Getronics
ICT SOLUTIONS AND SERVICES

N.V. Getronics Belgium S.A.

Rue de Genèvestraat 10

1140 BRUXELLES/BRUSSEL

☎ (32) 2 229.91.11

DG Energy & Transport

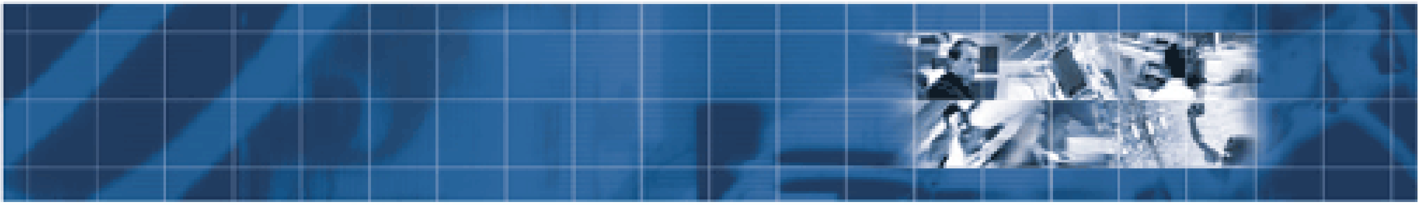
DG TREN

TACHOnet

Software Requirements Specification

01_00

21-Feb-03



Document Approval

	NAME	DATE	SIGNATURE
Prepared by:	F. Silvestre	21-Feb-03	
Checked by:	Ph. Francis	21-Feb-03	
Quality control by:	P. Delmée	21-Feb-03	
Approved by:	Yves Hardy (DG TREN)		

Distribution List

COMPANY	NAME	FUNCTION	FOR INFO / APPROVAL
DG TREN	Y. Hardy	Project Manager	Approval
Getronics	P. Delmée	Project Manager	Info
Getronics	Ph. Francis		
Getronics	W. Van Acker		

Change Control History

VERSION	DATE	AUTHOR	DESCRIPTION	PARAGRAPHS
00_01	04-Dec-03	F. Silvestre	Original issue	
01_00	21-Feb-03	F. Silvestre	Release iteration C1	

Document information

CREATION DATE:	04-Dec-03
FILENAME:	TCN-SRS-01_00-EN.doc
LOCATION:	
NUMBER OF PAGES:	76

CONTENTS

Introduction

Purpose

This document aims at capturing the complete software requirements for the system. It fully describes the external behaviour of the application(s) or subsystem(s) identified. It also describes non-functional requirements, design constraints and other factors necessary to provide a complete and comprehensive description of the requirements for the software.

The current version of this document is the one released at end of iteration C1.

References

The present document makes references to the following documents:

- [1] Specific Agreement n°36 under framework contract n° DI/02450-00 – 13-Nov-03
- [2] TCN XML Messaging Reference Guide V1.40.
- [3] Card Issuing Working Group – General Report – URBA 2000.

Abbreviations

- CIA – Card Issuing Authority
- MS – Member State
- SPOC – Single Point Of Contact
- TCN – TACHOnet

Structure of the document

The first chapter describes the functional and non-functional requirements. The second 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.

Chapter 1: 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,
- interface requirements and
- physical requirements.

Functionality (FUN)

Functional requirements may include:

- feature sets,
- capabilities, and
- security.

Continued on next page

Types of Requirements, Continued

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.

Reliability (REL)

Reliability requirements to be considered are:

- Availability (percentage of time available, hours of use, maintenance access,…)
- 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:

- throughput (e.g. transactions per second),
- response time,
- recovery time, or
- resource usage (memory, disk, cpu,…).

Continued on next page

Types of Requirements, Continued

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.

This section should indicate any design constraints on the system being built. Design constraints represent design decisions that have been mandated and must be adhered to. Examples include software languages, software process requirements, prescribed use of developmental tools, architectural and design constraints, purchased components, class libraries, etc.

Interface Requirement (INT)

This section defines the interfaces that must be supported by the application. It should contain adequate specificity, protocols, ports and logical addresses, etc., so that the software can be developed and verified against the interface requirements.

An interface requirement may be classified into:

- User interface (user interfaces that are to be implemented by the software)
- Hardware interface (hardware interfaces that are to be supported by the software, including logical structure, physical addresses, expected behavior, etc.)
- Software interface (software interfaces to other components of the software system. These may be purchased components, components reused from another application or components being developed for subsystems outside of the scope of this project, but with which this software application must interact).

Continued on next page

Types of Requirements, Continued

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

Applicable Standards Requirements (STD)

This section describes by reference any applicable standards and the specific sections of any such standards that apply to the system being described. For example, this could include legal, quality and regulatory standards, industry standards for usability, interoperability, internationalization, operating system compliance, etc.

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 2: 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.

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.

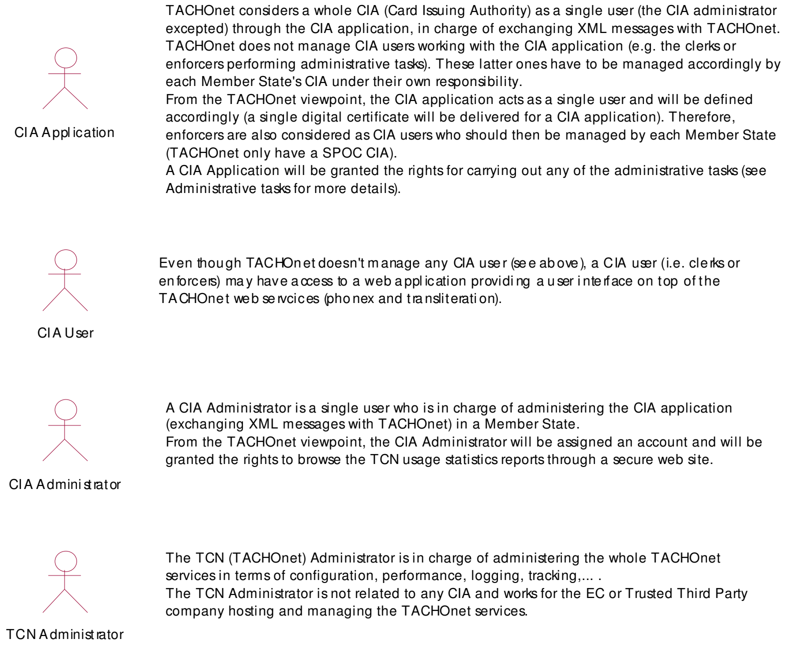
What’s a Use Case ?

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 map describes the list of identified actors.

List of actors The following figure describes the different actors:



CIA Application

TACHOnet considers a whole CIA (Card Issuing Authority) as a single user (the CIA administrator excepted) through the CIA application, in charge of exchanging XML messages with TACHOnet. TACHOnet does not manage CIA users working with the CIA application (e.g. the clerks or enforcers 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 application acts as a single user and will be defined accordingly (a single digital certificate will be delivered for a CIA application). 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 Application will be granted the rights for carrying out any of the administrative tasks (see Administrative tasks for more details).

CIA User

Even though TACHOnet doesn't manage any CIA user (see above), a CIA user (i.e. clerks or enforcers) may have access to a web application providing a user interface on top of the TACHOnet web servcices (phonex and transliteration).

CIA Administrator

A CIA Administrator is a single user who is in charge of administering the CIA application (exchanging XML messages with TACHOnet) in a Member State.
From the TACHOnet viewpoint, the CIA Administrator will be assigned an account and will be granted the rights to browse the TCN usage statistics reports through a secure web site.

