

Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime

---

*Status: This is the original version (as it was originally adopted).*

---

## ANNEX

### CHAPTER 1: Exchange of DNA-Data

#### 5. Application, security and communication architecture

##### 5.1. Overview

In implementing applications for the DNA data exchange within the framework of Decision 2008/615/JHA, a common communication network shall be used, which will be logically closed among the Member States. In order to exploit this common communication infrastructure of sending requests and receiving replies in a more effective way, an asynchronous mechanism to convey DNA and dactyloscopic data requests in a wrapped SMTP e-mail message is adopted. In fulfilment of security concerns, the mechanism s/MIME as extension to the SMTP functionality will be used to establish a true end-to-end secure tunnel over the network.

The operational TESTA (Trans European Services for Telematics between Administrations) is used as the communication network for data exchange among the Member States. TESTA is under the responsibility of the European Commission. Taking into account that national DNA databases and the current national access points of TESTA may be located on different sites in the Member States, access to TESTA may be set up either by:

1. using the existing national access point or establishing a new national TESTA access point; or by
2. setting up a secure local link from the site where the DNA database is located and managed by the competent national agency to the existing national TESTA access point.

The protocols and standards deployed in the implementation of Decision 2008/615/JHA applications comply with the open standards and meet the requirements imposed by national security policy makers of the Member States.

##### 5.2. Upper Level Architecture

In the scope of Decision 2008/615/JHA, each Member State will make its DNA data available to be exchanged with and/or searched by other Member States in conformity with the standardised common data format. The architecture is based upon an any-to-any communication model. There exists neither a central computer server nor a centralised database to hold DNA profiles.

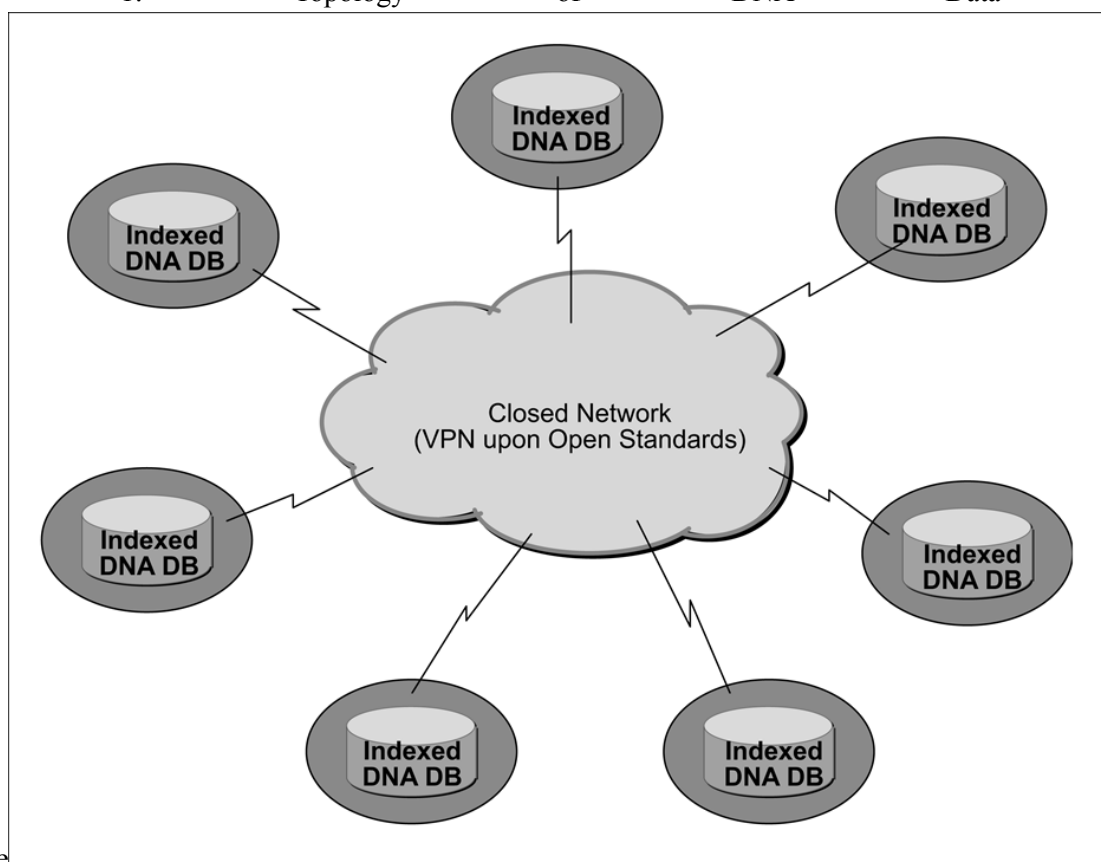
on...

