



2026/1064

10.6.2026

COMMISSION IMPLEMENTING DECISION (EU) 2026/1064

of 8 June 2026

laying down rules for the application of Regulation (EU) 2024/982 of the European Parliament and of the Council as regards the automated search and exchange of biometric data through the Prüm router

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2024/982 of the European Parliament and of the Council of 13 March 2024 on the automated search and exchange of data for police cooperation, and amending Council Decisions 2008/615/JHA and 2008/616/JHA and Regulations (EU) 2018/1726, (EU) 2019/817 and (EU) 2019/818 of the European Parliament and of the Council (the Prüm II Regulation) ⁽¹⁾, and in particular Article 5(3), Article 8(2) and (3), Article 9(3), Article 13(2) and (3), Article 14(2), Article 22(2) and (3), Article 23(2), Article 31 and Article 37(6) thereof,

Whereas:

- (1) Regulation (EU) 2024/982 establishes a framework for the automated search and exchange of certain categories of data for cross-border police cooperation, including the automated exchange of biometric data among Member States and Europol to prevent and combat cross-border crime.
- (2) Pursuant to Regulation (EU) 2024/982, the Commission is to specify the technical rules for automated search and exchange of biometric data, namely DNA profiles, dactyloscopic data and facial images, to be done via the Prüm router.
- (3) It is therefore necessary to define the technical standards, procedures and specifications for the operation of the Prüm router and the associated services to enable eu-LISA to define the design of the router, as well as to elaborate the technical specifications, testing and overall project management and coordination.
- (4) The effective exchange of biometric data requires standardised formats, unique identifiers and harmonised protocols for DNA profiles, dactyloscopic data, and facial images. The use of internationally recognised standards should ensure interoperability and compatibility among Member States' systems and with Europol. The relevant technical rules set out the entity codes, message structures, data payloads, and routing mechanisms to guarantee consistent and accurate automated processing.
- (5) The exchange of sensitive biometric data should be protected against unauthorised access, tampering, or loss and the Prüm router should operate as a high-availability system with redundancy across primary and backup sites. It is therefore necessary to define secure communication protocols, automated retry mechanisms and monitoring procedures. Such protocols, mechanisms and procedures should ensure system reliability, timely responses, and error handling for uninterrupted cross-border data exchange.
- (6) The exchange of DNA profiles, dactyloscopic data and facial images should comply with minimum quality standards to allow reliable identification and verification. Automated matching procedures should be complemented by manual forensic review for confirmation of matches and core data requests. It is therefore essential to establish technical rules governing profile formats, resolution, loci matching, candidate ranking, re-matching procedures and reporting. That should ensure that the data exchanged can be accurately interpreted and used for criminal investigations in accordance with Regulation (EU) 2024/982.
- (7) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2024/982 and is not bound by it or subject to its application. Denmark is therefore not bound by this Decision or subject to its application.
- (8) Ireland is bound by Regulation (EU) 2024/982 and is therefore bound by this Decision.

⁽¹⁾ OJ L, 2024/982, 5.4.2024, ELI: <http://data.europa.eu/eli/reg/2024/982/oj>.

- (9) The Prüm router contributes to the provision of a cross-border digital public service. As this Decision introduces binding requirements affecting its development, an interoperability assessment is required under Article 3 of Regulation (EU) 2024/903 of the European Parliament and of the Council ⁽²⁾ (Interoperable Europe Act). The assessment has been carried out, and the resulting report will be published on the Interoperable Europe Portal.
- (10) The European Data Protection Supervisor delivered an opinion on 27 January 2026.
- (11) The measures provided for in this Decision are in accordance with the opinion of the Prüm II Committee, established by Article 77 of Regulation (EU) 2024/982,

HAS ADOPTED THIS DECISION:

Article 1

For the purposes of this Decision, the following definitions apply:

- (a) 'entity' means either a Member State or Europol;
- (b) 'requesting entity' means a Member State or Europol that initiates a query;
- (c) 'requested entity' means a Member State or Europol that receives a query and initiates a response;
- (d) 'transaction' means one query transaction and its corresponding response transaction(s);
- (e) 'quota point' means a point used for each transaction received, processed and replied by the requested entity;
- (f) 'partial locus' means a locus with only one filled allele;
- (g) 'mugshot image' means a facial image taken in a controlled environment;
- (h) 'trace image' means a facial image taken in an uncontrolled environment;
- (i) 're-matching' means the task performed by the router for homogeneously ranking the candidates by comparing the biometric data used for querying and the biometric data supplied in the response transactions by the requested entities, in accordance with Article 37(4) of Regulation (EU) 2024/982.

Article 2

The specifications relating to the technical rules for the automated search and exchange of biometric data via the Prüm router shall be as set out in the Annex.

Article 3

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 8 June 2026.

For the Commission
The President
Ursula VON DER LEYEN

⁽²⁾ Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, ELI: <http://data.europa.eu/eli/reg/2024/903/oj>).

ANNEX

Technical rules for the automated search and exchange of biometric data via the Prüm router as referred to in Article 2

CHAPTER 1: Router

1. Entity code table

The requesting and requested entities are identified by a two-letter code from ISO 3166. Where the entity has no reserved ISO-code, this document defines one in Table 1.

Table 1

List of entity codes used in Prüm II automated exchanges

Entity name	Code
Austria	AT
Belgium	BE
Bulgaria	BG
Cyprus	CY
Czechia	CZ
Germany	DE
Estonia	EE
Spain	ES
Finland	FI
France	FR
Greece	GR
Croatia	HR
Hungary	HU
Ireland	IE
Italy	IT
Lithuania	LT
Luxembourg	LU
Latvia	LV
Malta	MT
Netherlands	NL
Poland	PL
Portugal	PT
Romania	RO
Sweden	SE
Slovenia	SI
Slovakia	SK
EU router	EU
Europol	EP

2. Technical procedure for the router to query Member States' databases and Europol data

The router shall use the TESTA Eurodomain ⁽¹⁾ or its subsequent implementations to exchange data with the entities. The router and entities exchange data via asynchronous transactions over webservices. All transactions between all entities shall be defined by eu-LISA.

