Council of the European Union

Brussels, 4 November 2019
(OR. en)

13556/19

LIMITE

DAPIX 311
CRIMORG 146
ENFOCUSTOM 174
ENFOPOL 464
JAI 1120
N 68
ISL 60
CH 58
FL 74

NOTE

From:	Austrian delegation
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	11227/18; 13426/18; 14370/18; 5556/19
Subject:	Next generation Prüm (Prüm.ng) - Reports from focus groups / Report on Fingerprints

The initiative to reflect on the development of a next generation Prüm (Prüm.ng) was launched by the 'Council Conclusions on the implementation of the Prüm Decisions ten years after their adoption'. Subsequently, the previous Presidency started discussions within DAPIX by means of a questionnaire and presented a summary of the replies to its discussion paper on Prüm.ng. DAPIX discussed in particular the intention to establish focus groups tasked to set out how to further develop the current data and information exchange mechanisms and to support the European Commission's Feasibility Study on improving information exchange under the 'Prüm Decisions'.

Delegations find in annex the final report of the focus group on "Fingerprints". This report represents solely the opinions and views of the delegates participating in this group, based on their personal expertise. DAPIX is invited to discuss the report at its forthcoming meeting.

Development of dactyloscopic data for PRÜM.ng-

Focus Working Group report

1st Expert Workshop Vienna, April 2019

2nd Expert Workshop Lisbon, June 2019

3rd Expert Workshop Wiesbaden, September 2019

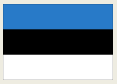
Supporting Member States:

 Austria (Chair)

 Netherlands

 Germany

 Poland

 Estonia

 Portugal

 Spain

 Romania

 Italy

 United Kingdom

 France

 Slovenia

 Denmark

Content

1 Introductory remarks

Based on the Council Conclusions of 16 July 2018 (11227/18) and the working methods adopted by DAPIX, focus groups were established, which were open to experts of all Member States. A first Focus Group meeting for Prüm dactyloscopic data exchange was held in Vienna in the second week of April 2019. The second Working Group meeting was hold in Lisbon in June 2019. The third and last workshop for face recognition as well as a combined FR, AFIS and DNA focus group session took place in September in Wiesbaden. National experts from Austria (lead of group), Denmark, Estonia, France, Germany, Italy, Netherlands, Poland, Portugal, Romania, Slovenia, Spain, United Kingdom supported the work of this focus group

The FP expert group decided to proceed both on the basis of written correspondence and several meetings in different supporting Member States. The aim was to submit to the Commission a document, commonly agreed upon by all participating national experts, which should contain the desired enlargement and further improvement of the currently successful Prüm cooperation network.

This document draws on the many years of experience of national experts. In support of the Commission, the focus group discussed preliminary results of the feasibility study on amending the current Prüm legislation, which was carried out by a consultancy firm on behalf of the Commission. Some proposals of these study were considered to be acceptable for further detailed discussions. Other proposals, in particular the proposal for a central data storage, were strictly rejected.

This document is a living document of the FP focus group and will be further specified in the ongoing discussion process.

2 Abbreviations, Acronyms, Synonyms used in this document

AFIS: Automated fingerprint identification system

EC: European Commission

Dactyloscopy: Fingerprint information analysis, comparison and verification to establish the identity of a person or to relate a crime scene latent with a person

eu-LISA: European Agency for large scale information systems for the law enforcement authorities

EU MS: European Union Member States

match / no-match: means the result of a machine (AFIS or DNA-match-engine). It would also mean that a no-match is always a no-hit. On the other hand, it is also possible that a match is a no-hit after the necessary forensic verification / validation

hit: means the confirmed positive identification result confirmed by a human being (expert) after forensic verification / validation.

(forensic) verification/validation: Manual procedure conducted by fingerprint experts to establish an identity between dactyloscopic reference data and/or a latent dactyloscopic data. Forensic confirmation has to be carried out in line with forensic quality management requirements (e.g. accreditation standards)

Dactyloscopic reference data: Tenprint card and palm prints which containing (digital) information about the dactyloscopic data of a person, usually taken during an enrollment process of such person by police or other authorities

Latent / stain / trace dactyloscopic data: (Digital) dactyloscopic data information (finger or palm prints) secured by crime scene investigators or forensic personal at crime scenes

Step 1 data exchange: Automated data exchange between the AFIS of the EU MS in the context of Prüm according to Art, 8 of the Council Decision 2008/615/JHA in form of anonymous biometric online search procedures

Step 2 'core' data exchange: Expert proposals of new Step 2 core data exchange functionality in form of personal 'core data' exchange in form of structured online data transmission via the same secure electronically infrastructure on which step 1 data exchange is processed (Prüm Testa NG communication) and after a match through step 1 is established as a hit.