ANNEX CHAPTER 1: Exchange of DNA-Data

Document Generated: 2023-08-18

*Status: This is the original version (as it was originally adopted).*

Figure 1: Topology of DNA Data Exchange



Exchange

In addition to the fulfilment of national legal constraints at Member States' sites, each Member State may decide what kind of hardware and software should be deployed for the configuration at its site to comply with the requirements set out in Decision 2008/615/JHA.

### 5.3. Security Standards and Data Protection

Three levels of security concerns have been considered and implemented.

#### 5.3.1. Data Level

DNA profile data provided by each Member State have to be prepared in compliance with a common data protection standard, so that requesting Member States will receive an answer mainly to indicate HIT or NO-HIT along with an identification number in case of a HIT, which does not contain any personal information. The further investigation after the notification of a HIT will be conducted at bilateral level pursuant to the existing national legal and organisational regulations of the respective Member States' sites.

#### 5.3.2. Communication Level

Messages containing DNA profile information (requesting and replying) will be encrypted by means of a state-of-the-art mechanism in conformity with open standards, such as s/MIME, before they are forwarded to the sites of other Member States.

#### 5.3.3. Transmission Level

All encrypted messages containing DNA profile information will be forwarded onto other Member States' sites through a virtual private tunnelling system administered by a trusted

---

*Status: This is the original version (as it was originally adopted).*

---

network provider at the international level and the secure links to this tunnelling system under the national responsibility. This virtual private tunnelling system does not have a connection point with the open Internet.

#### 5.4. Protocols and Standards to be used for encryption mechanism: s/MIME and related packages

The open standard s/MIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The protocol s/MIME (V3) allows signed receipts, security labels, and secure mailing lists and is layered on Cryptographic Message Syntax (CMS), an IETF specification for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data.

The underlying certificate used by s/MIME mechanism has to be in compliance with X.509 standard. In order to ensure common standards and procedures with other Prüm applications, the processing rules for s/MIME encryption operations or to be applied under various COTS (Commercial Product of the Shelves) environments, are as follows:

- the sequence of the operations is: first encryption and then signing,
- the encryption algorithm AES (Advanced Encryption Standard) with 256 bit key length and RSA with 1 024 bit key length shall be applied for symmetric and asymmetric encryption respectively,
- the hash algorithm SHA-1 shall be applied.

s/MIME functionality is built into the vast majority of modern e-mail software packages including Outlook, Mozilla Mail as well as Netscape Communicator 4.x and inter-operates among all major e-mail software packages.

Because of s/MIME's easy integration into national IT infrastructure at all Member States' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal 'Proof of Concept' in a more efficient way and reducing costs the open standard JavaMail API is however chosen for prototyping DNA data exchange. JavaMail API provides simple encryption and decryption of e-mails using s/MIME and/or OpenPGP. The intent is to provide a single, easy-to-use API for e-mail clients that want to send and received encrypted e-mail in either of the two most popular e-mail encryption formats. Therefore any state-of-the-art implementations to JavaMail API will suffice for the requirements set by Decision 2008/615/JHA, such as the product of Bouncy Castle JCE (Java Cryptographic Extension), which will be used to implement s/MIME for prototyping DNA data exchange among all Member States.

#### 5.5. Application Architecture

Each Member State will provide the other Member States with a set of standardised DNA profile data which are in conformity with the current common ICD. This can be done either by providing a logical view over individual national database or by establishing a physical exported database (indexed database).

