COUNCIL OF THE EUROPEAN UNION

Brussels, 4 February 2008

5660/08

CRIMORG 18
ENFOPOL 21

NOTE

From :	Presidency
To :	delegations
Subject :	Draft Council Decision on the implementation of Decision 2008/…/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime: Annex - Proposal for redrafting

1. In November 2007, the Council agreed on a general approach concerning the main part of the above-mentioned draft Council Decision. Subsequently, a Friends of the Presidency group was convened to discuss the Annex to this draft Decision.

2. The Friends of the Presidency group met on 30 November 2007, 8 January 2008 and 1 February 2008 and discussed the Annex in detail, also based on comments sent in by delegations in writing. The result of these discussions is set out hereunder.

3. Minor drafting amendments have been made in **Chapter 1** to clarify and/or correct a number of issues. The UK delegation has a reservation on this chapter pending further discussions between experts on specific points (parts 1.1, 1.2, 3.1, 4.1.1, 4.2.3.3, 4.2.3.7, 4.2.3.8, 4.2.3.9, 5.4, 5.5 and 5.6).

4. Among the outstanding points raised by the UK delegation, the main issue concerns the kind and number of loci necessary to do a comparison according to the Prüm Decision. It is evident that the accuracy of matches is enhanced by using a higher number of loci and comparisons should therefore be based on as many loci as possible. At the same time, it should be avoided that some older databases are excluded from comparisons by defining the comparison rules at too high a level.

   The aim is to ensure that the comparison is made on the basis of the highest number of loci that is technically possible between the concerned databases but to allow for a lower set of criteria where this is necessary to make comparisons with some older databases.

5. Delegations are invited to examine the drafting proposals that are set out in parts 1.1, 1.2 and 3.1 of Chapter 1, as well as in the footnotes to these paragraphs. The UK is invited to lift its reservation on this chapter.

6. In reaction to comments of delegations and/or to clarify some drafting, minor amendments and clarifications have been made in **Chapters 2 and 3**, which have been agreed upon subject to a UK scrutiny reservation.

7. The UK delegation is invited to lift its reservation on these chapters.

8. **Chapter 4** has been redrafted so that, while maintaining the original evaluation mechanism (questionnaire, pilot run and evaluation visit), the whole process is less bureaucratic and resource-intensive. Also, the part on expert meetings has been moved to a separate paragraph to allow these meetings to deal with other subjects relating to the implementation of the Prüm Decision than the evaluations. Notably the model for statistics will be defined by these experts. This chapter has been agreed.

9. In several instances, reference is made to "the relevant Council Working Group". It is not necessary nor useful to define in this Annex which Working Group is concerned. This is a matter to be decided upon at a later stage.

10. Subject to a solution for the issue set out in point 4 of this cover note and the lifting of the different reservations, the Article 36 Committee is invited to confirm the agreement on the Annex as set out below.

ANNEX

TABLE OF CONTENTS

10. Appendices to Chapter 2
    - 10.1 ASCII Separator Codes
    - 10.2 Calculation of Alpha-numeric check character
    - 10.3 Character codes
    - 10.4 Transaction summary
    - 10.5 Type-1 record definitions
    - 10.6 Type-2 record definitions
    - 10.7 Grayscale compression codes
    - 10.8 Mailspecification

Chapter 3: Exchange of vehicle registration data

1. Common data-set for automated search of vehicle registration data
    - 1.1 Definitions
    - 1.2 Vehicle/owner/holder search
2. Data Security
    - 2.1 Overview
    - 2.2 Security features related to message exchange
    - 2.3 Security features not related to message exchange
    - 2.4 Hardware security module
3. Technical conditions of the data exchange
    - 3.1 General description of the EUCARIS application
    - 3.2 Functional and Non Functional Requirements

Chapter 4: Evaluation

1. Evaluation procedure according to Article 18 b of the Implementing Decision (Preparation of Decisions according to Article 25 (2) of Council Decision 2008/…/JHA)
    - 1.1 Procedure
    - 1.2 Pilot run
    - 1.3 Evaluation visit
    - 1.4 Report to the Council
2. Evaluation procedure according to Article 19 of the Implementing Decision
    - 2.1 Statistics and Report
    - 2.2 Expert Meetings
    - 2.3 Revision
    - 2.4 Model for Statistics

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 7 grey loci in the top row are the present European Standard Set of Loci (ESSOL).[1]

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 6 loci and may contain other loci or blanks depending on their availability. The reference DNA profiles must contain at least 6 of the 7 ESS of loci. In order to raise the accuracy of matches, it is recommended that all available alleles be stored in the indexed DNA profile database. [2]

Mixed profiles are not allowed, so that the allele values of each locus will consist of only 2 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.

---

1 UK suggests to add the following sentence: "The Interpol Standard Set of Loci (ISSOL) contains the ESSOL and amelogenin."

2 UK suggest the following drafting: "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 6 **full designated** loci and may contain **additional** loci or blanks depending on their availability. The reference DNA profiles must contain at least 6 of the 7 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**.

- If 3 alleles are provided for one locus the first allele will be accepted and the remaining 2 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 & 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 Interpol database 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 2 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 6 loci (exclusive of amelogenin) must match between both DNA-profiles.[3]

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 2 DNA profiles (Quality 2, 3 and 4). A near match is only accepted if there are at least 6 fully matched loci in the 2 compared DNA profiles.[4]

---

[3] UK suggests the following drafting: "The comparison of 2 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 6 **full designated** loci (exclusive of amelogenin) must match between both DNA-profiles **before a hit responses is provided**.

[4] UK suggests the following drafting: "A near match is only accepted if there are at least 6 **full designated** matched loci in the 2 compared DNA profiles. **Any new matching rules adopted by ENFSI or EU should be implemented by each Member State in a coordinated manner.**

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 and near matches 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 Council Decision 2007…/JHA).

2. Member State code number table

In accordance with Decision 2008/.../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/…/JHA should reach the targeted database in the chronological order of arrival while answers should reach the requesting Member State within 15 minutes of the arrival of requests.[5]

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.

[5] UK suggests the following drafting: "Requests pursuant to Article 3 of Decision 2008/…/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 **from receipt** of **the** request, **subject to network performance**." SE supports.

