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

ANNEX

CHAPTER 1: Exchange of DNA-Data

1. DNA related forensic issues, matching rules and algorithms

1.1. Properties of DNA-profiles

The DNA profile may contain 24 pairs of numbers representing the alleles of 24 loci which are also used in the DNA-procedures of Interpol. The names of these loci are shown in the following table:

VWA	TH01	D21S11	FGA	D8S1179	D3S1358	D18S51	Amelogenin
TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539	D2S1338	D19S433
Penta D	Penta E	FES	F13A1	F13B	SE33	CD4	GABA

The seven grey loci in the top row are both the present European Standard Set (ESS) and the Interpol Standard Set of Loci (ISSOL).

Inclusion Rules:

The DNA-profiles made available by the Member States for searching and comparison as well as the DNA-profiles sent out for searching and comparison must contain at least six full designated[1] loci and may contain additional loci or blanks depending on their availability. The reference DNA profiles must contain at least six of the seven ESS of loci. In order to raise the accuracy of matches, all available alleles shall be stored in the indexed DNA profile database and be used for searching and comparison. Each Member State should implement as soon as practically possible any new ESS of loci adopted by the EU.

Mixed profiles are not allowed, so that the allele values of each locus will consist of only two numbers, which may be the same in the case of homozygosity at a given locus.

Wild-cards and Micro-variants are to be dealt with using the following rules:

— Any non-numerical value except amelogenin contained in the profile (e.g. ‘o’, ‘f’, ‘r’, ‘na’, ‘nr’ or ‘un’) has to be automatically converted for the export to a wild card (*) and searched against all,

— Numerical values ‘0’, ‘1’ or ‘99’ contained in the profile have to be automatically converted for the export to a wild card (*) and searched against all,

— If three alleles are provided for one locus the first allele will be accepted and the remaining two alleles have to be automatically converted for the export to a wild card (*) and searched against all,

— When wild card values are provided for allele 1 or 2 then both permutations of the numerical value given for the locus will be searched (e.g. 12, * could match against 12,14 or 9,12),

— Pentanucleotide (Penta D, Penta E and CD4) micro-variants will be matched according to the following:

x.1 = x, x.1, x.2
x.2 = x.1, x.2, x.3
x.3 = x.2, x.3, x.4
x.4 = x.3, x.4, x + 1,

— Tetranucleotide (the rest of the loci are tetranucleotides) micro-variants will be matched according to the following:

x.1 = x, x.1, x.2
x.2 = x.1, x.2, x.3
x.3 = x.2, x.3, x + 1.

1.2. Matching rules

The comparison of two DNA-profiles will be performed on the basis of the loci for which a pair of allele values is available in both DNA-profiles. At least six full designated loci (exclusive of amelogenin) must match between both DNA-profiles before a hit response is provided.

A full match (Quality 1) is defined as a match, when all allele values of the compared loci commonly contained in the requesting and requested DNA-profiles are the same. A near match is defined as a match, when the value of only one of all the compared alleles is different in the two DNA profiles (Quality 2, 3 and 4). A near match is only accepted if there are at least six full designated matched loci in the two compared DNA profiles.

The reason for a near match may be:

— a human typing error at the point of entry of one of the DNA-profiles in the search request or the DNA-database,
— an allele-determination or allele-calling error during the generation procedure of the DNA-profile.

1.3. Reporting rules

Both full matches, near matches and ‘no hits’ will be reported.

The matching report will be sent to the requesting national contact point and will also be made available to the requested national contact point (to enable it to estimate the nature and number of possible follow-up requests for further available personal data and other information associated with the DNA-profile corresponding to the hit in accordance with Articles 5 and 10 of Decision 2008/615/JHA).

2. Member State code number table

In accordance with Decision 2008/615/JHA, ISO 3166-1 alpha-2 code are used for setting up the domain names and other configuration parameters required in the Prüm DNA data exchange applications over a closed network.

ISO 3166-1 alpha-2 codes are the following two-letter Member State codes.

