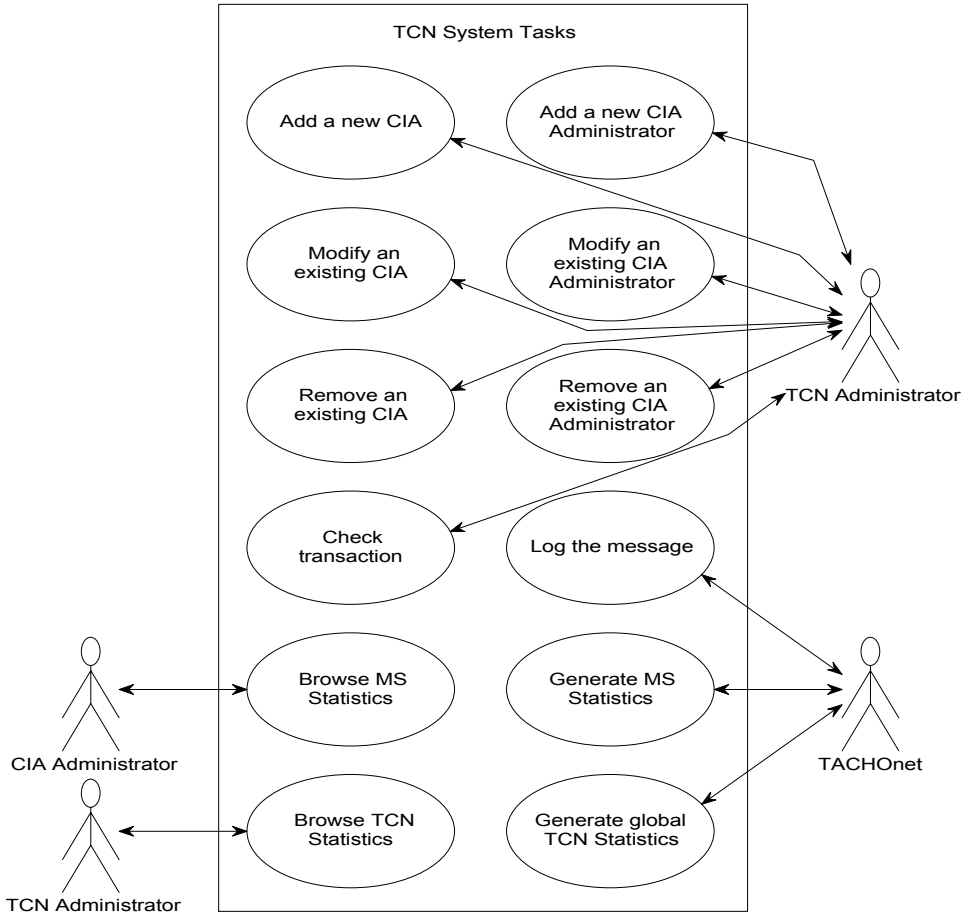


Figure 18 – Use Cases Diagram for TCN System Tasks

List of Use Cases

The table hereafter lists all the use cases along with their assigned id:

UC Id	UC Name
UC-01	Check driver(s)' issued cards
UC-02	Check tachograph card status
UC-03	Declaration of card status modification
UC-04	Send Card/Driving License Assignment
UC-05	Get Phonex Search Keys
UC-06	Get US/Ascii Transliteration

Continued on next page

Use Case Catalog, Continued

List of Use Cases (continued)

UC Id	UC Name
UC-07	Add a new CIA
UC-08	Modify an existing CIA
UC-09	Remove an existing CIA
UC-10	Add a new CIA Administrator
UC-11	Modify an existing CIA Administrator
UC-12	Remove an existing CIA Administrator
UC-13	Check transaction
UC-14	Log the message
UC-15	Generate MS Statistics
UC-16	Generate global TCN Statistics
UC-17	Browse MS Statistics
UC-18	Browse global TCN Statistics

Use Case 01 – Check driver(s)' issued cards

Description

This use case consists of processing a request for checking driver's issued card coming from a Card Issuing Authority (*CIA*). Such request could contain the data for a single driver (*online* mode) or several drivers (*batch* mode).

This use case is also used by enforcers (on behalf of CIA – as TACHOnet only sees CIA as SPOC) during road checks.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	TACHOnet logs the received request as-is in its tracking database.
2	TACHOnet deciphers the received request, assigns it a TACHOnet refid and validates its syntax.
3	TACHOnet will build a new request (from the data of the original request) by applying defined name encoding rules (see in [4]) to the given surname(s) and first name(s) in order to compute the search keys.
4	For each known Member State CIA, TACHOnet encrypts the new request, logs it as-is in its tracking database, sends it to them and waits for receiving each response.
5	For each received response, TACHOnet logs it as-is in its tracking database, deciphers it and validates its syntax. If it is valid, TACHOnet stores the response data (linked to the TCN refid) in the database (for later building the single consolidated response that TACHOnet will send when all responses are received or when the timeout is reached).
6	When all responses are received or when the timeout is reached, TACHOnet builds, from the received responses stored in its database, the single consolidated response.
7	TACHOnet encrypts the consolidated response, logs it as-is in its tracking database, sends it to the original caller.

Alternate flows

Several alternate flows may exist depending on the result of some events/actions of the basic flow:

Alternate flow	Description
ALT-01	When TACHOnet receives a negative response from a Member State CIA, it should log it, warn the TCN Administrator (via e-mail,...) and consider the request sent to that Member State CIA as completed (with error).