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/.../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 Art. 4 cases
</datas>  ]
</PRUEMDNAx
```

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 datas

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/.../JHA
4	Requests pursuant to Article 4 of Decision 2008/.../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

4.2.2.5 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/.../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 fulfillment of security concerns, the mechanism sMIME as extension to the SMTP functionality will be used to establish a true end-to-end secure tunnel over the network.

The operational TESTA (**T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations) 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:

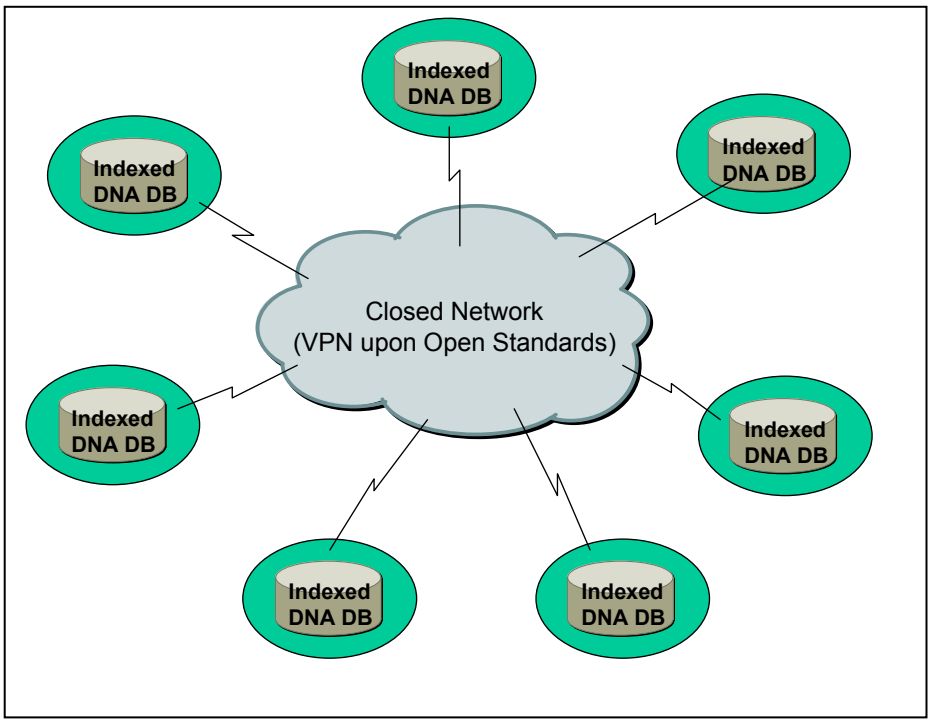
1) using the existing national access point or establishing a new national TESTA access point, or by
2) setting up a secure local link from the site where the DNA database is located and managed by the competent national agency to the existing national TESTA access point.

The protocols and standards deployed in the implementation of Decision 2008/.../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/.../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 standardized common data format. The architecture is based upon an any-to-any communication model. There exists neither a central computer server nor a centralized database to hold DNA profiles.

Fig. 1: Topology of DNA Data Exchange



In addition to the fulfillment 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/.../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 organizational 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 sMIME, 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 tunneling system administered by a trusted network provider at the international level and the secure links to this tunneling system under the national responsibility. This virtual private tunneling system does not have a connection point with the open Internet.

5.4. Protocols and Standards to be used for encryption mechanism: sMIME and related packages

The open standard sMIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The protocol sMIME (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 sMIME 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 sMIME 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 1024 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 sMIME'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/.../JHA, such as the product of Bouncy Castle JCE (**J**ava **C**ryptographic **E**xtension), which will be used to implement sMIME for prototyping DNA data exchange among all Member States.

5.5 Application Architecture

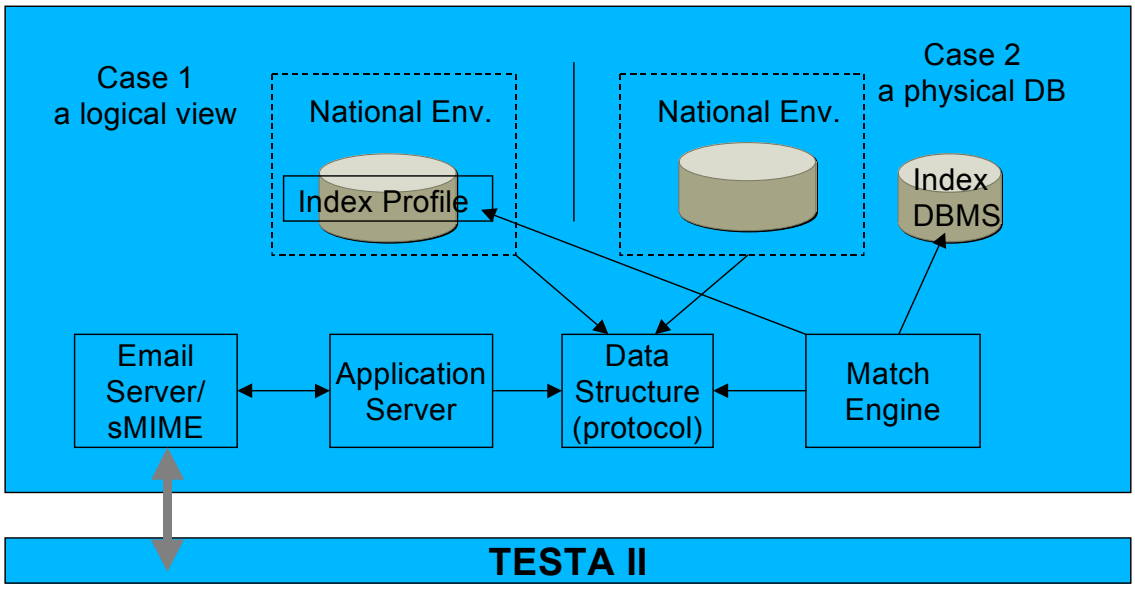
Each Member State will provide the other Member States with a set of standardized DNA profile data which are in conformity with the current common ICD. This can be done either by providing a logical view over individual national database or by establishing a physical exported database.

The four main components: E-mail server/sMIME, 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/.../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.

Fig. 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 e**X**tensible **M**arkup **L**anguage (**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

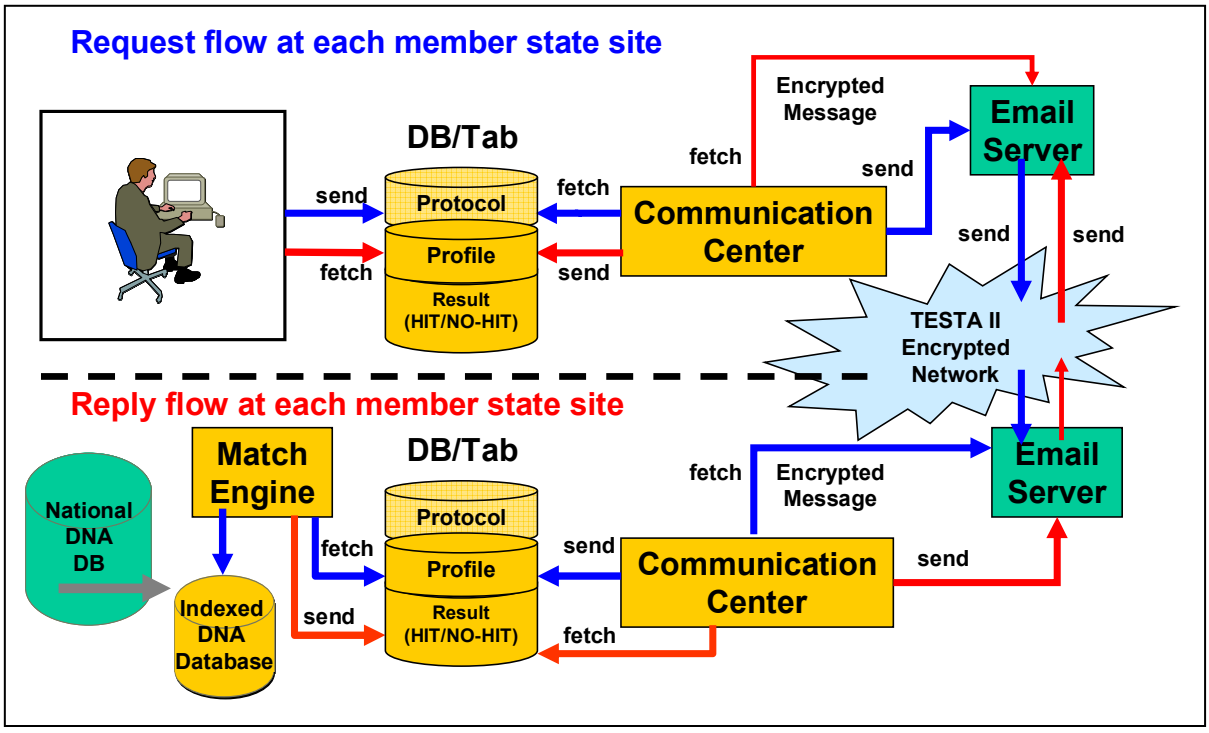
Open **D**ata**B**ase **C**onnectivity provides a standard software API method for accessing database management systems and making it independent of programming languages, database and operating systems. ODBC has, however, certain drawbacks. Administering a large number of client machines can involve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

5.6.3 JDBC

Java **D**ata**B**ase **C**onnectivity (**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.

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



5.7. Communication Environment

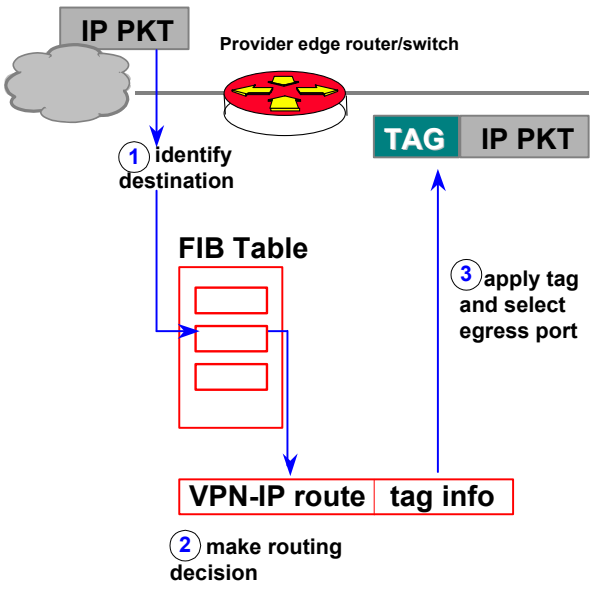
5.7.1 Common Communication Network: TESTA and its follow-up infrastructure

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 **D**omain **N**ame **S**ervices (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 sMIME 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 **M**ail **T**ransfer **P**rotocol 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 sMIME extension, permitting binary files to be transmitted almost as easily as plain text. The processing rules for sMIME operations are described in the section sMIME (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 **P**ost **O**ffice **P**rotocol 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/.../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/…/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, email 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	

Chapter 2: Exchange of dactyloscopic data (interface control document)

The purpose of the following document interface Control Document is to define the requirements for the exchange of dactyloscopic information between the Automated Fingerprint Identification Systems (AFIS) of the Member States. It is based on the Interpol-Implementation of ANSI/NIST-ITL 1-2000 (INT-I, Version 4.22b).

This version shall cover all basic definitions for Logical Records Type-1, Type-2, Type-4, Type-9, Type-13 and Type-15 required for image and minutiæ based dactyloscopic processing.

1. File Content Overview

A dactyloscopic file consists of several logical records. There are sixteen types of record specified in the original ANSI/NIST-ITL 1-2000 standard. Appropriate ASCII separation characters are used between each record and the fields and subfields within the records.

Only 6 record types are used to exchange information between the originating and the destination agency:

Type-1 -> Transaction information

Type-2 -> Alphanumeric persons/case data

Type-4 -> High resolution grayscale dactyloscopic images

Type-9 -> Minutiæ Record

Type-13 -> Variable resolution latent image record

Type-15 -> Variable resolution palmprint image record

1.1 Type-1 - File header

This record contains routing information and information describing the structure of the rest of the file. This record type also defines the types of transaction which fall under the following broad categories:

1.2 Type-2 - Descriptive text

This record contains textual information of interest to the sending and receiving agencies.

1.3 Type-4 - High resolution gray-scale image

This record is used to exchange high resolution gray-scale (eight bit) dactyloscopic images sampled at 500 pixels/inch. The dactyloscopic images shall be compressed using the WSQ algorithm with a ratio of not more than 15:1. Other compression algorithms or uncompressed images must not be used.

1.4 Type-9 - Minutiæ record

Type-9 records are used to exchange ridge characteristics or minutiæ data. Their purpose is partly to avoid unnecessary duplication of AFIS encoding processes and partly to allow the transmission of AFIS codes which contain less data than the corresponding images.

1.5 Type-13 - Variable-Resolution Latent Image Record

This record shall be used to exchange variable-resolution latent fingerprint and latent palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 gray-levels. If the quality of the latent image is sufficient it shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 gray-levels on bilateral agreement. In this case, it is strongly recommended to use JPEG 2000 (see Appendix 7).

1.6 Variable-Resolution Palmprint Image Record

Type-15 tagged field image records shall be used to exchange variable-resolution palmprint images together with textural alphanumerical information. The scanning resolution of the images shall be 500 pixels/inch with 256 gray-levels. To minimize the amount of data all palmprint images shall be compressed using WSQ-algorithm. If necessary the resolution of the images may be expanded to more than 500 pixels/inch and more than 256 gray-levels on bilateral agreement. In this case, it is strongly recommended to use JPEG 2000 (see Appendix 7).

2. Record format

A transaction file shall consist of one or more logical records. For each logical record contained in the file, several information fields appropriate to that record type shall be present. Each information field may contain one or more basic single-valued information items. Taken together these items are used to convey different aspects of the data contained in that field. An information field may also consist of one or more information items grouped together and repeated multiple times within a field. Such a group of information items is known as a subfield. An information field may therefore consist of one or more subfields of information items.

2.1 Information separators

In the tagged-field logical records, mechanisms for delimiting information are implemented by use of four ASCII information separators. The delimited information may be items within a field or subfield, fields within a logical record, or multiple occurrences of subfields. These information separators are defined in the standard ANSI X3.4. These characters are used to separate and qualify information in a logical sense. Viewed in a hierarchical relationship, the File Separator "FS" character is the most inclusive followed by the Group Separator "GS", the Record Separator "RS", and finally the Unit Separator "US" characters. Table 1 lists these ASCII separators and a description of their use within this standard.

Information separators should be functionally viewed as an indication of the type data that follows. The "US" character shall separate individual information items within a field or subfield. This is a signal that the next information item is a piece of data for that field or subfield. Multiple subfields within a field separated by the "RS" character signals the start of the next group of repeated information item(s). The "GS" separator character used between information fields signals the beginning of a new field preceding the field identifying number that shall appear. Similarly, the beginning of a new logical record shall be signalled by the appearance of the "FS" character.

The four characters are only meaningful when used as separators of data items in the fields of the ASCII text records. There is no specific meaning attached to these characters occurring in binary image records and binary fields – they are just part of the exchanged data.

Normally, there should be no empty fields or information items and therefore only one separator character should appear between any two data items. The exception to this rule occurs for those instances where the data in fields or information items in a transaction are unavailable, missing, or optional, and the processing of the transaction is not dependent upon the presence of that particular data. In those instances, multiple and adjacent separator characters shall appear together rather than requiring the insertion of dummy data between separator characters.

For the definition of a field that consists of three information items, the following applies. If the information for the second information item is missing, then two adjacent "US" information separator characters would occur between the first and third information items. If the second and third information items were both missing, then three separator characters should be used – two "US" characters in addition to the terminating field or subfield separator character. In general, if one or more mandatory or optional information items are unavailable for a field or subfield, then the appropriate number of separator character should be inserted.

It is possible to have side-by-side combinations of two or more of the four available separator characters. When data are missing or unavailable for information items, subfields, or fields, there must be one separator character less than the number of data items, subfields, or fields required.

Table 1: Separators Used

Code	Type	Description	Hexadecimal Value	Decimal Value
US	Unit Separator	Separates information items	1F	31
RS	Record Separator	Separates subfields	1E	30
GS	Group Separator	Separates fields	1D	29
FS	File Separator	Separates logical records	1C	28

2.2 Record layout

For tagged-field logical records, each information field that is used shall be numbered in accordance with this standard. The format for each field shall consist of the logical record type number followed by a period ".", a field number followed by a colon ":", followed by the information appropriate to that field. The tagged-field number can be any one-to-nine digit number occurring between the period "." and the colon ":". It shall be interpreted as an unsigned integer field number. This implies that a field number of "2.123:" is equivalent to and shall be interpreted in the same manner as a field number of "2.000000123:".

For purposes of illustration throughout this document, a three-digit number shall be used for enumerating the fields contained in each of the tagged-field logical records described herein. Field numbers will have the form of "TT.xxx:" where the "TT" represents the one- or two-character record type followed by a period. The next three characters comprise the appropriate field number followed by a colon. Descriptive ASCII information or the image data follows the colon.

Logical Type-1 and Type-2 records contain only ASCII textual data fields. The entire length of the record (including field numbers, colons, and separator characters) shall be recorded as the first ASCII field within each of these record types. The ASCII File Separator “FS” control character (signifying the end of the logical record or transaction) shall follow the last byte of ASCII information and shall be included in the length of the record.

In contrast to the tagged-field concept, the Type-4 record contains only binary data recorded as ordered fixed-length binary fields. The entire length of the record shall be recorded in the first four-byte binary field of each record. For this binary record, neither the record number with its period, nor the field identifier number and its following colon, shall be recorded. Furthermore, as all the field lengths of this record is either fixed or specified, none of the four separator characters (“US”, “RS”, ”GS”, or “FS”) shall be interpreted as anything other than binary data. For the binary record, the “FS” character shall not be used as a record separator or transaction terminating character.

