EU-MIDT

Card Issuing & Networking Committee

EU-MIDT/CINC/010-2006

TACHOnet Network and Security Reference Guide

Version 1.10

REF : EU-MIDT/CINC/010-2006

EU-MIDT SECRETARIAT DOCUMENT PREPARATION

OPERATION	NAME	ORGANISATION	DATE
PREPARED BY	DG TREN	European Commission	05/01/2004
CHECKED BY	Thierry GRANTURCO	Granturco & Partners	26/07/2006
APPROVED BY	Marie-Christine BONNAMOUR	Cybèle – MIDT Secretariat	26/07/2006
ISSUED BY	Secretariat MIDT	MIDT	27/07/2006

CHANGE CONTROL LIST

VERSION	DATE	NAME	DESCRIPTION

EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR ENERGY AND TRANSPORT

Rue de Mot 28

B-1040 Brussels, Belgium

DG TREN

TACHOnet

Network and Security Reference Guide

Version 1.10
05-Jan-04

Document Approval

	NAME	DATE	SIGNATURE
Prepared by:	Franck Silvestre	05-Jan-04	
Checked by:	Pierre Delmée	05-Jan-04	
Quality control by:	Pierre Delmée	05-Jan-04	
Approved by:	Yves Hardy (DG TREN)		

Distribution List

COMPANY	NAME	FUNCTION	FOR INFO / APPROVAL
DG TREN	Y. Hardy	Project Manager	Approval
DG TREN	L. Huberts		Info
CIWG TF2	Th. Granturco		Info

Change Control History

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	16/12/02	G. Poncelet	First Draft
0.2	17/12/02	G. Poncelet	Internal check (Structure)
0.3	17/12/02	G. Poncelet	Internal Check (contents)
0.4	13/02/03	G. Poncelet	Remarks from Yves Hardy & Marc Lombaerts (Types of connection)
0.5	20/02/03	G.Poncelet	Remarks from Marc Lombaerts (List of National contacts and Types of connections); Security part.
0.6	04/03/03	F. Silvestre	Remarks from Marc Lombaerts (03/03/03)
0.7	05/03/03	F. Silvestre	Remarks from Y. Hardy (04/03/03)
1.0	17/03/03	F. Silvestre	Release 1.0
1.10	05-Jan-04	F. Silvestre	Release 1.10

Document information

CREATION DATE:	05-Jan-04
FILENAME:	TCN-Network&SecurityRefGuide-01_10-EN.doc
LOCATION:	
NUMBER OF PAGES:	54

CONTENTS

Changes from version 1.0 to version 1.10

Introduction

Changes (insertions and deletions) to the document from previous version 1.0 to this version 1.10 are outlined in the following table. Changes are marked with a red outside border and are in red color.

Summary of changes

The following table sums up the changes brought to the document:

Page	Map / Block text	Description of the changes
18	Required bandwidth	Remove the sentence about "XML signature & encryption…".
33	Introduction to TACHOnet Security Features	The CIA Administrator will no longer use a digital certificate but a userid/password managed by the TCN Administrator (DG TREN).
38	IDA PKI Services	LRAO and SRAO will be played by Yves Hardy (DG TREN).
39	PKI Setup for TACHOnet	▪ Replace Medium Grade by High Grade server certificate. ▪ LRAO will be played by Yves Hardy (DG TREN).
40	PKI Setup for TACHOnet - TMSCO	▪ Remove the use of key generation wizard and sending via email. Requests will be send by post on a floppy disk. ▪ Remove CIA Administartor and TCN Administrator from the list of TCN user types having a digital certificate.
41-44	How can a Member State apply for a digital certificate?	New procedure.
45	How can a Member State revoke a digital certificate?	TSRAO: TACHOnet Suspension and Revocation Authority Officer (Yves Hardy at DG TREN).
47	Introduction to HTTPS in TACHOnet	▪ 1 way SSL for incoming XML messages. ▪ 2 way SSL for outgoing XML messages.
49-54	Annexes	Standard Certipost (E-Trust) certificate Web Server Order Form

Part II - Network Access Reference Guide

Overview

Introduction

The mission of the TACHOnet project rests essentially on the exchange of information between national administrations responsible for issuing tachograph smart cards for the enforcement of the driving and rest times of professional drivers.

TESTA II provides network services to the public administrations in Europe.

The TACHOnet information exchange will be done through the TESTA II network.

This part is intended to provide the national administrations responsible for the TACHOnet project in their country with the necessary information to connect to the EuroDomain.

Contents

The part contains the following chapters:

Chapter 1 - Introduction to the TESTA II network service

Overview

Introduction

TACHOnet will use the European official network: TESTA II.

This chapter helps in understanding the TESTA II network architecture and services.

Contents

This chapter contains the following topics:

What is IDA?

Definition

IDA means **I**nterchange of **D**ata between **A**dministrations.

It consists of a Community Programme responsible for developing network features that meet common user requirements, such as data collection, dissemination, exchange, and security.

Origin

The program has been adopted by the European Council and European Parliament and is applied since August 1999.

The Programme is based on two decisions, 1719/1999/EC and 1720/1999/EC [REF 1 and 2].

- Decision 1719/1999/EC defines the general principles for implementation of telematics projects in support of specific Community policies.
- Decision 1720/1999/EC calls on the Community to ensure a consistent and coordinated technical approach to telematics projects to safeguard interoperability and efficiency.

Mission

The IDA Programme brings together national and European decision makers and implementers.

It is both a forum for coordination and a provider of solutions for telematics networks.

Services

IDA provides the following services supporting the exchange of information at the trans-European level:

The service	Is responsible for the...	And provides...
TESTA	Information transport	An IP-based backbone that provides telecommunications services at the EuroDomain level
CIRCA	information handling	A document repository and group-work tool to manage information of the IDA projects
PKICUG	information security	Secure Access to web repositories (authentication of clients and servers, and confidentiality of exchanged information)

IDA also provides an interoperability framework proposing the IDA Architecture guidelines.

More Info

For more information, see the IDA intranet site (http://europa.eu.int/ispo/ida).

What is TESTA?

Definition

TESTA is the IDA project to provide **T**rans-**E**uropean **S**ervices for **T**elematics between **A**dministrations.

TESTA answers to the growing need for the information exchange between local administrations in Europe.

TESTA II

The IDA TESTA project started in 1996 and entered its second phase (TESTA II) in early 2000.

Mission

TESTA II provides a telecommunications infrastructure for administrations. It is a private network for public administrations.

It covers all Member States, EFTA countries and increasingly also the accession to Europe candidates.

Approach

Through a collaborative approach, TESTA II establishes national, regional or local administrative networks by forging these to a trans-European network.

Stakeholders

The different stakeholders of the TESTA network implementation and administration are:

The stakeholder	Is responsible for
IDA test team	Accepting a connection request and ordering the connection and services.
Assist	Coordinating and providing the technical study and advice for a new connection. It also controls the implementation of the connection by Equant and helps in troubleshooting problems.
Equant	Providing the infrastructure and associated services for the TESTA network

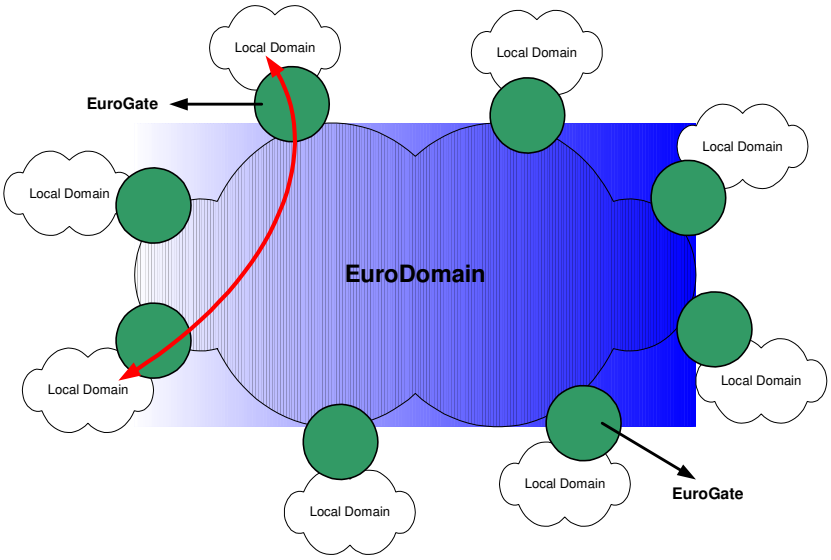
Description of the TESTA II network architecture

The basic components

The TESTA II architecture is composed of the following basic components derived from the IDA architecture guidelines:

- The "EuroDomain";
- The "Local Domain";
- The "EuroGate".

Illustration



EuroDomain

It consists of a common set of pan-European network services depending on the IDA community.

It enables transparent link between various local domains of the European Community of Member State Administrations and European Institutions.