Continued on next page

Use Case 01 – Check driver(s)' issued cards, Continued

Alternate flows (continued)

Alternate flow	Description
ALT-02	When TACHOnet receives multiple responses (corresponding to a single request) from a Member State CIA, it should log the superfluous responses, warn the TCN Administrator. The first received response is the processed one.
ALT-03	When TACHOnet doesn't receive within time a Member State CIA response, it should mention 'timeout' as status code for that Member State CIA in the consolidated response.
ALT-04	When TACHOnet receives a late Member State CIA response, it should log it and ignore it.
ALT-05	When TACHOnet receives a syntactically invalid request / response, it should always send back a negative receipt with 'Invalid Format request' as status code and warn the TCN Administrator.
ALT-06	When TACHOnet receives an invalid XML message (request, response), it will respond with a negative receipt mentioning the reason (invalid format).

Special requirements

- ~~Non-repudiation of transaction must be guaranteed~~
- Data privacy must also be guaranteed
- All Member State *CIA*s must provide services (using proposed messages formats below and proposed technical rules in [4]) for:
  - Sending a request for checking driver's issued cards to TACHOnet
  - Receiving and handling a TACHOnet request for checking driver's issued cards
  - Sending TACHOnet a response to such TACHOnet request (asynchronous)
  - Receiving and handling a TACHOnet response to original request for checking driver's issued cards (asynchronous)

Pre-conditions

- The *CIA* requesting the check must be defined in TACHOnet
- The *CIA* requesting the check must send its request using the TACHOnet required request format (see below)

Post-conditions

- The *CIA* requesting the check has received a receipt and a response to its request.

Actors

- A *CIA* requesting the check (CIA's clerk or enforcer)
- All *CIAs* to which TACHOnet will broadcast the request
- The TACHOnet system

Continued on next page

Use Case 01 – Check driver(s)' issued cards, Continued

Messages flow diagram

The following diagram outlines the flow of messages exchanged between actors:

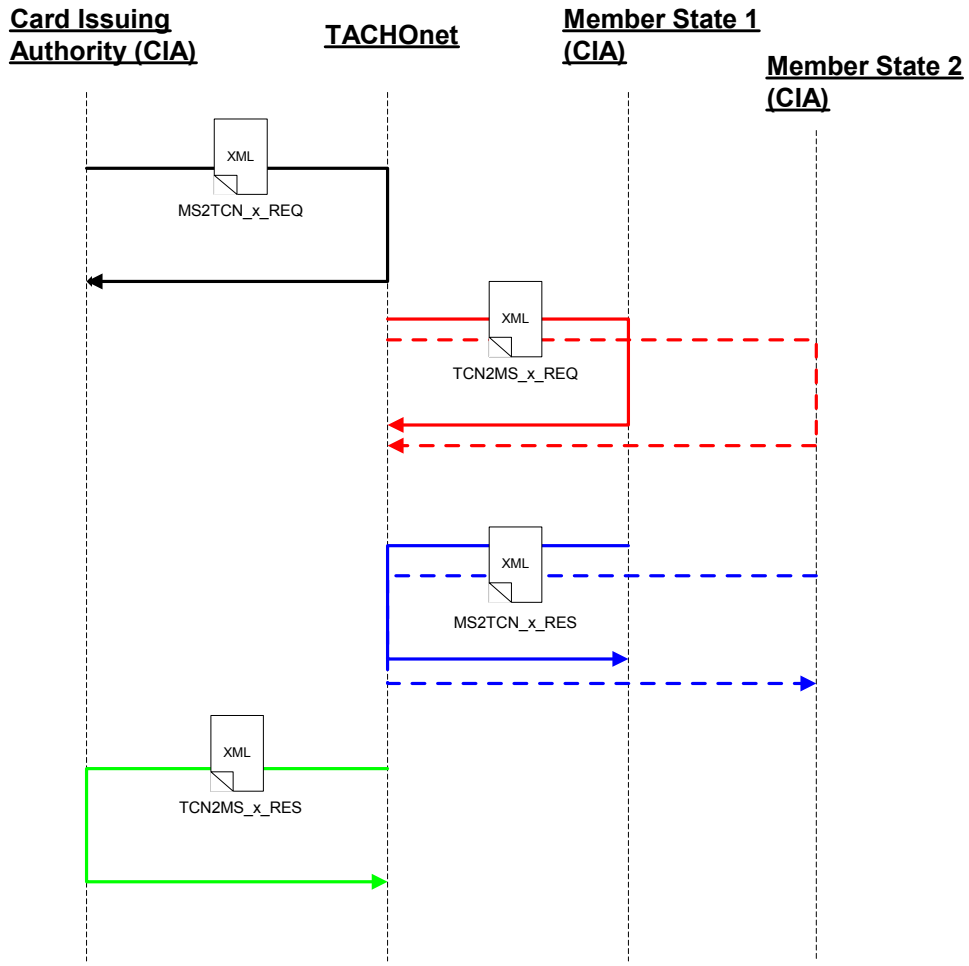


Figure 19 – UC-01 messages flow

XML Messages

Please refer to [7] for a complete description.