3. Type-1 Logical Record: the File Header

This record describes the structure of the file, the type of the file, and other important information. The character set used for Type-1 fields shall contain only the 7-bit ANSI code for information interchange.

3.1 Fields for Type-1 Logical Record

3.1.1 Field 1.001: Logical Record Length (LEN)

This field contains the total count of the number of bytes in the whole Type-1 logical record. The field begins with “1.001:”, followed by the total length of the record including every character of every field and the information separators.

3.1.2 Field 1.002: Version Number (VER)

To ensure that users know which version of the ANSI/NIST standard is being used, this four byte field specifies the version number of the standard being implemented by the software or system creating the file. The first two bytes specify the major version reference number, the second two the minor revision number. For example, the original 1986 Standard would be considered the first version and designated “0100” while the present ANSI/NIST-ITL 1-2000 standard is “0300”.

3.1.3 Field 1.003: File Content (CNT)

This field lists each of the records in the file by record type and the order in which the records appear in the logical file. It consists of one or more subfields, each of which in turn contains two information items describing a single logical record found in the current file. The subfields are entered in the same order in which the records are recorded and transmitted.

The first information item in the first subfield is "1", to refer to this Type-1 record. It is followed by a second information item which contains the number of other records contained in the file. This number is also equal to the count of the remaining subfields of field 1.003.

Each of the remaining subfields is associated with one record within the file, and the sequence of subfields corresponds to the sequence of records. Each subfield contains two items of information. The first is to identify the Type of the record. The second is the record's IDC. The "*US*" character shall be used to separate the two information items.

3.1.4 Field 1.004: Type of Transaction (TOT)

This field contains a three letter mnemonic designating the type of the transaction. These codes may be different from those used by other implementations of the ANSI/NIST standard.

CPS: Criminal Print-to-Print Search. This transaction is a request for a search of a record relating to a criminal offence against a prints database. The person’s prints must be included as WSQ-compressed images in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

⇒ 1-14 Type-4 Record

The CPS TOT is summarized in **Table A.6.1** (Appendix 6).

PMS: Print-to-Latent Search. This transaction is used when a set of prints shall to be searched against an Unidentified Latent database. The response will contain the **Hit/No-Hit** decision of the destination AFIS search. If multiple unidentified latents exist, multiple SRE transactions will be returned, with one latent per transaction. The person's prints must be included as WSQ-compressed images in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

⇒ 1 Type-13 Record

The PMS TOT is summarized in **Table A.6.1 (**Appendix 6**).**

MPS: Latent-to-Print Search. This transaction is used when a latent is to be searched against a Prints database. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

⇒ 1 Type-4 or Type-15 Record

The MPS TOT is summarized in **Table A.6.4 (**Appendix 6**)**.

MMS: Latent-to-Latent Search. In this transaction the file contains a latent which is to be searched against an Unidentified Latent database in order to establish links between various scenes of crime. The latent minutiæ information and the image (WSQ-compressed) must be included in the file.

In case of a **No-HIT**, the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

In case of a **HIT,** the following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

⇒ 1 Type-13 Record

The MMS TOT is summarized in **Table A.6.4 (**Appendix 6**)**.

SRE: This transaction is returned by the destination agency in response to dactyloscopic submissions. The response will contain the **Hit/No-Hit** decision of the destination AFIS search. If multiple candidates exist, multiple SRE transactions will be returned, with one candidate per transaction.

The SRE TOT is summarized in **Table A.6.2 (**Appendix 6**)**.

ERR: This transaction is returned by the destination AFIS to indicate a transaction error. It includes a message field (**ERM**) indicating the error detected. The following logical records will be returned:

⇒ 1 Type-1 Record

⇒ 1 Type-2 Record

The ERR TOT is summarized in **Table A.6.3** (Appendix 6).

Table 2: Permissible Codes in Transactions

Transaction Type	Logical Record Type					
	1	2	4	9	13	15
CPS	M	M	M	-	-	-
SRE	M	M	C	- (C in case of latent hits)	C	C
MPS	M	M	-	M (1*)	M	-
MMS	M	M	-	M (1*)	M	-
PMS	M	M	M*	-	-	M*
ERR	M	M	-	-	-	-

Key:

M = Mandatory

M* = Only one of both record-types may be included

O = Optional

C = Conditional on whether data is available

- = Not allowed

1* = Conditional depending on legacy systems

3.1.5 Field 1.005: Date of Transaction (DAT)

This field indicates the date on which the transaction was initiated and must conform to the ISO standard notation of: YYYYMMDD

where YYYY is the year, MM is the month and DD is the day of the month. Leading zeros are used for single figure numbers. For example, "19931004" represents 4 October 1993.

3.1.6 Field 1.006: Priority (PRY)

This optional field defines the priority, on a level of 1 to 9, of the request. "1" is the highest priority and "9" the lowest. Priority "1" transactions shall be processed immediately.

3.1.7 Field 1.007: Destination Agency Identifier (DAI)

This field specifies the destination agency for the transaction.

It consists of two information items in the following format: CC/*agency*.

The first information item contains the Country Code, defined in ISO 3166, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

3.1.8 Field 1.008: Originating Agency Identifier (ORI)

This field specifies the file originator and has the same format as the DAI (Field 1.007).

3.1.9 Field 1.009: Transaction Control Number (TCN)

This is a control number for reference purposes. It should be generated by the computer and have the following format: YYSSSSSSSSA

where YY is the year of the transaction, SSSSSSSS is an eight-digit serial number, and A is a check character generated by following the procedure given in Appendix 2.

Where a TCN is not available, the field, YYSSSSSSSS, is filled with zeros and the check character generated as above.

3.1.10 Field 1.010: Transaction Control Response (TCR)

Where a request was sent out, to which this is the response, this optional field will contain the transaction control number of the request message. It therefore has the same format as TCN (Field 1.009).

3.1.11 Field 1.011: Native Scanning Resolution (NSR)

This field specifies the normal scanning resolution of the system supported by the originator of the transaction. The resolution is specified as two numeric digits followed by the decimal point and then two more digits.

For all transactions pursuant to Decision 2008/.../JHA the sampling rate shall be 500 pixels/inch or 19.68 pixels/mm.

3.1.12 Field 1.012: Nominal Transmitting Resolution (NTR)

This five-byte field specifies the nominal transmitting resolution for the images being transmitted. The resolution is expressed in pixels/mm in the same format as NSR (Field 1.011).

3.1.13 Field 1.013: Domain name (DOM)

This mandatory field identifies the domain name for the user-defined Type-2 logical record implementation. It consists of two information items and shall be “INT-I{US}4.22{GS}”.

3.1.14 Field 1.014: Greenwich mean time (GMT)

This mandatory field provides a mechanism for expressing the date and time in terms of universal Greenwich Mean Time (GMT) units. If used, the GMT field contains the universal date that will be in addition to the local date contained in Field 1.005 (DAT). Use of the GMT field eliminates local time inconsistencies encountered when a transaction and its response are transmitted between two places separated by several time zones. The GMT provides a universal date and 24-hour clock time independent of time zones. It is represented as "CCYYMMDDHHMMSSZ", a 15-character string that is the concatenation of the date with the GMT and concludes with a "Z". The "CCYY" characters shall represent the year of the transaction, the "MM" characters shall be the tens and units values of the month, and the "DD" characters shall be the tens and units values of the day of the month, the "HH" characters represent the hour, the "MM" the minute, and the "SS" represents the second. The complete date shall not exceed the current date.

4. Type-2 Logical Record: Descriptive Text

The structure of most of this record is not defined by the original ANSI/NIST standard. The record contains information of specific interest to the agencies sending or receiving the file. To ensure that communicating dactyloscopic systems are compatible, it is required that only the fields listed below are contained within the record. This document specifies which fields are mandatory and which optional, and also defines the structure of the individual fields.

4.1 Fields for Type-2 Logical Record

4.1.1 Field 2.001: Logical Record Length (LEN)

This mandatory field contains the length of this Type-2 record, and specifies the total number of bytes including every character of every field contained in the record and the information separators.

4.1.2 Field 2.002: Image Designation Character (IDC)

The IDC contained in this mandatory field is an ASCII representation of the IDC as defined in the File Content field (CNT) of the Type-1 record (field 1.003).

4.1.3 Field 2.003: System Information (SYS)

This field is mandatory and contains four bytes which indicate which version of the INT-I this particular Type-2 record complies with.

The first two bytes specify the major version number, the second two the minor revision number. For example, this implementation is based on INT-I version 4 revision 22 and would be represented as “0422”.

4.1.4 Field 2.007: Case Number (CNO)

This is a number assigned by the local dactyloscopic bureau to a collection of latents found at a scene-of-crime. The following format is adopted: CC/*number*

where CC is the Interpol Country Code, two alpha-numeric characters in length, and the *number* complies with the appropriate local guidelines and may be up to 32 alpha-numeric characters long.

This field allows the system to identify latents associated with a particular crime.

4.1.5 Field 2.008: Sequence Number (SQN)

This specifies each sequence of latents within a case. It can be up to four numeric characters long. A sequence is a latent or series of latents which are grouped together for the purposes of filing and/or searching. This definition implies that even single latents will still have to be assigned a sequence number.

This field together with MID (Field 2.009) may be included to identify a particular latent within a sequence.

4.1.6 Field 2.009: Latent Identifier (MID)

This specifies the individual latent within a sequence. The value is a single letter or two letters, with 'A' assigned to the first latent, 'B' to the second, and so on up to a limit of 'ZZ'. This field is used analogue to the latent sequence number discussed in the description for SQN (Field 2.008).

4.1.7 Field 2.010: Criminal Reference Number (CRN)

This is a unique reference number assigned by a national agency to an individual who is charged for the first time with committing an offence. Within one country no individual ever has more than one CRN, or shares it with any other individual. However, the same individual may have Criminal Reference Numbers in several countries, which will be distinguishable by means of the country code.

The following format is adopted for CRN field: CC/*number*
where CC is the Country Code, defined in ISO 3166, two alpha-numeric characters in length, and the *number* complies with the appropriate national guidelines of the issuing agency, and may be up to 32 alpha-numeric characters long.
For transactions pursuant to Decision 2008/.../JHA this field will be used for the national criminal reference number of the originating agency which is linked to the images in Type-4 or Type-15 Records.

4.1.8 Field 2.012: Miscellaneous Identification Number (MN1)
This fields contains the CRN (field 2.010) transmitted by a CPS or PMS transaction without the leading country code.

4.1.9 Field 2.013: Miscellaneous Identification Number (MN2)
This fields contains the CNO (field 2.007) transmitted by an MPS or MMS transaction without the leading country code.

4.1.10 Field 2.014: Miscellaneous Identification Number (MN3)
This fields contains the SQN (field 2.008) transmitted by an MPS or MMS transaction.

4.1.11 Field 2.015: Miscellaneous Identification Number (MN4)
This fields contains the MID (field 2.009) transmitted by an MPS or MMS transaction.

4.1.12 Field 2.063: Additional Information (INF)
In case of an SRE transaction to a PMS request this field gives information about the finger which caused the possible HIT. The format of the field is:
NN where *NN* is the finger position code defined in table 5, two digits in length.
In all other cases the field is optional. It consists of up to 32 alpha-numeric characters and may give additional information about the request.

4.1.13 Field 2.064: Respondents List (RLS)

This field contains at least two subfields. The first subfield describes the type of search that has been carried out, using the three-letter mnemonics which specify the transaction type in TOT (Field 1.004). The second subfield contains a single character. An "**I**" shall be used to indicate that a HIT has been found and an "**N**" shall be used to indicate that no matching cases have been found (NOHIT). The third subfield contains the sequence identifier for the candidate result and the total number of candidates separated by a slash. Multiple messages will be returned if multiple candidates exist.

In case of a possible HIT the fourth subfield shall contain the score up to six digits long. If the HIT has been verified the value of this subfield is defined as "999999".

Example: "CPS{RS}I{RS}001/001{RS}999999{GS}"

If the remote AFIS does not assign scores, then a score of zero should be used at the appropriate point.

4.1.14 Field 2.074: Status/Error Message Field (ERM)