The EuroDomain can be seen as a backbone network, defined by the access options, the access point locations and the services provided between them.

Local Domain

It consists of a set of homogeneous network services used by national Administrations, or European institutions.

The local domain can range from a single LAN to a national network that acts itself as a national backbone.

Continued on next page

Description of the TESTA II network architecture, Continued

EuroGate

The **EuroGates** can be considered as a mediator between EuroDomain and Local domains.

It ensures the technical independence between the EuroDomain and the Local Domains.

It consists of a set of services, relying on hardware and software features, providing the necessary functions of connectivity and inter-operability between Local Domains and the EuroDomain.

It also defines the boundary of responsibility between Domains.

A EuroGate can be considered as a router directly giving access to and managed by the EuroDomain.

The EuroGates are defined in each country.

Description of the connection methods to TESTA II

Introduction

Connecting to TESTA II network means accessing the nearest TESTA II Eurogate located in each country.

Connection methods

The following table describes the available connection methods for TACHOnet. When possible, the national network connection should be preferred.

Connection method	Description
National network	In almost every country concerned by TACHONET, a national network is connected to TESTA II. Any new connection to TESTA II should use this **preferred connection method**.
Leased line	A router is installed on the local site allowing a permanent connection.

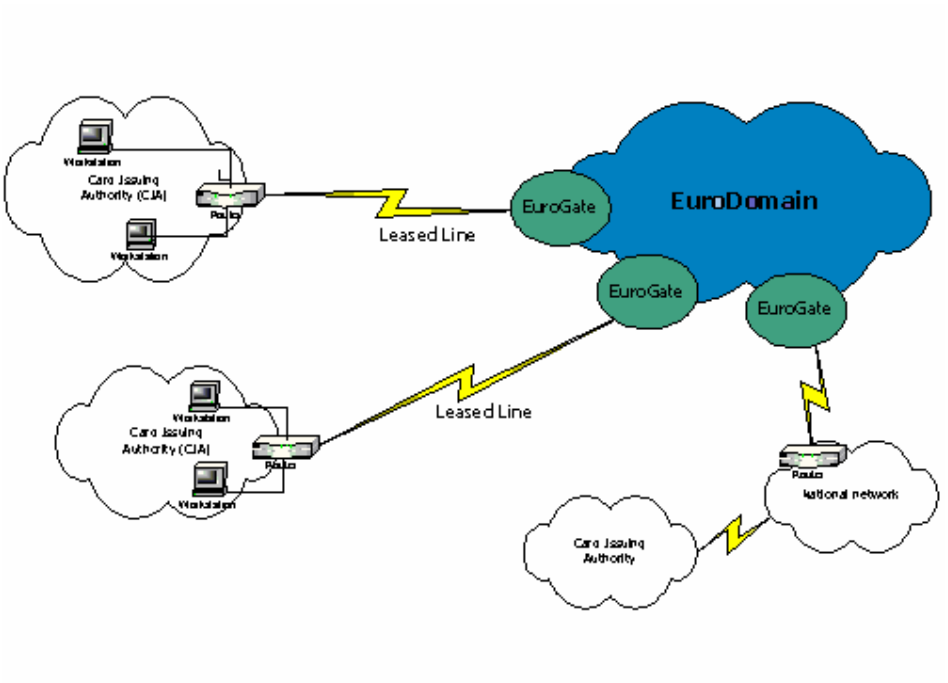
The choice of the method depends on the availability of a national network connected to TESTA II, on the needed line speed, on the number of workstations to be connected and on the cost of local implementation.

All those criteria will be analysis during the new connection method analysis phase (See Description of the process workflow for a new site connection on page 24).

Continued on next page

Description of the connection methods to TESTA II, Continued

Illustration



Access protocols and IP addressing

Access protocols

The EuroGates can be accessed using any state-of-the-art protocol, including leased lines (native IP), Frame Relay or ATM.

At connected sites, the customer interface will be a LAN-port on the router provided by the EuroDomain operator.

Permanent access to the EuroGates can be ordered at speeds from 64 Kbps up to 34 Mbps.

IP platform functions

Local Domains are interconnected through the EuroDomain, using TESTA II registered IP addresses.

The addresses are provider-independent, but the EuroDomain operator, Equant, manages them.

For each Local Domain, the entry point to TESTA II is configured with network address translation (NAT) translating Local Domain internal IP addresses to TESTA II registered IP addresses.

The address block 62.62.0.0 / 17 has been allocated by the European IP registration authority (RIPE) to TESTA II.
A part of this range has been set aside for future use (such as the candidate countries).

Address allocation will in general be driven by geography, with each country receiving a set of class C addresses.

An exception to this rule will be the European Institutions, which will receive address blocks from a separate part of the above range.

Description of the Services provided by Equant and Assist

Introduction

EQUANT is responsible for:

- Implementing the network;
- Installing new sites;
- Managing the problems (helpdesk);
- Managing the change requests.

ASSIST is responsible for

- Coordinating and providing the technical study and advice for a new connection.
- Controlling the implementation of the connection by Equant.
- Help troubleshooting between the different actors
- Provide information on TESTA
- The e-mail address of ASSIST is assist@be.unisys.com

Connection via a National network

In that case, Equant provides only services concerning the connection between the national network router and the Eurogate.

The responsibility of the connection between the Card Issuing Authority (CIA) and the national network is under the CIA and the National network contact. Equant will not intervene in that scenario

Direct leased line connection

In this case, Equant can provide the following services:

- Global Intranet VPN port with defined speed and service class / traffic profile (EuroGate);
- Access line (leased line capable of being upgraded to higher speeds up to 2Mb/s) from the Local Domain site to the EuroGate;
- ISDN backup of the access line (except for locations where SDH rings are preferred), including the backup equipment and the ISDN;
- CISCO router: rental and maintenance (on-site maintenance 24 hours x 7 days with 4 hours MTTR, including hardware maintenance and a field engineer arriving on customer site). A dial-in modem is also included for remote configuration and maintenance;
- VPN and router configuration (with defined addressing scheme, traffic profile, etc.);
- Network and router management services (including 24 hours/24 and 7 days/7 proactive monitoring).

Information about the connection costs

Backbone services

IDA finances all TESTA II backbone services for the whole duration of the services. These costs are covering the following aspects:

- the services provided at the EuroGates;
- the guarantee of services;
- the project management;
- the general co-ordination.

IDA also finances the accesses from the EuroDomain to theEuropean Institutions.

Connection via a National network

When the administration is connected to TESTA II through the national network, the connection costs are in charge of IDA.

The country only finances the cost related to the connection between the local domain of the Card Issuing Authority (CIA) and the national network.

The costs supported by the Card Issuing Authority (CIA) depend on the country.

Direct leased line connection

IDA finances the costs for a direct connection for a maximum duration of one year.

After that, the TESTA service provider can provide the services or the administration may select any other service provider for accessing the nearest EuroGate.

The cost financed by IDA are the following:

- The local loop (leased line)
- The router
- The backup equipment (if required)
- The provider's service charge (monitoring)

The costs for the local loop may be very different across Europe. They also depend on the location of the local site to be installed (distance from the nearest EuroGate).

As TACHOnet requires an availability of the local systems 24x7, a permanent direct connection with an ISDN backup is required.

The cost estimates presented below concern a direct connection to TESTA including:

- A router, capable of performing network address translation, implementing the addressing scheme adopted for the EuroDomain and the service classes and VPNs defined per access;
- A **128 Kb/sec leased line** to the nearest EuroGate;
- A Global IPVPN Port (Economy)
- 24 hour/24, 7 days/7 supervision
- ISDN back-up

Continued on next page

Information about the connection costs, Continued

Direct leased line connection (continued)

Cost estimations are given for all the Member States. However, in practice, only France, Switzerland and maybe Sweden will have to go through this type of direct connection (all the other Member States could have a connection via their own National network).

The following prices are expressed in EURO and are exclusive VAT.

Member State	128 Kbps Total installation charges (€)	128 Kbps Total Monthly charges (€)
Austria (Wien)	1.745,00	1.957,00
Belgium (Bruxelles)	2.338,00	1.869,00
Denmark (Kobenhavn)	2.703,00	1.711,00
Finland (Helsinki)	1.870,00	1.753,00
France (Paris)	2.820,00	2.048,00
Germany (Frankfurt)	2.962,00	2.094,00
Greece (Athens)	1.909,00	2.194,00
Ireland (Dublin)	3.076,00	1.868,00
Italy (Roma)	3.255,00	2.040,00
Luxemburg (Luxemburg)	2.299,00	1.948,00
Netherlands (Amsterdam)	1.971,00	2.093,00
Norway (Oslo)	2.597,00	1.850,00
Portugal (Lisboa)	960,00	1.865,00
Spain (Madrid)	2.094,00	2.035,00
Sweden (Stockholm)	4.452,00	1.811,00
United Kingdom (London)	2.075,00	1.991,00
Iceland (Reikjavik)	6.544,00	1.927,00
Liechtenstein	Tbp	Tbp
Switzerland (Geneve)	2.763,00	1.852,00

Continued on next page

Information about the connection costs, Continued

Required bandwidth & Cost estimates

The following table gives an estimation about the required bandwidth (Kbits/sec) computed for every Member State. Such estimation is based on:

- 1.662.500 driver's cards to be issued per year (i.e. 7.557 daily) within the European Community.
- 4.000 driver's card and 4.000 workshop card checks carried out daily by the enforcers during road check within the European Community.
- The use of HTTPS as security mechanism.