Additional remarks

- In case of problems (e.g. network problem,...) when sending a message (request, response), TACHOnet will automatically retry to send it at regular interval till request timeout. Afterwards, if still unsuccessful, it will record a 'Server Error' status code.
- The technical issues related to data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Use Case 02 – Check tachograph card status

Description

This use case consists of checking the status of a tachograph card based on its card number. This use case is very useful for *CIAs* in order to check the validity of a card prior to performing some administrative tasks (e.g. to avoid from declaring a lost/stolen card for a wrongly keyed-in card number,...). It is also useful for enforcement authorities during road-checks [8] where workshop could also be checked (beside driver cards).

The checked card is identified by its card number and its issuing Member State code. As an issued card must be unique, it should only exist in a single *CIA* data store (the *CIA* having issued the card).

Basic flow

The basic flow consists of the following steps:

Step	Action
1	TACHOnet logs the received request as-is in its tracking database.
2	TACHOnet deciphers the received request, assigns it a TACHOnet refid and validates its syntax.
3	TACHOnet will build as much new requests as issuing Member States identified in the original request. TACHOnet figures out the target issuing Member States from the issuing Member State code given for each to-be-checked card. Every new request only contains card numbers issued by a particular Member State.
4	For each identified issuing Member State(s), TACHOnet builds and encrypts the new request, logs it as-is in its tracking database, sends it to it and waits for receiving each response.
5	For each received response, TACHOnet logs it as-is in its tracking database, deciphers it and validates its syntax.
6	When all responses are received or when the timeout is reached, TACHOnet builds and encrypts the consolidated response, logs it as-is in its tracking database, sends it to the original caller.

Alternate flows

The same alternate flows as described for UC-01 (page 95) may exist depending on the result of some events/actions of the basic flow.

Special requirements

- ~~Non-repudiation of transaction must be guaranteed~~
- Data privacy must also be guaranteed
- All Member State *CIA*s must provide services (using proposed messages formats below and proposed technical rules in [4]) for:
  - Sending a request for checking a card number to TACHOnet
  - Receiving and handling a TACHOnet request for checking a card number
  - Sending TACHOnet a response to such TACHOnet request (asynchronous)
  - Receiving and handling a TACHOnet response to original request for checking a card number (asynchronous)

Continued on next page

Use Case 02 – Check tachograph card status, Continued

Pre-conditions

- The *CIA* sending the request must be defined in TACHOnet
- The *CIA* sending the request must send it using the TACHOnet required request format (see below)

Post-conditions

- The *CIA* sending the request has received a receipt and a response to its request.

Actors

- A *CIA* requesting the check (CIA's clerk or enforcer)
- All *CIAs* to which TACHOnet will broadcast the request
- The TACHOnet system

XML Messages

Please refer to [7] for a complete description.

Continued on next page

Use Case 02 – Check tachograph card status, Continued

Messages flow diagram

The following diagram outlines the flow of messages exchanged between actors (assuming a single card number is specified in the original request, meaning TACHOnet has to forward the request to the Member State having issued the card):

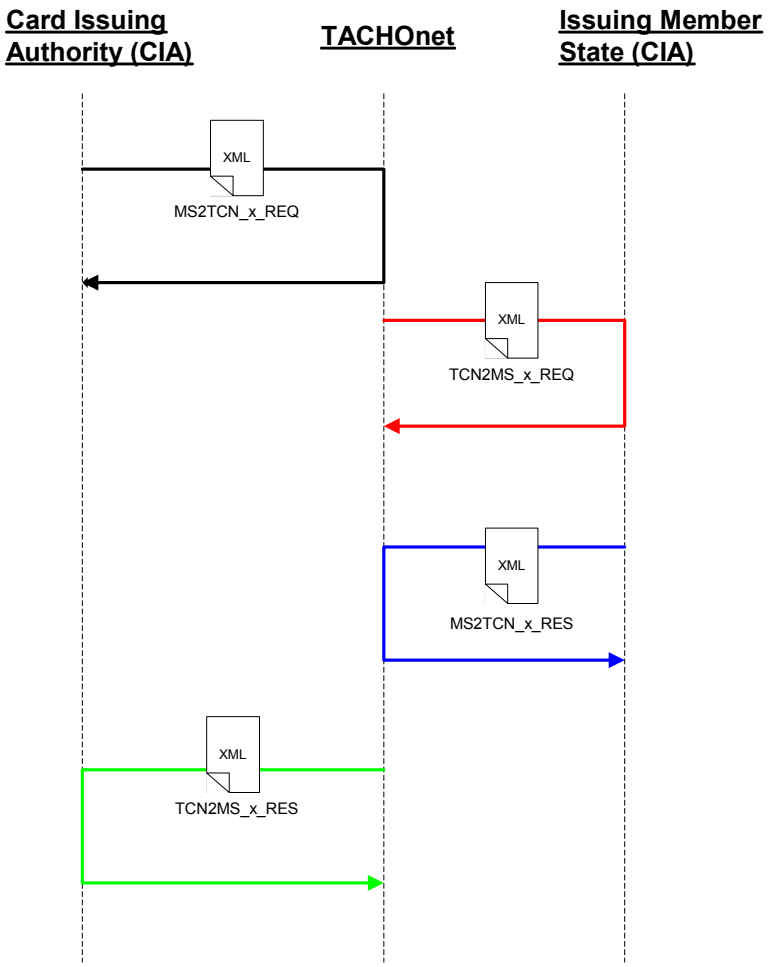


Figure 20 – UC-03 messages flow

Additional remarks

- In case of problems (e.g. network problem,...) when sending a message (request, receipt, response), TACHOnet will automatically retry to send it at regular interval till request timeout. Afterwards, if still unsuccessful, it will record a 'Server Error' status code.
- The technical issues related to data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Use Case 03 – Declaration of card status modification

Description

This use case consists of processing a request for declaring the modification of the status of card. It can be asked by CIA clerks or by enforcers.