This field contains error messages resulting from transactions, which will be sent back to the requester as part of an Error Transaction.

Table 3: Error messages

Numeric Code (1-3)	Meaning (5-128)
003	ERROR: UNAUTHORISED ACCESS
101	MANDATORY FIELD MISSING
102	INVALID RECORD TYPE
103	UNDEFINED FIELD
104	EXCEED THE MAXIMUM OCCURRENCE
105	INVALID NUMBER OF SUBFIELDS
106	FIELD LENGTH TOO SHORT
107	FIELD LENGTH TOO LONG
108	FIELD IS NOT A NUMBER AS EXPECTED
109	FIELD NUMBER VALUE TOO SMALL
110	FIELD NUMBER VALUE TOO BIG
111	INVALID CHARACTER
112	INVALID DATE
115	INVALID ITEM VALUE
116	INVALID TYPE OF TRANSACTION
117	INVALID RECORD DATA
201	ERROR: INVALID TCN
501	ERROR: INSUFFICIENT FINGERPRINT QUALITY
502	ERROR: MISSING FINGERPRINTS
503	ERROR: FINGERPRINT SEQUENCE CHECK FAILED
999	ERROR: ANY OTHER ERROR. FOR FURTHER DETAILS CALL DESTINATION AGENCY.

Error messages in the range between 100 and 199:

These error messages are related to the validation of the ANSI/NIST records and defined as:

<error_code 1>: IDC <idc_number 1> FIELD <field_id 1> <dynamic text 1> LF

<error_code 2>: IDC <idc_number 2> FIELD <field_id 2> <dynamic text 2>…

where

- error_code is a code uniquely related to a specific reason (see table 3)
- field_id is the ANSI/NIST field number of the incorrect field (e.g. 1.001, 2.001, ...) in the format <record_type>.<field_id>.<sub_field_id>
- dynamic text is a more detailed dynamic description of the error
- LF is a Line Feed separating errors if more then one error is encountered
- for type-1 record the ICD is defined as "-1"

Example:
201: IDC -1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION

This field is mandatory for error transactions.

4.1.15 Field 2.320: Expected Number of Candidates (ENC)

This field contains the maximum number of candidates for verification expected by the requesting agency. The value of ENC must not exceed the values defined in table 11.

5. Type-4 Logical Record: High Resolution Gray-Scale Image

It should be noted that Type-4 records are binary rather than ASCII in nature. Therefore each field is assigned a specific position within the record, which implies that all fields are mandatory.
The standard allows both image size and resolution to be specified within the record. It requires Type-4 Logical Records to contain dactyloscopic image data that are being transmitted at a nominal pixel density of 500 to 520 pixels per inch. The preferred rate for new designs is at a pixel density of 500 pixels per inch or 19.68 pixels per mm. 500 pixels per inch is the density specified by the INT-I, except that similar systems may communicate with each other at a non-preferred rate, within the limits of 500 to 520 pixels per inch.

5.1 Fields for Type-4 Logical Record

5.1.1 Field 4.001: Logical Record Length (LEN)

This four-byte field contains the length of this Type-4 record, and specifies the total number of bytes including every byte of every field contained in the record.

5.1.2 Field 4.002: Image Designation Character (IDC)

This is the one-byte binary representation of the IDC number given in the header file.

5.1.3 Field 4.003: Impression Type (IMP)

The impression type is a single-byte field occupying the sixth byte of the record.

Table 4 : Finger Impression Type

Code	Description
0	Live-scan of plain fingerprint
1	Live-scan of rolled fingerprint
2	Non-live scan impression of plain fingerprint captured from paper
3	Non-live scan impression of rolled fingerprint captured from paper
4	Latent impression captured directly
5	Latent tracing
6	Latent photo
7	Latent lift
8	Swipe
9	Unknown

5.1.4 Field 4.004: Finger Position (FGP)

This fixed-length field of 6 bytes occupies the seventh through twelfth byte positions of a Type-4 record. It contains possible finger positions beginning in the left most byte (byte 7 of the record). The known or most probable finger position is taken from table 5. Up to five additional fingers may be referenced by entering the alternate finger positions in the remaining five bytes using the same format. If fewer than five finger position references are to be used the unused bytes are filled with binary 255. To reference all finger positions code 0, for unknown, is used.

Table 5: Finger position code and maximum size

Finger position	Finger code	Width (mm)	Length (mm)
Unknown	0	40.0	40.0
Right thumb	1	45.0	40.0
Right index finger	2	40.0	40.0
Right middle finger	3	40.0	40.0
Right ring finger	4	40.0	40.0
Right little finger	5	33.0	40.0
Left thumb	6	45.0	40.0
Left index finger	7	40.0	40.0
Left middle finger	8	40.0	40.0
Left ring finger	9	40.0	40.0
Left little finger	10	33.0	40.0
Plain right thumb	11	30.0	55.0
Plain left thumb	12	30.0	55.0
Plain right four fingers	13	70.0	65.0
Plain left four fingers	14	70.0	65.0

For scene of crime latents only the codes 0 to 10 should be used.

5.1.5 Field 4.005: Image Scanning Resolution (ISR)

This one-byte field occupies the 13th byte of a Type-4 record. If it contains “0” then the image has been sampled at the preferred scanning rate of 19.68 pixels/mm (500 pixels per inch). If it contains “1” then the image has been sampled at an alternative scanning rate as specified in the Type-1 record.

5.1.6 Field 4.006: Horizontal Line Length (HLL)

This field is positioned at bytes 14 and 15 within the Type-4 record. It specifies the number of pixels contained in each scan line. The first byte will be the most significant.

5.1.7 Field 4.007: Vertical Line Length (VLL)

This field records in bytes 16 and 17 the number of scan lines present in the image. The first byte is the most significant.

5.1.8 Field 4.008: Gray-scale Compression Algorithm (GCA)

This one-byte field specifies the gray-scale compression algorithm used to encode the image data. For this implementation, a binary code 1 indicates that WSQ compression (Appendix 7) has been used.

5.1.9 Field 4.009: The Image

This field contains a byte stream representing the image. Its structure will obviously depend on the compression algorithm used.

6. Type-9 Logical Record: Minutiæ Record

Type-9 records shall contain ASCII text describing minutiæ and related information encoded from a latent. For latent search transaction, there is no limit for these Type-9 records in a file, each of which shall be for a different view or latent.

6.1 Minutiæ extraction

6.1.1 Minutia type identification

This standard defines three identifier numbers that are used to describe the minutia type. These are listed in table 6. A ridge ending shall be designated Type 1. A bifurcation shall be designated Type 2. If a minutia cannot be clearly categorized as one of the above two types, it shall be designated as "other", Type 0.

Table 6: Minutia types

Type	Description
0	Other
1	Ridge ending
2	Bifurcation

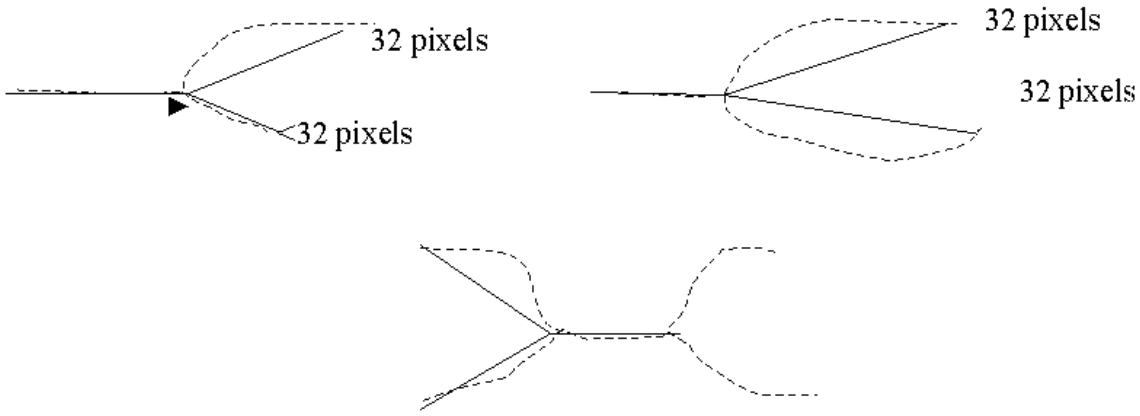
6.1.2 Minutia placement and type

For templates to be compliant with Section 5 of the ANSI INCITS 378-2004 standard, the following method, which enhances the current INCITS 378-2004 standard, shall be used for determining placement (location and angular direction) of individual minutiae.

The position or location of a minutia representing a ridge ending shall be the point of forking of the medial skeleton of the valley area immediately in front of the ridge ending. If the three legs of the valley area were thinned down to a single-pixel-wide skeleton, the point of the intersection is the location of the minutia. Similarly, the location of the minutia for a bifurcation shall be the point of forking of the medial skeleton of the ridge. If the three legs of the ridge were each thinned down to a single-pixel-wide skeleton, the point where the three legs intersect is the location of the minutia.
After all ridge endings have been converted to bifurcations, all of the minutiae of the dactyloscopic image are represented as bifurcations. The X and Y pixel coordinates of the intersection of the three legs of each minutia can be directly formatted. Determination of the minutia direction can be extracted from each skeleton bifurcation. The three legs of every skeleton bifurcation must be examined and the endpoint of each leg determined. Figure 6.1.2 illustrates the three methods used for determining the end of a leg that is based on a scanning resolution of 500 ppi.
The ending is established according to the event that occurs first. The pixel count is based on a scan resolution of 500 ppi. Different scan resolutions would imply different pixel counts.

- A distance of .064" (the 32nd pixel)
- The end of skeleton leg that occurs between a distance of .02" and .064" (the 10th through the 32nd pixels); shorter legs are not used
- A second bifurcation is encountered within a distance of .064" (before the 32nd pixel)

Figure 6.1.2



The angle of the minutiae is determined by constructing three virtual rays originating at the bifurcation point and extending to the end of each leg. The smallest of the three angles formed by the rays is bisected to indicate the minutiae direction.

6.1.3 Coordinate system

The coordinate system used to express the minutiae of a fingerprint shall be a Cartesian coordinate system. Minutiae locations shall be represented by their x and y coordinates. The origin of the coordinate system shall be the upper left corner of the original image with x increasing to the right and y increasing downward. Both x and y coordinates of a minutiae shall be represented in pixel units from the origin. It should be noted that the location of the origin and units of measure is not in agreement with the convention used in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.1.4 Minutiæ direction

Angles are expressed in standard mathematical format, with zero degrees to the right and angles increasing in the counter clockwise direction. Recorded angles are in the direction pointing back along the ridge for a ridge ending and toward the centre of the valley for a bifurcation. This convention is 180 degrees opposite of the angle convention described in the definitions of the Type 9 in the ANSI/NIST-ITL 1-2000.

6.2 Fields for Type-9 Logical record INCITS-378 Format

All fields of the Type-9 records shall be recorded as ASCII text. No binary fields are permissible in this tagged-field record.

6.2.1 Field 9.001: Logical record length (LEN)

This mandatory ASCII field shall contain the length of the logical record specifying the total number of bytes, including every character of every field contained in the record.

6.2.2 Field 9.002: Image designation character (IDC)

This mandatory two-byte field shall be used for the identification and location of the minutiæ data. The IDC contained in this field shall match the IDC found in the file content field of the Type-1 record.

6.2.3 Field 9.003: Impression type (IMP)

This mandatory one-byte field shall describe the manner by which the dactyloscopic image information was obtained. The ASCII value of the proper code as selected from table 4 shall be entered in this field to signify the impression type.

6.2.4 Field 9.004: Minutiæ format (FMT)

This field shall contain a "U" to indicate that the minutiae are formatted in M1-378 terms. Even though information may be encoded in accordance with the M1-378 standard, all data fields of the Type-9 record must remain as ASCII text fields.

6.2.5 Field 9.126: CBEFF information

This field shall contain three information items. The first information item shall contain the value "27" (0x1B). This is the identification of the CBEFF Format Owner assigned by the International Biometric Industry Association (IBIA) to INCITS Technical Committee M1. The <US> character shall delimit this item from the CBEFF Format Type that is assigned a value of "513" (0x0201) to indicate that this record contains only location and angular direction data without any Extended Data Block information. The <US> character shall delimit this item from the CBEFF Product Identifier (PID) that identifies the "owner" of the encoding equipment. The vendor establishes this value. It can be obtained from the IBIA website (www.ibia.org) if it is posted.

6.2.6 Field 9.127: Capture equipment identification

This field shall contain two information items separated by the <US> character. The first shall contain "APPF" if the equipment used originally to acquire the image was certified to comply with Appendix F (IAFIS Image Quality Specification, January 29, 1999) of CJIS-RS-0010, the Federal Bureau of Investigation's Electronic Fingerprint Transmission Specification. If the equipment did not comply it will contain the value of "NONE". The second information item shall contain the Capture Equipment ID which is a vendor-assigned product number of the capture equipment. A value of "0" indicates that the capture equipment ID is unreported.

6.2.7 Field 9.128: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image. The maximum horizontal size is limited to 65,534 pixels.

6.2.8 Field 9.129: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image. The maximum vertical size is limited to 65,534 pixels.

6.2.9 Field 9.130: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a "2" indicates pixels per centimetre. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

6.2.10 Field 9.131: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the horizontal component of the pixel aspect ratio.

6.2.10 Field 9.132: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

6.2.11 Field 9.133: Finger view

This mandatory field contains the view number of the finger associated with this record's data. The view number begins with "0" and increments by one to "15".

6.2.12 Field 9.134: Finger position (FGP)

This field shall contain the code designating the finger position that produced the information in this Type-9 record. A code between 1 and 10 taken from table 5 or the appropriate palm code from table 10 shall be used to indicate the finger or palm position.

6.2.13 Field 9.135: Finger quality

The field shall contain the quality of the overall finger minutiæ data and shall be between 0 and 100. This number is an overall expression of the quality of the finger record, and represents quality of the original image, of the minutia extraction and any additional operations that may affect the minutiæ record.

6.2.14 Field 9.136: number of minutiæ

The mandatory field shall contain a count of the number of minutiæ recorded in this logical record.

6.2.15 Field 9.137: Finger minutiæ data