Member State names	**Code**	**Member State names**	**Code**
Belgium	BE	Luxembourg	LU
Bulgaria	BG	Hungary	HU
Czech Republic	CZ	Malta	MT
Denmark	DK	Netherlands	NL
Germany	DE	Austria	AT
Estonia	EE	Poland	PL
Greece	EL	Portugal	PT

Spain	ES	Romania	RO
France	FR	Slovakia	SK
Ireland	IE	Slovenia	SI
Italy	IT	Finland	FI
Cyprus	CY	Sweden	SE
Latvia	LV	United Kingdom	UK
Lithuania	LT		

3. Functional analysis

3.1. Availability of the system

Requests pursuant to Article 3 of Decision 2008/615/JHA should reach the targeted database in the chronological order that each request was sent, responses should be dispatched to reach the requesting Member State within 15 minutes of the arrival of requests.

3.2. Second step

When a Member State receives a report of match, its national contact point is responsible for comparing the values of the profile submitted as a question and the values of the profile(s) received as an answer to validate and check the evidential value of the profile. National contact points can contact each other directly for validation purposes.

Legal assistance procedures start after validation of an existing match between two profiles, on the basis of a ‘full match’ or a ‘near match’ obtained during the automated consultation phase.

4. DNA interface control document

4.1. Introduction

4.1.1. *Objectives*

This Chapter defines the requirements for the exchange of DNA profile information between the DNA database systems of all Member States. The header fields are defined specifically for the Prüm DNA exchange, the data part is based on the DNA profile data part in the XML schema defined for the Interpol DNA exchange gateway.

Data are exchanged by SMTP (Simple Mail Transfer Protocol) and other state-of-the-art technologies, using a central relay mail server provided by the network provider. The XML file is transported as mail body.

4.1.2. *Scope*

This ICD defines the content of the message (mail) only. All network-specific and mail-specific topics are defined uniformly in order to allow a common technical base for the DNA data exchange.

This includes:

— the format of the subject field in the message to enable/allow for an automated processing of the messages,

— whether content encryption is necessary and if yes which methods should be chosen,

— the maximum length of messages.

4.1.3. *XML structure and principles*

The XML message is structured into;

— header part, which contains information about the transmission, and

— data part, which contains profile specific information, as well as the profile itself.

The same XML schema shall be used for request and response.

For the purpose of complete checks of unidentified DNA profiles (Article 4 of Decision 2008/615/JHA) it shall be possible to send a batch of profiles in one message. A maximum number of profiles within one message must be defined. The number is depending from the maximum allowed mail size and shall be defined after selection of the mail server.

XML example:

<?version="1.0" standalone="yes"?>

<PRUEMDNAx xmlns:msxsl="urn:schemas-microsoft-com:xslt"

xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<header>

(…)

</header>

<datas>

(…)

</datas>

[<datas> datas structure repeated, if multiple profiles sent by (….) a single SMTP message, only allowed for Article 4 cases

</datas>]

</PRUEMDNA>

4.2. XML structure definition

The following definitions are for documentation purposes and better readability, the real binding information is provided by an XML schema file (PRUEM DNA.xsd).

4.2.1. *Schema PRUEMDNAx*

It contains the following fields:

Fields	**Type**	**Description**
header	PRUEM_header	Occurs: 1
datas	PRUEM_datas	Occurs: 1 … 500

4.2.2. *Content of header structure*

4.2.2.1. PRUEM header

This is a structure describing the XML file header. It contains the following fields:

Fields	Type	Description
direction	PRUEM_header_dir	Direction of message flow
ref	String	Reference of the XML file
generator	String	Generator of XML file
schema_version	String	Version number of schema to use
requesting	PRUEM_header_info	Requesting Member State info
requested	PRUEM_header_info	Requested Member State info

4.2.2.2. PRUEM_header dir

Type of data contained in message, value can be:

Value	Description
R	Request
A	Answer

4.2.2.3. PRUEM header info

Structure to describe Member State as well as message date/time. It contains the following fields:

Fields	Type	Description
source_isocode	String	ISO 3166-2 code of the requesting Member State
destination_isocode	String	ISO 3166-2 code of the requested Member State
request_id	String	unique Identifier for a request
date	Date	Date of creation of message
time	Time	Time of creation of message

4.2.3. *Content of PRUEM Profile data*

4.2.3.1. PRUEM_datas

This is a structure describing the XML profile data part. It contains the following fields:

Fields	Type	Description
reqtype	PRUEM request type	Type of request (Article 3 or 4)
date	Date	Date profile stored

type	PRUEM_datas_type	Type of profile
result	PRUEM_datas_result	Result of request
agency	String	Name of corresponding unit responsible for the profile
profile_ident	String	Unique Member State profile ID
message	String	Error Message, if result = E
profile	IPSG_DNA_profile	If direction = A (Answer) AND result ≠ H (Hit) empty
match_id	String	In case of a HIT PROFILE_ID of the requesting profile
quality	PRUEM_hitquality_type	Quality of Hit
hitcount	Integer	Count of matched Alleles
rescount	Integer	Count of matched profiles. If direction = R (Request), then empty. If quality!=0 (the original requested profile), then empty.

4.2.3.2. PRUEM_request_type

Type of data contained in message, value can be:

Value	Description
3	Requests pursuant to Article 3 of Decision 2008/615/JHA
4	Requests pursuant to Article 4 of Decision 2008/615/JHA

4.2.3.3. PRUEM_hitquality_type

Value	Description
0	Referring original requesting profile: Case ‘No Hit’: original requesting profile sent back only; Case ‘Hit’: original requesting profile and matched profiles sent back.
1	Equal in all available alleles without wildcards
2	Equal in all available alleles with wildcards
3	Hit with Deviation (Microvariant)

4	Hit with mismatch

4.2.3.4. PRUEM_data_type

Type of data contained in message, value can be:

Value	Description
P	Person profile
S	Stain

4.2.3.5. PRUEM_data_result

Type of data contained in message, value can be:

Value	Description
U	Undefined, If direction = R (request)
H	Hit
N	No Hit
E	Error

4.2.3.6. IPSG_DNA_profile

Structure describing a DNA profile. It contains the following fields:

Fields	Type	Description
ess_issol	IPSG_DNA_ISSOL	Group of loci corresponding to the ISSOL (standard group of Loci of Interpol)
additional_loci	IPSG_DNA_additional_loci	Other loci
marker	String	Method used to generate of DNA
profile_id	String	Unique identifier for DNA profile

4.2.3.7. IPSG_DNA_ISSOL

Structure containing the loci of ISSOL (Standard Group of Interpol loci). It contains the following fields:

Fields	Type	Description
vwa	IPSG_DNA_locus	Locus vwa
th01	IPSG_DNA_locus	Locus th01
d21s11	IPSG_DNA_locus	Locus d21s11

fga	IPSG_DNA_locus	Locus fga
d8s1179	IPSG_DNA_locus	Locus d8s1179
d3s1358	IPSG_DNA_locus	Locus d3s1358
d18s51	IPSG_DNA_locus	Locus d18s51
amelogenin	IPSG_DNA_locus	Locus amelogin

4.2.3.8. IPSG_DNA_additional_loci

Structure containing the other loci. It contains the following fields:

Fields	**Type**	**Description**
tpox	IPSG_DNA_locus	Locus tpox
csf1po	IPSG_DNA_locus	Locus csf1po
d13s317	IPSG_DNA_locus	Locus d13s317
d7s820	IPSG_DNA_locus	Locus d7s820
d5s818	IPSG_DNA_locus	Locus d5s818
d16s539	IPSG_DNA_locus	Locus d16s539
d2s1338	IPSG_DNA_locus	Locus d2s1338
d19s433	IPSG_DNA_locus	Locus d19s433
penta_d	IPSG_DNA_locus	Locus penta_d
penta_e	IPSG_DNA_locus	Locus penta_e
fes	IPSG_DNA_locus	Locus fes
f13a1	IPSG_DNA_locus	Locus f13a1
f13b	IPSG_DNA_locus	Locus f13b
se33	IPSG_DNA_locus	Locus se33
cd4	IPSG_DNA_locus	Locus cd4
gaba	IPSG_DNA_locus	Locus gaba

4.2.3.9. IPSG_DNA_locus

Structure describing a locus. It contains the following fields:

Fields	**Type**	**Description**
low_allele	String	Lowest value of an allele
high_allele	String	Highest value of an allele