TCN Administrator

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 EC or Trusted Third Party company hosting and managing the TACHOnet services.

Figure 1 – List of Actors

Use Case Catalog

Introduction

This map describes the list of identified use cases. For clarity reasons, use cases are organized as packages. The description of each of the use cases packages is given in the next sections.

Use Case Model Diagram

The following figure outlines the actors and use cases of the TACHOnet system:

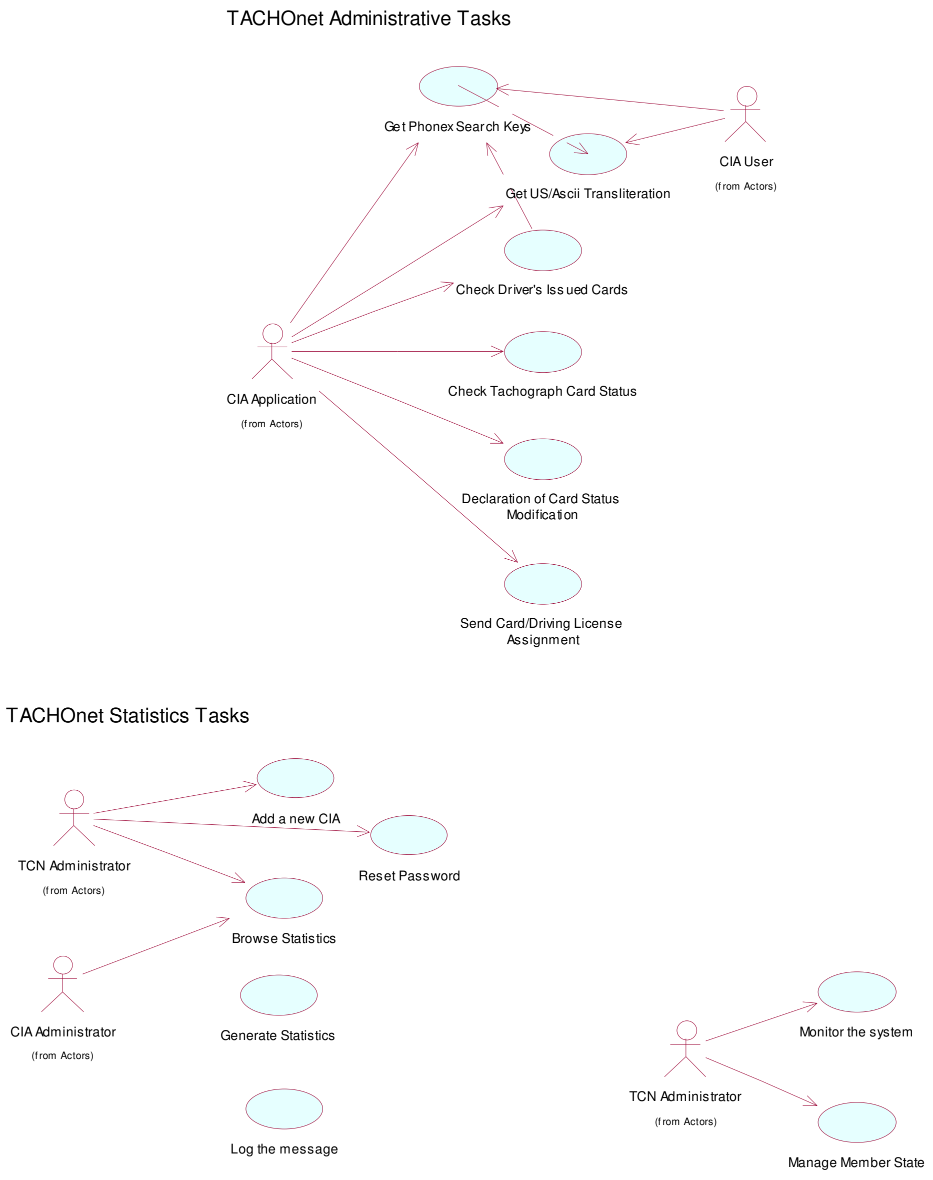


Figure 2 – Use Case Model Diagram

Continued on next page

Use Case Catalog, Continued

List of Use Case Packages

For organizational purposes, use cases are gathered in packages. The list of the TCN Use Case Packages is outlined in the following diagram:

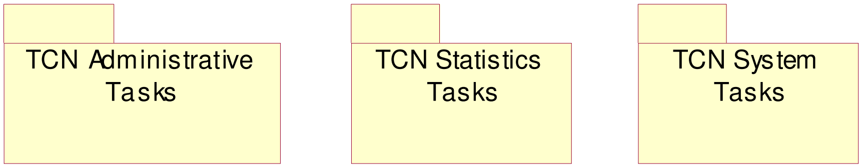


Figure 3 – List of Use Case Packages

List of Use Cases

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

The UC Package…	**Contains the following Use Cases…**
TCN Administrative Tasks	▪ Check Driver's Issued Cards ▪ Check Tachograph Card Status ▪ Declaration of Card Status Modification ▪ Send card/Driving License Assignment ▪ Get Phonex Search Keys ▪ Get US/Ascii Transliteration
TCN Statistics Tasks	▪ Add a new CIA ▪ Reset Password ▪ Browse Statistics ▪ Generate Statistics ▪ Log the message
TCN System Tasks	▪ Monitor the system ▪ Manage Member State

Section 2.1 - Use Case Package "TCN Administrative Tasks"

Overview

Introduction

This section describes the use cases related to the "TCN Administrative Tasks" package. The following diagram gives a high-level view of the use cases of this package:

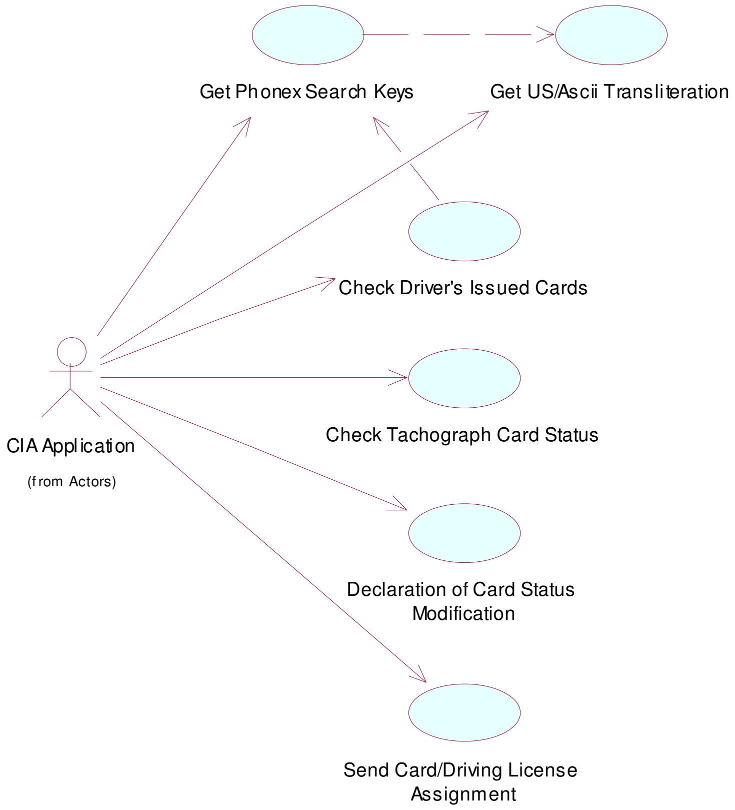

Get Phonex Search Keys
Get US/Ascii Transliteration
Check Driver's Issued Cards
CIA Application
(from Actors)
Check Tachograph Card Status
Declaration of Card Status Modification
Send Card/Driving License Assignment