This mandatory field has six information items separated by the <US> character. It consists of several subfields, each containing the details of single minutiae. The total number of minutiae subfields must agree with the count found in field 136. The first information item is the minutiae index number, which shall be initialized to "1" and incremented by "1" for each additional minutia in the fingerprint. The second and third information items are the 'x' coordinate and 'y' coordinates of the minutiae in pixel units. The fourth information item is the minutiae angle recorded in units of two degrees. This value shall be nonnegative between 0 and 179. The fifth information item is the minutiae type. A value of "0" is used to represent minutiae of type "OTHER", a value of "1" for a ridge ending and a value of "2" for a ridge bifurcation. The sixth information item represents the quality of each minutiae. This value shall range from 1 as a minimum to 100 as a maximum. A value of "0" indicates that no quality value is available. Each subfield shall be separated from the next with the use of the <RS> separator character.

6.2.16 Field 9.138: Ridge count information

This field consists of a series of subfields each containing three information items. The first information item of the first subfield shall indicate the ridge count extraction method. A "0" indicates that no assumption shall be made about the method used to extract ridge counts, nor their order in the record. A "1" indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in four quadrants, and ridge counts for each centre minutia are listed together. A "2" indicates that for each centre minutiae, ridge count data was extracted to the nearest neighbouring minutiae in eight octants, and ridge counts for each centre minutia are listed together. The remaining two information items of the first subfield shall both contain "0". Information items shall be separated by the <US> separator character. Subsequent subfields will contain the centre minutiae index number as the first information item, the neighbouring minutiae index number as the second information item, and the number of ridges crossed as the third information item. Subfields shall be separated by the <RS> separator character.

6.2.17 Field 9.139: Core information

This field will consist of one subfield for each core present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the core recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

6.2.18 Field 9.140: Delta information

This field will consist of one subfield for each delta present in the original image. Each subfield consists of three information items. The first two items contain the 'x' and 'y' coordinate positions in pixel units. The third information item contains the angle of the delta recorded in units of 2 degrees. The value shall be a nonnegative value between 0 and 179. Multiple cores will be separated by the <RS> separator character.

7. Type-13 variable-resolution latent image record

The Type-13 tagged-field logical record shall contain image data acquired from latent images. These images are intended to be transmitted to agencies that will automatically extract or provide human intervention and processing to extract the desired feature information from the images.

Information regarding the scanning resolution used, the image size, and other parameters required to process the image, are recorded as tagged-fields within the record.

Table 7: Type-13 variable-resolution latent record layout

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	13.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	13.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	13.003	IMPRESSION TYPE	A	2	2	1	1	9
SRC	M	13.004	SOURCE AGENCY / ORI	AN	6	35	1	1	42
LCD	M	13.005	LATENT CAPTURE DATE	N	9	9	1	1	16
HLL	M	13.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
VLL	M	13.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	13.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	13.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	13.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	13.011	COMPRESSION ALGORITHM	A	5	7	1	1	14
BPX	M	13.012	BITS PER PIXEL	N	2	3	1	1	10
FGP	M	13.013	FINGER POSITION	N	2	3	1	6	25
RSV		13.014 13.019	RESERVED FOR FUTURE DEFINITION	--	--	--	--	--	--
COM	O	13.020	COMMENT	A	2	128	0	1	135
RSV		13.021 13.199	RESERVED FOR FUTURE DEFINITION	--	--	--	--	--	--
UDF	O	13.200 13.998	USER-DEFINED FIELDS	--	--	--	--	--	--
DAT	M	13.999	IMAGE DATA	B	2	--	1	1	--

Key for character type: N = Numeric; A = Alphabetic; AN = Alphanumeric; B = Binary

7.1 Fields for the Type-13 logical record

The following paragraphs describe the data contained in each of the fields for the Type-13 logical record.

Within a Type-13 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-13 record, table 7 lists the "condition code" as being mandatory "M" or optional "O", the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the "field size per occurrence" include all character separators used in the field. The "maximum byte count" includes the field number, the information, and all the character separators including the "GS" character.

7.1.1 Field 13.001: Logical record length (LEN)

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-13 logical record. Field 13.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

7.1.2 Field 13.002: Image designation character (IDC)

This mandatory ASCII field shall be used to identify the latent image data contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

7.1.3 Field 13.003: Impression type (IMP)

This mandatory one- or two-byte ASCII field shall indicate the manner by which the latent image information was obtained. The appropriate latent code choice selected from table 4 (finger) or table 9 (palm) shall be entered in this field.

7.1.4 Field 13.004: Source agency / ORI (SRC)

This mandatory ASCII field shall contain the identification of the administration or organization that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/*agency*.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

7.1.5 Field 13.005: Latent capture date (LCD)

This mandatory ASCII field shall contain the date that the latent image contained in the record was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and unit values of the day in the month. For example, 20000229 represents February 29, 2000. The complete date must be a legitimate date.

7.1.6 Field 13.006: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

7.1.7 Field 13.007: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

7.1.8 Field 13.008: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a "2" indicates pixels per centimetre. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

7.1.9 Field 13.009: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the horizontal component of the pixel aspect ratio.

7.1.10 Field 13.010: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

7.1.11 Field 13.011: Compression algorithm (CGA)

This mandatory ASCII field shall specify the algorithm used to compress grayscale images. See Appendix 7 for the compression codes.

7.1.12 Field 13.012: Bits per pixel (BPX)

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of “8” for normal grayscale values of “0” to “255”. Any entry in this field greater than “8” shall represent a grayscale pixel with increased precision.

7.1.13 Field 13.013: Finger / palm position (FGP)

This mandatory tagged-field shall contain one or more the possible finger or palm positions that may match the latent image. The decimal code number corresponding to the known or most probable finger position shall be taken from table 5 or the most probable palm position from table 10 and entered as a one- or two-character ASCII subfield. Additional finger and/or palm positions may be referenced by entering the alternate position codes as subfields separated by the “RS” separator character. The code "0", for "Unknown Finger", shall be used to reference every finger position from one through ten. The code “20”, for “Unknown Palm”, shall be used to reference every listed palmprint position.

7.1.14 Field 13.014-019: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.15 Field 13.020: Comment (COM)

This optional field may be used to insert comments or other ASCII text information with the latent image data.

7.1.16 Field 13.021-199: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

7.1.17 Fields 13.200-998: User-defined fields (UDF)

These fields are user-definable fields and will be used for future requirements. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

7.1.18 Field 13.999: Image data (DAT)

This field shall contain all data from a captured latent image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, "13.999:" is followed by image data in a binary representation.

Each pixel of uncompressed grayscale data shall normally be quantized to eight bits (256 gray levels) contained in a single byte. If the entry in BPX Field 13.012 is greater or less than "8", the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the GCA field.

7.2 End of Type-13 variable-resolution latent image record

For the sake of consistency, immediately following the last byte of data from field 13.999 an "FS" separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-13 record.

8. Type-15 variable-resolution palmprint image record

The Type-15 tagged-field logical record shall contain and be used to exchange palmprint image data together with fixed and user-defined textual information fields pertinent to the digitized image. Information regarding the scanning resolution used, the image size and other parameters or comments required to process the image are recorded as tagged-fields within the record. Palmprint images transmitted to other agencies will be processed by the recipient agencies to extract the desired feature information required for matching purposes.

The image data shall be acquired directly from a subject using a live-scan device, or from a palmprint card or other media that contains the subject's palmprints.

Any method used to acquire the palmprint images shall be capable of capturing a set of images for each hand. This set shall include the writer's palm as a single scanned image, and the entire area of the full palm extending from the wrist bracelet to the tips of the fingers as one or two scanned images. If two images are used to represent the full palm, the lower image shall extend from the wrist bracelet to the top of the interdigital area (third finger joint) and shall include the thenar, and hypothenar areas of the palm. The upper image shall extend from the bottom of the interdigital area to the upper tips of the fingers. This provides an adequate amount of overlap between the two images that are both located over the interdigital area of the palm. By matching the ridge structure and details contained in this common area, an examiner can confidently state that both images came from the same palm.

As a palmprint transaction may be used for different purposes, it may contain one or more unique image areas recorded from the palm or hand. A complete palmprint record set for one individual will normally include the writer's palm and the full palm image(s) from each hand. Since a tagged-field logical image record may contain only one binary field, a single Type-15 record will be required for each writer's palm and one or two Type-15 records for each full palm. Therefore, four to six Type-15 records will be required to represent the subject's palmprints in a normal palmprint transaction.

8.1 Fields for the Type-15 logical record

The following paragraphs describe the data contained in each of the fields for the Type-15 logical record.

Within a Type-15 logical record, entries shall be provided in numbered fields. It is required that the first two fields of the record are ordered, and the field containing the image data shall be the last physical field in the record. For each field of the Type-15 record, table 8 lists the "condition code" as being mandatory "M" or optional "O", the field number, the field name, character type, field size, and occurrence limits. Based on a three digit field number, the maximum byte count size for the field is given in the last column. As more digits are used for the field number, the maximum byte count will also increase. The two entries in the "field size per occurrence" include all character separators used in the field. The "maximum byte count" includes the field number, the information, and all the character separators including the "GS" character.

8.1.1 Field 15.001: Logical record length (LEN)

This mandatory ASCII field shall contain the total count of the number of bytes in the Type-15 logical record. Field 15.001 shall specify the length of the record including every character of every field contained in the record and the information separators.

8.1.2 Field 15.002: Image designation character (IDC)

This mandatory ASCII field shall be used to identify the palmprint image contained in the record. This IDC shall match the IDC found in the file content (CNT) field of the Type-1 record.

8.1.3 Field 15.003: Impression type (IMP)

This mandatory one-byte ASCII field shall indicate the manner by which the palmprint image information was obtained. The appropriate code selected from table 9 shall be entered in this field.

8.1.4 Field 15.004: Source agency/ORI (SRC)

This mandatory ASCII field shall contain the identification of the administration or organization that originally captured the facial image contained in the record. Normally, the Originating Agency Identifier (ORI) of the agency that captured the image will be contained in this field. It consists of two information items in the following format: CC/*agency*.

The first information item contains the Interpol Country Code, two alpha-numeric characters long. The second item, *agency*, is a free text identification of the agency, up to a maximum of 32 alpha-numeric characters.

8.1.5 Field 15.005: Palmprint capture date (PCD)

This mandatory ASCII field shall contain the date that the palmprint image was captured. The date shall appear as eight digits in the format CCYYMMDD. The CCYY characters shall represent the year the image was captured; the MM characters shall be the tens and unit values of the month; and the DD characters shall be the tens and units values of the day in the month. For example, the entry 20000229 represents February 29, 2000. The complete date must be a legitimate date.

8.1.6 Field 15.006: Horizontal line length (HLL)

This mandatory ASCII field shall contain the number of pixels contained on a single horizontal line of the transmitted image.

8.1.7 Field 15.007: Vertical line length (VLL)

This mandatory ASCII field shall contain the number of horizontal lines contained in the transmitted image.