The webservices shall be based on the same communication protocols and message format in use by the European Search Portal (ESP). Webservices shall be implemented by all entities to process the following transactions:

- (a) First step query from the requesting entity via the router to one or more requested entities
 - (1) DNA query
 - (2) Dactyloscopy query
 - (3) Facial image query
- (b) First step response from one or more requested entities via the router to the requesting entity
 - (1) DNA response
 - (2) Dactyloscopy response
 - (3) Facial image response
- (c) Second step request for core data from the requesting entity via the router to the requested entity
 - (1) DNA core data request
 - (2) Dactyloscopy core data request
 - (3) Facial image core data request
- (d) Second step core data response from the requested entity via the router to the requesting entity
 - (1) DNA core data response
 - (2) Dactyloscopy core data response
 - (3) Facial image core data response

The webservices shall communicate with corresponding services in the router in order to correctly process and route the data to the other entities.

Each webservice may be accessible via a specific IP-addressing scheme to cater for situations where several different authorities are involved in the exchange.

Webservices may be combined into one or more national contact points.

For each transaction, a specific routing envelope shall be defined by eu-LISA.

The routing envelope shall contain the following routing information:

- the requesting entity;
- the requested entities;
- the type of transaction for the query and the Transaction Query Code (TQC);
- the type of transaction for the response and the Transaction Response Code (TRC);
- the type of transaction for the re-matching option, if asked for by requesting entity; this routing information is not applicable to DNA profiles;
- the number of candidates requested.

The routing envelope may contain additional routing information, such as the optional features and the anonymous data necessary for the creation of statistics as defined in Section 5.4.

⁽¹⁾ The TESTA Eurodomain is a secure, private, EU-wide network that enables encrypted and reliable data exchange between EU institutions, Member States' authorities and agencies, specifically for sensitive information like law enforcement and justice data.

Within the routing envelope, the actual data payload shall be inserted.

The data-payload shall be defined by eu-LISA. The requesting entity shall ensure that the data payload is correctly formatted. The requested entity shall ensure that the response is correctly formatted.

In case of re-matching, the router shall validate the data payload. In all other cases, the router shall not validate the data payload.

The requested entity shall validate the data payload to ensure it can be processed correctly.

If the requested entity is unable to process the data payload correctly, an error-transaction message shall be sent back to the requesting entity through the router. The format and details of that standardised error-transaction message shall be defined by eu-LISA. It shall contain error-codes related to the requested entity and the router.

3. The format of the router replies and the process

Each transaction sent to a query webservice ('query transaction') shall be identified by a Transaction Query Code (TQC) consisting of the requesting entity's two-letter code followed by a unique code consisting of the date and time of the query and the query number.

Each transaction sent to a response webservice ('response transaction') shall reference the TQC from the query transaction.

Each response transaction from the requested entities shall be identified by a Transaction Response Code (TRC) consisting of the requested entity's two-letter code followed by a unique code consisting of the date and time of the response and the response number.

The format and details of TQC and TRC shall be defined by eu-LISA.

Where the router receives a response transaction, that response transaction shall be returned per requested entity to the requesting entity. It shall reference the TQC from the original query transaction and the TRC from the response transaction. In case the router declares a timeout, the TRC shall be generated by the router, according to the format that will be set out by eu-LISA. Any responses received by the router, after the router has declared a timeout for a specific transaction, shall be deleted by the router.

Each transaction shall be acknowledged by the corresponding web service.

Within each query transaction, each biometric reference data (DNA reference data, dactyloscopic reference data or facial image reference data) is uniquely labelled with a Data Reference Number (DRN) created by the requesting entity, in accordance with Articles 7, 12 and 21 of Regulation (EU) 2024/982.

Within each response transaction, each matching biometric data (DNA profiles, dactyloscopic data or facial images) is uniquely labelled with a DRN created by the requested entity, in accordance with Articles 9, 15 and 24 of Regulation (EU) 2024/982. The format and details of the DRN shall be decided by the entities.

These DRN shall uniquely identify the biometric data and shall be used when requesting the core data.

4. Re-matching option: technical rules for comparing and ranking the candidates between biometric data

In accordance with Article 37(4) of Regulation (EU) 2024/982, for dactyloscopic data and facial images query transactions, the requesting entity may ask the router, per transaction, to perform a re-matching comparison between its biometric data and biometric data received from the requested entities.

The re-matching shall be performed by the biometric re-matcher as an isolated service on the platform also hosting the shared Biometric Matching Service (sBMS).

Regardless of whether the requesting entity has chosen the re-matching comparison or not, the requesting entity shall receive the candidate lists, including the NIST files with a complete set of dactyloscopic data or facial images of each requested entity as the router receives them from the requested entity. The router shall generate a time-out message as soon as the time-out is being detected.

4.1. Re-matching comparison for latent fingerprint to tenprint searches

When the re-matching comparison is chosen by the requesting entity for latent fingerprint to tenprint searches, the router shall temporarily retain the candidate lists received from the requested entities and shall use specific functionalities from the platform hosting the sBMS, to perform a re-matching between the latent fingerprint from the requesting entity and the candidates received from the requested entities.

The re-matching shall only take place between the latent fingerprint and the fingerprint in the tenprint set that is indicated as possible match.

The re-matching process shall create a newly ranked list of all the records received from the requested entities. This newly ranked list shall use the identifiers of the tenprint sets. The requesting entity may request all the NIST files with the tenprint fingerprint images to be forwarded as part of the newly ranked list to the requesting entity, as part of an optional parameter in the transaction envelope.

When the re-matching comparison option is activated by the requesting entity in the first query transaction, the router shall trigger the re-matching comparison on the candidates effectively received.

The newly ranked list shall indicate which requested entities have not responded within the timeout period.

4.2. Re-matching comparison for latent palmprint to palmprint searches

When the re-matching comparison is chosen by the requesting entity for latent palmprint to palmprint searches, the process described in point 4.1 shall apply.

4.3. Re-matching comparison for trace image to mugshot image searches

When the re-matching comparison is chosen by the requesting entity for trace image to mugshot image searches, the process described in point 4.1 shall apply.

5. System description

5.1. Availability of the system

A primary router will be built and managed in eu-LISA's primary site and a backup router will be built and managed in its backup site.

The primary router shall be built and managed as a high-availability system with full redundancy in eu-LISA's primary site.