But how such use case fit within the analysed business processes? Well, from TACHOnet point of view, the following business processes merely consists of sending a message to the issuing *CIA* asking for changing the actual status of card to a new status:

Process	New card status①	Description
Lost card declaration	*Lost*	The *CIA* having issued the card should change the card status at successful completion of the request
Stolen card declaration	*Stolen*	The *CIA* having issued the card should change the card status at successful completion of the request
Malfunctioning card declaration	*Defective*	The *CIA* having issued the card should change the card status at successful completion of the request
Suspended card declaration	*Suspended*	The *CIA* having issued the card should change the card status at successful completion of the request
Lost/stolen card hand in declaration	*StolenButHandedIn* *LostButHandedIn*	The *CIA* having issued the card should change the card status at successful completion of the request
Exchange of a card (start)	*InExchange*	The *CIA* having issued the old card should change the card status at successful completion of the request
Exchange of a card (delivery of new card)	*Exchanged*	The *CIA* having issued the old card should change the card status at successful completion of the request

① assumes the actual card status allows for such modification

Table 1 – New card status

Basic flow

The basic flow consists of the following steps:

Step	Action
1	TACHOnet logs the received request as-is in its tracking database.
2	TACHOnet deciphers the received request, assigns it a TACHOnet refid and validates its syntax.

Continued on next page

Use Case 03 – Declaration of card status modification,
Continued

Basic flow (continued)

Step	Action
3	TACHOnet will build as much new requests as issuing Member States identified in the original request. TACHOnet figures out the target issuing Member States based on the CIA country code given in the original request. Every new request only contains card numbers issued by a particular Member State.
4	For each identified issuing Member State(s), TACHOnet builds and encrypts the new request, logs it as-is in its tracking database, sends it to it and waits for receiving each receipt and response.
5	For each received response, TACHOnet logs it as-is in its tracking database, deciphers it and validates its syntax.
6	When all responses are received or when the timeout is reached, TACHOnet builds and encrypts the consolidated response, logs it as-is in its tracking database, sends it to the original caller.

Alternate flows

The same alternate flows as described for UC-01 (page 95) may exist depending on the result of some events/actions of the basic flow.

Special requirements

- ~~Non-repudiation of transaction must be guaranteed~~
- Data privacy must also be guaranteed
- All Member State *CIA*s must provide services (using proposed messages formats below and proposed technical rules in [4]) for:
  - Sending a request for declaring card status modification to TACHOnet
  - Receiving and handling a TACHOnet request for declaring card status modification
  - Sending TACHOnet a response to such TACHOnet request (asynchronous)
  - Receiving and handling a TACHOnet response to original request for declaring card status modification (asynchronous)

Pre-conditions

- The *CIA* sending the declaration must be defined in TACHOnet
- The *CIA* sending the declaration must send its request using the TACHOnet required request format (see below)
- The *CIA* sending the declaration must have first sent a request for checking the card number for which status modification is required.

Post-conditions

- The *CIA* sending the declaration has received a receipt and a response to its request.
- The *CIA* having issued the card has received the request and processed it.

Continued on next page

Use Case 03 – Declaration of card status modification,
Continued

Actors

- A *CIA* declaring the card status modification (CUA's clerk or enforcer)
- The *CIA* having issued the card
- The TACHOnet system

Messages flow diagram

The following diagram outlines the flow of messages exchanged between actors (assuming a single card number is specified in the original request, meaning TACHOnet has to forward the request to the Member State having issued the card):