Figure 4 –Use Case Package "TCN Administrative Tasks"

Continued on next page

Overview, Continued

Contents This section contains the following topics:

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 deciphers the received request and logs the received request as-is in its tracking database.
2	TACHOnet validates its syntax and assigns it a TACHOnet refid (TCNRefId).
3	TACHOnet will build as many new requests as issuing Member State codes identified in the original request (+ another one for all sub-requests not mentioning any issuing Member State code) by applying defined name encoding rules to the given surname(s) and first name(s) in order to compute the search keys.
4	For each issuing Member State identified (if any) in the original request, TACHOnet builds, logs and encrypts a new request (only containing sub-requests for the corresponding issuing Member State), sends it to the corresponding Member State's CIA application and waits for receiving the response. For the sub-request mentioning any issuing Member State code (if any), TACHOnet builds, logs and encrypts a new request (only containing sub-requests not mentioning any issuing Member State), broadcasts it to all the Member States configured in TACHOnet (except the Member State having sent the original request) and waits for receiving each response.
5	For each received response, TACHOnet deciphers it, logs it as-is in its tracking database 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 logs the consolidated response is in its tracking database, encrypts it and sends it to the original caller.

Continued on next page

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

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 and consider the request sent to that Member State CIA as completed (with error).
ALT-02	When TACHOnet receives multiple responses (corresponding to a single request) from a Member State CIA, it should ignore the superfluous additional responses. 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 [2]) 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 response to its request.

Continued on next page

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

Actors

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

Messages flow diagram

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

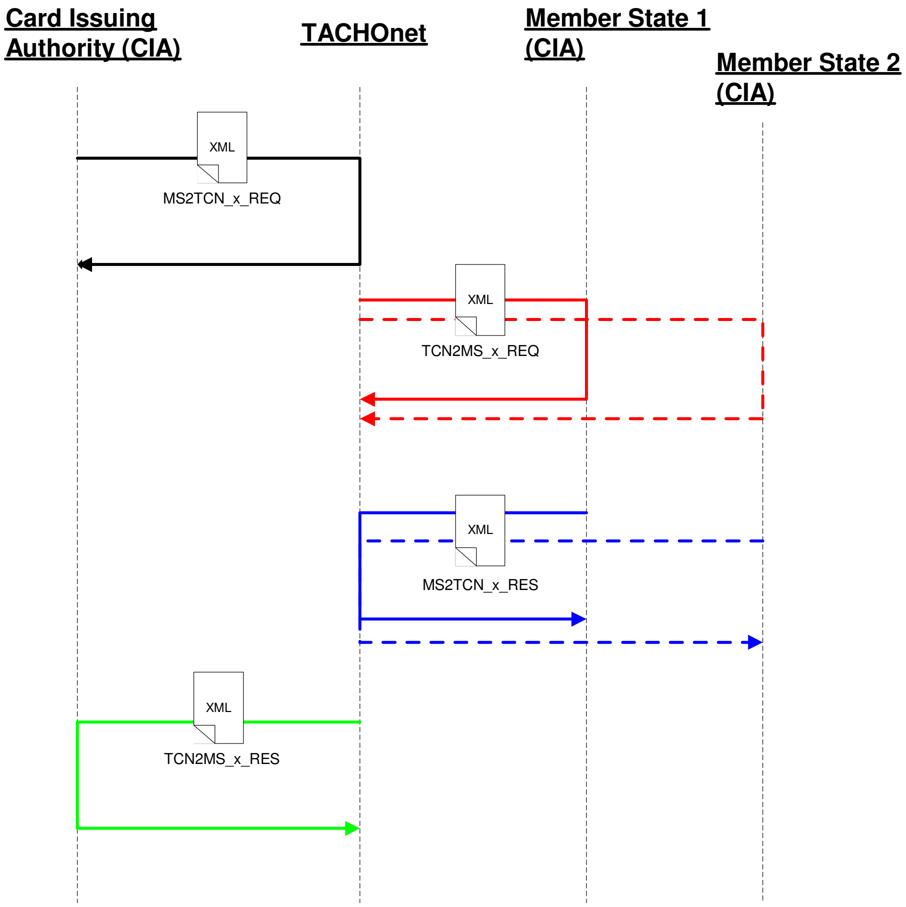


Figure 5 – UC-01 messages flow

XML Messages

Please refer to [2] 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 3 times at regular interval till request timeout. Afterwards, if still unsuccessful, it will record a 'Server Error' status code.

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 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 deciphers the received request and logs the received request as-is in its tracking database.
2	TACHOnet validates its syntax and assigns it a TACHOnet refid (TCNRefId).
3	TACHOnet will build as many new requests as issuing Member State codes identified in the original request. TACHOnet figures out the target issuing Member State(s) from the issuing Member State code given for each to-be-checked card. Every new request only contains card number(s) issued by a particular Member State.
4	For each identified issuing Member State(s), TACHOnet builds, logs and encrypts the new request, sends it to it and waits for receiving the response.
5	For each received response, TACHOnet deciphers it, logs it as-is in its tracking database and validates its syntax. If it's valid, TACHOnet stores the response message (linked to the TCNRefId) 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, logs and encrypts the consolidated response (from the responses received so far), and sends it to the original caller.

Alternate flows

The same alternate flows as described for UC-01 (page 23) may exist depending on the result of some events/actions of the basic flow.

Continued on next page

Use Case 02 – Check tachograph card status, 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 [2]) 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)

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 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 [2] 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):

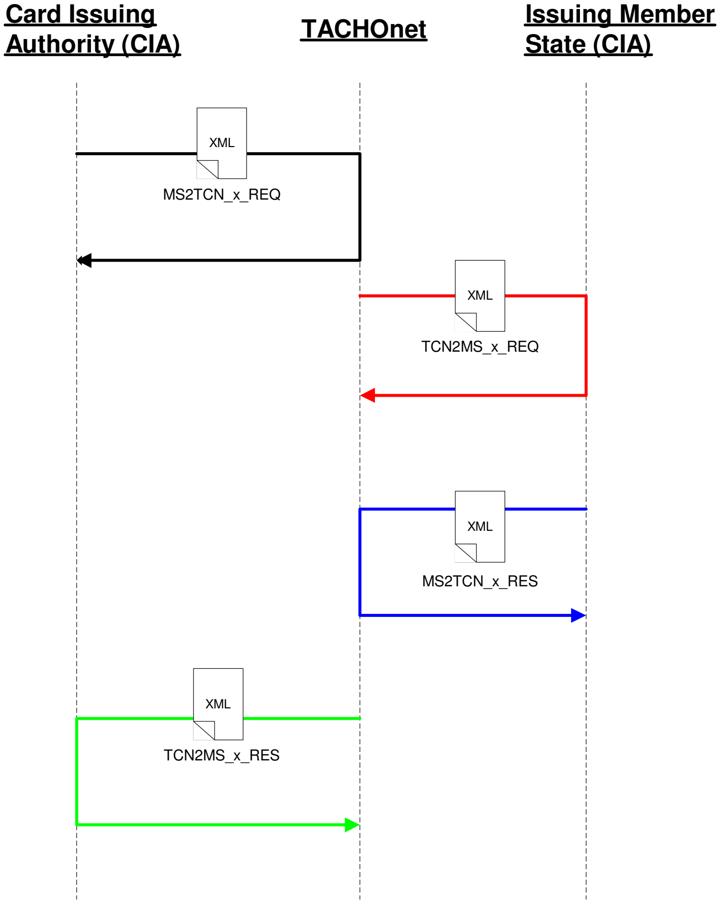


Figure 6 – UC-03 messages flow

Additional remarks

- In case of problems (e.g. network problem,...) when sending a message (request, response), TACHOnet will automatically retry to send it 3 times at regular interval till request timeout. Afterwards, if still unsuccessful, it will record a 'Server Error' status code.