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

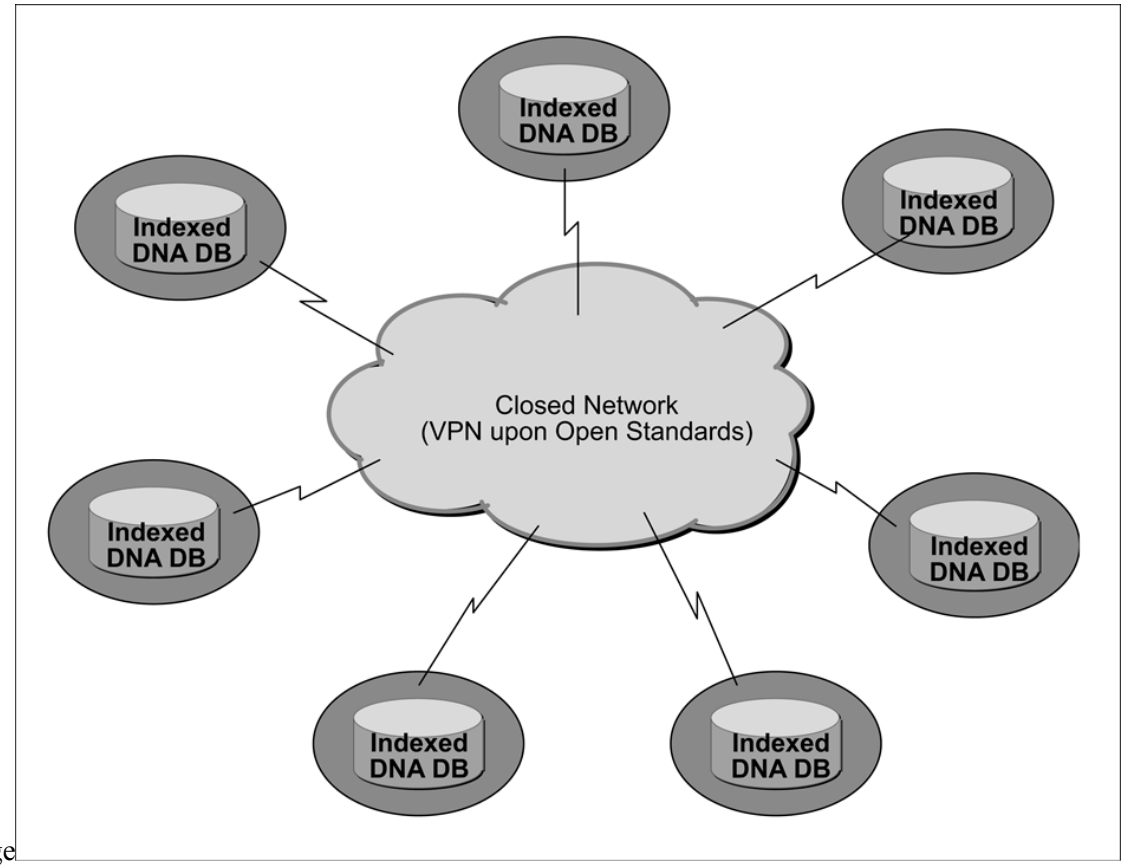
2. setting up a secure local link from the site where the DNA database is located and managed by the competent national agency to the existing national TESTA access point.

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.

Figure 1: Topology of DNA Data 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

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).