8.1.8 Field 15.008: Scale units (SLC)

This mandatory ASCII field shall specify the units used to describe the image sampling frequency (pixel density). A "1" in this field indicates pixels per inch, or a "2" indicates pixels per centimeter. A "0" in this field indicates no scale is given. For this case, the quotient of HPS/VPS gives the pixel aspect ratio.

8.1.9 Field 15.009: Horizontal pixel scale (HPS)

This mandatory ASCII field shall specify the integer pixel density used in the horizontal direction providing the SLC contains a "1" or a "2". Other-wise, it indicates the horizontal component of the pixel aspect ratio.

8.1.10 Field 15.010: Vertical pixel scale (VPS)

This mandatory ASCII field shall specify the integer pixel density used in the vertical direction providing the SLC contains a "1" or a "2". Otherwise, it indicates the vertical component of the pixel aspect ratio.

Table 8: Type-15 variable-resolution palmprint record layout

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
LEN	M	15.001	LOGICAL RECORD LENGTH	N	4	8	1	1	15
IDC	M	15.002	IMAGE DESIGNATION CHARACTER	N	2	5	1	1	12
IMP	M	15.003	IMPRESSION TYPE	N	2	2	1	1	9
SRC	M	15.004	SOURCE AGENCY / ORI	AN	6	35	1	1	42
PCD	M	15.005	PALMPRINT CAPTURE DATE	N	9	9	1	1	16

Ident	Cond. code	Field Number	Field Name	Char type	Field size per occurrence		Occur count		Max byte count
					min.	max.	min	max	
HLL	M	15.006	HORIZONTAL LINE LENGTH	N	4	5	1	1	12
VLL	M	15.007	VERTICAL LINE LENGTH	N	4	5	1	1	12
SLC	M	15.008	SCALE UNITS	N	2	2	1	1	9
HPS	M	15.009	HORIZONTAL PIXEL SCALE	N	2	5	1	1	12
VPS	M	15.010	VERTICAL PIXEL SCALE	N	2	5	1	1	12
CGA	M	15.011	COMPRESSION ALGORITHM	AN	5	7	1	1	14
BPX	M	15.012	BITS PER PIXEL	N	2	3	1	1	10
PLP	M	15.013	PALMPRINT POSITION	N	2	3	1	1	10
RSV		15.014 15.019	RESERVED FOR FUTURE INCLUSION	--	--	--	--	--	--
COM	O	15.020	COMMENT	AN	2	128	0	1	128
RSV		15.021 15.199	RESERVED FOR FUTURE INCLUSION	--	--	--	--	--	--
UDF	O	15.200 15.998	USER-DEFINED FIELDS	--	--	--	--	--	--
DAT	M	15.999	IMAGE DATA	B	2	--	1	1	--

Table 9 : Palm Impression Type

Description	Code
Live-scan palm	10
Nonlive-scan palm	11
Latent palm impression	12
Latent palm tracing	13
Latent palm photo	14
Latent palm lift	15

8.1.11 Field 15.011: Compression algorithm (CGA)

This mandatory ASCII field shall specify the algorithm used to compress grayscale images. An entry of "NONE" in this field indicates that the data contained in this record are uncompressed. For those images that are to be compressed, this field shall contain the preferred method for the compression of tenprint fingerprint images. Valid compression codes are defined in Appendix 7.

8.1.12 Field 15.012: Bits per pixel (BPX)

This mandatory ASCII field shall contain the number of bits used to represent a pixel. This field shall contain an entry of “8” for normal grayscale values of “0” to “255”. Any entry in this field greater than or less than “8” shall represent a grayscale pixel with increased or decreased precision respectively.

Table 10: Palm Codes, Areas & Sizes

Palm Position	Palm code	Image area (mm^2)	Width (mm)	Height (mm)
Unknown Palm	20	28387	139.7	203.2
Right Full Palm	21	28387	139.7	203.2
Right Writer s Palm	22	5645	44.5	127.0
Left Full Palm	23	28387	139.7	203.2
Left Writer s Palm	24	5645	44.5	127.0
Right Lower Palm	25	19516	139.7	139.7
Right Upper Palm	26	19516	139.7	139.7
Left Lower Palm	27	19516	139.7	139.7
Left Upper Palm	28	19516	139.7	139.7
Right Other	29	28387	139.7	203.2
Left Other	30	28387	139.7	203.2

8.1.13 Field 15.013: Palmprint position (PLP)

This mandatory tagged-field shall contain the palmprint position that matches the palmprint image. The decimal code number corresponding to the known or most probable palmprint position shall be taken from table 10 and entered as a two-character ASCII subfield. Table 10 also lists the maximum image areas and dimensions for each of the possible palmprint positions.

8.1.14 Field 15.014-019: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.15 Field 15.020: Comment (COM)

This optional field may be used to insert comments or other ASCII text information with the palmprint image data.

8.1.16 Field 15.021-199: Reserved for future definition (RSV)

These fields are reserved for inclusion in future revisions of this standard. None of these fields are to be used at this revision level. If any of these fields are present, they are to be ignored.

8.1.17 Fields 15.200-998: User-defined fields (UDF)

These fields are user-definable fields and will be used for future requirements. Their size and content shall be defined by the user and be in accordance with the receiving agency. If present they shall contain ASCII textual information.

8.1.18 Field 15.999: Image data (DAT)

This field shall contain all of the data from a captured palmprint image. It shall always be assigned field number 999 and must be the last physical field in the record. For example, "15.999:" is followed by image data in a binary representation. Each pixel of uncompressed grayscale data shall normally be quantized to eight bits (256 gray levels) contained in a single byte. If the entry in BPX Field 15.012 is greater or less than 8, the number of bytes required to contain a pixel will be different. If compression is used, the pixel data shall be compressed in accordance with the compression technique specified in the CGA field.

8.2 End of Type-15 variable-resolution palmprint image record

For the sake of consistency, immediately following the last byte of data from field 15.999 an "FS" separator shall be used to separate it from the next logical record. This separator must be included in the length field of the Type-15 record.

8.3 Additional Type-15 variable-resolution palmprint image records

Additional Type-15 records may be included in the file. For each additional palmprint image, a complete Type-15 logical record together with the "FS" separator is required.

Table 11: Maximum numbers of candidates accepted for verification per transmission

Type of AFIS Search	TP/TP	LT/TP	LP/PP	TP/UL	LT/UL	PP/ULP	LP/ULP
Maximum Number of Candidates	1	10	5	5	5	5	5

Search types:

TP/TP: ten-print against ten-print

LT/TP: fingerprint latent against ten-print

LP/PP: palmprint latent against palmprint

TP/UL: ten-print against unsolved fingerprint latent

LT/UL: fingerprint latent against unsolved fingerprint latent

PP/ULP: palmprint against unsolved palmprint latent

LP/ULP: palmprint latent against unsolved palmprint latent

10. Appendices to Chapter 2 (exchange of dactyloscopic data)

10.1 Appendix 1 ASCII Separator Codes

ASCII	Position[1]	Description
LF	1/10	Separates error codes in field 2.074
FS	1/12	Separates logical records of a file
GS	1/13	Separates fields of a logical record
RS	1/14	Separates the subfields of a record field
US	1/15	Separates individual information items of the field or subfield

10.2 Appendix 2 Calculation of Alpha-Numeric Check Character

For TCN and TCR (Fields 1.09 and 1.10):

The number corresponding to the check character is generated using the following formula:

$$(YY * 10^8 + SSSSSSSS) \text{ Modulo } 23$$

Where YY and SSSSSSSS are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

For CRO (Field 2.010)

The number corresponding to the check character is generated using the following formula:

$$(YY * 10^6 + NNNNNN) \text{ Modulo } 23$$

Where YY and NNNNNN are the numerical values of the last two digits of the year and the serial number respectively.

The check character is then generated from the look-up table given below.

1 This is the position as defined in the ASCII standard.

Check Character Look-up Table

1-A	9-J	17-T
2-B	10-K	18-U
3-C	11-L	19-V
4-D	12-M	20-W
5-E	13-N	21-X
6-F	14-P	22-Y
7-G	15-Q	0-Z
8-H	16-R	

10.3 Appendix 3 Character Codes

7-bit ANSI code for information interchange

ASCII Character Set										
+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
30				**!**	**"**	**#**	**$**	**%**	**&**	**'**
40	**(**	**)**	*****	**+**	**,**	**-**	**.**	**/**	**0**	**1**
50	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**:**	**;**
60	**<**	**=**	**>**	**?**	**@**	**A**	**B**	**C**	**D**	**E**
70	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**
80	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**
90	**Z**	**[**	****	**]**	**^**	**_**	**`**	**a**	**b**	**c**
100	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
110	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**
120	**x**	**y**	**z**	**{**	**|**	**}**	**~**			

10.4 Appendix 4 Transaction Summary

Type 1 Record (mandatory)

Identifier	Field Number	Field Name	CPS/PMS	SRE	ERR
LEN	1.001	Logical Record Length	M	M	M
VER	1.002	Version Number	M	M	M
CNT	1.003	File Content	M	M	M
TOT	1.004	Type of Transaction	M	M	M
DAT	1.005	Date	M	M	M
PRY	1.006	Priority	M	M	M
DAI	1.007	Destination Agency	M	M	M
ORI	1.008	Originating Agency	M	M	M
TCN	1.009	Transaction Control Number	M	M	M
TCR	1.010	Transaction Control Reference	C	M	M
NSR	1.011	Native Scanning Resolution	M	M	M
NTR	1.012	Nominal Transmitting Resolution	M	M	M
DOM	1.013	Domain name	M	M	M
GMT	1.014	Greenwich mean time	M	M	M

Under the Condition Column:

O = Optional; M = Mandatory; C = Conditional if transaction is a response to the origin agency

Type 2 Record (mandatory)

Identifier	Field Number	Field Name	CPS/ PMS	MPS/ MMS	SRE	ERR
LEN	2.001	Logical Record Length	M	M	M	M
IDC	2.002	Image Designation Character	M	M	M	M
SYS	2.003	System Information	M	M	M	M
CNO	2.007	Case Number	-	M	C	-
SQN	2.008	Sequence Number	-	C	C	-
MID	2.009	Latent Identifier	-	C	C	-
CRN	2.010	Criminal Reference Number	M	-	C	-
MN1	2.012	Miscellaneous Identification Number	-	-	C	C
MN2	2.013	Miscellaneous Identification Number	-	-	C	C
MN3	2.014	Miscellaneous Identification Number	-	-	C	C
MN4	2.015	Miscellaneous Identification Number	-	-	C	C
INF	2.063	Additional Information	O	O	O	O
RLS	2.064	Respondents List	-	-	M	-
ERM	2.074	Status/Error Message Field	-	-	-	M
ENC	2.320	Expected Number of Candidates	M	M	-	-

Under the Condition Column:

O = Optional; M = Mandatory; C = Conditional if data is available

*) = if the transmission of the data is in accordance with national law (not covered by the Council Decision 2007/.../JHA)

10.5 Appendix 5 Type-1 Record Definitions

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	1.001	Logical Record Length	N	1.001:230{GS}
VER	M	1.002	Version Number	N	1.002:0300{GS}
CNT	M	1.003	File Content	N	1.003:1{US}15{RS}2{US}00{RS}4{US}01{RS}4{US}02{RS}4{US}03{RS}4{US}04{RS}4{US}05{RS}4{US}06{RS}4{US}07{RS}4{US}08{RS}4{US}09{RS}4{US}10{RS}4{US}11{RS}4{US}12{RS}4{US}13{RS}4{US}14{GS}
TOT	M	1.004	Type of Transaction	A	1.004:CPS{GS}
DAT	M	1.005	Date	N	1.005:20050101{GS}
PRY	M	1.006	Priority	N	1.006:4{GS}
DAI	M	1.007	Destination Agency	1*	1.007:DE/BKA{GS}
ORI	M	1.008	Originating Agency	1*	1.008:NL/NAFIS{GS}
TCN	M	1.009	Transaction Control Number	AN	1.009:0200000004F{GS}
TCR	C	1.010	Transaction Control Reference	AN	1.010:0200000004F{GS}
NSR	M	1.011	Native Scanning Resolution	AN	1.011:19.68{GS}
NTR	M	1.012	Nominal Transmitting Resolution	AN	1.012:19.68{GS}
DOM	M	1.013	Domain Name	AN	1.013: INT-I{US}4.22{GS}

GMT	M	1.014	Greenwich Mean Time	AN	1.014:20050101125959Z

Under the Condition Column: O= Optional, M= Mandatory, C= Conditional

Under the Character Type Column: A= Alpha, N= Numeric, B= Binary

1* allowed characters for agency name are ["0..9", "A..Z", "a..z", "_", ".", " ", "-"]

10.6 Appendix 6 Type-2 Record Definitions

Table A.6.1: CPS- and PMS-Transaction

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	M	2.010	Criminal Reference Number	AN	2.010:DE/E999999999{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Table A.6.2: SRE-Transaction

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CRN	C	2.010	Criminal Reference Number	AN	2.010:NL/2222222222{GS}
MN1	C	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
RLS	M	2.064	Respondents List	AN	2.064:CPS{RS}I{RS}001/001{RS}999999{GS}

Table A.6.3: ERR-Transaction

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
MN1	M	2.012	Miscellaneous Identification Number	AN	2.012:E999999999{GS}
MN2	C	2.013	Miscellaneous Identification Number	AN	2.013:E999999999{GS}
MN3	C	2.014	Miscellaneous Identification Number	N	2.014:0001{GS}
MN4	C	2.015	Miscellaneous Identification Number	A	2.015:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ERM	M	2.074	Status/Error Message Field	AN	2.074: 201: IDC -1 FIELD 1.009 WRONG CONTROL CHARACTER {LF} 115: IDC 0 FIELD 2.003 INVALID SYSTEM INFORMATION {GS}

Table A.6.4: MPS- and MMS-Transaction

Identifier	Condition	Field Number	Field Name	Character Type	Example Data
LEN	M	2.001	Logical Record Length	N	2.001:909{GS}
IDC	M	2.002	Image Designation Character	N	2.002:00{GS}
SYS	M	2.003	System Information	N	2.003:0422{GS}
CNO	M	2.007	Case Number	AN	2.007:E999999999{GS}
SQN	C	2.008	Sequence Number	N	2.008:0001{GS}
MID	C	2.009	Latent Identifier	A	2.009:A{GS}
INF	O	2.063	Additional Information	1*	2.063:Additional Information 123{GS}
ENC	M	2.320	Expected Number of Candidates	N	2.320:1{GS}

Under the Condition Column: O= Optional, M= Mandatory, C= Conditional

Under the Character Type Column: A= Alpha, N= Numeric, B= Binary

1* allowed characters are ["0..9", "A..Z", "a..z", "_", ".", " ", "-", ","]

10.7 Appendix 7 Grayscale Compression Codes

Compression Codes

Compression	Value	Remarks
Wavelet Scalar Quantization Grayscale Fingerprint Image Compression Specification IAFIS-IC-0010(V3), dated December 19, 1997	WSQ	Algorithm to be used for the compression of grayscale images in Type-4, Type-7 and Type-13 to Type-15 records. Shall not be used for resolutions >500dpi.
JPEG 2000 [ISO 15444 / ITU T.800]	J2K	To be used for lossy and losslessly compression of grayscale images in Type-13 to Type-15 records. Strongly recommended for resolutions >500 dpi

10.8 Appendix 8 Mailspecification

To improve the internal workflow the mailsubject of a PRUEM transaction has to be filled with the country code (CC) of the Member State that send the message and the Type of Transaction (TOT Field 1.004).

Format: CC/*type of transaction*

Example: "DE/CPS"

The mailbody can be empty.

Chapter 3: Exchange of vehicle registration data

1. Common data-set for automated search of vehicle registration data

1.1 Definitions

The definitions of mandatory data elements and optional data elements set out in Article 16(4) are as follows:

Mandatory (M):

The data element has to be communicated when the information is available in a Member States's national register. Therefore there is an **obligation** to exchange the information **when available**.

Optional (O):