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.

The following table describes which new card status codes are allowed when declaring a card status modification:

Card Status	MS2TCN_ModCardStatus_Req	Reason
Application	N	
Approved	N	
Personalised	N	
Dispatched	N	
HandedOver	**Y**	**valid again (after wrong declaration)**
Confiscated	**Y**	**Confiscation card declaration**
Suspended	**Y**	**Suspended card declaration**
Withdrawn	N	
Surrendered	N	Card returned to CIA and no longer needed
Lost	**Y**	**Lost card declaration**
Stolen	**Y**	**Stolen card declaration**
Malfunctioning	**Y**	**Defective card declaration**
Expired	N	
Replaced	N	
Renewed	N	
InExchange	**Y**	**Exchange of a card (start)**
Exchanged	**Y**	**exchange of a card (end)**

The card status values in red ('Y' in 2nd column) will be defined as the only values allowed as new card status values in the TCN "ModCardStatus" transaction (XML message). TCN will not check the validity of the state transition declared in this transaction (e.g. it will not prevent declaring a card 'Exchanged' while its current status was 'Stolen' as TCN doesn't know the current card status). It's up the MS responsibility to check the validity of such state transition (and return a ModStatusCode=CardStatusInvalid in the XML response message).

Table 1 – New card status

Basic flow

The basic flow consists of the following steps:

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

Continued on next page

Use Case 03 – Declaration of card status modification,
Continued

Basic flow (continued)

Step	Action
3	TACHOnet will build as many new requests as issuing Member State codes 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 number(s) issued by a particular Member State.
4	For each identified issuing Member State(s), TACHOnet builds, logs and encrypts the new request, sends it to the Member State and waits for receiving the response.
5	For each received response, TACHOnet deciphers it, logs it as-is in its tracking database and validates its syntax. If it's valid, TACHOnet stores the response message (linked to the TCNRefId) 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, logs and encrypts the consolidated response (from the responses received so far), and sends it to the original caller.

Alternate flows

The same alternate flows as described for UC-01 (page 23) 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 [2]) 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.

Continued on next page

Use Case 03 – Declaration of card status modification,
Continued

Post-conditions

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

Actors

- A *CIA* declaring the card status modification (CIA'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):

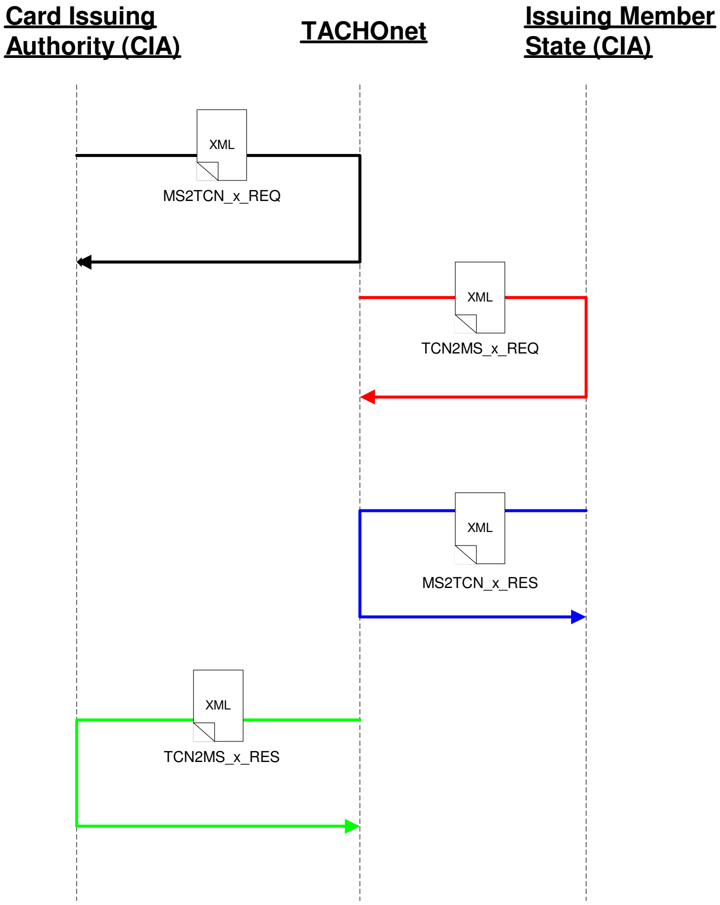


Figure 7 – UC-03 messages flow

Continued on next page

Use Case 03 – Declaration of card status modification,

Continued

XML Messages

Please refer to [2] 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 3 times at regular interval till request timeout.

Use Case 04 – Send Card/Driving License Assignment

Description

This use case is born from the “Luxemburg agreement” (see [3] 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 deciphers the received request and logs the received request as-is in its tracking database.
2	TACHOnet validates its syntax and assigns it a TACHOnet refid (TCNRefId).
3	TACHOnet will build as many new requests as issuing Member State codes identified in the original request (e.g. if more than one card/driving license number is given in the request). TACHOnet figures out the issuing Member State code(s) based on the driving license issuing nation (and not the card issuing Member State code) given for each sub request. Every new request only contains card and driving license number(s) issued by a particular Member State.
4	For each identified issuing Member State(s), TACHOnet builds, logs and encrypts the new request, sends it to the Member State and waits for receiving the response.
5	For each received response, TACHOnet deciphers it, logs it as-is in its tracking database and validates its syntax. If it’s valid, TACHOnet stores the response message (linked to the TCNRefId) 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, logs and encrypts the consolidated response (from the responses received so far), and sends it to the original caller.

Alternate flows

The same alternate flows as described for UC-01 (page 23) 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 [2]) 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 [2] 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):

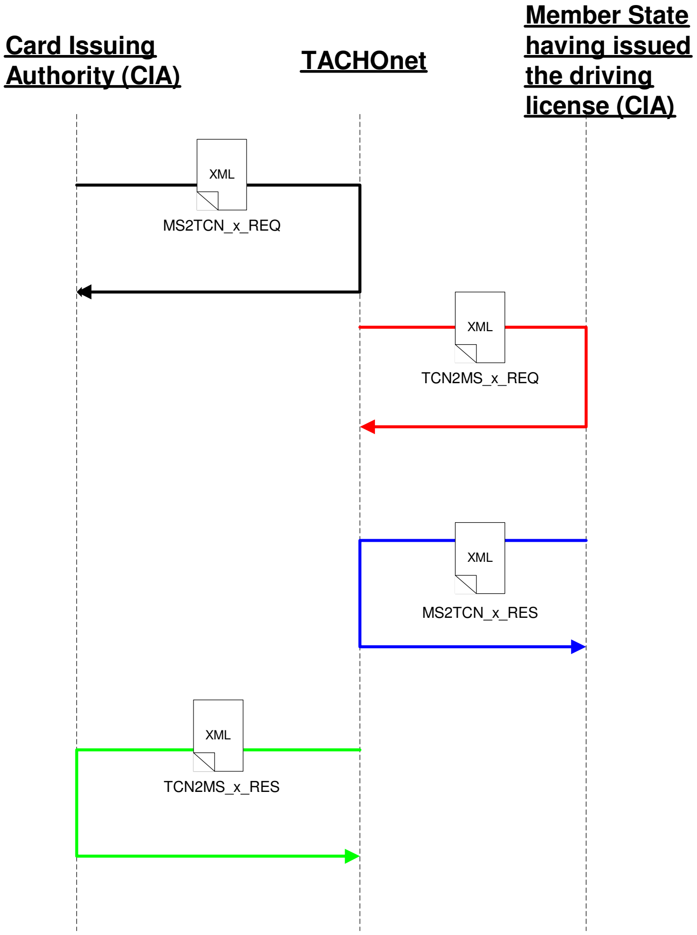

Card Issuing Authority (CIA)
TACHOnet
Member State having issued the driving license (CIA)
XML
MS2TCN_x_REQ
XML
TCN2MS_x_REQ
XML
MS2TCN_x_RES
XML
TCN2MS_x_RES

Figure 8 – UC-04 messages flow

Additional remarks

- In case of problems (e.g. network problem,...) when sending a message (request, response), TACHOnet will automatically retry to send 3 times it at regular interval till request timeout.