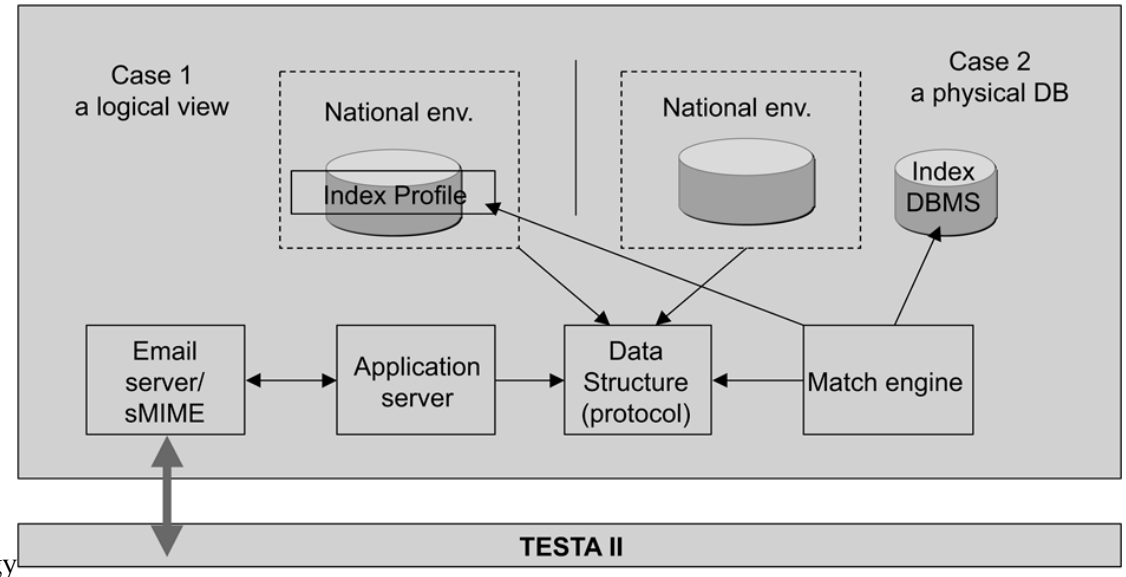
The four main components: E-mail server/s/MIME, Application Server, Data Structure Area for fetching/feeding data and registering incoming/outgoing messages, and Match Engine implement the whole application logic in a product-independent way.

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,

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 Topology



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*

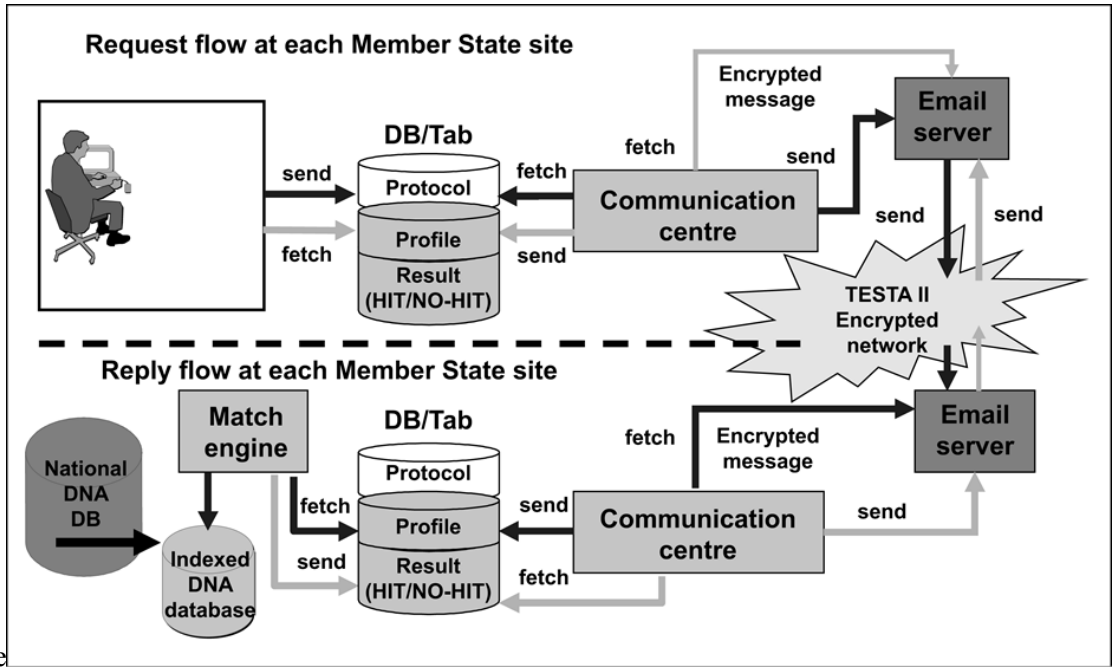
Open DataBase Connectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has, however, certain drawbacks. Administering a large number of client machines can involve a diversity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