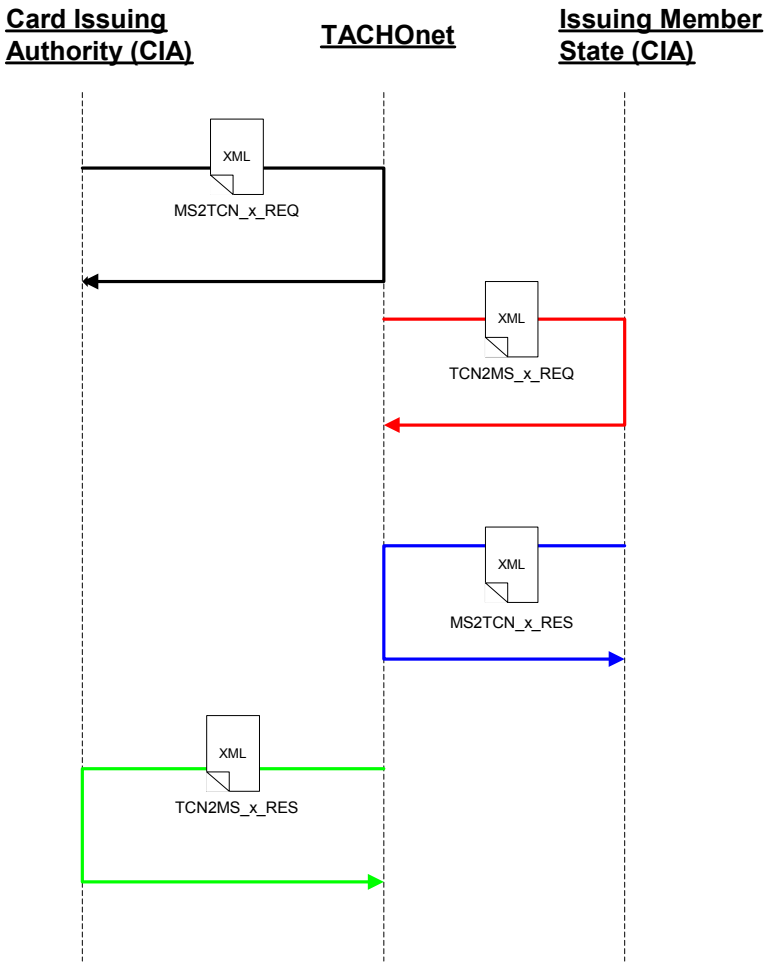


Figure 21 – UC-03 messages flow

XML Messages

Please refer to [7] for a complete description.

Continued on next page

Use Case 03 – Declaration of card status modification,
Continued

Additional remarks

- In case of problems (e.g. network problem,...) when sending a message (request, receipt, response), TACHOnet will automatically retry to send it at regular interval till request timeout.
- The technical issues related to data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Use Case 04 – Send Card/Driving License Assignment

Description

This use case is born from the "Luxemburg agreement" (see page 25 or [5] for more details). It should be used by CIAs in the particular case when a card has been issued to a driver who showed a foreign driving license. The CIA must then warn, via TACHOnet, the Member State having issued the driving license that a brand new card has been issued with the corresponding driving license number. Upon receipt of such request, the Member State having issued the driving license should store that information (issued card number associated to the driving license number) in its own local data store.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	TACHOnet logs the received request as-is in its tracking database.
2	TACHOnet deciphers the received request, assigns it a TACHOnet refid and validates its syntax.
3	TACHOnet will build as much new requests as issuing Member States identified in the original request (e.g. if more than one card/driving license number is given in the request). TACHOnet figures out the target driving license issuing Member State(s) from the issuing Member State code given for each card. Every new request only contains card and driving license numbers issued by a particular Member State.
4	For each identified issuing Member State(s), TACHOnet builds and encrypts the new request, logs it as-is in its tracking database, sends it to it and waits for receiving each response.
5	For each received response, TACHOnet logs it as-is in its tracking database, deciphers it and validates its syntax.
6	When all responses are received or when the timeout is reached, TACHOnet builds and encrypts the consolidated response, logs it as-is in its tracking database, sends it to the original caller.

Alternate flows

The same alternate flows as described for UC-01 (page 95) may exist depending on the result of some events/actions of the basic flow.

Continued on next page

Use Case 04 – Send Card/Driving License Assignment,
Continued

Special requirements

- ~~Non-repudiation of transaction must be guaranteed~~
- Data privacy must also be guaranteed
- All Member State *CIA*s must provide services (using proposed messages formats below and proposed technical rules in [4]) for:
  - Sending a request for checking a card number to TACHOnet
  - Receiving and handling a TACHOnet request for checking a card number
  - Sending TACHOnet a response to such TACHOnet request (asynchronous)
  - Receiving and handling a TACHOnet response to original request (asynchronous)

Pre-conditions

- The *CIA* sending the request must be defined in TACHOnet
- The *CIA* sending the request must send it using the TACHOnet required request format (see below)

Post-conditions

- The *CIA* sending the request has received a receipt and a response to its request.

Actors

- A *CIA* requesting the update
- All *CIAs* to which TACHOnet will broadcast the request
- The TACHOnet system

XML Messages

Please refer to [7] for a complete description.

Continued on next page

Use Case 04 – Send Card/Driving License Assignment,
Continued

Messages flow diagram

The following diagram outlines the flow of messages exchanged between actors (assuming a single card number is specified in the original request, meaning TACHOnet has to forward the request to the Member State having issued the card):