The four main components: E-mail server/s/MIME, Application Server, Data Structure Area for fetching/feeding data and registering incoming/outgoing messages, and Match Engine implement the whole application logic in a product-independent way.

In order to provide all Member States with an easy integration of the components into their respective national sites, the specified common functionality has been implemented by means of open source components, which could be selected by each Member State depending on its national IT policy and regulations. Because of the independent features to be implemented to get access to indexed databases containing DNA profiles covered by Decision 2008/615/JHA,

on...

ANNEX CHAPTER 1: Exchange of DNA-Data

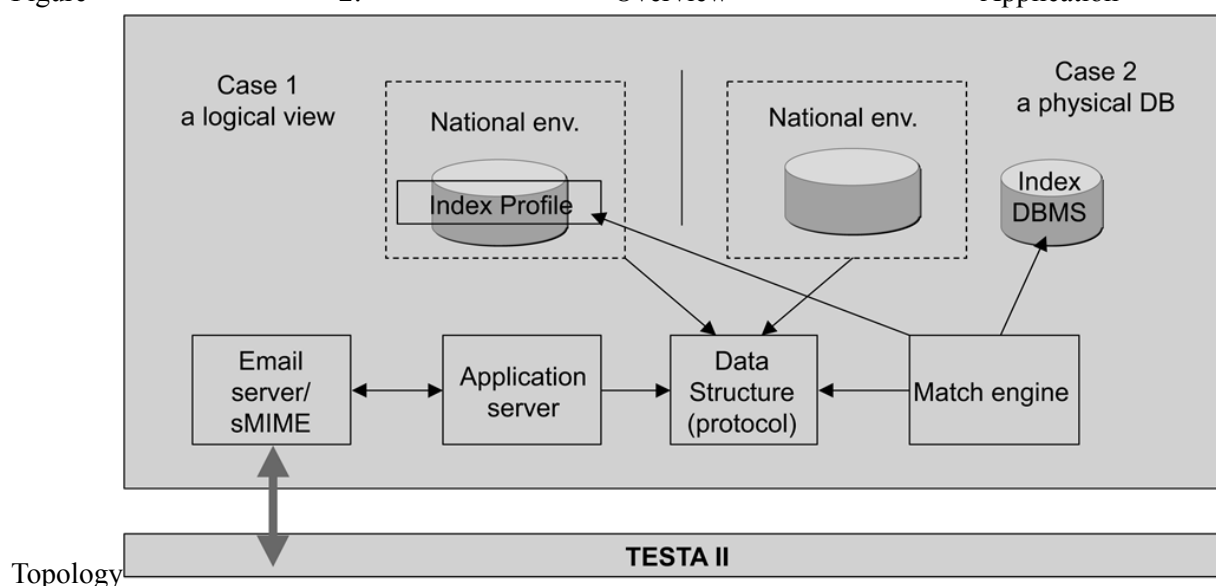
Document Generated: 2023-08-18

*Status: This is the original version (as it was originally adopted).*

each Member State can freely select its hardware and software platform, including database and operating systems.

A prototype for the DNA Data Exchange has been developed and successfully tested over the existing common network. The version 1.0 has been deployed in the productive environment and is used for daily operations. Member States may use the jointly developed product but may also develop their own products. The common product components will be maintained, customised and further developed according to changing IT, forensic and/or functional police requirements.

Figure 2: Overview Application



## 5.6. Protocols and Standards to be used for application architecture:

### 5.6.1. XML

The DNA data exchange will fully exploit XML-schema as attachment to SMTP e-mail messages. The eXtensible Markup Language (XML) is a W3C-recommended general-purpose markup language for creating special-purpose markup languages, capable of describing many different kinds of data. The description of the DNA profile suitable for exchange among all Member States has been done by means of XML and XML schema in the ICD document.

### 5.6.2. ODBC

Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has, however, certain drawbacks. Administering a large number of client machines can involve a diversity of drivers and DLLs. This complexity can increase system administration overhead.