Member State	Required bandwidth (Kbits/sec)
Austria	42
Belgium	42
Denmark	41
Finland	41
France	51
Germany	55
Greece	42
Ireland	41
Italy	50
Luxemburg	40
Netherlands	43
Norway	42
Portugal	42
Spain	48
Sweden	42
United Kingdom	51
Iceland	40
Liechtenstein	40
Switzerland	42

Chapter 2 - Getting Access to the TESTA II network service

Overview

Introduction

A TESTA II network connection is required for the exchange of the TACHONET information. The connection request should be introduced in collaboration with the National TESTA co-ordinators in the case of a connection via the National Network.

This chapter describes how the connection should be requested for a connection via the National Network as well as a direct connection, and what happens from the moment the request has been introduced until the connection is effective.

It also gives an approximate idea of the waiting period.

Contents

This chapter contains the following topics:

The list of the national TESTA co-ordinators

Introduction

There are usually two national representatives for TESTA II in each country: an administrative co-ordinator and a technical co-ordinator.
These two functions can be completely fulfilled by one person (depending on the country).

This list is only useful in the case of a connection via a National Network.

Role of the co-ordinator

The national TESTA co-ordinator acts as the single point of contact between TESTA II and the national administrative network.

He/She is responsible for the following tasks:

- Providing information to the Local Domains in his country interested in connecting to the TESTA II network using the national network;
- Coordinating new connections of a local domain to TESTA II via the national network;
- Coordinating problem solving when connectivity problems arise between the local domain and TESTA II;
- Informing IDA about concerns, plans, ideas... of the national administrative network that are related to TESTA II;
- Participating to workgroup meetings with other national network co-ordinators, organised by IDA.

List

The following table lists the Administrative and technical co-ordinators of the concerned countries. If not otherwise specified, a connection through a national network is available in every Member State.

An up-to-date list can be obtained from ASSIST (assist@be.unisys.com).

Austria	
Coordinator: Leopold Koppensteiner ✉ Leopold.Koppensteiner@bmf.gv.at ☎ +43 1 71123-2525	Technical contact: Michael Wickenhauser ✉ Michael.Wickenhauser@portal.at ☎ +43 664 1016853
Belgium	
Coordinator: FEDENET Plasschaert Roland roland.plasschaert@premier.fed.be ☎+32 2 501.04.38	Coordinator: FEDENET Plasschaert Roland roland.plasschaert@premier.fed.be ☎+32 2 501.04.38

Continued on next page

The list of the national TESTA co-ordinators, Continued

List (continued)

Denmark

Coordinator:	Technical contact:
Poul Bernt Jensen	Henrik Lynnerup
✉ pbj@fsk.dk	✉ hlynncru@csc.dk
☎+45 3392 9886	+45 3614 6574

Finland

Coordinator:	Technical contact:
Seppo Riihimaki	Ville Hagelberg
✉ Seppo.riihimaki@vnk.vn.fi	✉ Ville.Hagelberg@vnk.vn.fi
☎ +358 9 1602139	☎ +358 9 1602137

France

No possibility of connection through a national network but direct connection at their own costs.

Coordinator:
Julien Frangais
✉ julien.frangais@mtic.pm.gouv.fr
☎ +33 1 42755246

Germany

Thüringer Innenministerium, Abteilung 1-
Referat 13
Steigerstrasse 24, 099096 Erfurt

Coordinator:	Technical contact:
Sigurd Wilke	Andreas Munde
✉ SWilke@TIM.thueringen.de	✉ amunde@tlrz.thueringen.de
☎ +49 361 379 3313	☎ +49 361 379 3313

Greece

Coordinator:	Technical contact:
Greek Informatics Development Agency 2-4 Filoxenou & Spintharou Athens Greece	
Coordinator:	Technical contact:
Christos MOSCHONAS	Christos MOSCHONAS
✉ c.mos@syzefxis.gov.gr	✉ c.mos@syzefxis.gov.gr
☎ +30 1 9023713	☎ +30 1 9023713

Iceland

Coordinator:	Technical contact:
Johann Gunnarsson	Bjorn Haraldsson
✉ johann.gunnarsson@fjr.stjr.is	✉ bjorn.haraldsson@fjr.stjr.is

Continued on next page

The list of the national TESTA co-ordinators, Continued

List (continued)

Ireland

Coordinator:	Technical contact:
Tim Duggan	Eddie McGinn
✉ Tim_Duggan@cmod.finance.irlgov.ie	✉ eddie_mcginn@cmod.finance.gov.ie
☎ +351 1 6045065	☎ +353 1 6045138

Italy

Coordinator:	Technical contact:
Marino Di Nillo	Marino Di Nillo
✉ mdinillo@centrotecnico.g-net.it	✉ mdinillo@centrotecnico.g-net.it
☎ +39 0685264453	☎ +39 0685264453

Liechtenstein

The national network is not connected yet. Still waiting for information about whether Liechtenstein will use TACHOnet or not.

Luxembourg

Centre Informatique de l'Etat
BP-1011 Luxembourg

Coordinator:	Technical contact:
Daniel Nickels	Serge SPANIER
✉ daniel.nickels@cie.etat.lu	✉ serge.spanier@cie.etat.lu
☎ +352 49925 608	☎ +352 49925 753

Netherlands

Coordinator: RINIS Network	Technical contact:
Annet Sikkel	Henk-Jan Oostenbrink
✉ asikkel@rinis.nl	✉ hjoostenbrink@rinis.nl
☎ +31 20 5651436	☎+31 20 5451430

Norway

Coordinator:	Technical contact:
Morten Rennesund	Erik Linnerud
✉ morten.rennesund@ft.dep.telemax.no	✉ erik.linnerud@ft.dep.telemax.no
☎ +47 22 24 99 13	☎+47 22 24 97 72

Portugal

Coordinator:	Technical contact:
Fernanda Costa	Fernanda Costa
✉ fernanda.costa@inst-informatica.pt	✉ fernanda.costa@inst-informatica.pt
☎ +351+21 4723189	☎ +351+21 4723189

Continued on next page

The list of the national TESTA co-ordinators, Continued

List (continued)

Spain

Ministerio de Administraciones Públicas
C/María de Molina 50, 28006 Madrid

Coordinator:	Technical contact:
Luis de Eusebio Ramos	Miguel A. Amutio Gómez
✉ luis.deeusebio@map.es	✉ miguel.amutio@sgci.dgopti.map.es
☎ + 34 91 5861899	☎ + 34 91 5862990

Sweden

The connection through a National Network is in progress but not yet officially approved by the European Commission.

Coordinator:	Technical contact:
Irene Andersson	Irene Andersson
✉ irene.andersson@statskontoret.se	✉ irene.andersson@statskontoret.se
☎ +46 8 454 4600	☎ +46 8 454 4600

Switzerland

No possibility of connection through a national network but direct connection at their own costs.

United Kingdom

GSI Nerve Centre
E-mail: gnc@ccta.gsi.gov.uk

Coordinator:	Technical contact:
Chris Simmons	Alan Collier
✉ christopher.simmons@ccta.gsi.gov.uk	✉ mailto:alan.collier@ccta.gsi.gov.uk
☎ +44 1424 432946	☎ +44 1603 704400

Description of the process workflow for a new site connection

Introduction

This map describes the steps to follow to get a connection to the TESTA II network:

- Either via the National Network
- Or via a direct connection.

The possibility to get the connection via the National Network will analysed in step 3.

Stakeholders

The following stakeholders will intervene in the workflow for connecting a new site:

Stakeholder	Role
Local site contact	The person responsible for the TACHOnet site implementation (local administration).
National TESTA Co-ordinator	The national TESTA administrative or technical co-ordinator (see The list of the national TESTA co-ordinators at page 20).
IDA – TESTA team	The TESTA team at the European Commission.
Project Officer	DG TREN is responsible of the TACHOnet project. It is represented by the Sector Project Officer.
ASSIST	ASSIST is the contractor responsible for the co-ordination and technical study of the new connections.
EQUANT	EQUANT is the contractor responsible for providing the infrastructure and the services associated with the infrastructure of the TESTA network.