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 to allow the CIA users to access manually these TACHOnet services.
- A downloadable version of this web service should also be made available (.NET and Java) 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:

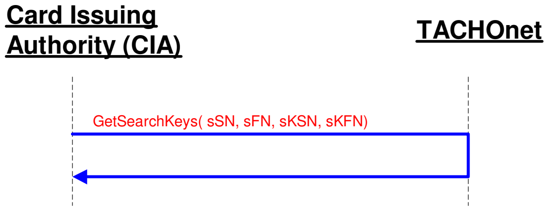

Card Issuing Authority (CIA)
TACHOnet
GetSearchKeys(sSN, sFN, sKSN, sKFN)

Figure 9 – 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.
- These services are opened to anyone connected on TESTA (no special security).

Open issues

-

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 to allow the CIA users to access manually these TACHOnet services.
- A downloadable version of this web service should also be made available (.NET and Java) 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:

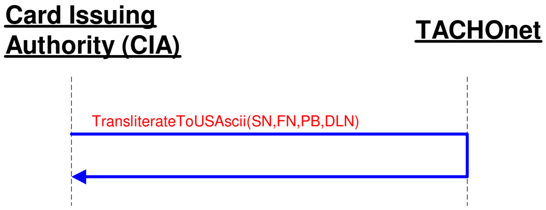

Card Issuing Authority (CIA)
TACHOnet
TransliterateToUSAscii(SN,FN,PB,DLN)

Figure 10 – 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.
- These services are opened to anyone connected on TESTA (no special security).

Open issues

-

Section 2.2 - Use Case Package "TCN Statistics Tasks"

Overview

Introduction

This section describes the use cases related to the "TCN Statistics Tasks" package. The following diagram lists the use cases of this package:

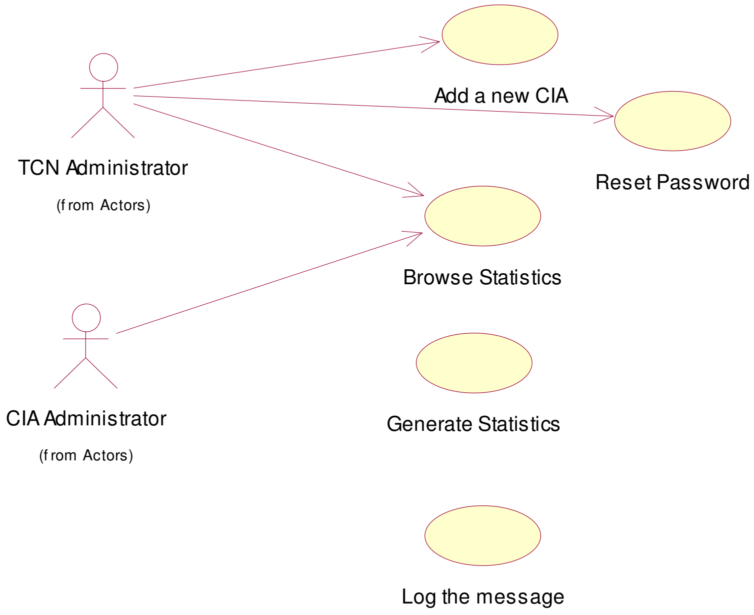


Figure 11 –Use Case Package "TCN Statistics Tasks"

Contents

This section contains the following topics:

Use Case 07 – "Add a new CIA"

Brief Description

In order to get access to the Statistics Reporting part of the TACHOnet system, every Member State will be assigned a CIA Administrator's account (and password).

This use case enables the TCN Administrator to create a new CIA Administrator account in the Active Directory for a CIA Administrator using the `Microsoft Management Console Active Directory Users and Computers (MMC).`

Primary Actor

TCN Administrator (or delegates to the operator).

Preconditions

The actor has access to the `Microsoft Management Console Active Directory Users and Computers`.

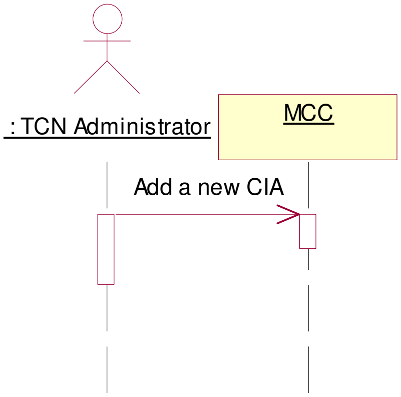
Postconditions

The new CIA Administrator has been created and has now access to the ReportManager Web site.

Stakeholders and Interest

Access to the ReportManager Web site (providing the TCN usage statistics reports) should only be allowed to the CIA Administrators. Therefore, every CIA Administrator must be assigned a user account and password.

Sequence Diagram



Continued on next page

Use Case 07 – "Add a new CIA", Continued

Basic Flow

-

Step	Action
1	A new Member State is added to the TACHOnet configuration (see Use-Case 13 – "Manage Member State" at page 55). The TCN Administrator (or operator) creates the new CIA Administrator account (and password) using the `Microsoft Management Console Active Directory Users and Computers`.

Alernative Flow

-

Technology and Data Variations List

- Access to the ReportManager web site will be secured by using Windows accounts.

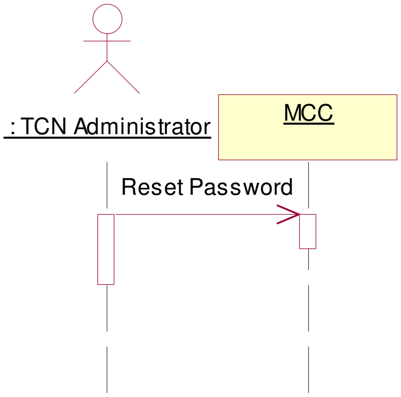
Assumptions

- The TCN Administrator has access to the `Microsoft Management Console Active Directory Users and Computers`. In the production environment (if not, he may ask the operator to perform the steps).
- Only one CIA Administrator account will be created per Member State.
- All users are managed in the Active Directory.
- The TACHOnet Administrator will also be assigned one account.