All entities shall communicate with one single router, for all webservices, at any given time.

Switching all entities from the primary site to the backup site (and vice-versa) shall be supported by automated mechanisms, implemented by all entities and based on the status of the router-sites that will be decided by eu-LISA.

The webservices on the router are not implemented to guarantee persistency of received data across sites. Any transaction is 'fixed' to complete within one specific router. When the primary router becomes unavailable, the entities are informed automatically, based on a decision by eu-LISA, and subsequent transactions shall be directed to the backup site router. Any ongoing transactions not yet fully completed in the primary router, shall be considered as lost and shall result in timeout.

Each client of a webservice, being a requesting entity, a requested entity or the router itself, shall implement an automated retry-mechanism. Should the corresponding service not be available, the client and router shall re-try until a time-out was reached. The time-out value shall be specific for each webservice and for each entity and shall be defined by eu-LISA.

Each entity shall implement error-handling within its own webservices to allow this entity a complete overview of their own unsuccessful incoming and outgoing transactions.

The router webservices shall implement an error-handling and reporting mechanism, based on technical acknowledgements received or not received from the entities, which shall allow eu-LISA to be informed of any entity's webservices not being available. Eu-LISA shall contact the entity which has a webservice that was consistently unavailable for a longer period. Eu-LISA shall also contact the entity that consistently leads to timeouts in the router.

The router shall provide for a system-to-system transaction enabling to regularly and automatically query the actual status of availability of the webservices at the various entities. All entities may query the collected health statuses via a webservice provided by the router.

Where a client request terminated with a time-out, the requesting entity shall be informed and shall need to decide to re-do the specific transaction to the requested entity that was unable to complete the previous transaction. The requested entity shall be informed of the incomplete transactions which shall not be deducted from the daily quota by the requested entity.

5.2. Automated searching (query and response)

For the automated searching of DNA profiles in accordance with Article 6(2) and (3) of Regulation (EU) 2024/982, for the automated searching of dactyloscopic data in accordance with Article 11(1) of Regulation (EU) 2024/982 and for the automated searching of facial images in accordance with Article 20(1) of Regulation (EU) 2024/982, queries shall be processed by a fully automated procedure. For the kinship matching on DNA profiles, queries shall be processed by a semi-automated procedure.

The process of automated searching of DNA profiles is described in Chapter 2. The process of automated searching of dactyloscopic data is described in Chapter 3. The process of automated searching of facial images is described in Chapter 4.

If a requesting entity sends a query transaction which is not supported by the requested entity, a business message shall be sent back to the requesting entity informing that the requested transaction is not supported by the requested entity.

Each DNA profile query transaction, from a requesting entity to one requested entity or more requested entities via the router, may contain up to 500 profiles. The corresponding response transaction, from the requested entity to the requesting entity via the router shall then contain none, one or more matching candidates for each queried profile.

5.3. Core data exchange (query and response)

In accordance with Article 6(6) and (7), Article 11(2) and Article 20(2) of Regulation (EU) 2024/982, after the requesting entity has received the replies from the router, it may decide to confirm a match between two biometric data. Where the requesting entity decides to confirm a match, it shall manually review the results in order to confirm a match.

Via a single transaction through the router, the requesting entity shall inform the requested entity about the confirmed match and shall transmit a description of the facts and an indication of the underlying offence using the common table of offence categories as set out in the implementing act adopted pursuant to Article 11b(1)(a) of Council Framework Decision 2009/315/JHA ⁽²⁾. The router shall standardise this transmission with the codes of the common table of offence categories.

The requesting entity shall send the Transaction Query Code (TQC), the Transaction Response Code (TRC) and the Data Reference Number (DRN) of the matching biometric data received from the requested entity to the requested entity owning this data. The combination of these three codes is unique and may be used by the requested entity to verify accurateness of the core data request.

The requested entity shall use the DRN to gather the core data of the biometric data record that was identified as a potential match. The requested entity shall send the core data back to the requesting entity within 48 hours in accordance with Article 47(1) of Regulation (EU) 2024/982.

⁽²⁾ Council Framework Decision 2009/315/JHA of 26 February 2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States (OJ L 93, 7.4.2009, p. 23, ELI: http://data.europa.eu/eli/dec_framw/2009/315/oj).

In accordance with Article 47, once a match has been manually confirmed and a description of the facts and an indication of the underlying offence have been transmitted by the requesting entity, a set of core data shall be returned by the requested entity via the router within 48 hours. The return of a core data does not apply where a search by a requested Member State resulted in a match against third country data provided by Europol. In this case, the follow-up shall take place in accordance with Regulation (EU) 2016/794 of the European Parliament and of the Council ⁽³⁾.

The requested entity shall indicate in the response if it gives to the requesting entity its prior authorisation to process the biometric data and the core data provided, for other purposes in accordance with Article 50(1) of Regulation (EU) 2024/982.

In accordance with Article 6(7) of Regulation (EU) 2024/982, the requested entity may also decide to confirm a match between two DNA profiles. Where the requested entity decides to confirm a match, it shall manually review the results in order to confirm a match and initiate an independent and unsolicited transaction via the router to the requesting entity in order to request the core data. The same core data exchange procedure applies in this case.

The core data structure shall follow the Universal Message Format (UMF). The technical specifications of the core data exchange shall be defined by eu-LISA.

In case: (i) the requested entity cannot send the core data following the assessment of the proportionality of the request in accordance with Article 47(1), point (c), of Regulation (EU) 2024/982; or (ii) the judicial authorisation was denied in accordance with Article 47(2) of Regulation (EU) 2024/982; or (iii) the requested entity has another DNA profile in the national database corresponding to the same person containing additional loci which disconfirm the match in accordance with Chapter 2 Part 5, the requesting entity shall be informed through the router.

5.4. Statistics

The router shall analyse the routing envelope of the incoming and outgoing transactions, both ways, from requesting and requested entities, in order to extract statistics.