Step 3 data exchange: Classical police and justice cooperation via various channels (e.g. Interpol, Europol) to request / exchange further information after a match through step 1 is established as a hit.

Core data: Defined limited data set with the most important data contents for the identification of persons, such as alphanumeric personal data (e.g. names, date of birth citizenship), information of biometrics acquisition information linked to 1step hit files (e.g. date, authority and reason for data acquisition), additional biometric data (e.g. dactyloscopic data, pictures (face), information related to identity documents (e.g. numbers, type, issuing authority, date of issuance and valid until, scan of ID documents), additional important information (e.g. existing arrest warrant information, information to other forensic data or lab quality information)

Interoperability (IO): Interconnection of EU (biometric) information systems under Regulation (EU) 2019/817 of 20 May 2019 in the field of borders and visa and Regulation (EU) 2019/818 of 20 May 2019 in the field of police and judicial cooperation, asylum and migration

TP/TP: Ten print to ten print search

LT/TP: Latent fingerprint to reference ten print search

LT/UL: Latent fingerprint to unsolved latent fingerprint search

LP/PP: latent palm print against reference palm print search

PP/ULP: reference palm print against unsolved palm print search

SMTP: Standard protocol for e-mail communication in computer-based networks

Web service: Communication technique for machine-machine communication on the basis of internet protocols (e. g. http)

ICD: Interface control document

XML: Extensible Markup Language (XML) is a technical markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable

3 Prüm Dactyloscopic data solution – possible upgrades of present Prüm AFIS solution – general overview

The experts agreed that the current Prüm AFIS functionalities of step 1 work very well and meet the needs of the law enforcement authorities (LEA) to identify suspects with tenprint cards, and in terms of forensic searches performed, to match crime scene latents.

A provision, such as identifying missing persons or unidentified corpses by means of fingerprints, whether or not such missing or killed persons are connected with a criminal offence as offender or victim, should be added to an amended Prüm legislation.

Humanitarian Prüm identification searches, which would be very important in daily police practice, e.g. after a disaster or an accident, are currently not allowed in all EU MS. A legal clarification like the one already provided by the EU Interoperability Regulations for the biometric databases of the EU central systems would also be desirable for the Prüm cooperation.

Prüm AFIS functionalities have meanwhile become a worldwide technical / forensic standard for international criminal police cooperation. They enable dactyloscopic comparisons of both biometric personal (reference) data records (usually ten print cards) and biometric unsolved crime scene (latents) data records. They ensure highest forensic quality standards and possible usage in investigations and penal court procedures. The forensic verification process between sent data and received match candidates, which is provided by the present legislation, is very important and should be maintained in the future before localized biographic data records of confirmed hits can be requested from partner countries.

However, the greatest need for improvement is seen in the acceleration of the follow-up data exchange, particularly in the area of dactyloscopic identification of individuals such as suspects. This data exchange must be speeded up, since the data comparisons sometimes take place when international acting criminals and terrorists – often using wrong alias identities - are present at the police stations or in arrest of the searching Prüm country. Only if the follow-up core background and identification data (minimum core data sets still to be defined) are exchanged quickly, it will be possible, for example, to carry out investigative measures following arrest warrants by the requesting Prüm partner states.

The Prüm AFIS should continue to function in a decentralized network system. The provisions related to storage and use of reference and trace-images should be based on national legislation. Only searching in the EU partner databases and no permanent storage of transmitted data in searched Partner states should be provided for.

The first version of the feasibility study on amending the current Prüm legislation suggested an alternative data storage. However, national experts strictly rejected the option to store national biometric data or templates of such data on central EU servers.

From a forensic point of view, such storage is not useful for dactyloscopic latents search and storage functionalities in all possible search transaction types, and could also endanger the entire proven Prüm cooperation. It was considered essential that the sovereignty over the sensitive LEA data remains exclusively with the Member State that has recorded this data in accordance with its national legislation. Lawfulness of data processing and data retention should be defined by the relevant national legislation.

Only if national competent fingerprint experts have confirmed, in line with binding quality assurance standards (EN/ISO 17025 accreditation standards), a potential AFIS 'match' candidate as a correct 'hit', further personal data processing should be foreseen.