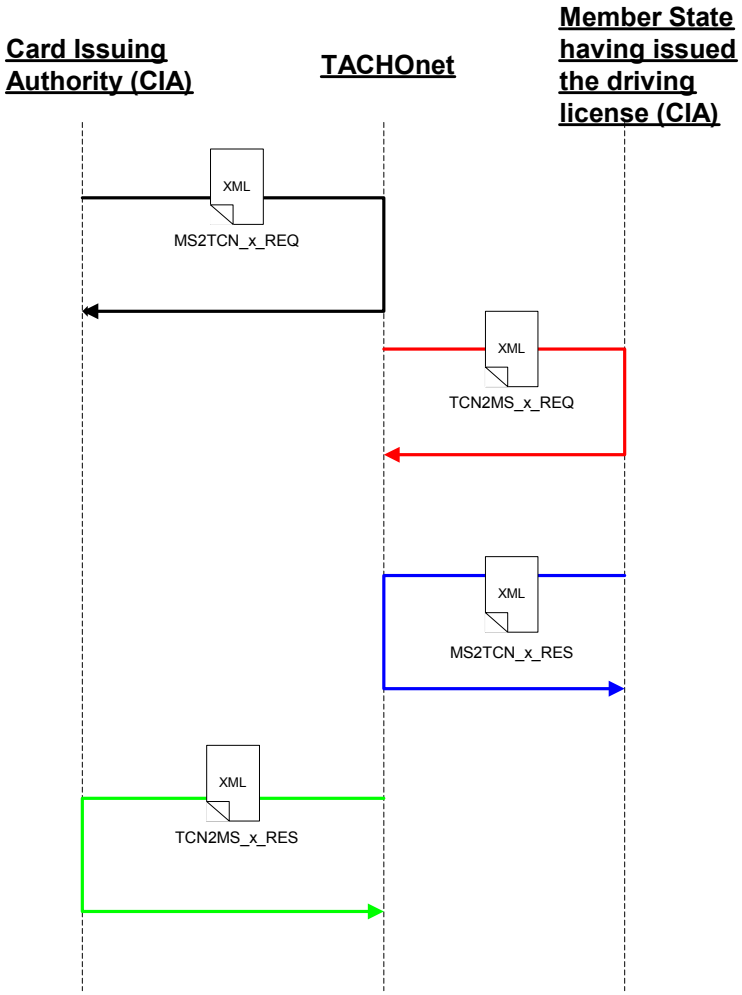


Figure 22 – UC-04 messages flow

Additional remarks

- In case of problems (e.g. network problem,...) when sending a message (request, receipt, response), TACHOnet will automatically retry to send it at regular interval till request timeout.
- The technical issues related to data encoding, name encoding rules, security, network,... will be analysed in details in [4].

Use Case 05 – Get Phonex Search Keys

Description

This use case consists of getting from TACHOnet the computed search keys (based on the Phonex algorithm) corresponding to the given last name and first names.

The Member State CIAs should call upon this service when issuing a new card to get the computed search keys of the driver's surname and first names, so to store them in their local data store. When a Member State CIA will receive a TACHOnet request for checking driver's issued card, it should use the search keys given in the request to search against their local data store (along with the given driver's birth date). It's therefore of major importance to use a common algorithm and to store computed search keys in the local data store.

Nevertheless, Member States are free to use their own Phonetic algorithm (if existing like in Germany). In such a case, it's the Member State responsibility to compute the search keys based on the given driver's surname and first of the first names.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	The CIA calls the TACHOnet service giving the driver's surname and first names.
2	TACHOnet checks the input parameters and, if valid, computes the corresponding surname and first of the first names search keys.
3	TACHOnet returns the computed search keys as output parameters.

Alternate flows

2a If the input parameters are invalid (e.g. illegal character,…), TACHOnet returns a negative status code to the request.

Special requirements

- This service should ideally be implemented as a synchronous Web Service.
- A web interface on top of this service should also be supplied.
- A downloadable version of this web service should also be made available to enable some Member States to install and use it locally.

Pre-conditions

The caller must provide the mandatory input parameters.

Post-conditions

The caller has received the computed search keys (or a negative error code).

Actors

- A *CIA* (when issuing a new card) or an enforcer (via a CIA)
- The TACHOnet system

Continued on next page

Use Case 05 – Get Phonex Search Keys, Continued

Message flow diagram

The following diagram outlines the flow of messages exchanged between actors:

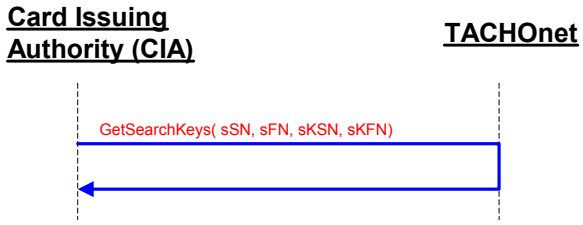


Figure 23 – UC-05 messages flow

Input data

- **Surname (sSN):** driver's surname
- **First names (sFN):** driver's first names

Output data

- **Surname (sKSN):** computed search key of driver's surname
- **First names (sKFN):** computed search key of driver's first of first names

Additional remarks

- Parameters should be UTF-8 encoded.

Open issues

- Should such service provide confidentiality (through encryption)?

Use Case 06 – Get US/Ascii Transliteration

Description

This use case consists of getting from TACHOnet the US/Ascii (ISO 646 IRV) transliteration (From Latin or Greek) of the given driver's surname, first names, place of birth and driving license number.

Up to now, this use case only provides the transliteration from Greek (according to the ISO 843:1997 standard) or Latin to US/Ascii. Other transliterations (e.g. Cyrillic to US/Ascii according to ISO 9:1995) will be provided when needed.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	The CIA calls the TACHOnet service giving the driver's surname, first names, place of birth and driving license number.
2	TACHOnet checks the input parameters and, if valid, transliterates the corresponding values into US/Ascii.
3	TACHOnet returns the transliterated values as output parameters.

Alternate flows

2a If the input parameters are invalid (e.g. illegal character,…), TACHOnet returns a negative status code to the request.

Special requirements

- This service should ideally be implemented as a synchronous Web Service.
- A web interface on top of this service should also be supplied.
- A downloadable version of this web service should also be made available to enable some Member States to install and use it locally.

Pre-conditions

The caller must provide the mandatory input parameters.

Post-conditions

The caller has received the computed search keys (or a negative error code).