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



5.7. Communication Environment

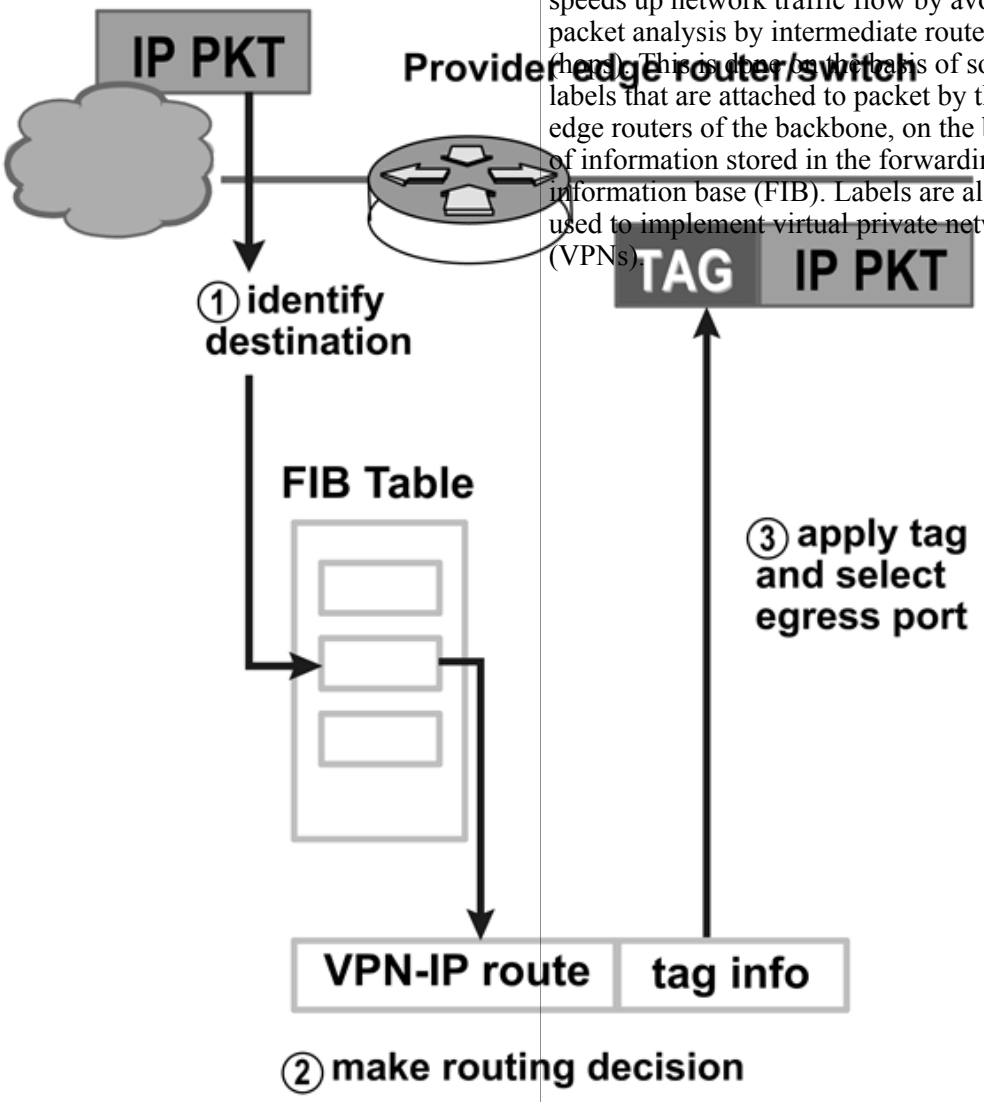
5.7.1. *Common Communication Network: TESTA and its follow-up infrastructure*

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 is an IETF standard technology that speeds up network traffic flow by avoiding packet analysis by intermediate routers (hops). This is done on the basis of so-called labels that are attached to packet by the edge routers of the backbone, on the basis of information stored in the forwarding information base (FIB). Labels are also used to implement virtual private networks (VPNs).

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

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

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:

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

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

UK	***dna*.pruem.uk**.eu-admin.net	
	***fp*.pruem.uk**.eu-admin.net	

(**1**) ‘Full designated’ means the handling of rare allelle values is included.