The router shall be able to extract a combination of anonymised data from this routing envelope to forward to the central repository for reporting and statistics (CRRS) in order to create the following statistics:

- (a) Number of outgoing queries per requesting entity and per data category, by priority indicator (if relevant) and with timing information
- (b) Number of requested entities per outgoing request (per requesting entity)
- (c) Number of unique DNA reference data per query transaction (only DNA profile)
- (d) Activated options for the outgoing request (per requesting entity)
- (e) Number of incoming replies from requested entities, with timing information
- (f) Number of candidates asked for by requesting entities and per data category
- (g) Number of candidates in the responses from requested entities and per data category
- (h) Number of matches per response transaction (only DNA profile)
- (i) Number of confirmed matches where there were exchanges of core data
- (j) Number of confirmed matches where there were no exchanges of core data
- (k) Comparison of ranking by the requested entities compared to new ranking by re-matching
- (l) Number of core data requests, per requesting and per requested entity, and per data category, correlated with the first query and response and with timing information
- (m) Number of core-data responses, per requested entity and per data category, with timing information
- (n) Number of core-data responses per type of criminal offence
- (o) Number of queries to the Common Identity Repository via the router

⁽³⁾ Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53, ELI: <http://data.europa.eu/eli/reg/2016/794/oj>).

- (p) Number of matches per type as follows:
- (1) identified data (person) – unidentified data (trace);
 - (2) unidentified data (trace) – identified data (person);
 - (3) unidentified data (trace) – unidentified data (trace);
 - (4) identified data (person) – identified data (person).

5.5. Protocols and standards to be used for encryption mechanism

The Mutual Transport Layer Security (mTLS) protocol shall be used to authenticate every single server hosting any part of a webservice, in all environments made available. Where entities host webservices on different servers, separate certificates shall be provided for each server. The security certificates shall be generated and managed by eu-LISA.

CHAPTER 2: Exchange of DNA profiles

1. Properties of DNA profiles and relevant European or international standards for DNA profiles exchange

Member States shall exchange all the loci of the profile, according to their national legislation.

The DNA profile may contain all the pairs of values available representing the alleles of autosomal loci, the partial loci, amelogenin and the Y-STR loci.

The names of these loci are shown in the following two tables:

(a) List of loci of the European Standard Set (ESS)

VWA	TH01	D21S11	FGA	D8S1179	D3S1358
D18S51	D1S1656	D2S441	D10S1248	D12S391	D22S1045

The twelve loci are the present European Standard Set (ESS) as defined in the Council Resolution 2009/C 296/01 ⁽⁴⁾. The automated exchange of DNA profiles shall consider any new development of the ESS.

(b) Non-exhaustive list of loci that can be exchanged

Amelogenin	All Y-STR loci	TPOX	CSF1P0	D13S317	D7S820	D5S818	D16S539
D2S1338	D19S433	Penta D	Penta E	SE33	D6S1043	D6S474	D1S1677
D2S1776	D3S4529	D4S2408	D5S2800	D12ATA63	D14S1434	D17S1301	D20S482
D9S1122	CD4	FES	F13A1	F13B	GABA		

In addition, amelogenin and all Y-STR loci may be exchanged. They are not compared but they may be used as additional information for the forensic verification of a match.

Member States may extract and exchange any other type of autosomal loci not listed in the tables. Where information from additional loci than the ESS loci is available, Member States are urged to provide this when exchanging DNA profiles. The number of loci to be exchanged shall not be limited.

Member States shall use DNA kits that analyse at least the ESS loci. When establishing a profile, the analysis shall cover all ESS loci in force at the time of the analysis.

The data interchange specifications shall be defined by eu-LISA.

⁽⁴⁾ Council Resolution of 30 November 2009 on the exchange of DNA analysis results (OJ C 296, 5.12.2009, p. 1).

The data subject categories shall be harmonized with ISO/IEC 19794-14 where possible:

- P = identified person;
- S = unidentified stain;
- U = unidentified human remains;
- M = missing person;
- K = kinship missing person.

An identified DNA profile corresponds to the profiles of 'identified person' (P) and 'kinship missing person' (K).

An unidentified DNA profile corresponds to the profiles of 'unidentified stain' (S), 'unidentified human remains' (U) and 'missing person' (M).

Table 2

Search matrix defining which type of DNA profiles are searched against each other

DNA profiles matching by category	P	S	U	M	K
P	Yes	Yes	Yes	Yes	No
S	Yes	Yes	Yes	Yes	No
U	Yes	Yes	Yes	Yes	Yes
M	Yes	Yes	Yes	Yes	Yes
K	No	No	Yes	Yes	No

Profiles of kinship missing person (K) shall only be matched against profiles of unidentified human remains (U) or missing persons (M).

The unidentified human remains profile (U) shall also be matched against identified profiles (P) and unidentified profiles (S+U+M).

2. Minimum quality standards

For the automated searching of DNA profiles in accordance with Article 6(1) of Regulation (EU) 2024/982, all DNA profiles shall be compared in the first automated search at the time of initial connection to the router.

For the automated searching of DNA profiles in accordance with Article 6(2) and (3) of Regulation (EU) 2024/982, the new DNA profiles exchanged shall respect the following quality standards.

The quality standards for identified DNA profiles are differentiated from those for unidentified DNA profiles.

The quality standards only apply to DNA profiles exchanged under Regulation (EU) 2024/982 and sent by the requesting entities for automated exchanges. They do not apply to the storage of DNA profiles in the national database.

The identified DNA profiles (P) shall contain at least 10 full designated autosomal loci including 8 ESS loci and 2 additional full designated loci.

The unidentified DNA profiles (S, U and M) shall contain at least 6 full designated autosomal loci. The unidentified DNA profiles do not have to contain any minimal number of ESS loci.

The DNA profiles not respecting the quality standards cannot be sent for comparison. However, they can be made available for matching against profiles received from requesting entities. A list of entities using this possibility shall be included in Prüm handbook.

In order to raise the accuracy of matches, all available alleles shall be stored in the indexed DNA profile database and be used for comparison and verification. Each Member State should implement as soon as practically possible any new ESS loci adopted by the EU.

Rare allele values mean existing values outside from DNA kit predefined different ladder values. These existing values shall be shared as such without being transformed in a wild card (*).

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

For the order of allele values of a locus, a lower valued allele should be put at the first position and the higher one at the second position. A dot must be used as delimiter of micro variant allele values.

In partial locus, empty spaces (blanks) should be left as they are, i.e. no substitute.