Actors

- A *CIA* (when issuing a new card) or an enforcer (via a CIA)
- The TACHOnet system

Continued on next page

Use Case 06 – Get US/Ascii Transliteration, Continued

Message flow diagram

The following diagram outlines the flow of messages exchanged between actors:

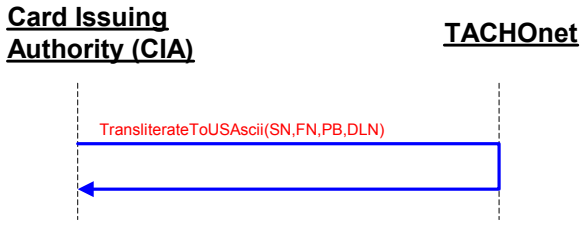


Figure 24 – UC-06 messages flow

Input data

- **Surname (SN):** driver's surname
- **First names (FN):** driver's first names
- **Place of Birth (PB):** driver's place of birth
- **Driving license number (DLN):** driver's driving license number

Output data

The transliterated values as an array of strings

Additional remarks

- Parameters should be UTF-8 encoded.

Open issues

- Should such service provide confidentiality (through encryption)?

Use Cases 07 up to 13

Description

These use cases consists of those related to Users & access rights management (UCs 07-12) and to the "Check transaction" request (UC 13).

As already mentioned in the "Analysis of the Business Processes" chapter, these use cases will be processed **manually** according sound procedures and policies that need to be defined by a kind of TCN User Group (or Management Board).

Use Case 14 – Log the message

Description

This use case consists of logging as-is every message sent or received by TACHOnet.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	Upon receiving a message, TACHOnet should log it as-is in the tracking database.
2	Prior to sending a message, TACHOnet should log it as-is in the tracking database.

Alternate flows

- TACHOnet should also provide a system for archiving (e.g. removing from the tracking database to flat files) "old" messages (how long should TACHOnet keep track of a message?).

Special requirements

- Great care must be taken when setting up the tracking database in terms of sizing (the number of the messages to be logged might quickly become huge), performance (the logging mechanism should not impede overall TACHOnet system performance), availability (high availability must be guaranteed through clustering,...) and security (restricted administrative access, strong backup policies,...).

Pre-conditions

- A message (request, response) is received by TACHOnet or about to be sent by TACHOnet.

Post-conditions

- The received/sent message is logged as-is in the tracking database

Actors

- TACHOnet system

Additional remarks

-

Open issues

Please refer to page 74.

Use Case 15 – Generate MS statistics

Description

This use case consists of generating usage statistics reports for each *CIA*-typed user defined in TACHOnet and to make this report available (for browsing via a secure Web interface) to the corresponding *CIA Administrator*.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	The timer triggers the generation of the reports (on a daily and/or weekly and/or monthly and/or yearly basis) for the different Member States (*CIA*).
2	The reports are generated (see "Statistics management" for more details) and made available to the different *CIA administrators* (keeping in mind a *CIA administrator* may only access reports dealing with the Member State he's administrator of).

Alternate flows

-

Special requirements

- The generated reports should be dynamic reports, accessible for browsing through a Web interface (e.g. using tools such BusinessObjects Webi)

Pre-conditions

- A timer triggers the generation process (weekly, monthly, quarterly, yearly)

Post-conditions

- The generated reports are made available (for browsing via a secure Web interface) to their corresponding *CIA Administrators*.

Actors

- TACHOnet system

Additional remarks

-

Open issues

- Which tool should be used to generate such reports?
- What's the final structure of the reports?
- Please refer to page 72.

Use Case 17 – Generate global TACHOnet statistics

Description

This use case consists of generating some statistics info for TACHOnet internal purposes, i.e. not aimed at being distributed to the Member States. Such statistics should be made available (for browsing via a secure Web interface) to the TCN Administrator.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	The timer triggers the generation of the report (on a daily and/or weekly and/or monthly and/or yearly basis).
2	The report- is generated (see "Statistics management" for more details) and made available to the *TCN administrator*.

Alternate flows

-

Special requirements

- The generated report should be a dynamic report, accessible for browsing through a Web interface (e.g. using tools such BusinessObjects Webi)

Pre-conditions

- A timer triggers the generation process.

Post-conditions

- The statistics are generated.

Actors

- TACHOnet system

Additional remarks

-

Open issues

- Which tool should be used to generate such reports?
- What's the final structure of the reports?
- Please refer to page 72.

Use Case 17 – Browse MS statistics

Description

This use case consists of allowing every *CIA-Administrator*-typed user defined in TACHOnet to browse, via a secure Web interface, the usage statistics report corresponding to the Member State he's administrator of.

Basic flow

The basic flow consists of the following steps:

Step	Action
1	The CIA administrator gets connected to the TACHOnet Reports Web application (using his own certificate for secure access)
2	The CIA administrator types in his user name and password.
3	TACHOnet checks the credentials and grants (or denies) access to the reports.
4	If granted, the CIA Administrator may then select a report (among a list of prepared reports) and browse through it.

Alternate flows

-

Special requirements

- The generated reports should be dynamic reports, accessible for browsing through a Web interface (e.g. using tools such BusinessObjects Webi)

Pre-conditions

- The reports should have been generated and made available

Post-conditions

- A *CIA Administrator* has browsed reports dealing with the Member State he's administrator of.

Actors

- *CIA Administrator*

Additional remarks

-

Open issues

- Which tool should be used to browse such reports?
- What's the final structure of the reports?
- Please refer to page 72.