The data element may be communicated when the information is available in a Member State's national register. Therefore there is **no obligation** to exchange the information even when the information is available.

An indication (Y) is given for each element in the data set where the element is specifically identified as important in relation with the Decision 2008/.../JHA.

1.2. Vehicle/owner/holder search

1.2.1 Triggers for the search

There are two different ways to search for the information as defined in the next paragraph:

- By Chassis Number (VIN), Reference Date and Time (optional);
- By License Number, Chassis Number (VIN) (optional), Reference Date and Time (optional).

By means of these search criteria, information related to one and sometimes more vehicles will be returned. If information for only one vehicle has to be returned, all the items are returned in **one** response. If more than one vehicle is found, the requested Member State itself can determine which items will be returned; all items or only the items to refine the search (e.g. because of privacy reasons or because of performance reasons).

The items necessary to refine the search are pictured in paragraph 1.2.2.1. In paragraph 1.2.2.2 the complete information set is described.

When the search is done by Chassis Number, Reference Date and Time, the search can be done in **one or all** of the participating Member States.

When the search is done by License Number, Reference Data and Time, the search has to be done in **one specific** Member State.

Normally the actual Date and Time is used to make a search, but it is possible to conduct a search with a Reference Date and Time in the past. When a search is made with a Reference Date and Time in the past and historical information is not available in the register of the specific Member State because no such information is registered at all, the actual information can be returned with an indication that the information is actual information.

1.2.2 Data set

1.2.2.1 Items to be returned necessary for the refinement of the search

Item	**M/O[1]**	**Remarks**	**Prüm Y/N[2]**
Data relating to vehicles			
Licence number	M		**Y**
Chassis number / VIN	M		**Y**
Country of registration	M		**Y**
Make	M	(D.1[3]) e.g. Ford, Opel, Renault etc.	**Y**
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	**Y**
EU Category Code	M	(J) mopeds, motorbikes, cars etc.	**Y**

[1] M = mandatory when available in national register, O = optional
[2] All the attributes specifically allocated by the Member States are indicated with Y.
[3] Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

1.2.2.2 Complete data set

Item	M/O[1]	Remarks	Prüm Y/N
Data relating to holders of the vehicle		**(C.1[2])** The data refer to the holder of the specific registration certificate.	
Registration holders' (company) name	M	(C.1.1.) separate fields will be used for surname, infixes, titles etc., and the name in printable format will be communicated	**Y**
First name	M	(C.1.2) separate fields for first name(s) and initials will be used, and the name in printable format will be communicated	**Y**
Address	M	(C.1.3) separate fields will be used for Street, House number and Annex, Zip code, Place of residence, Country of residence etc., and the Address in printable format will be communicated	**Y**
Gender	M	Male, female	**Y**
Date of birth	M		**Y**
Legal entity	M	individual, association, company, firm etc.	**Y**
Place of Birth	O		**Y**
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport	N

[1] M = mandatory when available in national register, O = optional
[2] Harmonised document abbreviation, see Council Directive 1999/37/EC, 29-04-1999

Item	M/O[1]	Remarks	Prüm Y/N
		number).	
Start date holdership	O	Start date of the holdership of the car. This date will often be the same as printed under (I) on the registration certificate of the vehicle.	N
End date holdership	O	End data of the holdership of the car.	N
Type of holder	O	If there is no owner of the vehicle (C.2) the reference to the fact that the holder of the registration certificate: - is the vehicle owner - is not the vehicle owner - is not identified by the registration certificate as being the vehicle owner	N
Data relating to owners of the vehicle		**(C.2)**	
Owners' (company) name	M	(C.2.1)	**Y**
First name	M	(C.2.2)	**Y**
Address	M	(C.2.3)	**Y**
Gender	M	male, female	**Y**
Date of birth	M		**Y**
Legal entity	M	individual, association, company, firm etc.	**Y**
Place of Birth	O		**Y**
ID Number	O	An identifier that uniquely identifies the person or the company.	N
Type of ID Number	O	The type of ID Number (e.g. passport number).	N
Start date ownership	O	Start date of the ownership of the car.	N
End date ownership	O	End data of the ownership of the car.	N

Item	M/O[1]	Remarks	Prüm Y/N
Data relating to vehicles			
Licence number	M		**Y**
Chassis number / VIN	M		**Y**
Country of registration	M		**Y**
Make	M	(D.1) e.g. Ford, Opel, Renault etc.	**Y**
Commercial type of the vehicle	M	(D.3) e.g. Focus, Astra, Megane	**Y**
Nature of the vehicle / EU Category Code	M	(J) mopeds, motorbikes, cars etc.	**Y**
Date of first registration	M	(B) date of first registration of the vehicle somewhere in the world	**Y**
Start date (actual) registration	M	(I) Date of the registration to which the specific certificate of the vehicle refers	**Y**
End date registration	M	End data of the registration to which the specific certificate of the vehicle refers. It is possible this date indicates the period of validity as printed on the document if not unlimited (document abbreviation = H).	**Y**
Status	M	scrapped, stolen, exported etc.	**Y**
Start date status	M		**Y**
End date status	O		N
kW	O	(P.2)	**Y**
Capacity	O	(P.1)	**Y**
Type of licence number	O	regular, transito etc.	**Y**
Vehicle document id 1	O	The first unique document ID as printed on the vehicle document	**Y**
Vehicle document id 2[1]	O	A second document ID as printed on the vehicle document.	**Y**
Data relating to			

[1] In Luxembourg two separate vehicle registration document ID's are used.

Item	M/O[1]	Remarks	Prüm Y/N
insurances			
Insurance company name	O		**Y**
Begin date insurance	O		**Y**
End date insurance	O		**Y**
Address	O		**Y**
Insurance number	O		**Y**
ID Number	O	An identifier that uniquely identifies the company.	N
Type of ID Number	O	The type of ID Number (e.g. number of the Chamber of Commerce)	N

2. Data Security

2.1. Overview

The Eucaris software application handles secure communication to the other Member States and communicates to the back-end legacy systems of Member States using XML. Member States exchange messages by directly sending them to the recipient. The data center of a Member State is connected to the TESTA network of EU.

The XML-messages sent over the network are encrypted. The technique to encrypt these messages is SSL. The messages sent to the back-end are plain text XML-messages since the connection between the application and the back-end shall be in a protected environment.

A client application is provided which can be used within a Member State to query their own register or other Member States' registers. The clients will be identified by means of user-id/password or a client certificate. The connection to a user may be encrypted, but this is the responsibility of each individual Member State.

2.2 Security Features related to message exchange

The security design is based on a combination of HTTPS and XML signature. This alternative uses XML-signature to sign all messages sent so the server and can authenticate the sender of the message by checking the signature. 1-sided SSL (only a server certificate) is used to protect the confidentiality and integrity of the message in transit and provides protection against deletion/replay and insertion attacks. Instead of bespoke software development to implement 2-sided SSL, XML-signature is implemented. Using XML-signature is closer to the web services roadmap than 2-sided SSL and therefore more strategic.

The XML-signature can be implemented in several ways but the chosen approach is to use XML Signature as part of the Web Services Security (WSS). WSS specifies how to use XML-signature. Since WSS builds upon the SOAP standard, it is logical to adhere to the SOAP standard as much as possible.

2.3 Security features not related to message exchange

2. 3.1. Authentication of users

The users of the Eucaris web application authenticate themselves using a username and password. Since standard Windows authentication is used, Member States can enhance the level of authentication of users if needed by using client certificates.

2.3.2. User roles

The Eucaris software application supports different user roles. Each cluster of services has its own authorization. E.g. (exclusive) users of the "Treaty of Eucaris"- functionality" may not use the "Prüm"- functionality". Administrator services are separated from the regular end-user roles.

2.3.3. Logging and tracing of message exchange

Logging of all message types is facilitated by the Eucaris software application. An administrator function allows the national administrator to determine which messages are logged: requests from end-users, incoming requests from other Member States, provided information from the national registers, etc.

The application can be configured to use an internal database for this logging, or an external (Oracle) database. The decision on what messages have to be logged clearly depends on logging facilities elsewhere in the legacy systems and connected client applications.
The header of each message contains information on the requesting Member State, the requesting organization within that Member State and the user involved. Also the reason of the request is indicated.
By means of the combined logging in the requesting and responding Member State complete tracing of any message exchange is possible (e.g. on request of a citizen involved).

Logging is configured through the Eucaris web client (menu Administration, Logging configuration). The logging functionality is performed by the Core System. When logging is enabled, the complete message (header and body) is stored in one logging record. Per defined service, and per message type that passes along the Core System, the logging level can be set.

Logging Levels

The following logging levels are possible:
Private – Message is logged: The logging is NOT available to the extract logging service but is available on a national level only, for audits and problem solving.
None – Message is not logged at all.

Message Types

Information exchange between Member States consists of several messages, of which a schematic representation is given in the figure below.
The possible message types (in the figure shown for the Eucaris Core System of Member State X) are the following:

1. Request to Core System_Request message by Client
2. Request to Other Member State_Request message by Core System of this Member State
3. Request to Core System of this Member State_Request message by Core System of other Member State
4. Request to Legacy Register_Request message by Core System
5. Request to Core System_Request message by Legacy Register
6. Response from Core System_Request message by Client
7. Response from Other Member State_Request message by Core System of this Member State
8. Response from Core System of this Member State_Request message by other Member State
9. Response from Legacy Register_Request message by Core System
10. Response from Core System_Request message by Legacy Register

The following information exchanges are shown in the figure:

- Information request from Member State X to Member State Y – blue arrows. This request and response consists of message types 1, 2, 7 and 6, respectively.
- Information request from Member State Z to Member State X – red arrows. This request and response consists of message types 3, 4, 9 and 8, respectively.
- Information request from the legacy register to its core system (this route also includes a request from a custom client behind the legacy register) – green arrows. This kind of request consists of message types 5 and 10.

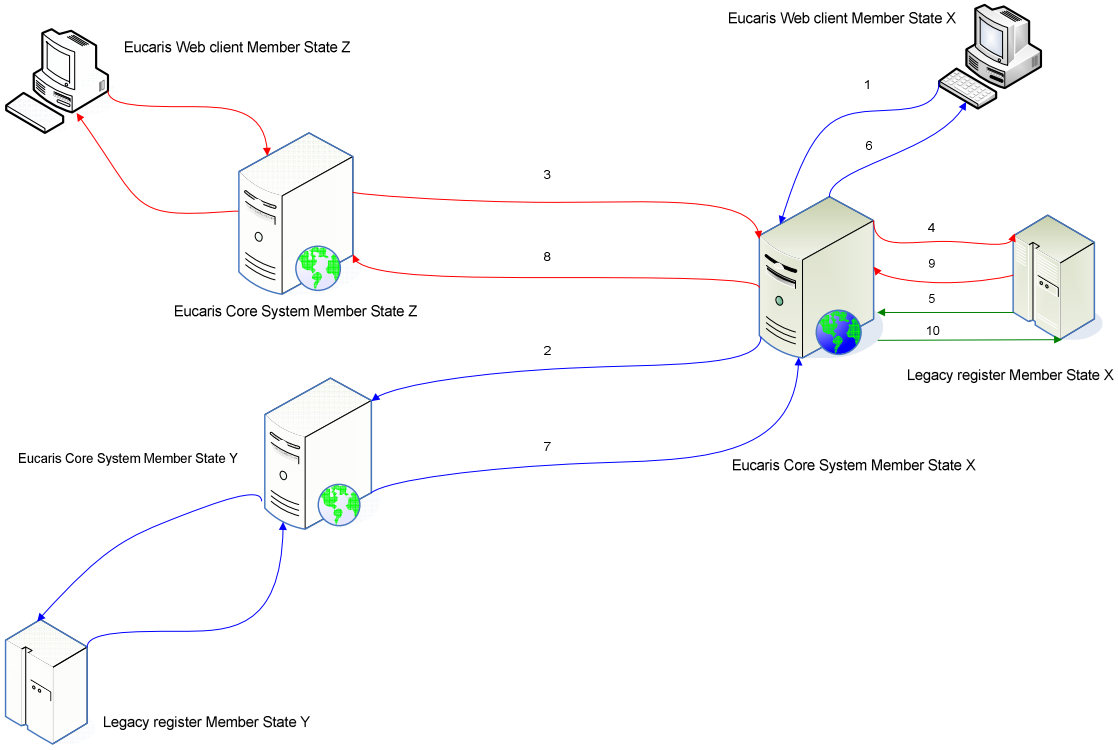


Figure : Message types for logging

2.3.4. Hardware Security Module

A Hardware Security Module is not used.

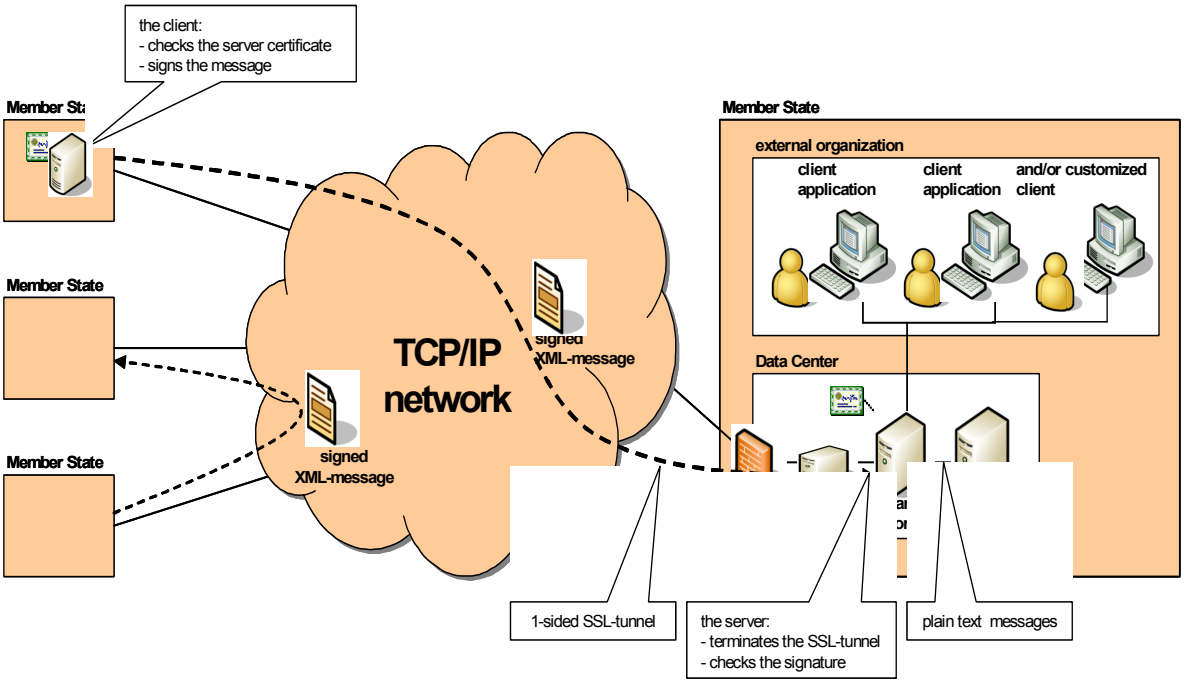
A Hardware Security Module (HSM) provides good protection for the key used to sign messages and to identify servers. This adds to the overall level of security but an HSM is expensive to buy/maintain and there are no requirements to decide for a FIPS 140-2 level 2 or level 3 HSM. Since a closed network is used that mitigates threats effectively, it is decided not to use an HSM initially. If an HSM is necessary e.g. to obtain accreditation, it can be added to the architecture.

3. Technical conditions of the data exchange

3.1 General description of the EUCARIS application

3.1.1 Overview

The Eucaris application connects all participating Member States in a mesh network where each Member State communicates directly to another Member State. There is no central component needed for the communication to be established. The Eucaris application handles secure communication to the other Member States and communicates to the back-end legacy systems of Member States using XML. The following picture visualizes this architecture.



Member State exchange messages by directly sending them to the recipient. The data center of a Member State is connected to the network used for the message exchange (TESTA). To access the TESTA network, Member States connect to TESTA via their national gate. A firewall shall be used to connect to the network and that a router connects the Eucaris application to the firewall. Depending on the alternative chosen to protect the messages, a certificate is used either by the router or by the Eucaris application.

A client application is provided which can be used within a Member State to query its own register or other Member States' registers. The client application connects to Eucaris. The clients will be identified by means of user-id/password or a client certificate. The connection to a user in an external organization (e.g. police) may be encrypted but this is the responsibility of each individual Member State.

3.1.2 Scope of the system

The scope of the Eucaris system is limited to the processes involved in the exchange of information between the Registration Authorities in the Member States and a basic presentation of this information. Procedures and automated processes in which the information is to be used, are outside the scope of the system.