Personal and/or case data such as names, crime types etc. should be provided without further delay in case of a hit. However, such information should never be provided in an automated way within the 1st step procedure, but only on request and after a hit has been confirmed by a competent expert of the requesting Member States. The follow-up data should be retrievable in electronic form and according to technical solutions via encrypted network state-of-the-art solutions.

Technical improvements could in principle also be realized by developing a simplified encryption workflow organised at central level. That would at the same time allow a better monitoring of the operational readiness of Prüm Member State through the use of new communication technologies (web services).

However, even in the case of future technical developments such as e.g. web solutions, all experts noted that the existing Prüm functionalities must stay operational at any time. These functionalities must be maintained at least until all Prüm partners can switch to other technologies without running the risk of operative interruption. It is therefore of great importance that parallel operation is possible at any time, for example with different and open protocol systems (SMTP + WEB Service),.

Furthermore, technical developments, such as new automated second step core data exchange solutions, should not be planned and developed on different technical protocol systems but only in new WEB service and XML based technical standards.

It is essential that all Prüm partners remain reachable for operational cooperation notwithstanding the situation that new technical solutions, both for the Prüm 1st step and 2nd step, could not have been implemented by all at the same time and different technical approaches to provide follow-up data would result in different response times. Once the new legal and technical documents have been drawn up, the Member States are called upon to adapt standards and implement new technical solutions as soon as possible. Nevertheless, binding implementation periods (deadlines) for such technical conversions were not recommended.

4 Legal structure of the technical documents of Prüm Decisions

The experts considered the integration of the technical documents (Interface Control Documents – ICD) into Decision 2008/616/JHA on the implementation of Decision 2008/615/JHA as one of the main obstacles to amend the Prüm system at technical level. As an Annex to Decision 2008/616/JHA, the technical documents are an integral part of the legal text. Amending the technical parts would have meant to re-open discussion on the Decision as a whole, which would have implied a complicated EU legislative procedure.

4.1 Technical details into implementing act

Future technical documents should be amended in another procedure - for example by implementing acts in line with (EU) Regulation 182/2011 - in order to keep the respective technical and forensic standards up to date.

Technical details should be fixed in such implementation acts and not in complex legal acts. This would allow for more flexibility after a test period.

4.2 Changes only with bilateral agreements and notifications outside of formal legislative procedures

Certain necessarily very flexible agreements, such as changes of daily quotas, notifications of national organizational structures (e.g. national NCPs, etc.) don't need to be regulated by such formal implementing acts. Instead, they can be amended by bilateral agreements or by notifications to the Council Working Group DAPIX, as already well regulated in this area.

4.3 Expert working group for developing the technical aspects of Prüm

The experts proposed to establish a technical working group to monitor and discuss technical progression on a regular basis (comparable to the technical working groups installed on the level of DAPIX when Prüm was first introduced). In this body – which might function in a similar manner as the advisory groups installed under the umbrella of the eu-LISA management board, technical experts of all Member States would come together to draft amendments to the technical documents relating to Prüm cooperation. Furthermore, this body might be also used to discuss obstacles or impediments during the operational exchange.

5 System Architecture

5.1 Workflow-functionalities PRÜM AFIS 1st step

As already mentioned in the introduction, the Prüm AFIS 1step workflow processes function so well that they have already become a worldwide standard and security authorities outside of Europe have already legally and technically copied this cooperation. Changes to this cooperation should therefore be planned with great caution in order not to jeopardize its great success. However, technical updates and developments are also possible in this very well running Prüm AFIS 1st step cooperation.

5.2 No central data base solution on EU-Level

All suggestions of the study contractor towards a data storage of personal or case data on central servers of the EU (e.g. sBMS)[1]) were unanimously and strictly rejected by all experts. This was based on forensic and organizational reasons related to work processes and quality requirements of international criminal police cooperation and crime scene stain processing. Such proposals would undoubtedly jeopardize the successful and well-functioning Prüm cooperation and cannot create any operational benefits.

The experts also refused as inappropriate the proposed functional and architectural links between the planned interoperability solutions and the non-comparable criminal investigation solutions in the further planning[2]. In this area, synergetic solutions are conceivable as far as those might be realized through technical standards that are as uniform as possible, but never through the shared use of data on euLISA servers.

Such links would undoubtedly jeopardize the successful and well-functioning Prüm cooperation for both legal and forensic operational reasons and cannot create any operational benefits.