Common steps

The start of the workflow is composed of 3 common steps:

Step	Action	Actors	Estimated Duration
1	Request the connection: Fill in the *New installation form* and send the request to IDA	Local Site Contact Project Officer ASSIST	1-2 weeks
2	Acceptance from IDA	IDA	1-2 weeks
3	Feasibility study and define the type of connection. **A direct leased line connection must be considered if it is not possible to access TESTA via the National Network.**	Local site contact ASSIST National coordinator Project officer Equant	+/- 5 weeks

Continued on next page

Description of the process workflow for a new site connection, Continued

Next steps for a connection via a National Network

The following table describes the next steps in case the connection via a National Network is possible:

Step	Action	Actors	Estimated Duration
4	Connection of local site to the National Network.	Local site contact National coordinator	2-4 weeks
5	Configuration of NATing on the EuroGate if needed.	Local site contact ASSIST Equant	1 week
6	Test of the logical connection and the access to the TESTA services : DNS, portal, application.	Local site contact National coordinator ASSIST	1-3 weeks

Next steps for a direct leased line connection

The following table describes the next steps in case the connection via a National Network is **not** possible. A direct leased line connection must be installed:

Step	Action	Actors	Estimated Duration
4	Ordering of the connection by IDA to Equant	IDA Equant Project officer	+- 1 week
5	Fill in the *Technical Questionnaire*	Local site contact ASSIST Equant	1-2 weeks
6	Installation of the physical connection, and configuration.	Equant Local site contact	+- 12 weeks
7	Test of the logical connection and the access to the TESTA services : DNS, portal, application	Local site contact ASSIST Equant	1-3 weeks

How to request TESTA II services

Introduction

The procedure for requesting services is simple.

Interested parties should notify the IDA unit of their interest, indicating which sites require access to TESTA II and whom they need to communicate with, as well as what type of service is requested.

Information of the legal basis of their exchange of data should also be provided so that IDA can check the eligibility.

After being authorised to connect, technical information needs to be communicated before the connection can be implemented.

Procedure

Follow the following steps to request a connection to the TESTA II network:

Step	Action
1	Contact the TESTA co-ordinators of your country (see "The list of the national TESTA co-ordinators" on page 20).
2	Fill in the **New site installation form** with your national TESTA co-ordinator(s) (see "Description of the "New site installation form" on page" 27)
3	After IDA has accepted your request and only in the case of a direct connection, fill in the **Roll-out technical form** with your national TESTA co-ordinator(s) and ASSIST (see "Description of the "Roll-out technical form"" on page 28).

Description of the "New site installation form"

Form

New Site Installation Order Form	
Administratvie Contact	
Contact Name	
Title	
Location Name	
Address	
City	
Post code	
Country	
Telephone	
Fax*	
Email	
Technical Contact	
Contact Name	
Title	
Location Name	
Address	
City	
Post code	
Country	
Telephone	
Fax*	
Email	
Site Address:	
Location Name	
Street Address	
Building	
Room Number	
City	
Post Code	
Country	
Line Speed	
ISDN Back-Up (Yes or No)	
Type of site (Agency/Sector/National Network/etc)	

Administrative Contact

Legal justification. Provide details about a local administrative contact person.

Technical Contact

Provide details of the local technical contact person.

Site Address

Provide details about the physical site location

Line Speed

Bandwidth requirement (Kbits/sec). Please refer to the bandwidth requirements per Member States.

ISDN Back-Up

Yes/No. Must be YES for TACHOnet.

Type of site

Agency / Sector / National Network...

Description of the "Roll-out technical form"

Introduction

The objective of the Roll-out technical information is to give technical information about the necessary installation. It will be completed in collaboration with the national TESTA technical co-ordinator and with the ASSIST consultants.

It is composed of different parts. Each part is described in this section as a separate topic.

Overview

The Roll-out form is described in the following topics:

Roll-out technical form - Connection to the local domain

Form

ADMINISTRATIVE INFORMATION		
COMPLETE SITE ADDRESS (where the access will have to be delivered)	Street	
	Street	
	Town	
	Zip Code	
	Country	
LOCAL TECHNICAL CONTACT (located on the site where the access will have to be delivered)	Name	
	Given Name	
	Phone Number	
	Fax Number	
	e-mail address	

ACCESS TO THE EURODOMAIN		
REQUESTED INFORMATION	RESPONSE	COMMENTS
Access speed		
Traffic Profile		

CONNECTION OF THE CE ROUTER TO THE LOCAL DOMAIN		
REQUESTED INFORMATION	RESPONSE	COMMENTS
PSTN NUMBER (for remote connection to the CE router installed by Equant)		
LAN TYPE (Ethernet, token ring, etc.)		
LOCAL DOMAIN NETWORK IP subnet masking scheme / address hierarchy (attached with diagram if possible)		
CURRENT IP ROUTING PROTOCOL		
LAN IP ADDRESS ASSIGNED TO THE CE ROUTER installed by Equant (including mask), from Local Domain address range		
IP ADDRESS OF THE FIREWALL (if one present)		
Next Hop:		

Administrative information

Provide details about local site location and local technical contact person.

Access to the Eurodomain

Provide required bandwidth and traffic profile.

Connection of the CE router

Connection of the CE router to the local domain

Roll-out technical form - Connection to TESTA II

Form

LIST OF PROPAGATED LAN SUBNETS advertised on the WAN Interface of the CE router installed by Global One (to the EuroDomain)			
IP address	**Mask**	**Description**	**Comments**

WORKSTATIONS / CLIENTS that will have to communicate over the TESTA II EuroDomain - Only if NAT performed on the Router		
SIZING (simultaneous workstations / clients)		
REQUESTED NUMBER OF SIMULTANEAOUS CONNECTIONS	**Value / comments**	**Pool of TESTA II - IP address (Equant)**
Number of *simultaneous* workstations / clients **(immediate)**		62.62.
Number of additional *simultaneous* workstations / clients **(future)**		62.62.

LIST OF LOCAL WORKSTATIONS / CLIENTS WITH STATIC IP ADDRESS				
IP address	**Mask**	**TESTA II - IP address (Equant)**	**Description**	**Comments**
		62.62.		
		62.62.		
		62.62.		

LOCAL HOSTS / SERVERS that will have to communicate over the TESTA II EuroDomain		
SIZING		
REQUESTED NUMBER	**Value**	**Comments**
Number of hosts / servers **(immediate)**		
Number of additional hosts / servers **(future)**		

LIST OF LOCAL HOSTS / SERVERS ALREADY IDENTIFIED				
IP address	**Mask**	**TESTA II - IP address (Equant)**	**URL (on TESTA II)**	**Description / comments**
		62.62.	.eu-admin.net	
		62.62.	.eu-admin.net	
		62.62.	.eu-admin.net	
		62.62.	.eu-admin.net	
		62.62.	.eu-admin.net	

LAN subnets

List of the propagated LAN subnets advertised on the WAN Interface of the CE router installed by Equant (to the EuroDomain)

Workstations / Clients

WORKSTATIONS / CLIENTS that will have to communicate over the TESTA II EuroDomain - Only if NAT performed on the Router

This part is useless for TACHOnet.

Local Hosts / Servers

Local Hosts / Servers that will have to communicate over the TESTA II EuroDomain

Roll-out technical form - Traffic over TESTA II

Form

TESTA II TRAFFIC - Only if Quality of Service is Required								
Source			Destination			Traffic		
IP address	Mask	Port(s)	IP address (or location)	Mask (or URL/ name)	Ports	Transport type (TCP/UDP/IP)	Class of Service	Description / Comments Application / Protocol
Local subnets (workstations / clients)			Remote hosts / servers					
Local hosts / servers			Remote subnets (workstations / clients)					
E-MAIL TRAFFIC								
Existing local E-MAIL domain name				Comments				

TESTA II traffic

Only if Quality of Service is Required

E-Mail Traffic

This part is useless for TACHOnet.

Part III - Security Reference Guide

Overview

Introduction

TACHOnet acts as a service provider for allowing Member States to exchange information about tachograph smart cards so that Member States can check that a driver doesn't already hold any valid driver card in another Member State or that a tachograph card is still valid (via enforcers during road check).

This part is intended to provide the national administrations in charge of the TACHOnet project in their country with the necessary information about the security features that must be used to exchange data between Member States using TACHOnet.

Contents

This part contains the following topics:

Chapter 1 - Introduction to TACHOnet Security Features

Introduction

This map outlines the different TACHOnet security requirements, i.e.:

- Authentication
- Confidentiality
- Integrity

Authentication

Every TACHOnet user must be authenticated. But what is a TACHOnet user?

A TACHOnet user can be either:

- A CIA Application (running on a web server or application server) that will process the exchange of XML messages with the TACHOnet central system. Therefore, the CIA users (clerks,…) and the enforcers are not considered as TACHOnet users. It's up to each Member State to manage these users in the more appropriate secure way.
- A CIA Administrator (one dedicated person per Member State who will be granted access to the statistics information supplied by TACHOnet as a web browser-based application).