Member States can choose either to use the Eucaris client functionality or to set up their own customized client application. In the table below, it is described which aspects of the Eucaris system are mandatory to use and/or prescribed and which are optional to use and/or free to determine by the Member States.

EUCARIS aspects	**M/O** [1]	**Remark**
Network concept	M	The concept is an "any-to-any" communication.
Physical network	M	TESTA
Core application	M	The core application of EUCARIS has to be used to connect to the other Member States. The following functionality is offered by the core: ▪ Encrypting and signing of the messages; ▪ Checking of the identity of the sender; ▪ Authorization of Member States and local users; ▪ Routing of messages; ▪ Queuing of asynchronous messages if the recipient service is temporally unavailable; ▪ Multiple country inquiry functionality;

[1] M = mandatory to use or to comply with O = optional to use or to comply with

EUCARIS aspects	M/O [1]	Remark
		▪ Logging of the exchange of messages; ▪ Storage of incoming messages
Client application	O	In addition to the core application the EUCARIS II client application can be used by a Member State. When applicable, the core and client application are modified under auspices of the EUCARIS organisation.
Security concept	M	The concept is based on XML-signing by means of client certificates and SSL-encryption by means of service certificates.
Message specifications	M	Every Member State has to comply with the message specifications as set by the EUCARIS organisation and this Council Decision. The specifications can only be changed by the EUCARIS organisation in consultation with the Member States.
Operation and Support	M	The acceptance of new Member States or a new functionality is under auspices of the EUCARIS organisation. Monitoring and help desk functions are managed centrally by an appointed Member State.

3.2 Functional and Non Functional Requirements

3.2.1 Generic functionality

In this section the main generic functions have been described in general terms.

Nr.	Description
1.	The system allows the Registration Authorities of the Member States to exchange request and response messages in an interactive way.
2.	The system contains a client application, enabling end-users to send their requests and presenting the response information for manual processing
3.	The system facilitates 'broadcasting', allowing a Member State to send a request to all other Member States. The incoming responses are consolidated by the core application in one response message to the client application (this functionality is called a 'Multiple Country Inquiry').
4.	The system is able to deal with different types of messages. User roles, authorization, routing, signing and logging are all defined per specific service.
5.	The system allows the Member States to exchange batches of messages or messages containing a large number of requests or replies. These messages are dealt with in an asynchronous way.
6.	The system queues asynchronous messages if the recipient Member State is temporarily unavailable and guarantees the deliverance as soon as the recipient is up again.
7.	The system stores incoming asynchronous messages until they can be processed.
8.	The system only gives access to Eucaris applications of other Member States, not to individual organisations within those other Member States, i.e. each Registration Authority acts as the single gateway between its national end-users and the corresponding Authorities in the other Member States.
9.	It is possible to define users of different Member States on one Eucaris server and to authorize them following the rights of that Member State.
10.	Information on the requesting Member State, organisation and end user are included in the messages.
11.	The system facilitates logging of the exchange of messages between the different Member States and between the core application and the national registration systems.

Nr.	Description
12.	The system allows a specific secretary, which is an organisation or Member State explicitly appointed for this task, to gather logged information on messages sent/received by all the participating Member States, in order to produce statistical reports.
13.	Each Member State indicates itself what logged information is made available for the secretary and what information is 'private'.
14.	The system allows the National Administrators of each Member State to extract statistics of use.
15.	The system enables addition of new Member States through simple administrative tasks.

3.2.2 Usability

Nr.	Description
16.	The system provides an interface for automated processing of messages by back-end systems/legacy and enables the integration of the user interface in those systems (customised user-interface).
17.	The system is easy to learn, self explanatory and contains help-text.
18.	The system is documented to assist Member States in integration, operational activities and future maintenance (e.g. reference guides, functional/technical documentation, operational guide,….).
19.	The user interface is multi-lingual and offers facilities for the end-user to select a preferred language.
20.	The user interface contains facilities for a Local Administrator to translate both screen-items and coded information to the national language.

3.2.3 Reliability

Nr.	Description
21.	The system is designed as a robust and dependable operational system which is tolerant to operator errors and which will recover cleanly from power cuts or other disasters. It must be possible to restart the system with no or minimal loss of data.
22.	The system must give stable and reproducible results.
23.	The system has been designed to function reliably. It is possible to implement the

Nr.	Description
	system in a configuration that guarantees an availability of 98% (by redundancy, the use of back-up servers etc.) in each bilateral communication.
24.	It is possible to use part of the system, even during failure of some components (if Member State C is down, Member States A and B are still able to communicate). The number of single points of failure in the information chain should be minimised.
25.	The recovery time after a severe failure should be less than one day. It should be possible to minimise down-time by using remote support e.g. by a central service desk.

3.2.4 Performance

Nr.	Description
26.	The system can be used 24x7. This time-window (24x7) is then also required from the Member States' legacy systems.
27.	The system responds rapidly to user requests irrespective of any background tasks. This is also required from the Parties legacy systems to ensure acceptable response time. An overall response time of 10 seconds maximum for a single request is acceptable.
28.	The system has been designed as a multi-user system and in such a way that background tasks can continue while the user performs foreground tasks.
29.	The system has been designed to be scaleable in order to support the potential increase of number of messages when new functionality is added or new organisations or Member States are added.

3.2.5 Security

Nr.	Description
30.	The system is suited (e.g. in its security measures) for the exchange of messages containing privacy-sensitive personal data (e.g. car owner/holders), classified as EU restricted.
31.	The system is maintained in such a way that unauthorised access to the data is prevented.
32.	The system contains a service for the management of the rights and permissions of

Nr.	Description
	national end-users.
33.	Member States are able to check the identity of the sender (at Member State level), by means of XML-signing.
34.	Member States must explicitly authorise other Member States to request specific information.
35.	The system provides at application level a full security and encryption policy compatible with the level of security required in such situations. Exclusiveness and integrity of the information is guaranteed by the use of XML-signing and encryption by means of SSL-tunnelling.
36.	All exchange of messages can be traced by means of logging.
37.	Protection is provided against deletion attacks (a third party deletes a message) and replay or insertion attacks (a third party replays or inserts a message).
38.	The system makes use of certificates of a Trusted Third Party (TTP).
39.	The system is able to handle different certificates per Member State, depending on the type of message or service.
40.	The security measures at application level are sufficient to allow the use of non accredited networks.
41.	The system is able to use novice security techniques such as an XML-firewall.

3.2.6 Adaptability

Nr.	Description
42.	The system is extensible with new messages and new functionality. The costs of adaptations are minimal. Due to the centralised development of application components.
43.	Member States are able to define new message types for bilateral use. Not all Member States are required to support all message types.

3.2.7 Support and Maintenance

Nr.	Description
44.	The system provides monitoring facilities for a central service-desk and/or operators concerning the network and servers in the different Member States.
45.	The system provides facilities for remote support by a central service-desk.

Nr.	Description
46.	The system provides facilities for problem analysis.
47.	The system can be expanded to new Member States.
48.	The application can easily be installed by staff with a minimum of IT-qualifications and experience. The installation procedure shall be as much as possible automated.
49.	The system provides a permanent testing and acceptance environment.
50.	The annual costs of maintenance and support has been minimised by adherence to market standards and by creating the application in such a way that as little support as possible from a central service-desk is required.

3.2.8 Design requirements

Nr.	Description
51.	The system is designed and documented for an operational lifetime of many years.
52.	The system has been designed in such a way that it is independent of the network provider.
53.	The system is compliant with the existing HW/SW in the Member States by interacting with those registration systems using open standard web service technology (XML, XSD, SOAP, WSDL, HTTP(s), Web services, WSS, X.509 etc.).

3.2.9 Applicable standards

Nr.	Description
54.	The system is compliant with data protection issues as stated in Regulation EC 45/2001 (Articles 21, 22 & 23) and Directive 95/46/EC.
55.	The system complies with the IDA Standards.
56.	The system supports UTF8.

Chapter 4: Evaluation

1. Evaluation procedure according to Article 20 (Preparation of Decisions according to Article 25(2) of Decision 2008/…/JHA)

1.1 Questionnaire

The relevant Council Working Group shall draw up a questionnaire concerning each of the automated data exchanges set out in Chapter 2 of Decision 2008/…/JHA.

As soon as a Member State believes it fulfils the prerequisites for sharing data in the relevant data category, it shall answer the relevant questionnaire.

1.2 Pilot run

With a view to evaluating the results of the questionnaire, the Member State that wishes to start sharing data shall carry out a pilot run together with one or more other Member States already sharing data under the Council Decision. The pilot run takes place shortly before or shortly after the evaluation visit.

The conditions and arrangements for this pilot run will be identified by the relevant Council Working Group and be based upon prior individual agreement with the concerned Member State. The Member States taking part in the pilot run will decide on the practical details.

1.3 Evaluation visit

With a view to evaluating the results of the questionnaire, an evaluation visit shall take place in the Member State that wishes to start sharing data.

The conditions and arrangement for this visit will be identified by the relevant Working Group and be based upon prior individual agreement between the concerned Member State and the evaluation team. The concerned Member State will enable the evaluation team to check the automated exchange of data in the data category or categories to be evaluated, in particular by organizing a programme for the visit which takes into account the requests of the evaluation team.

Within one month, the evaluation team will produce a report on the evaluation visit and will forward it to the Member State concerned for its comments. If appropriate, this report will be revised by the evaluation team on the basis of the Member State's comments.

The evaluation team will consist of no more than 3 experts, designated by the Member States taking part in the automated data exchange in the data categories to be evaluated, who have experience regarding the concerned data category, have the appropriate national security clearance to deal with these matters and are willing to take part in at least one evaluation visit in another Member State. The Commission will be invited to join the evaluation team as observer.

The members of the evaluation team will respect the confidential nature of the information they acquire when carrying out their task.

1.4 Report to the Council

An overall evaluation report, summarising the results of the questionnaires, the evaluation visit and the pilot run, will be presented to the Council for its decision pursuant to Article 25(2) of Decision 2008/.../JHA.

2. Evaluation procedure according to Article 21

2.1 Statistics and report

Each Member State will compile statistics on the results of the automated data exchange. In order to ensure comparability, the model for statistics will be compiled by the relevant Council Working Group.

These statistics will be forwarded annually to the General Secretariat, which will produce a summary overview for the elapsed year, and to the Commission.

In addition, Member States will be requested on a regular basis not to exceed once per year further information on the administrative, technical and financial implementation of automated data exchange as needed to analyse and improve the process. On the basis of this information, a report will be produced for the Council.

2.2 Revision

Within reasonable time, the Council will examine the evaluation mechanism described here and revise it as necessary.

3. Expert meetings

Within the relevant Council Working Group, experts will meet regularly to organise and implement the above-mentioned evaluation procedures as well as to share experience and discuss possible improvements. Where applicable, the results of these expert discussions will be incorporated into the report referred to in 2.1 above.