Open issues

-

Use Case 08 – "Reset Password"

Brief Description	This use case enables the TCN Administrator to reset in the Active Directory the password of a CIA Administrator using the `Microsoft Management Console Active Directory Users and Computers (MMC).`
Primary Actor	TCN Administrator (or delegates to the operator).
Preconditions	The actor has access to the `Microsoft Management Console Active Directory Users and Computers` and the CIA Administrator's account has already been created.
Postconditions	The CIA Administrator's password has been reset.
Stakeholders and Interest	A CIA Administrator might forget her password. Therefore, the TCN Administrator should be able to reset it.
Sequence Diagram	

Continued on next page

Use Case 08 – “Reset Password”, Continued

Basic Flow

-

Step	Action
1	The CIA Administrator warns (via email) the TCN Administrator that she forgots her password.
2	The TCN Administrator (or operator) resets the corresponding CIA Administrator account’s password using the Microsoft Management Console Active Directory Users and Computers.
3	The TCN Administrator warns the CIA Administrator (via email) to log on again and change her password.

Alernative Flow

-

Technology and Data Variations List

Access to the ReportManager web site will be secured by using Windows accounts.

Assumptions

- The TCN Administrator has access to the Microsoft Management Console Active Directory Users and Computers. In the production environment (if not, he may ask the operator to perform the steps).
- Only one CIA Administrator account will be created per Member State.
- All users are managed in the Active Directory.
- The TACHOnet Administrator will also be assigned one account.

Open issues

-

Use Case 09 – “Generate Statistics”

Brief Description

This use case consists of transferring (at regular interval – nightly basis) all expired TACHOnet transactions (completed or after timeout), storing them and generating some usage statistics for the TCN Administrator and every CIA Administrators.

The usage statistics should give information about the incoming requests (from a CIA to TACHOnet) for a given period:

- The list of requests for the last 14 days (List).
- The percentage of each status code values (Timeout, ServerError,…) for each CIA (Consolidated chart).
- The count and percentage of each status code values for each CIA (Consolidated list).
- The count and percentage of each CIA for each type of requests (Consolidated list).
- The count and percentage of each type of requests (CheckIssuedCards, CheckCardStatus,…) for each mode – Batch and On-line - (Consolidated list).

The usage statistics should give information about the outgoing requests (from TACHOnet to a CIA) for a given period:

- The list of requests for the last 14 days (List).
- The percentage of OK status code value for each CIA (Consolidated chart).
- The percentage of each status code values (Timeout, ServerError,…) for each CIA (Consolidated chart).
- The count and percentage of each status code values for each CIA (Consolidated list).
- The count and percentage of each CIA for each type of requests (Consolidated list).
- The count and percentage of each type of requests for each mode – Batch and On-line - (Consolidated list).

The consolidated lists should also give information about the minimum, maximum and average value of the time it took to complete the transaction and for the given timeout value.

Primary Actor

TCN Reporting System.

Preconditions

Expired transactions are available and the Agent is scheduled on a nightly base.

Continued on next page

Use Case 09 – "Generate Statistics", Continued

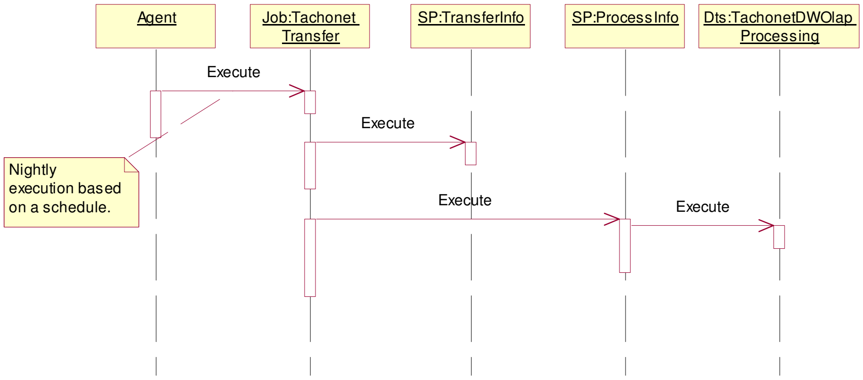
Postconditions

Transactions are transferred and statistics are generated.

Stakeholders and Interests

Statistics are a major measurement tool for identifying potential problems, assessing the overall usage of the system.

Sequence Diagram



Basic Flow

The basic flow for this use case is the following.

Step	Action
1	The Agent executes the Job: Tachonet Transfer based on its schedule.
2	The Job: Tachonet Transfer executes the SP: TransferInfo which transfers expired transactions from the production database to the datawarehouse database.
3	The Job: Tachonet Transfer executes the SP: ProcessInfo.
4	The SP: ProcessInfo executes the Dts: TachonetDWOlap Processing which processes cubes in the OLAP database.

Alernative Flow

-

Continued on next page

Use Case 09 – "Generate Statistics", Continued

Special Requirements

There are two special requirements.

Requirement Id	Description
1	Usage statistics should be made available as a web-based interface.
2	The web-based interface should support download of the rendered statistics in different formats as xml and Excel.

Technology and Data Variations List

- SQL Reporting Services (brand new service of SQL Server 2000) will be used to provide the whole TCN reporting solution (user interface, report generation, report design,…).

Assumptions

-

Open issues

-

Use Case 10 – “Browse Statistics”

Brief Description

This use case consists of allowing the TCN Administrator and every CIA Administrator to browse, via a secure Web interface, the usage statistics reports.

There are five reports available:

- **Requests from MS – List** for the list of requests for the last 14 days (List).
- **Requests from MS – Consolidation** for the percentage of each status code value for each CIA (Consolidated chart), the count and percentage of each status code value for each CIA (Consolidated list), the count and percentage of each CIA for each type of requests (Consolidated list) and the count and percentage of each type of requests for each mode – Batch and On-line - (Consolidated list).
- **Requests to MS – List** for the list of requests for the last 14 days (List).
- **Requests to MS – Top** for the percentage of OK status code value for each CIA (Consolidated chart).
- **Requests to MS – Consolidation** for the percentage of each status code value for each CIA (Consolidated chart), the count and percentage of each status code value for each CIA (Consolidated list), the count and percentage of each CIA for each type of requests (Consolidated list) and the count and percentage of each type of requests for each mode – Batch and On-line - (Consolidated list).

Primary Actor

- TCN Administrator.
- CIA Administrator.

Preconditions

- Transactions are transferred and statistics are generated.
- The actor has access to the ReportManager Web site.

Postconditions

The actor has browsed and downloaded report(s).

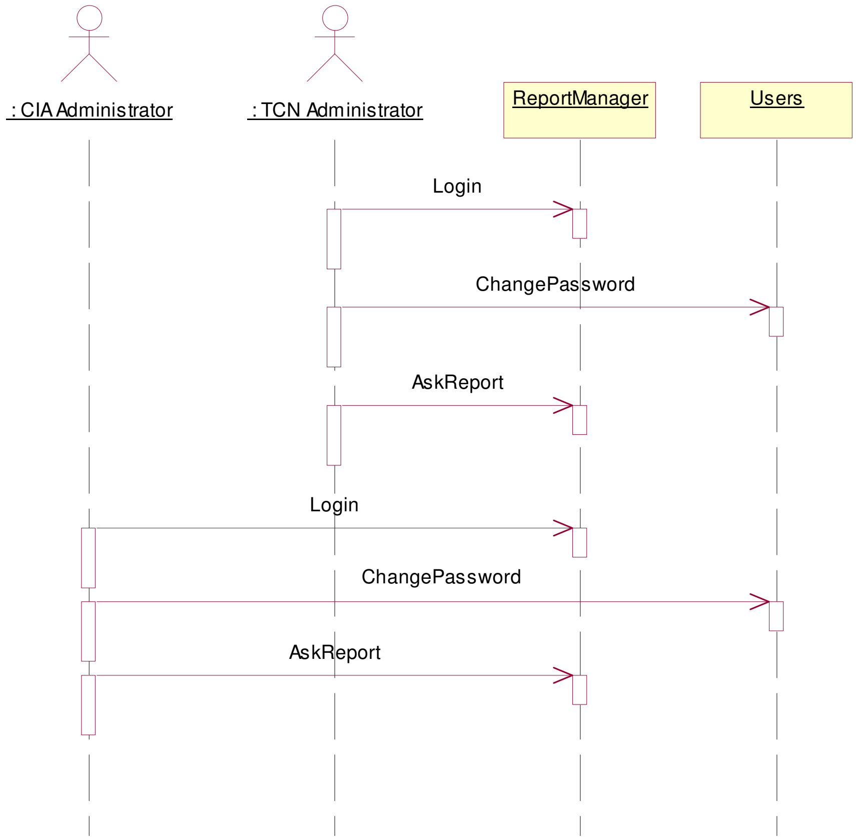
Stakeholders and Interests

Statistics are a major measurement tool for identifying potential problems, assessing the overall usage of the system.