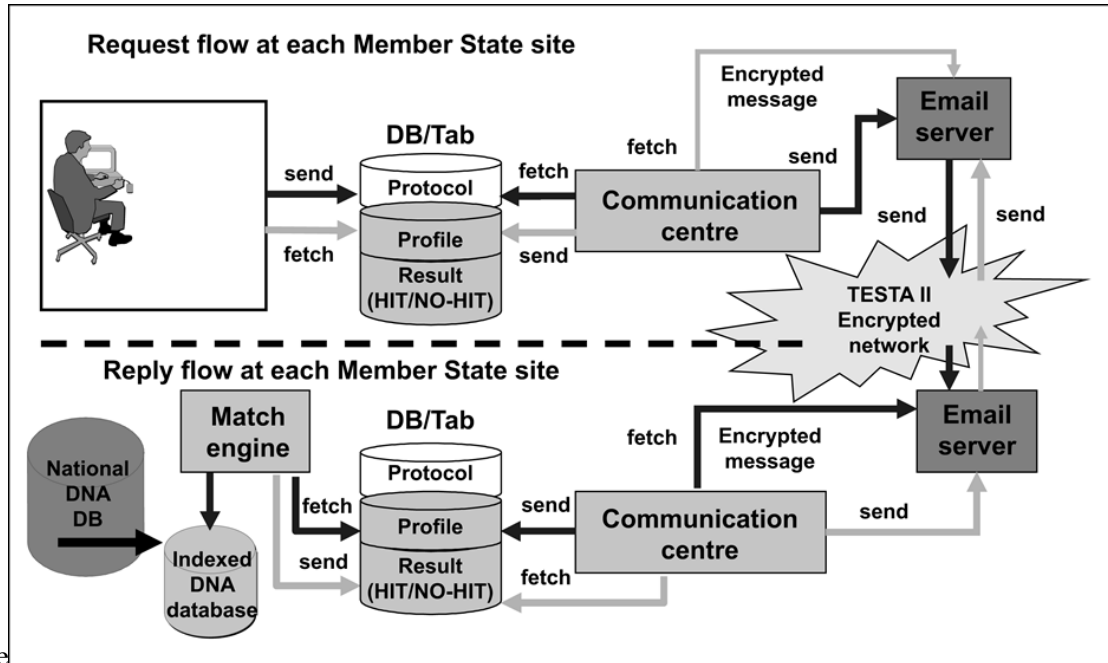
### 5.6.3. JDBC

Java DataBase Connectivity (JDBC) is an API for the Java programming language that defines how a client may access a database. In contrast to ODBC, JDBC does not require to use a certain set of local DLLs at the Desktop.

The business logic to process DNA profile requests and replies at each Member States' site is described in the following diagram. Both requesting and replying flows interact with a neutral data area comprising different data pools with a common data structure.