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

- A wild card cannot substitute a missing value or 'empty space' in DNA profiles.
- More than one wildcard may be used in a DNA profile.
- Match engine should be implemented, so that both positions of the numerical values will be checked, i.e. to allow permutation check.
- Any non-numeric allele values, except amelogenin, is excluded.
- Tri-allelic values: A tri-allelic valued locus, especially of a reference profile, mostly indicates a case of rare value. The tri-allelic loci of a stain profile may contradict this assertion. The first allele will be accepted and other two alleles shall be automatically converted for the export to a wild card (*) and searched against all. Applications at national sites should do this conversion before a tri-allelic locus will be included into the indexed DNA database.
- Homozygosity: In the case of homozygosity a blank allele space has to be substituted by the same value of the other allele of the locus. In consideration of the CODIS system, a locus, e.g., with a value pair of 'a', " shall be transformed into the value pair of 'a', 'a' before being put into the DNA indexed database for search and comparison by other Member States.
- 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),
- Microvariant Tolerance Equations (MTE):
 - (1) Pentanucleotide (e.g. Penta D and Penta E) micro-variants will be matched according to the following:
 - $x = (x-1).4, x, x.1$
 - $x.1 = x, x.1, x.2$
 - $x.2 = x.1, x.2, x.3$
 - $x.3 = x.2, x.3, x.4$
 - $x.4 = x.3, x.4, x + 1$
 - (2) Trinucleotides (e.g. D22S1045) micro-variants will be matched according to the following:
 - $x = (x-1).2, x, x.1$
 - $x.1 = x, x.1, x.2$
 - $x.2 = x.1, x.2, x+1$
 - (3) Tetranucleotide (the rest of the loci are mostly tetranucleotides) micro-variants will be matched according to the following:
 - $x = (x-1).3, x, x.1$
 - $x.1 = x, x.1, x.2$
 - $x.2 = x.1, x.2, x.3$
 - $x.3 = x.2, x.3, x + 1.$

3. Matching rules (minimum number of loci)

The comparison of two DNA profiles shall be performed on the basis of the loci for which a pair of allele values is available in at least one DNA profile. For two profiles in which the same locus is partially filled, this partial locus shall not be compared jointly.

A full designated locus shall contain numerical values or a wildcard and should not contain any empty space substituting analytical voids.

The match count value shall be calculated from the matches between two full designated loci. The mismatches on full designated loci and on partial locus shall be counted for exclusion. Partial locus shall be shared as additional information for the forensic verification of a match, to determine the number of mismatches and to exclude false positives.

3.1. Regular automated matching rules

The regular automated matching rules apply to the search with the DNA profiles of 'identified person' (P), 'unidentified stain' (S), 'unidentified human remains' (U) and 'missing person' (M).

A full match (Quality 1) is defined as one where a certain number of full designated numerical loci (exclusive of amelogenin and the Y-STR loci) are matched identical, and all allele values of the compared loci (full designated and partial locus) commonly contained in the requesting and requested DNA profiles are the same.

A near match (Quality 2, 3 and 4) is defined as a match, where the value of only one of all the compared alleles is different in the two DNA profiles. A near match consists of three categories by a difference of wildcard, micro-variant or other different numerical value.

The first wildcard encountered is considered a difference. The other wild card(s) should be considered only in the case that the corresponding loci containing the further wildcard(s) are not present in the profile to be compared.

The reasons 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,
- a loci or allele dropout resulting from degraded DNA samples or a mutation,
- the use of a different analysis method,
- a false positive, some profiles are not relevant because of a low discriminating value.

There are four match quality levels defined:

- **Match Quality 1 (exact/full match):** a match of at least 6 full designated loci with all the same numerical allele values compared in both DNA profiles accepting no difference in any additional values;
- **Match Quality 2 (near match/wild card):** a match of at least 6 full designated numerical loci accepting one or more wild card(s) for the substitution of a rare allele value which is allowed in addition to the 6 full designated loci (6 full + ≥ 1 wild card);
- **Match Quality 3 (near match/micro variant):** a match of at least 6 full designated numerical loci accepting one difference in the case of micro variant which is allowed in addition to the 6 full designated loci (6 full + 1 micro variant);
- **Match Quality 4 (near match/mismatch):** a match of at least 8 full designated numerical loci accepting one difference (other than wild card or micro variant) which is allowed in addition to the 8 full designated loci (8 full + 1 difference). Only one difference value in one allele of one locus is allowed.

Entities may decide which match quality levels to verify. The matching engine user interface may be configured to only display the match quality levels that the entity wants to verify.

Two difference values in two different loci or in the same loci of a DNA profile result in a no match.

Table 3

Description of the match quality levels

Situation	Outcome	Locus 1		Locus 2		Locus 3		Locus 4		Locus 5		Locus 6		Locus 7		Locus 8		Locus 9	
		Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2
1 locus match	Non-Match	=	=	≠	≠	≠	≠	≠	≠	≠	≠	≠	≠						
2 loci match	Non-Match	=	=	=	=	≠	≠	≠	≠	≠	≠	≠	≠						
3 loci match	Non-Match	=	=	=	=	=	=	≠	≠	≠	≠	≠	≠						
4 loci match	Non-Match	=	=	=	=	=	=	=	=	≠	≠	≠	≠						
5 loci match	Non-Match	=	=	=	=	=	=	=	=	=	=	≠	≠						
>=6 loci match & >= 1 full mismatch	Non-Match	=	=	=	=	=	=	=	=	=	=	=	=	≠	≠				
6 loci match & >= 1 allele mismatch	Non-Match	=	=	=	=	=	=	=	=	=	=	=	=	≠	∅				
6 loci match & >= 1 allele mismatch	Non-Match	=	=	=	=	=	=	=	=	=	=	=	=	=	≠				
7 loci match & >= 1 allele mismatch	Non-Match	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	≠		
7 loci match & >= 1 allele mismatch	Non-Match	=	=	=	=	=	=	=	=	=	=	=	=	=	=	≠	∅		
>= 6 loci match	Q1 Match	=	=	=	=	=	=	=	=	=	=	=	=						
>= 6 loci match & >= 1 allele match	Q1 Match	=	=	=	=	=	=	=	=	=	=	=	=	=	∅				
>= 6 loci match & >= 1 allele wildcard	Q2 Match	=	=	=	=	=	=	=	=	=	=	=	=	=	*				