Continued on next page

Use Case 10 – "Browse Statistics", Continued

Sequence Diagram



Basic Flow

The basic flow for this use case is the following.

Step	Action
1	The actor logs in the system using the standard basic security mechanism of the web browser.
2	If the login succeeded, the actor browses the reports on the ReportManager Web site.
3	If it is the first access of the actor, he may change his password on the Users Web site.

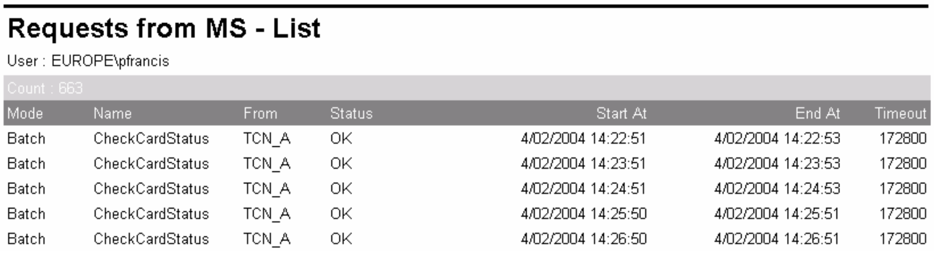
Continued on next page

Use Case 10 – “Browse Statistics”, Continued

Alernative Flow Some alternatives are described below, referred to in the basic flow.

Step	Action
2b	If the login failed, the actor calls the TCN Administrator to reset his password or to do the adequate operation.

Requests from MS – List Report



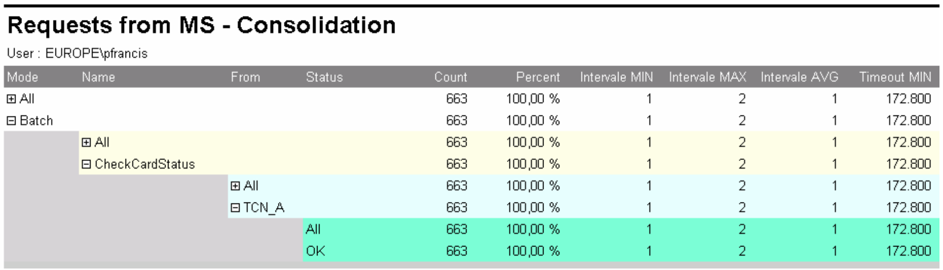
Requests from MS - List

User : EUROPE\pfrancis

Count : 663

Mode	Name	From	Status	Start At	End At	Timeout
Batch	CheckCardStatus	TCN_A	OK	4/02/2004 14:22:51	4/02/2004 14:22:53	172800
Batch	CheckCardStatus	TCN_A	OK	4/02/2004 14:23:51	4/02/2004 14:23:53	172800
Batch	CheckCardStatus	TCN_A	OK	4/02/2004 14:24:51	4/02/2004 14:24:53	172800
Batch	CheckCardStatus	TCN_A	OK	4/02/2004 14:25:50	4/02/2004 14:25:51	172800
Batch	CheckCardStatus	TCN_A	OK	4/02/2004 14:26:50	4/02/2004 14:26:51	172800

Requests from MS – Consolidation Report

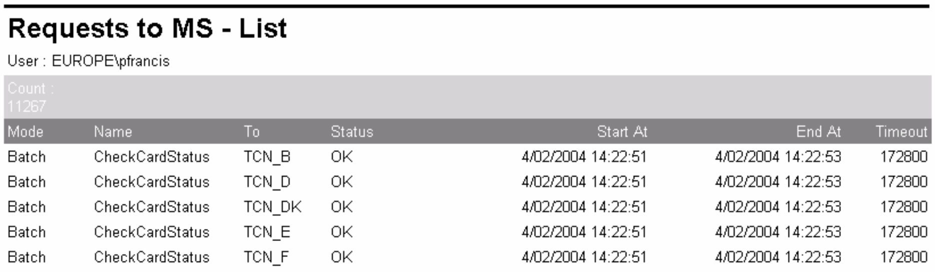


Requests from MS - Consolidation

User : EUROPE\pfrancis

Mode	Name	From	Status	Count	Percent	Intervale MIN	Intervale MAX	Intervale AVG	Timeout MIN
⊞ All				663	100,00 %	1	2	1	172.800
⊟ Batch				663	100,00 %	1	2	1	172.800
	⊞ All			663	100,00 %	1	2	1	172.800
	⊟ CheckCardStatus			663	100,00 %	1	2	1	172.800
		⊞ All		663	100,00 %	1	2	1	172.800
		⊟ TCN_A		663	100,00 %	1	2	1	172.800
			All	663	100,00 %	1	2	1	172.800
			OK	663	100,00 %	1	2	1	172.800

Requests to MS – List Report



Requests to MS - List

User : EUROPE\pfrancis

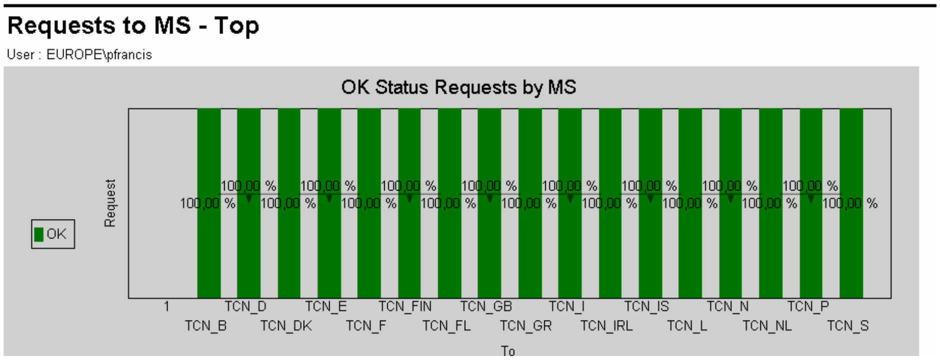
Count : 11267

Mode	Name	To	Status	Start At	End At	Timeout
Batch	CheckCardStatus	TCN_B	OK	4/02/2004 14:22:51	4/02/2004 14:22:53	172800
Batch	CheckCardStatus	TCN_D	OK	4/02/2004 14:22:51	4/02/2004 14:22:53	172800
Batch	CheckCardStatus	TCN_DK	OK	4/02/2004 14:22:51	4/02/2004 14:22:53	172800
Batch	CheckCardStatus	TCN_E	OK	4/02/2004 14:22:51	4/02/2004 14:22:53	172800
Batch	CheckCardStatus	TCN_F	OK	4/02/2004 14:22:51	4/02/2004 14:22:53	172800