Confidentiality

Some Member States require that the information exchanged between the Member States via TACHOnet be treated as confidential. Therefore, the data transmitted (XML messages) between the CIA applications and the central TACHOnet system will be encrypted.

Integrity

Integrity guarantees that no data has been altered.

Proposed solution

For the exchange of XML messages between the CIA applications and the central TACHOnet system, authentication, confidentiality and integrity will ensured by sending the XML messages using HTTPS and digital certificates (one digital certificate will be issued per CIA application). From the different alternatives that have been analyzed (HTTPS, S/MIME over HTTP, XML Signature & Encryption, WS-Security), the first one (using HTTPS) has been chosen for its simplicity and cost-effectiveness.

To enable every CIA administrator to access the statistics information provided by TACHOnet as a web browser-based application, authentication, confidentiality and integrity will ensured using HTTPS (1-way SSL) and userid/password. This userid/password will be managed by the TACHOnet administrator (DG TREN).

Digital certificates will be issued using the IDA PKI services (see "TACHOnet Digital Certificates and IDA PKI Services" at page 34 for more details).

Signing and encryption will be carried out at transport level using HTTPS (see "Using HTTPS" at page 46 for more details).

Chapter 2 - TACHOnet Digital Certificates and IDA PKI Services

Overview

Introduction

This chapter describes what's a digital certificate used for, what are the IDA PKI services and what are the procedures that the Member States should follow to request or revoke a digital certificate.

Contents

This chapter contains the following topics:

Introduction to Digital Certificates

The concept: How does it work?

Security solutions using digital certificates rely on public key cryptography in which each user has a pair of cryptographic keys: one private key that is kept private by the user, and one related public key widely made public.

A **Digital Certificate** is a digitally signed statement that certifies the binding between the owner's identity information and his/her electronic public key.

This certified public key can be used to encrypt confidential information to the certificate owner and/or to verify digital signatures generated by the certificate owner.

The certified public key is linked to the private key of the certificate owner in such a way that:

- A **digital signature** is computed from the message and the private key of the signer. It is a small size coded file appended to the signed message. Verification of a digital signature involves the certified public key of the signer. If the check succeeds, the recipient is convinced about its origin and has the guarantee that nothing has been modified in the message since the signature process.
- **Confidentiality** is obtained from the ciphering of the message with the certified public key of the recipient. The only way to decrypt a ciphered message is to use the corresponding private key that is supposed to be known only to the certificate owner.

Digital certificates provide thus solid assurance that a public key actually belongs to the right entity whose identity has been certified by a **Certification Authority**, a known trusted third party, which controls and confirms the accuracy of the binding between a public key and its legitimate owner.

Digital certificates are the Internet passports that prevent you to disclose confidential information to unauthorised persons, and/or to accept an imposter's digital signature as authorisation for a critical electronic business transaction.

Introduction to PKI

What's a PKI?

PKI stands for Public Key Infrastructure. The PKIX Working Group defines a PKI as "*The set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography*".

Public-key cryptography meets the major requirements of confidentiality, integrity, authenticity and non-repudiation. However, to accomplish this, one needs to know:

- Who issues the certificates?
- Where will the private key be stored?
- Where to find certificates?

A digital certificate based security system, such as a public-key infrastructure (PKI), provides the foundations for the resolution of all of these questions.

Components of a PKI

A PKI comprises the following components:

Components	Description
Certificate Authorities (CAs)	responsible for issuing and revoking certificates
Registration Authorities (RAs)	verify the binding between public keys and the identities of their holders.
Certificate holders (or subjects)	people, machines, software agents that have been issued with certificates and can use them to sign digital documents.
Clients	validate digital signatures and certification paths from a trusted CA's public key.
Repositories	store and make available certificates and certificate revocation list (CRLs)
Security policy	sets out and defines the organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. It is described in the Certificate Practice Statement (CPS).

Continued on next page

Introduction to PKI, Continued

Functions of a PKI

Here below is a summary of the major functions performed within a PKI:

Function	Description
Registration	process in which a prospective certificate holder presents itself to the CA in order to request a certificate.
Certification	the CA issues a certificate (with the subject's public key), delivers it to the subject and publishes it in a suitable public repository.
Key generation	if the CA is responsible for generating the key pair, it does so and supplies them to the subject as an encrypted file or physical token (e.g. smart card).
Key recovery	the CA backs up all subjects' private keys so that a key can be recovered later by the right subject.
Key update	All key pairs (and associated certificates) should be updated at regular intervals in case the date of a certificate reaches its expiration date or a private key is compromised.
Cross-certification	process allowing users from one administrative domain to trust certificates issued by a CA operating in a different administrative domain.
Revocation	some events necessitate the early revocation of a certificate's validity (subject changes of name, employee leaves the company, compromise of a private key,...). The revoked certificates are listed in a certificate revocation list (CRL) published, at regular intervals, by the CA into the same repository as the certificates themselves.

IDA PKI Services

What's IDA?

IDA (Interchange of Data between Administrations) is a Community Programme to promote the application of information technology (IT) in the information exchanges between European administrations.

What are IDA PKI services?

The IDA PKI is a particular infrastructure devoted to the IDA user communities and provides the following services:

- A set of trusted procedures and of associated services to create, renew and revoke public key certificates with the participation of enabling actors, the Registration Authorities (RA) and Local Registration Authorities (LRA)
- Availability of the public keys associated with each user, under the form of Public Key Certificates (PKC) guaranteed by a Certification Authority (CA)
- Availability of Certification Revocation List (CRL), allowing the user to check the validity of a given certificate

IDA PKI services operate under the CPS (Certification Practice Statement) published by Belgacom E-Trust™ .

Additional components to PKI organisation

Compared to the general organisation of a PKI described earlier (see "Components of a PKI" on page 36), the generic IDA PKI adds two new concepts:

- ***Closed User Group*** (CUG): the creation of a CUG means that the stringent requirements imposed by the CA on public Registration Authorities can be relaxed towards the needs of the CUG. The CA will only sign IDA-CUG certificates for the users who have been approved by the relevant RA. In the frame of TACHOnet, a specific TACHOnet CUG will be set up.
- ***Local Registration Authority*** (LRA): the LRA stands between the certificate holders (end users) and the Registration Authority (RA). Its goal is to verify the identity of the users requesting the certificate, and approving or rejecting the certificate request. In the frame of TACHOnet, there will be a single LRA played by the European Commission (DG TREN) and represented by Yves Hardy acting as Local Registration Authority Officer.
- ***Suspension and Revocation Authority*** (SRA): the SRA's goal is to handle all revocation requests of the CUG users. The TACHOnet SRA will be DG TREN and represented by Yves Hardy acting as TACHOnet Suspension and Revocation Authority Officer (TSRAO).

IDA PKI Technical aspects

The generic IDA PKI architecture is based on the market standards:

- Certificates follow the X.509 V3 standard
- Compatible with the PKIX standard

PKI set-up for TACHOnet

Introduction

The IDA PKI services perfectly covers the security needs required by TACHOnet in terms of the management of the digital certificates. Obviously, other mechanisms (based on the use of the digital certificates) must be put in place at application level to apply the security requirements.

Using digital certificates supplied by IDA PKI services (via Belgacom E-Trust™) requires a dedicated TACHOnet CUG (Closed User Group) to be set up, some people to be trained to carry out special security-related functions and the type of certificates to be defined.

PKI Infrastructure

The PKI infrastructure that will be used is the the Belgacom E-Trust™ Infrastructure used to issue the standard Belgacom E-Trust™ High Grade server certificates.

Type of certificate

High grade server certificates will be issued for the TACHOnet users. Such type of certificate may be requested either, by means of face to face registration, meaning that the Member State has to come in Belgium with its duly completed and signed order form in order to obtain its own server certificate, or, remotely via the LRAO, on behalf of the legal representative. In this latter case, the Member State shall submit proof of fact that this person is duly authorised to sign for the legal representative

These digital certificates will be RSA certificates with a 1024 bit key length valid for one year.

TACHOnet PKI CUG

A dedicated TACHOnet PKI CUG will be defined and managed by the European Commission (DG TREN).

The TACHOnet CUG requires a TACHOnet Local Registration Authority Officer (LRAO at European Commission – see TLRAO below) and a TACHOnet "Member State Certificated Officer" (see TMSCO below) for every Member State.

TACHOnet Local Registration Authority Officer (TLRAO)

DG TREN will be the TACHOnet Local Registration Authority and represented by Yves Hardy acting as acting as TACHOnet Local Registration Authority Officer (TLRAO).

The role of the TLRAO is the single point of contact between the Member States (TMSCO) and Belgacom E-Trust™. He will receive, from the corresponding TMSCO, the requests/revocations for digital certificates, verify them, forward them to Belgacom E-Trust™, receive back the generated digital certificate and send it back to the corresponding TMSCO.