		Locus 1		Locus 2		Locus 3		Locus 4		Locus 5		Locus 6		Locus 7		Locus 8		Locus 9	
Situation	Outcome	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2	Allele 1	Allele 2
>= 6 loci match & = 1 allele micro-variant difference	Q3 Match	=	=	=	=	=	=	=	=	=	=	=	=	=	n.x-1 n.x+1				
>= 8 loci match & = 1 allele mismatch	Q4 Match	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	≠
>= 8 loci match & = 1 allele mismatch	Q4 Match	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	=	≠	∅

Legend	
=	equal
≠	different
∅	empty/null
*	wildcard
n.x-1 n.x+1	micro-variant difference

3.2. Matching rules for kinship matching

Entities may choose to implement kinship matching. The list of entities implementing kinship matching shall be included in the Prüm handbook.

For the kinship matching, queries shall be processed by a semi-automated procedure.

The concept of kinship matching is based on the use of a genealogy tree.

The kinship missing person profile contains and is limited to the profiles of parents of the missing person, children of the missing person, the other parent of the children of the missing person, or siblings of the missing person. The type of relationship shall be shared in the queries.

3.2.1. Kinship profile based on one profile

The kinship profile may contain one profile, either of a biological parent or a biological child, with at least 15 full designated loci. It can also contain Y-STR loci and mtDNA for the forensic verification.

The matching threshold shall be 15 full designated loci matching. In addition to the match count value, the requesting entity may calculate and use the likelihood ratio for further processing.

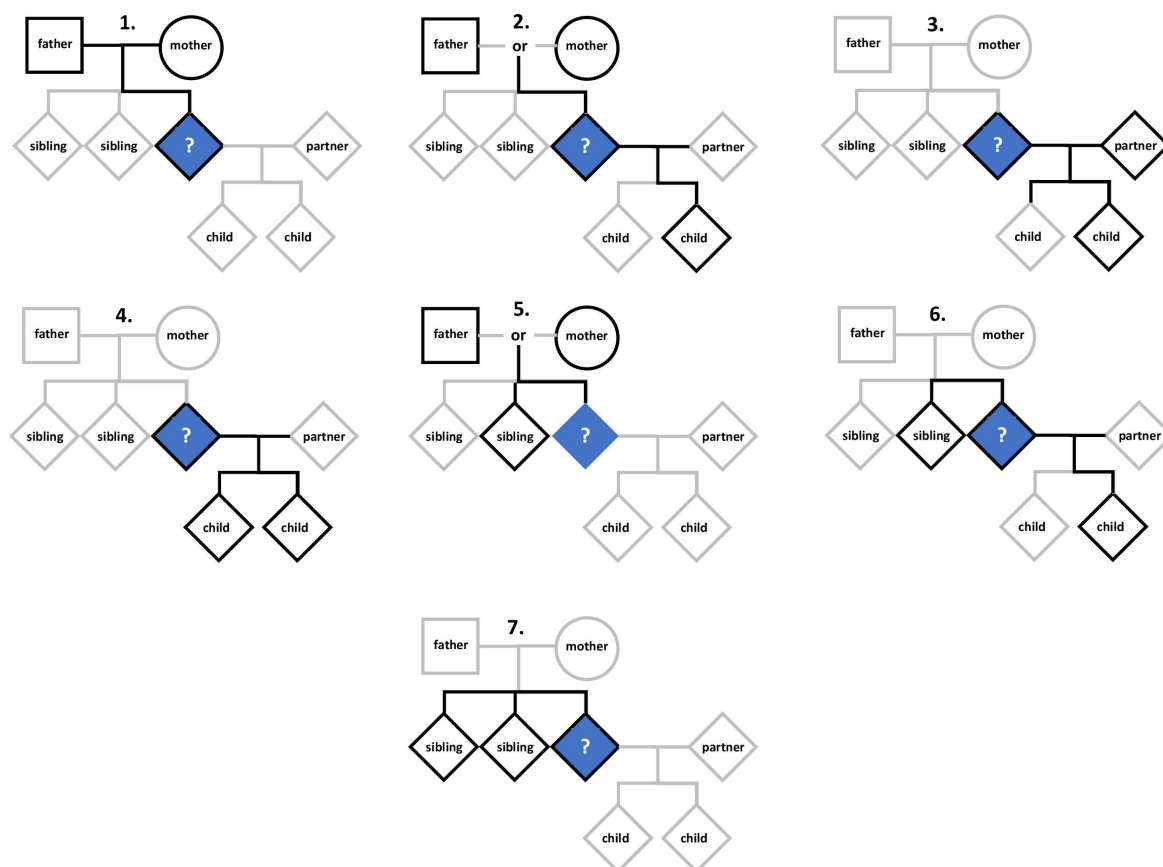
3.2.2. Kinship profile based on two or more profiles

The kinship profile may contain at least two or more profiles in the following possible combinations:

- (1) Biological father + biological mother
- (2) Biological father or mother + biological child
- (3) Biological child + the other biological parent of this child
- (4) Biological child + another biological child
- (5) Biological father or mother + biological sibling
- (6) Biological sibling + biological child
- (7) Biological sibling + another biological sibling

Table 4

Visualisation of all possible combinations



The kinship profile based on two profiles shall contain at least 15 full designated loci. It can also contain Y-STR loci and mtDNA for the forensic verification.

The matching threshold shall be 15 full designated loci matching. In addition to the match count value, the requesting entity may calculate and use the likelihood ratio for further processing.

This kinship matching does not apply to 'monozygotic twins' since the profile of the identical twin shall be directly used as the profile of the missing person.

The kinship matching applies only in these four specific cases:

- Unidentified human remains (U) against kinship missing person (K)
- Kinship missing person (K) against unidentified human remains (U)
- Missing person (M) against kinship missing person (K)
- Kinship missing person (K) against missing person (M)

The comparison of kinship missing person profiles (K) shall be limited to unidentified human remains (U) and missing persons (M) only.

The unidentified human remains profile (U) and the missing person profile (M) may be matched against kinship missing person profiles (K) where the requested Member State has adopted the required national legislation.