Use Case 18 – Browse global TACHOnet statistics

Description

This use case consists of browsing, via a secure Web interface, statistics info for TACHOnet (*TCN Administrator* only).

Basic flow

The basic flow consists of the following steps:

Step	Action
1	The TCN administrator gets connected to the TACHOnet Reports Web application (using his own certificate for secure access)
2	The TCN administrator types in his user name and password.
3	TACHOnet checks the credentials and grants (or denies) access to the report.
4	If granted, the TCN Administrator may then browse the internal statistics info.

Alternate flows

-

Special requirements

- The generated report should be a dynamic report, accessible for browsing through a Web interface (e.g. using tools such BusinessObjects Webi)

Pre-conditions

- The reports should have been generated and made available.

Post-conditions

- The TCN Administrator has browsed the internal statistics info.

Actors

- TCN Administrator

Additional remarks

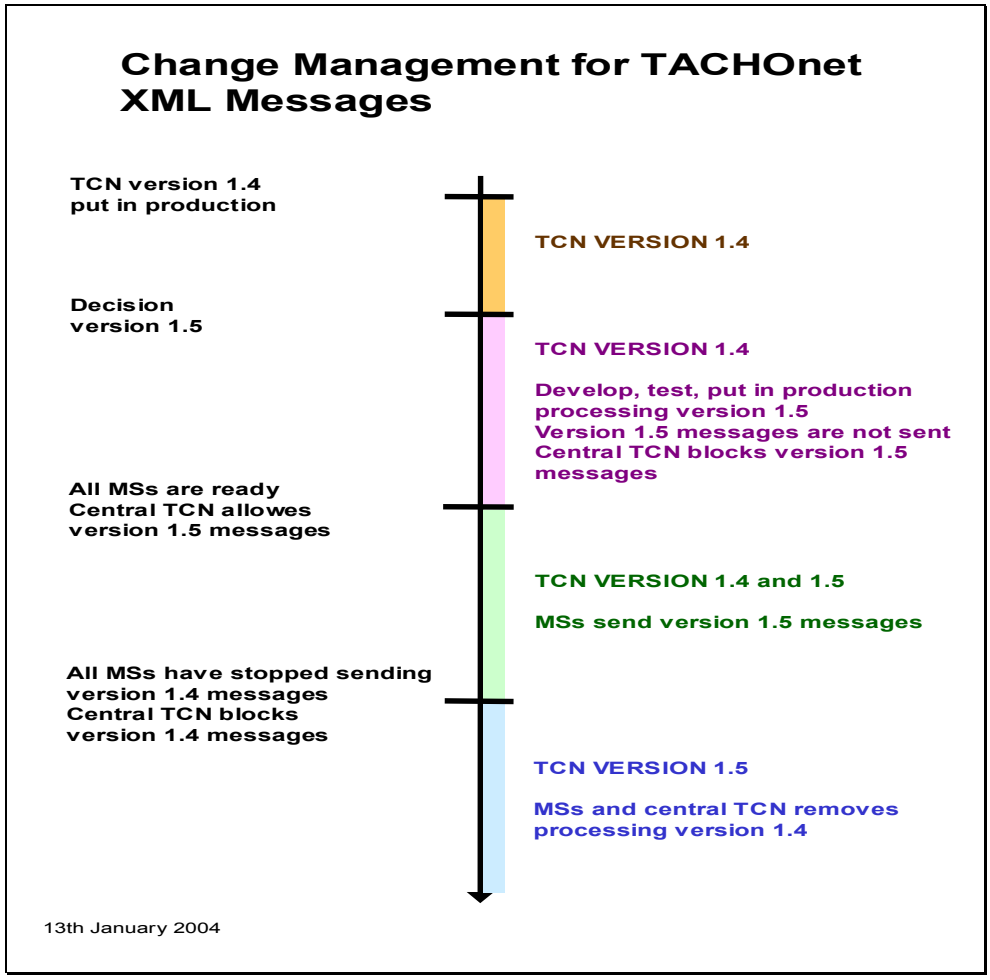
-

Open issues

- Which tool should be used to browse such reports?
- What's the final structure of the reports?
- Please refer to page 72.

Annex – TACHOnet Change Management Procedure

Roadmap



Explanation

The specific version 1.4 and 1.5 are used only to exemplify how the change would be performed using this method. No change to TACHOnet is suggested, and there is not a 1.5 version planned or decided for the time being.

Then starting from the assumption that Member States have agreed on the change and a new version 1.5 of XML Messaging Reference Guide has been issued, Member States will implement version 1.5 during a certain period of time. This period could be some months, and each Member States would be able to find a suitable date. This date may be different for each Member State, no Big Bang.

The processing of the version 1.4 is not yet removed from Member States TACHOnet system and only 1.4 queries/reports are sent. However, the TACHOnet system is ready to reply to 1.5 messages.

Explanation, *contd*

When all Member States completed the implementation, those latter may start sending 1.5 messages.

This is also done during a certain period of time and it is possible for Member States to choose different dates. Since all Member States can reply to both 1.4 and 1.5, no conversion by central TACHOnet to/from 1.4 to 1.5 is needed.

Member States will also receive replies to their messages of the same version as they were sent.

When all Member States are using 1.5 messages, 1.4 processing may be removed from the TACHOnet system. This could also be done at a convenient point of time, for instance when next changes, version 1.6, are implemented.