*Status: This is the original version (as it was originally adopted).*

Figure 3: Overview Application Workflow at each Member State's



site

## 5.7. Communication Environment

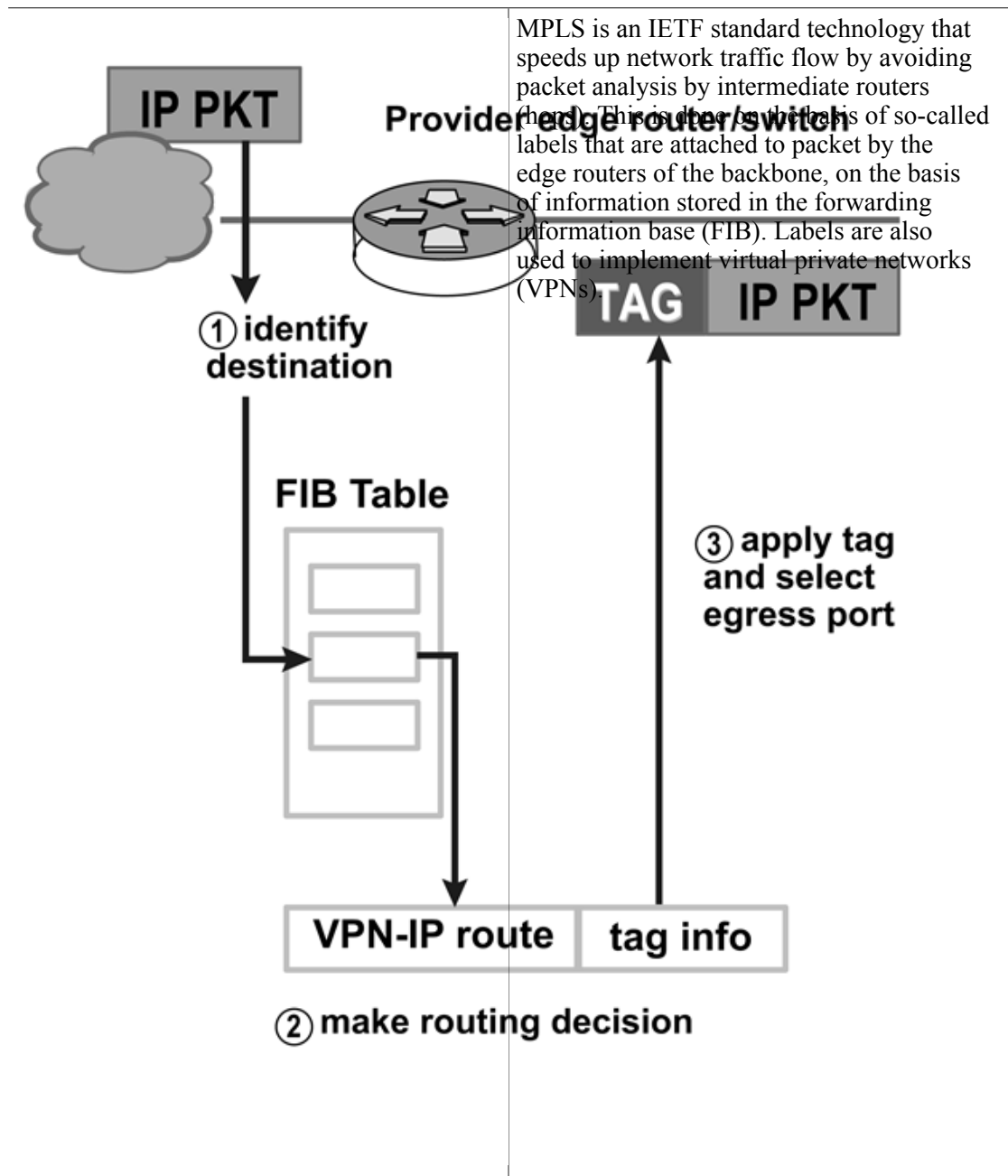
### 5.7.1. Common Communication Network: TESTA and its follow-up infrastructure

The application DNA data exchange will exploit the e-mail, an asynchronous mechanism, to send requests and to receive replies among the Member States. As all Member States have at least one national access point to the TESTA network, the DNA data exchange will be deployed over the TESTA network. TESTA provides a number of added-value services through its e-mail relay. In addition to hosting TESTA specific e-mail boxes, the infrastructure can implement mail distribution lists and routing policies. This allows TESTA to be used as a clearing house for messages addressed to administrations connected to the EU wide Domains. Virus check mechanisms may also be put in place.

The TESTA e-mail relay is built on a high availability hardware platform located at the central TESTA application facilities and protected by firewall. The TESTA Domain Name Services (DNS) will resolve resource locators to IP addresses and hide addressing issues from the user and from applications.

### 5.7.2. Security Concern

The concept of a VPN (Virtual Private Network) has been implemented within the framework of TESTA. Tag Switching Technology used to build this VPN will evolve to support Multi-Protocol Label Switching (MPLS) standard developed by the Internet Engineering Task Force (IETF).



MPLS combines the benefits of layer 3 routing with the advantages of layer 2 switching. Because IP addresses are not evaluated during transition through the backbone, MPLS does not impose any IP addressing limitations.

Furthermore e-mail messages over the TESTA will be protected by s/MIME driven encryption mechanism. Without knowing the key and possessing the right certificate, nobody can decrypt messages over the network.