The kinship missing person profile (K) may be matched against unidentified human remains profiles (U) or missing person profile (M) where the requested Member State has adopted the required national legislation.

4. Reporting rules

Matches and corresponding qualities as well as no match information shall be generated by the requested entities' system and reported to the requesting entity in an automated procedure via the router. The matching report may include the calculated likelihood ratio. The matching report shall be sent to the requesting national contact point. The matching report shall 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 confirmed match.

The requesting entities shall not record DNA profiles received from requested entities in their national DNA profiles database. The requesting entities may record the DNA profile received from a requested entity solely with the prior authorisation of the Member State which provided the data in accordance with Article 50(1) of Regulation (EU) 2024/982.

5. Confirmation of the match

Only the entity wishing to obtain the core data set is required to manually review and confirm a match.

National contact points of requesting and requested entities may contact each other directly for the forensic verification.

The entity providing the core data may manually review the match in case of other DNA profiles corresponding to the same person are recorded in the national database. If a forensic verification concludes that another DNA profile corresponding to the same person contains additional loci which disconfirm the match, the entity shall inform the requesting Member State and shall not send the core data.

For matches on 8 or more full designated loci regardless of the match quality level, the request for core data shall include:

- (1) A confirmation of the manual review of the match by a qualified member of staff in accordance with Article 6(6) and (7) of Regulation (EU) 2024/982
- (2) A description of the facts and an indication of the underlying offence in accordance with Article 47(1)(c) of Regulation (EU) 2024/982

For matches on 6 full designated loci or on 7 full designated loci regardless of the match quality level, the requesting entity shall perform additional analysis of the DNA profile if possible.

If additional analysis of the DNA profile is unfeasible, the request for core data shall include:

- (1) A confirmation of the manual review of the match by a qualified member of staff in accordance with Article 6(6) and (7) of Regulation (EU) 2024/982
- (2) A description of the facts and an indication of the underlying offence in accordance with Article 47(1)(c) of Regulation (EU) 2024/982
- (3) A confirmation that a forensic accredited laboratory has verified the match (*a tick-box Yes/No*)
- (4) The name of the forensic accredited laboratory
- (5) The name of the DNA kit(s) used for the analysis of the DNA profile, the list of the confirmed matching allele values not shared in the automated exchange and any additional information not shared in the automated exchange.

The request for core data may also include the electropherogram and the calculated likelihood ratio.

CHAPTER 3: Exchange of dactyloscopic data

1. Minimum quality standards

Dactyloscopic data must have a minimum resolution of 500 dpi.

Image compression algorithm for 500 dpi images is Wavelet Scalar Quantisation (WSQ) with a maximum image compression ratio of 1:15.

Image compression format for 1 000 dpi images is JPEG 2000.

The dactyloscopic data image must be recognisable by the encoder as a dactyloscopic data image.

Latent fingerprints and latent palmprints must be of sufficient quality to allow extraction of at least 6 minutiae.

Tenprint sets shall have the correct sequence with no duplicate fingers in the set.

2. Relevant European or international standards for dactyloscopic data exchange

Dactyloscopic data shall be transferred inside a NIST file container. The NIST file shall contain fields related to dactyloscopic data and other fields for alphanumerical data, but it shall not contain fields related to facial images.

The specifications of the NIST container shall be defined by eu-LISA and based on an INTERPOL implementation. Eu-LISA shall adapt existing NIST file formats and shall support new NIST file formats to ensure the compatibility of the router to changes in the respective standards.

The NIST file format shall be verified by the entities and pass without any errors.

Eu-LISA shall provide a NIST validator tool to all entities in order to check the correct implementation of their NIST-creation-tool in their national Automated Fingerprint Identification System (AFIS).

3. Specifications for dactyloscopic data searches

The dactyloscopic data search contains eight possible transactions:

All entities shall implement the four following transactions:

- TP/TP: Tenprint to Tenprint searches;
- LT/TP: Latent fingerprint to Tenprint searches;
- TP/LT: Tenprint to Latent fingerprint searches;
- LT/LT: Latent fingerprint to Latent fingerprint searches.

Entities may implement the four other following transactions:

- PP/PP: Palmprint to Palmprint searches;
- LP/PP: Palmprint latent to Palmprint searches;
- PP/LP: Palmprint to Palmprint latent searches;
- LP/LP: Palmprint latent to Palmprint latent searches.

For each dactyloscopic data query transaction, the requesting entity may specify a number of candidates per response transaction.

The maximum number of candidates per response transaction may not be higher than 10.

The candidates shall be ranked in a list, in an automated manner, according to their matching scores by the requested entity.

The candidate list shall contain at least one fingerprint, one palmprint or one latent print image per candidate.

For a Tenprint to Tenprint transaction, the requested entity shall return candidates, up to the maximum number indicated by the requesting entity, containing a complete tenprint set of fingerprint images per candidate. The related palmprint images shall not be provided.

For a Palmprint to Palmprint transaction, the requested entity may return candidates, up to the maximum number indicated by the requesting entity, containing the palmprint images available per candidate. The palmprint that provided the highest matching score shall be clearly marked. The related fingerprint images shall not be provided.

For a Latent fingerprint to Tenprint transaction, the requested entity shall return candidates, up to the maximum number indicated by the requesting entity, containing the tenprint set of fingerprint images available per candidate. The fingerprint within the tenprint set that provided the highest matching score shall be clearly marked. If the tenprint set is not available, the matching fingerprint shall be returned. Implementation details shall be provided by eu-LISA. The related palmprint images shall not be provided.

For a Latent Palmprint to Palmprint transaction, the requested entity may return candidates, up to the maximum number indicated by the requesting entity, containing the palmprint images available per candidate. The palmprint that provided the highest matching score shall be clearly marked. The related fingerprint images shall not be provided.

For a Tenprint to latent fingerprint transaction, the requested entity shall return candidates, up to the maximum number indicated by the requesting entity, containing the latent fingerprint images available per candidate. The latent fingerprint that provided the highest matching score shall be clearly marked.

For a Palmprint to Latent Palmprint transaction, the requested entity may return candidates, up to the maximum number indicated by the requesting entity, containing the latent palmprint images available per candidate. The latent palmprint that provided the highest matching score shall be clearly marked.