Continued on next page

PKI set-up for TACHOnet, Continued

TACHOnet "Member State Certificated Officer" (TMSCO)

Every Member State should designate a local (National) administrator in charge of requesting, installing and managing the server certificate at National level.

The role of the TMSCO is the single point of contact between a Member State and the TACHOnet LRAO. He will send his requests for digital certificates (see "How can a Member State apply for a digital certificate?" for more details) on a floppy disk by post to the TACHOnet LRAO. He will receive back (via floppy disk) the requested digital certificate for installation.

PKI needs for TACHOnet

Every TACHOnet user will be assigned a digital certificate to guarantee confidentiality and authentication when exchanging messages. The table below describes the different types of TACHOnet users and their corresponding type of certificate:

TACHOnet User Type	Description
CIA application	A *CIA* (Card Issuing Authority) application (developed by Member States for managing/issuing cards) will make use of the TACHOnet services and is therefore considered for TACHOnet as a single user. Security related to the relevant access rights to this CIA application (clerks,...) is under the full responsibility of the Member State. TACHOnet only provides security mechanism between Card Issuing Authorities (CIA) applications and the TACHOnet central system. Consequently, a digital certificate will be assigned to every *CIA* application (to be installed on the web/application server receiving XML messages).
TACHOnet application	The *TACHOnet* application typed user stands for the central system that will offer the services for exchanging XML messages (requests, responses) between the *CIA* applications. Therefore, a single digital certificate will be assigned to the single TACHOnet system (to be installed on the application server sending the XML messages).

How can a Member State apply for a digital certificate?

Introduction

The procedure for requesting a digital certificate is described below. This procedure is the same for the renewal of the certificates (every year after expiration). In case of renewal, the CA reminds him, before the expiry date, that he will have to issue that renewal request.

Prerequisites

Prior to applying for a digital server certificate, every Member State must set up a web server (the one that will receive TACHOnet XML messages) at their local (National) site. Belgacom E-Trust (also known as Certificate Authority – CA) delivers server certificates for any server compatible with the **X509 v3** standard digital certificates and that are able to make a PKCS # 10 (PEM encoded) electronic certificate request. This covers most of the recent web servers available nowadays.

The web server must then be compatible with the **X509 v3** protocol that enables secure end-to-end electronic data exchange.

The web server should also have a DNS domain name registered in its configuration file. During the generation of the certificate request, you will be prompted to enter some specific information about your server. This information is very important since it will be the one that will be certified by Belgacom E-Trust CA. The most important part to enter correctly is the name of your server (CN). **It MUST correspond to the registered Web site server name you will protect**. Indeed, if the real server name does not match the name in the certificate, you will never be able to start your SSL Web Server sessions.

In the framework of the TACHOnet project, it has been decided that the full DNS domain name should be registered as follows on the web server of every Member State:

TCN.<Country_Code>.EU-ADMIN.NET

<Country_Code> is composed of two characters of your country (i.e. Belgium: **BE**, Netherlands: **NL**, …).

Stakeholders

The following stakeholders will intervene in the workflow for requesting a digital certificate:

Stakeholder	Role
CA	Certificate Authority (Belgacom E-Trust™)
TLRAO	TACHOnet Local Registration Authority Officer
TMSCO	TACHOnet "Member State Certificated Officer"

Continued on next page

How can a Member State apply for a digital certificate?,
Continued

Procedure The procedure is the following:

<table>
<tr><th>Step</th><th>Action</th><th>Actor</th></tr>
<tr><td>1</td><td>Install the Certipost E-Trust™ primary and root certificates:
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Open your browser (Netscape Navigator 3.x or higher, Netscape Communicator or Microsoft IE 3.x or higher) and go to http://www.e-trust.belgacom.be/page.asp?lang=en&s=274</td></tr>
<tr><td>2</td><td>Click on the “Accept the Certipost Qualified CA certificates” hyperlink and save it to your hard disk.</td></tr>
<tr><td>3</td><td>Click on the “Accept the Certipost Normalised CA certificates” hyperlink and save it to your hard disk</td></tr>
<tr><td>4</td><td>Click on the “Certificate Installation Guide” hyperlink to learn about how to install the certificates in your web browser.</td></tr>
</table>
If you encounter any difficulties at this stage of the installation, please do not hesitate to post your queries to the Digital Tachograph Interest Group located on our Circa web site. In the newsgroup, there is a special topic called: PKI for all the open issues.</td><td>TMSCO</td></tr>
<tr><td>2</td><td>Generate your server certificate request:
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Open your browser and go to http://www.e-trust.belgacom.be/page.asp?lang=en&s=399&ss=129 and read the section “Tested and Recommended Servers” for examples for Netscape Enterprise Servers, Microsoft IIS or Apache. If your web server is not listed, please refer to the Internet site of your supplier in order to know how to deal with the installation and the configuration of the SSL protocol. Most recent web servers support the SSL protocol. The rules remain the same for any kind of web server available on the market.</td></tr>
<tr><td>2</td><td>On your web server, generate a (RSA) 1024-bit private key and store it in the file “server.key” encrypted by a given pass phrase using the triple-des encryption algorithm (des3 option).</td></tr>
<tr><td>3</td><td>On your web server, generate the certificate request file using the “server.key” file generated above and store it in the “server.csr” file.</td></tr>
</table></td><td>TMSCO</td></tr>
</table>

Continued on next page

How can a Member State apply for a digital certificate?,
Continued

Procedure (continued)

Step	Action	Actor
3	Beside the server certificate request file, please prepare the following documents: ▪ Firstly, read the General Terms and Conditions (Object Identification, Number OID: 0.3.2062.9.6.2.4.2.4) that form an integral part hereof. It's available on http://195.13.1.46/en/uploads/Q&Ncps-uk-20011101.pdf ▪ Duly complete and sign the "Standard Certipost (E-Trust) certificate Web Server Order Form" document (see p.50 for more details). ▪ Sign a copy of both sides of your identity card, passport or similarly valid official document ▪ A copy of the electronic certificate application on a diskette, since the key pair will have been generated by you (see step 2 for more details). ▪ A copy of the current official memorandum and articles of association of the company/organisation you officially represent, or failing this, an excerpt from the register of companies or any other valid official documents, including the relevant excerpt or a similar document. ▪ If the person signs the order form is acting on behalf of the legal representative, the Customer shall submit proof of fact that this person is duly authorized to sign for the legal representative. ▪ Proof that the server domain name for the business (see server_cert_order_form.doc file where it is referred to as "The Organization") has been registered and is therefore unique	TMSCO
4	Copy all the documents and the server certificate request file on a floppy disk and send it out to the TLRAO (Yves Hardy) at the following postal address: European Commision DG Transports and Energy Mr. Yves Hardy Rue de Mot, 28 – 02/40 1040 Brussels Belgium **Pay attention on the fact that these documents must be sent by post or handed over during one of the next TF2 meetings but NOT via email.**	TMSCO

Continued on next page

How can a Member State apply for a digital certificate?,
Continued

Procedure (continued)

<table>
<tr><th>Step</th><th>Action</th><th>Actor</th></tr>
<tr><td>5</td><td>Install the generated server certificate on your web server:
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Once generated by Belgacom E-Trust, your server certificate (file “server.crt”in PEM format) will be sent out to you (TMSCO) by the TLRAO either via post or via TF2 meeting or via email (if the TMSCO accepts this latter choice).</td></tr>
<tr><td>2</td><td>Install this “server.cert” file on your web server so that it can enable the use of the SSL protocol when receiving TACHOnet XML messages (enable SSL + require client certificates).</td></tr>
</table>
Pay attention on the fact that the server certificate that will be generated by Belgacom E-Trust (our Certificate Authority) will only operate on the machine where you have generated the “server.csr” file. The key is unique per server and cannot be copied or even reused on other machines.</td><td>TLRAO
TMSCO</td></tr>
</table>

How can a Member State revoke a digital certificate?

Introduction

This procedure describes how to revoke an existing digital certificate.

When to revoke?

Revoking a digital certificate might occur when the private key is lost or accidentally shared. A presumption of hacking is also an urgent reason for revocation.

Prerequisites

Same as the procedure for requesting a digital certificate (see page 41).

Stakeholders

The following stakeholders will intervene in the workflow for requesting a digital certificate:

Stakeholder	Role
CA	Certificate Authority (Belgacom E-Trust™)
TSRAO	TACHOnet Suspension and Revocation Authority Officer (Yves Hardy at DG TREN)
TMSCO	TACHOnet "Member State Certificated Officer"

Procedure

The procedure is the following:

Step	Action	Actor
1	Call immediately the TSRAO. If the TSRAO (and his backup) is not available, call or fax (using a fax template available on request to IDA PKI) immediately Belgacom E-Trust™ at the following numbers: ▪ Phone: +32 78 152470 ▪ Fax: +32 2 2014927 In any circumstance, the TSRAO must be kept informed.	TMSCO
2	As soon as the revocation is being acted, the TMSCO must apply for a new digital certificate.	TMSCO

Chapter 3 - Using HTTPS

Overview

Introduction

In order to ensure authentication, privacy and integrity around the exchange of XML messages between the Member States and the central TACHOnet system, HTTPS must be used along with the supplied digital certificates. This chapter gives a description of HTTPS and some hints about how to use it within the TACHOnet framework.