5.7.3. *Protocols and Standards to be used over the communication network*

5.7.3.1. SMTP

---

*Status: This is the original version (as it was originally adopted).*

---

Simple Mail Transfer Protocol is the de facto standard for e-mail transmission across the Internet. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and then the message text is transferred. SMTP uses TCP port 25 upon the specification by the IETF. To determine the SMTP server for a given domain name, the MX (Mail eXchange) DNS (Domain Name Systems) record is used.

Since this protocol started as purely ASCII text-based it did not deal well with binary files. Standards such as MIME were developed to encode binary files for transfer through SMTP. Today, most SMTP servers support the 8BITMIME and s/MIME extension, permitting binary files to be transmitted almost as easily as plain text. The processing rules for s/MIME operations are described in the section s/MIME (see Chapter 5.4).

SMTP is a 'push' protocol that does not allow one to 'pull' messages from a remote server on demand. To do this a mail client must use POP3 or IMAP. Within the framework of implementing DNA data exchange it is decided to use the protocol POP3.

#### 5.7.3.2. POP

Local e-mail clients use the Post Office Protocol version 3 (POP3), an application-layer Internet standard protocol, to retrieve e-mail from a remote server over a TCP/IP connection. By using the SMTP Submit profile of the SMTP protocol, e-mail clients send messages across the Internet or over a corporate network. MIME serves as the standard for attachments and non-ASCII text in e-mail. Although neither POP3 nor SMTP requires MIME-formatted e-mail, essentially Internet e-mail comes MIME-formatted, so POP clients must also understand and use MIME. The whole communication environment of Decision 2008/615/JHA will therefore include the components of POP.

#### 5.7.4. *Network Address Assignment*

##### Operative environment

A dedicated block of C class subnet has currently been allocated by the European IP registration authority (RIPE) to TESTA. Further address blocks may be allocated to TESTA in the future if required. The assignment of IP addresses to Member States is based upon a geographical schema in Europe. The data exchange among Member States within the framework of Decision 2008/615/JHA is operated over a European wide logically closed IP network.

##### Testing Environment

In order to provide a smooth running environment for the daily operation among all connected Member States, it is necessary to establish a testing environment over the closed network for new Member States which prepare to join the operations. A sheet of parameters including IP addresses, network settings, e-mail domains as well as application user accounts has been specified and should be set up at the corresponding Member State's site. Moreover, a set of pseudo DNA profiles has been constructed for the test purposes.

#### 5.7.5. *Configuration Parameters*

A secure e-mail system is set up using the eu-admin.net domain. This domain with the associated addresses will not be accessible from a location not on the TESTA EU wide domain, because the names are only known on the TESTA central DNS server, which is shielded from the Internet.

The mapping of these TESTA site addresses (host names) to their IP addresses is done by the TESTA DNS service. For each Local Domain, a Mail entry will be added to this TESTA central DNS server, relaying all e-mail messages sent to TESTA Local Domains to the TESTA central Mail Relay. This TESTA central Mail Relay will then forward them to the specific Local Domain e-mail server using the Local Domain e-mail addresses. By relaying the e-mail in this



on...

ANNEX CHAPTER 1: Exchange of DNA-Data

Document Generated: 2023-08-18

*Status: This is the original version (as it was originally adopted).*

way, critical information contained in e-mails will only pass the Europe - wide closed network infrastructure and not the insecure Internet.

It is necessary to establish sub-domains (***bold italics***) at the sites of all Member States upon the following syntax:

'***application-type.pruem.Member State-code.eu-admin.net***', where:

'***Member State-code***' takes the value of one of the two letter-code Member State codes (i.e. AT, BE, etc.).

'***application-type***' takes one of the values: DNA and FP.

By applying the above syntax, the sub domains for the Member States are shown in the following table:

<b>MS</b>	<b>Sub Domains</b>	<b>Comments</b>
BE	<b><i>dna.pruem.be.eu-admin.net</i></b>	Setting up a secure local link to the existing TESTA II access point
	<b><i>fp.pruem.be.eu-admin.net</i></b>	
BG	<b><i>dna.pruem.bg.eu-admin.net</i></b>	
	<b><i>fp.pruem.bg.eu-admin.net</i></b>	
CZ	<b><i>dna.pruem.cz.eu-admin.net</i></b>	
	<b><i>fp.pruem.cz.eu-admin.net</i></b>	
DK	<b><i>dna.pruem.dk.eu-admin.net</i></b>	
	<b><i>fp.pruem.dk.eu-admin.net</i></b>	
DE	<b><i>dna.pruem.de.eu-admin.net</i></b>	Using the existing TESTA II national access points
	<b><i>fp.pruem.de.eu-admin.net</i></b>	
EE	<b><i>dna.pruem.ee.eu-admin.net</i></b>	
	<b><i>fp.pruem.ee.eu-admin.net</i></b>	
IE	<b><i>dna.pruem.ie.eu-admin.net</i></b>	
	<b><i>fp.pruem.ie.eu-admin.net</i></b>	
EL	<b><i>dna.pruem.el.eu-admin.net</i></b>	
	<b><i>fp.pruem.el.eu-admin.net</i></b>	
ES	<b><i>dna.pruem.es.eu-admin.net</i></b>	Using the existing TESTA II national access point
	<b><i>fp.pruem.es.eu-admin.net</i></b>	
FR	<b><i>dna.pruem.fr.eu-admin.net</i></b>	Using the existing TESTA II national access point
	<b><i>fp.pruem.fr.eu-admin.net</i></b>	
IT	<b><i>dna.pruem.it.eu-admin.net</i></b>	

---

*Status: This is the original version (as it was originally adopted).*

---

	<b><i>fp.pruem.it.eu-admin.net</i></b>	
CY	<b><i>dna.pruem.cy.eu-admin.net</i></b>	
	<b><i>fp.pruem.cy.eu-admin.net</i></b>	
LV	<b><i>dna.pruem.lv.eu-admin.net</i></b>	
	<b><i>fp.pruem.lv.eu-admin.net</i></b>	
LT	<b><i>dna.pruem.lt.eu-admin.net</i></b>	
	<b><i>fp.pruem.lt.eu-admin.net</i></b>	
LU	<b><i>dna.pruem.lu.eu-admin.net</i></b>	Using the existing TESTA II national access point
	<b><i>fp.pruem.lu.eu-admin.net</i></b>	
HU	<b><i>dna.pruem.hu.eu-admin.net</i></b>	
	<b><i>fp.pruem.hu.eu-admin.net</i></b>	
MT	<b><i>dna.pruem.mt.eu-admin.net</i></b>	
	<b><i>fp.pruem.mt.eu-admin.net</i></b>	
NL	<b><i>dna.pruem.nl.eu-admin.net</i></b>	Intending to establish a new TESTA II access point at the NFI
	<b><i>fp.pruem.nl.eu-admin.net</i></b>	
AT	<b><i>dna.pruem.at.eu-admin.net</i></b>	Using the existing TESTA II national access point
	<b><i>fp.pruem.at.eu-admin.net</i></b>	
PL	<b><i>dna.pruem.pl.eu-admin.net</i></b>	
	<b><i>fp.pruem.pl.eu-admin.net</i></b>	
PT	<b><i>dna.pruem.pt.eu-admin.net</i></b>	.....
	<b><i>fp.pruem.pt.eu-admin.net</i></b>	.....
RO	<b><i>dna.pruem.ro.eu-admin.net</i></b>	
	<b><i>fp.pruem.ro.eu-admin.net</i></b>	
SI	<b><i>dna.pruem.si.eu-admin.net</i></b>	.....
	<b><i>fp.pruem.si.eu-admin.net</i></b>	.....
SK	<b><i>dna.pruem.sk.eu-admin.net</i></b>	
	<b><i>fp.pruem.sk.eu-admin.net</i></b>	
FI	<b><i>dna.pruem.fi.eu-admin.net</i></b>	<i>[To be inserted]</i>
	<b><i>fp.pruem.fi.eu-admin.net</i></b>	
SE	<b><i>dna.pruem.se.eu-admin.net</i></b>	
	<b><i>fp.pruem.se.eu-admin.net</i></b>	

---

**Status:** This is the original version (as it was originally adopted).

---

UK	<b><i>dna.pruem.uk</i></b> .eu-admin.net	
	<b><i>fp.pruem.uk</i></b> .eu-admin.net	