For a Latent print to Latent print transaction, either fingerprint or palmprint, the requested entity shall return candidates, up to the maximum number indicated by the requesting entity, containing the latent print images available per candidate. The latent print that provided the highest matching score shall be clearly marked.

The requesting entity may specify a priority indicator for each transaction, as defined in the NIST standard. If a priority indicator is not specified, then the transaction shall be considered at the lowest priority.

The requested entity decides how to execute the priority indicator.

The types of transaction implemented by each entity shall be specified in the Prüm II practical handbook, to be adopted pursuant to Article 79 of Regulation (EU) 2024/982.

4. Quotas of transactions (maximum numbers of transactions accepted)

Each requested entity shall define for each requesting entity a maximum daily quota of dactyloscopic data transactions for the following types of transaction covering both fingerprints and palmprints:

- Print to Print searches (TP/TP; PP/PP)
- Latent to Print searches (LT/TP; LP/PP)
- Print to Latent searches (TP/LT; PP/LP)
- Latent to Latent searches (LT/LT; LP/LP)

Each entity shall keep the other entities, eu-LISA and the Commission informed about the maximum quotas for each type of transaction. Each entity may temporarily or permanently raise those search capacities at any time, including in a case of urgency.

The requested entity may reject a transaction if it exceeds the quota defined by the requested entity. The requesting entity shall be informed of this rejection via the router.

5. Distribution of unused search capacities

The requested entity may redistribute its unused incoming daily transactions to other entities in a manual or automated manner.

The router shall provide for a system-to-system transaction enabling to regularly and automatically query the real-time status of the transactions performed during a day with the remaining transactions until the maximum quota.

CHAPTER 4: Exchange of facial images

1. Minimum quality standards

The facial image transferred shall contain only one face. The image shall not contain more than one face or no face to prevent any rejection or error.

The facial image shall be pre-processed, where possible, to only show one face.

The facial image shall have sufficient image resolution and quality to be used in automated biometric matching. The required properties of the facial image shall be defined by eu-LISA.

Facial images shall be compressed with JPG (ISO/IEC 10918), JPEG 2000 (ISO/IEC 15444-1) or PNG (ISO/IEC 15948 Portable Network Graphics) image compression standards and coding system.

The facial images shall be used as they are stored in the entities' databases. Downscaling is only allowed when the resulting NIST file would exceed the maximum file size specified by eu-LISA.

The frontal mugshot image of a person used for an automated search shall have a minimum of 60 pixels inter-eye distance.

The minimum quality standard does not apply to facial images stored in the national database. It only applies to facial images used by the requesting entity to search in the requested entity's database.

2. Relevant European or international standards for facial images exchange

Facial image reference data shall be transferred inside a NIST file container. The NIST file shall contain fields related to facial images and other fields for alphanumerical data, but it shall not contain fields related to dactyloscopic data.

The specifications of the NIST container shall be defined by eu-LISA and based on an INTERPOL implementation. Eu-LISA shall adapt existing NIST file formats and shall support new NIST file formats to ensure the compatibility of the router to changes in the respective standards.

The NIST file format shall be verified by the entities and pass without any errors.

Eu-LISA shall provide a NIST validator tool to all entities in order to check the correct implementation of their NIST-creation-tool in their national facial images database.

3. Specifications for facial image searches

The requesting entity may use facial images from identified persons as well as facial images from unidentified persons, either in the form of a mugshot image or a trace image. The facial image can be a frontal, semi profile or profile image.

A query transaction shall contain only one single facial image.

The facial image search contains four possible transactions: (i) mugshot images to mugshot images; (ii) trace images to mugshot images; (iii) mugshot images to trace images; (iv) trace images to trace images.

All entities shall implement the following transactions:

- Mugshot images to mugshot images searches
- Trace images to mugshot images searches

Entities may also implement the two following transactions:

- Mugshot images to trace images searches
- Trace images to trace images searches

For each facial image query transaction, the requesting entity may specify a number of candidates per response transaction. The maximum number of candidates per response transaction, returned by a requested entity, may not be higher than 30. In exceptional cases, a requesting entity may request up to 100 candidates per response transaction. It will be for the requesting entity to assess if exceptional circumstances occur.

The candidate list shall contain the number of candidates specified by the requesting entity to the extent supported by the technical capabilities of the requested entity.

The candidates shall be ranked in a list, in an automated manner, according to their scores by the requested entity.

The candidate list shall contain only facial image reference data and at least one facial image reference data per candidate. The NIST file containing the facial images reference data may also contain relevant meta data which are not personal data, such as date and origin of the facial image.

The candidate list may contain multiple candidates. Images of different candidates may originate from the same person.

Each candidate shall be contained in one NIST file. Where multiple facial images of the same person are available in the requested entity's database, all images may be included in the same NIST file. The exact behaviour depends on the configuration of the system used by the requested entity.

The requesting entity may specify a priority indicator for each transaction, as defined in the NIST standard. If a priority indicator is not specified, then the transaction shall be considered at the lowest priority.

The requested entity decides how to execute the priority indicator.

The types of facial images (mugshot, traces, frontal, profile, semi-profile...) available in requested entities' databases and the types of transaction implemented by each entity shall be specified in the Prüm II handbook.

4. Quotas of transactions (maximum numbers of transactions accepted)

Each requested entity shall define for each requesting entity a maximum daily quota of facial image transactions per each type of transaction:

- Mugshot images to mugshot images searches
- Trace images to mugshot images searches
- Mugshot images to trace images searches (where relevant)
- Trace images to trace images searches (where relevant)

Each entity shall keep the other entities, eu-LISA and the Commission informed about the maximum quotas for facial image transaction. Each entity may temporarily or permanently raise those search capacities at any time, including in a case of urgency.

The requested entity may reject a transaction if it exceeds the quota defined by the requested entity. The requesting entity shall be informed of this rejection via the router.

5. Distribution of unused search capacities

The requested entity may redistribute its unused incoming daily transactions to other entities in a manual or automated manner.

The router shall provide for a system-to-system transaction enabling to regularly and automatically query the real-time status of the transactions performed during a day with the remaining transactions until the maximum quota.