Continued on next page

Use Case 10 – "Browse Statistics", Continued

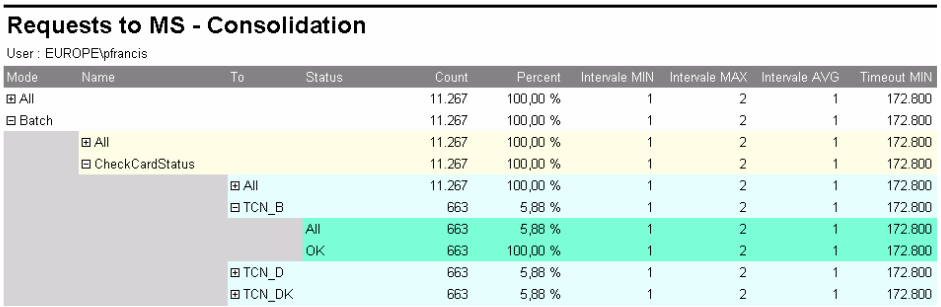
Requests to MS – Top Report



Requests to MS - Top

User : EUROPE\pfrancis

Requests to MS – Consolidation Report



Requests to MS - Consolidation

User : EUROPE\pfrancis

Mode	Name	To	Status	Count	Percent	Intervale MIN	Intervale MAX	Intervale AVG	Timeout MIN
⊞ All				11.267	100,00 %	1	2	1	172.800
⊟ Batch				11.267	100,00 %	1	2	1	172.800
	⊞ All			11.267	100,00 %	1	2	1	172.800
	⊟ CheckCardStatus			11.267	100,00 %	1	2	1	172.800
		⊞ All		11.267	100,00 %	1	2	1	172.800
		⊟ TCN_B		663	5,88 %	1	2	1	172.800
			All	663	5,88 %	1	2	1	172.800
			OK	663	100,00 %	1	2	1	172.800
		⊞ TCN_D		663	5,88 %	1	2	1	172.800
		⊞ TCN_DK		663	5,88 %	1	2	1	172.800

Special Requirements

There is one special requirement.

Requirement Id	Description
1	The generated reports should be dynamic reports.

Technology and Data Variations List

- SQL Reporting Services (brand new service of SQL Server 2000) will be used to provide the whole TCN reporting solution (user interface, report generation, report design,…).

Assumptions

- A special web site (single page) will also be built to allow the CIA Administrator to change her account's password.
- Only one CIA Administrator account will be created per Member State.
- All users are managed in the Active Directory.
- The TACHOnet Administrator will also be assigned one account.

Continued on next page

Use Case 10 – “Browse Statistics”, Continued

Open issues -

Use Case 11 – Log the message

Description

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

Such logging is provided out-of-the-box by BizTalk and will be configured at the channel level using the `BizTalk Messaging Manager` tool.

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 in the tracking database

Actors

- TACHOnet system

Additional remarks

-

Open issues

- How long should TACHOnet keep track of a message?

Section 2.3 - Use Case Package "TCN System Tasks"

Overview

Introduction

This section describes the use cases related to the "TCN Monitoring" package. The following diagram lists the use cases of this package:

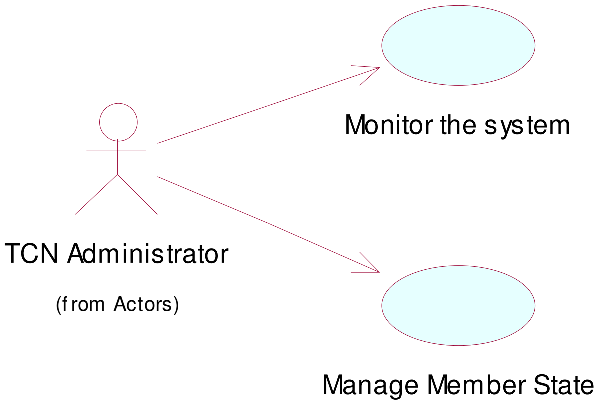


Figure 12 –Use Case Package "TCN System Tasks"

Contents

This section contains the following topics:

Use-Case 12 – “Monitor the system”

Brief Description

This use case consists of monitoring the whole TACHOnet system.

Such monitoring will be based on the MOM (Microsoft Operations Manager) product, used as standard monitoring tool by the EC DI’s Data Center.

Managing BizTalk through MOM is made possible by installing the BizTalk Management Pack for MOM. Nevertheless, as this pack consists of more than 700 rules, some configuration need to be made (in close collaboration with EC DI’s Data Center people) to configure the set of rules required for monitoring the BizTalk configuration of TACHOnet.

Primary Actor

- TCN Administrator

Preconditions

The TCN Administrator has access to the MOM console.

Postconditions

The TCN Administrator has managed alerts sent through the MOM console.

Stakeholders and Interests

In order to constantly keep the availability and performance of the TACHOnet system at an optimum level, the system must constantly monitored and should raise some events when particular problems (HW, SW,…) occur.

Basic Flow

See MOM documentation.

Technology and Data Variations List

-

Assumptions

- MOM is used as central monitoring system.

Open issues

- Will the TACHOnet servers be directly monitored from the central MOM console or should TACHOnet provide ?
- Is there any special FW configuration between the TACHOnet servers and the central MOM console?
- What are the BizTalk rules that need be configured in MOM and how?

Use-Case 13 – "Manage Member State"

Brief Description

This use case consists of managing a Member State CIA in terms of TACHOnet configuration (add, edit, remove a Member State CIA).

Primary Actor

- TCN Administrator

Preconditions

The TCN Administrator has access to the `BizTalk Messaging Manager` and `BizTalk Server Administration` tools.

Postconditions

The Member State CIA configuration in TACHOnet has been updated.

Stakeholders and Interests

All Member States will not be ready at production day 1. Moreover, new candidate Member States will potentially join TACHOnet in the near future. The configuration of existing Member States could also change. Therefore, it's important to provide the TCN Administrator with the tools or procedures to manage the TACHOnet configuration of a Member State.

Basic Flow

Managing Member States consists of adding a new Member State or modifying the current configuration of a Member State (url address, digital certificates,…) or removing a Member State (?). All these manual tasks will be described in details in the "**TCN Operational Guide"** document. Anyway, some of these major tasks are outlined below:

Adding a new Member State:

The following table lists the activities to carry out to add a new Member State in the TACHOnet configuration:

- BizTalk configuration:
  - Create the BizTalk organization corresponding to the new Member State ("`TCN_<countrycode>`") with its relevant properties.
  - Create the corresponding BizTalk messaging ports.
  - Create the corresponding BizTalk distribution list ("`All-<countrycode>`").
  - Update all the other BizTalk distribution lists to add the new messaging port (send request) corresponding to the new Member State.
  - Create the corresponding BizTalk channels.
  - Create the corresponding BizTalk receive functions (in test environment).
- Reporting System:
  - Add a new CIA Administrator account

Continued on next page

Use-Case 13 – “Manage Member State”, Continued

Basic Flow (continued)

Modifying the current configuration of a Member State:

- Changing the phone/fax/email of the Member State:
    - Update the custom properties of the BizTalk organization corresponding to the Member State
- Changing the url address where TACHOnet should send XML messages:
    - Update the transport type of the BizTalk messaging port corresponding to the Member State.

Technology and Data Variations List

- BizTalk Server 2002 provides the necessary tools to manage its configuration. These will be leveraged to update the Member States configuration.

Assumptions

The TCN Administrator is a BizTalk Administrator and has access to the `BizTalk Messaging Manager` and `BizTalk Server Administration` tools (or will delegate to the effective BizTalk Administrator).

Open issues

-

<End of the document/>