Contents

This chapter contains the following topics:

Introduction to HTTPS in TACHOnet

Introduction

A brief introduction of HTTPS usage in TACHOnet is given below.

What's HTTPS?

HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Secure Socket Layer (SSL) as a sub-layer under the regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.). SSL is an integral part of most Web browsers (clients) and Web servers

HTTPS and SSL support the use of X.509 digital certificates from the server so that, if necessary, a user can authenticate the server. SSL is an open, non-proprietary protocol that Netscape has proposed as a standard to the World Wide Consortium (W3C).

HTTPS with Server Certificate (1-way SSL)

Due to DI's Data Center constraints (reverse proxy stopping the SSL tunnel), 1-way SSL will only be supported when Member States CIA applications will send XML messages to the central TACHOnet system.

Such a solution fulfills data integrity (through signing), confidentiality (through encryption) and authentication of the central TACHOnet server (through the DI Data Center reverse proxy server certificate). However, authentication of the client (the Member State CIA application sending the XML message) is not provided by this solution. But this could be acceptable due to the asynchronous nature of the data exchange and the fact that an XML response will always be sent asynchronously to the Member State CIA mentioned in the incoming XML request.

HTTPS with Client & Server Certificates (2-way SSL)

2-way SSL will be used when the central TACHOnet system will send XML messages to the Member State CIA applications. Such a solution fulfills data integrity (through signing), confidentiality (through encryption) and authentication of both client and server (through the usage of the Member State CIA web server's server certificate and the central TACHOnet server's server certificate).

That solution requires the exact same installation (as above) for the installation of digital certificates (provided by IDA PKI) on the central TACHOnet application server and on the Member State CIA web servers. These web servers need also to be configured to require HTTPS (port 443) and client certificates for accessing their single page receiving the incoming TACHOnet XML messages (requests or responses). These CIA web servers should only grant access to the TACHOnet server digital certificate, while the TACHOnet application server should grant access to only the CIA digital certificates.

How to use HTTPS for the exchange of XML messages in TACHOnet?

Introduction

As described in the "TACHOnet XML Messaging Reference Guide", different XML messages (requests and responses) will be exchanged between CIA applications and the central TACHOnet system. HTTPS has been proposed to guarantee data integrity, confidentiality and authentication for the exchange of these XML messages.

HTTPS and Incoming of XML messages

In TACHOnet, as XML messages are sent via HTTPS, the first recipient of any sent XML message is always the web server of the target recipient (either the central TACHOnet web server or a MS CIA web server). Once received at application level, the XML message is in clear (setting up the SSL session is carried out behind the scenes). Each TACHOnet stakeholder (the central TACHOnet system and every MS CIA application) should supply a single address (url to a single page on the web server) for receiving XML messages (requests or responses).

The following steps must be followed in order to set up correctly HTTPS on the web servers:

Step	Action
1	A digital certificate must be installed on each of these web servers in order to identify them (guaranteeing at least authentication of the recipient server). See "TACHOnet Digital Certificates and IDA PKI Services" at page 34 for more details about how to get these digital certificates.
2	HTTPS (port 443) must be configured on these web servers for accessing their single page receiving the incoming XML messages (requests or responses). Firewalls and/or proxies should also be configured to allow HTTPS from/to these web servers.

HTTPS and Sending of XML messages

Once HTTPS configured on the web servers (for receiving incoming XML messages via HTTPS), the sending of XML messages via HTTPS is actually straightforward at implementation level. Indeed, current development environments (Java, .NET,…) provides interfaces for sending XML message via HTTPS in less than 10 lines of code (opening the HTTPS url connection, sending the XML message, checking for the expected '202 Accepted'), hiding the HTTP and SSL intricacies.

The recipient's server certificate must be installed on the application servers sending the XML messages. In other words:

- The central TACHOnet server's digital certificate must be installed in a certificate store (for authentication) on every CIA application server.
- The different CIA web servers' digital certificates must be installed in a certificate store (for authentication) on the central TACHOnet application server.

Chapter 4 - Annexes

Overview

Introduction

This chapter includes some annexes referred to in the previous chapters.

Contents

This chapter contains the following topics:

Standard Certipost (E-Trust) certificate Web Server Order Form

Introduction

This document must be filled in by every TMSCO in order to apply for a server certificate.

This document and the "PKI Help" document are available on the CIRCA site (Library\Card Issuing Working Groups\Working Group\PKI - Server Certificates).

Page 2 - Information for checking your identity

This part must be filled in by the Member State representative only if she comes herself to Belgacom E-Trust in Belgium to request her digital certificate.

If the Member State asks the TACHOnet LRAO to request the digital certificate, then this part must be filled in by the TACHOnet LRAO.

Continued on next page

Standard Certipost (E-Trust) certificate Web Server Order Form, Continued

Page 1

certipost

OID: 0.3.2062.9.6.2.4.1.4

Certipost (E-Trust) certification services

Standard Certipost (E-Trust) certificate
Web Server Order Form
Version 4.0, Automated Local Registration Authority Operator (LRAO)

Reserved for the Local Registration Authority (LRA)

Customer name:.....

LRA operator (LRAO): .....

Contract number: .....
Date of receipt: .....
Place where the copy of the registration documents is held in safekeeping:
.....

Hereby certifies that this Order Form and the appendixes hereto are duly authenticated and validated.

1 URL
2 URLs
3 URLs

Server certificate

Wildcard server certificate

Signature of the LRAO: .....

Continued on next page

Standard Certipost (E-Trust) certificate Web Server Order Form, Continued

Page 2

certipost

OID: 0.3.2062.9.6.2.4.1.4

Data to be certified[1]

The data that follows shall form an integral part of your digital certificate. Some fields are optional, which means that you are not obliged to have this data certified. Where this is the case, you do not have to fill in the fields concerned. The certificate will have the same probative value regardless of whether these optional fields are filled in.

The fields in *italics* are optional; the others are mandatory.

URL Web server (1)[2]	
URL Web server (2)[2] (optional)	
URL Web server (3)[2] *(optional)*	
Nationality (country)	
Organization (official name as published in the memorandum and articles of association)	
Department or unit (optional)	
Customer's e-mail address	

The content of the following fields must be an accurate reflection of the probative documents submitted. Certification shall not otherwise be provided.

Information for checking your identity[3]

This information will be used by Certipost to check your identity. This information shall not be placed in the public domain and Certipost undertakes to treat it as confidential[2].

Last name	
First names	
Private address Street	
Number	

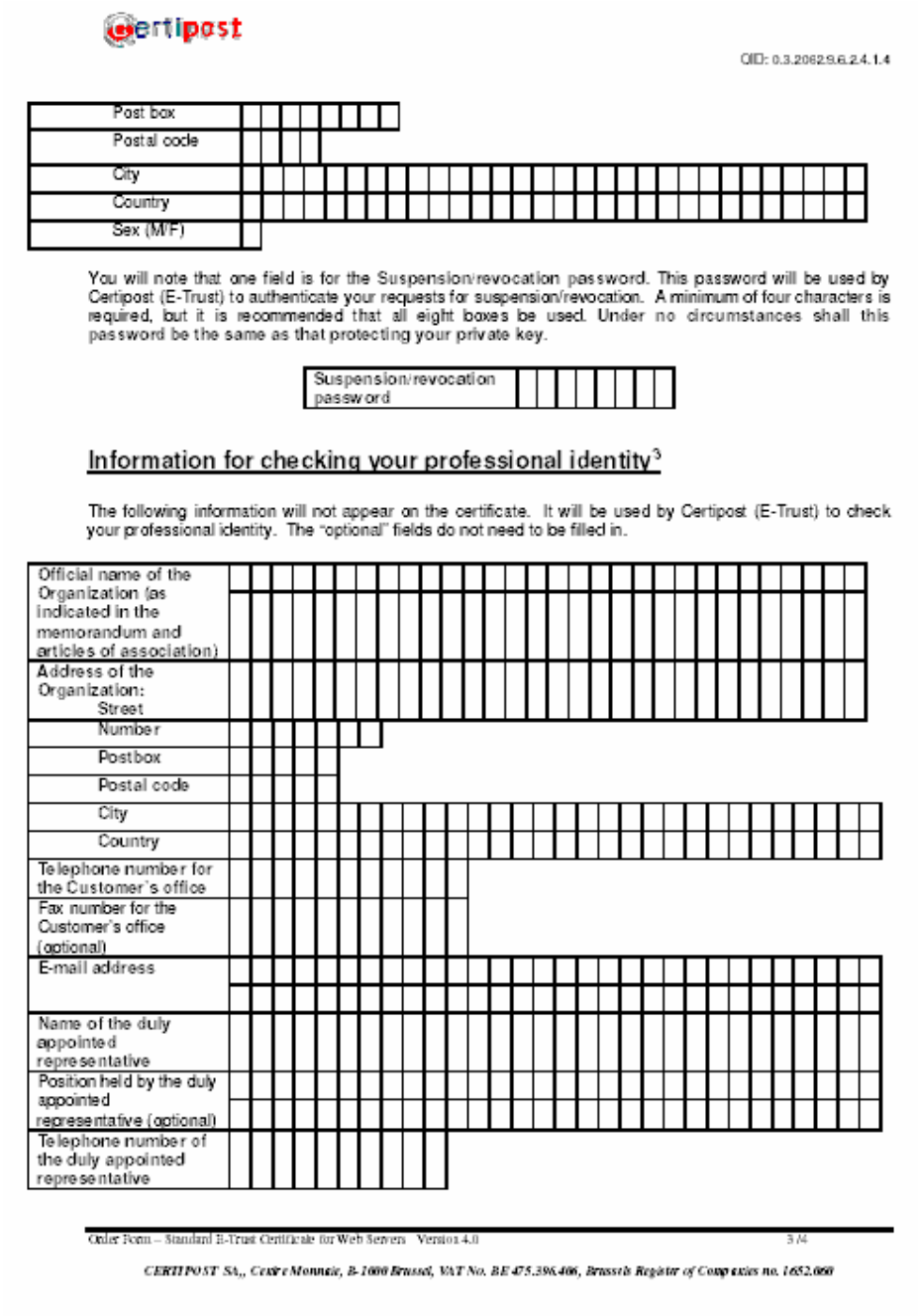
[1] Personal data communicated by the applicant to Certipost (Belgacom E-Trust)will be incorporated into files held by Certipost S.A., Centre Monnaie, B-1000 Brussels, and, as appropriate, in files held by the LRA. This data shall only be used for the purposes of providing Certipost (Belgacom E-Trust) services. This personal data may be inspected and rectified by the Customer, who, at no cost, may prohibit its use for direct marketing purposes.

[2] The amount charged varies depending on whether it is a wildcard certificate and/or a multiple URL certificate and is indicated in the "Charges and Payment" section. Please enter a "*" if you are applying for a wildcard certificate.

Continued on next page

Standard Certipost (E-Trust) certificate Web Server Order Form, Continued

Page 3



certipost

OID: 0.3.2062.9.6.2.4.1.4

Post box	
Postal code	
City	
Country	
Sex (M/F)	

You will note that one field is for the Suspension/revocation password. This password will be used by Certipost (E-Trust) to authenticate your requests for suspension/revocation. A minimum of four characters is required, but it is recommended that all eight boxes be used. Under no circumstances shall this password be the same as that protecting your private key.

Suspension/revocation password	

Information for checking your professional identity[3]

The following information will not appear on the certificate. It will be used by Certipost (E-Trust) to check your professional identity. The "optional" fields do not need to be filled in.

Official name of the Organization (as indicated in the memorandum and articles of association)	
Address of the Organization: Street	
Number	
Postbox	
Postal code	
City	
Country	
Telephone number for the Customer's office	
Fax number for the Customer's office (optional)	
E-mail address	
Name of the duly appointed representative	
Position held by the duly appointed representative (optional)	
Telephone number of the duly appointed representative	

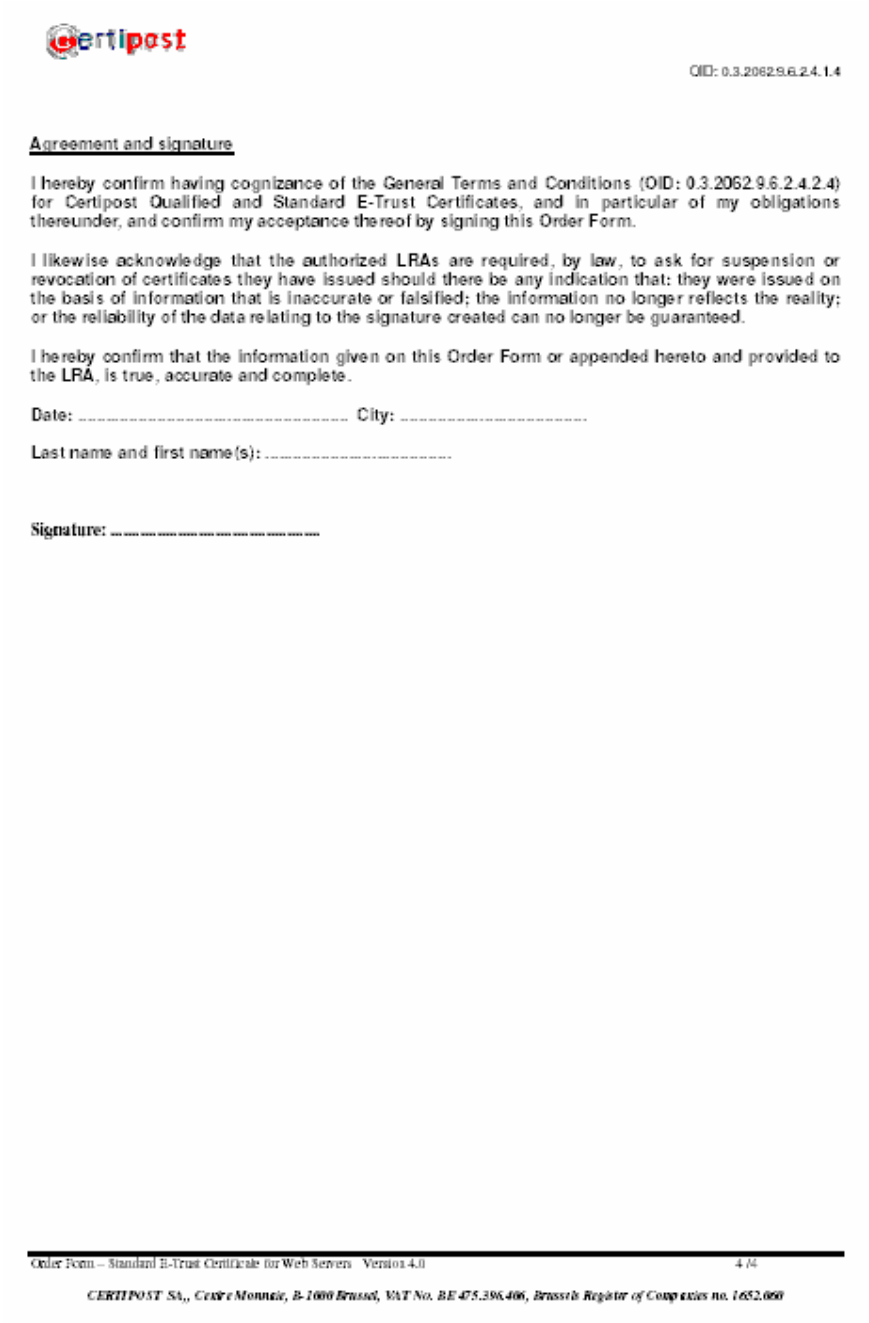
Order Form – Standard E-Trust Certificate for Web Servers Version 4.0 3/4

CERTIPOST SA,, Cour e Monnaie, B-1000 Brussel, VAT No. BE 475.396.406, Brussels Register of Companies no. 1652.060

Continued on next page

Standard Certipost (E-Trust) certificate Web Server Order Form, Continued

Page 4



certipost

OID: 0.3.2062.9.6.2.4.1.4

Agreement and signature

I hereby confirm having cognizance of the General Terms and Conditions (OID: 0.3.2062.9.6.2.4.2.4) for Certipost Qualified and Standard E-Trust Certificates, and in particular of my obligations thereunder, and confirm my acceptance thereof by signing this Order Form.

I likewise acknowledge that the authorized LRAs are required, by law, to ask for suspension or revocation of certificates they have issued should there be any indication that: they were issued on the basis of information that is inaccurate or falsified; the information no longer reflects the reality; or the reliability of the data relating to the signature created can no longer be guaranteed.

I hereby confirm that the information given on this Order Form or appended hereto and provided to the LRA, is true, accurate and complete.

Date: ..... City: .....

Last name and first name(s): .....

Signature: .....

Order Form – Standard E-Trust Certificate for Web Servers Version 4.0 4/4

CERTIPOST SA,, Centre Monnaie, B-1000 Brussel, VAT No. BE 475.396.406, Brussels Register of Companies no. 1652.060