---

1 Study on the Feasibility of Improving Information Exchange under the Prüm Decisions published on Workshop 27th March 2019 – Area 4 of this study

2 Study on the Feasibility of Improving Information Exchange under the Prüm Decisions, published on Workshop 27th March 2019 – Area 4, Opportunity 4.3 and 4.4 of this study

5.3 Monitoring operative status of national Prüm systems

Not all EU MS currently implemented functionalities to monitor their own or their partner countries operative status (same situation in Prüm AFIS as in Prüm DNA cooperation).

Such monitoring functionalities are basically possible with SMTP communication functions. Technically common SMTP solutions are automated warning (E-Mail) messages when no response is returned by a state for a longer period of time. The Prüm ICDs always provide binding feedback after a search (in minimum with a no hit or error message), which is a very positive precondition. It always allows such monitoring, since it is clearly recognizable when a search transaction is not completed. The big advantage of the SMTP solutions is also that transmitted transactions are never lost but remain on one of the mail servers, even if the Prüm AFIS is not operational. When the E-Mail servers are reconnected to operative biometric servers, the transactions are also processed (delayed) and answered.

5.4 Monitoring methods of operative status of national Prüm systems with WEB and thinkable central router solutions

With WEB solutions, such monitoring functions could be significantly accelerated. However, such a solution becomes much more complex from a technical point of view and neds to be discussed in detail. For example, detailed response time behaviour specifications would have to be defined. Such operational checks could probably be implemented pragmatically if the communication runs via a central router (message broker), which continuously checks this operational availability of all linked systems. The Prüm EUCARIS solution as a web service has such a monitoring function implemented. From there, every 10 minutes dummy VIN searches are set off against all connected systems by the central web service and, if there is no response after a fixed period of time from a partner, the technical central office of the Member State that does not respond would be contacted

Yet even with such central router solutions, it seemed essential to all experts that there should be no significant delays in the operative response time. For example, there should be no central consolidation of all results, as this would mean that a requesting Member State would have to wait for the answer of the last sending Member State or a technical error message in case a Member State is technically unable to send a respond. This also excludes a possible central re-matching of all results received for minimizing the workload in the requesting Member State. However, such functionalities might be implemented on national level if applicable and desired.

5.5 Daily search quota

In replying to the study contractor's questionnaire, some Member States had apparently defined the maximum daily search quota as a relevant Prüm problem. On this subject, the expert group noted that the fixing of such quotas is of great importance so as to sufficiently guarantee the AFIS availability of the Member States. It is also very positive in the current Prüm regulation that precisely this fixing of the possible daily searches is not regulated in the relevant legal acts, but can be changed at any time by simple agreement between the Member States within the DAPIX Council Working Group or in case of urgency without problems on a bilateral basis. The Council Secretariat (GSC) always updates these search quota lists following such requests for permanent changes, so that a current status is always apparent.

As experience has shown, the totality of the daily search queries granted was never not even nearly fully exploited. The supposed problem therefore lies rather in the presumed unfamiliarity of some national competent authorities that these figures can be changed easily and at any time if needed. Experience has also shown that many Member States have indicated their desired number of enquiries from other partner countries far too low (according to classical police cooperation experience). Prüm searches, however, open up a wide range of (also systematic) search transactions, because they do not burden the requested partners with expert work. On this point, therefore, it would rather be necessary to raise awareness in the respective competent authorities that the number of enquiries can easily be increased. Only very few very small states had a problem in the past to increase their systems for the most needed TP/TP searches quota, because they operate very small national AFIS with only small license rights from their AFIS provider. In the meantime these TP/TP search license costs are fairly low and could be extended by all Member States in order to grant the desired query quantities across the board. If individual Member States should nevertheless have financial problems for such license extensions, EU financial support would also have to be considered to solve such problems.

Today, the requesting Member State has to ensure not to exceed the daily quota applicable (cf. Art, 13, 2008/616/JHA). Most Member States have installed technical systems to monitor incoming and outgoing requests. Especially the monitoring of incoming transactions (with the ability of denying searches over quota) cannot be seen as fully in line with the legal framework today. Therefore, a new legal act allow for the monitoring of incoming requests from connected Member State.

5.6 Inclusion of a specific data category “important quota exceeding”

Member States might occasionally need to exceed the agreed query quota after very important criminal offences (e.g. after a terrorist attack). In principle, such quota overruns also work sufficiently well, as affected Member States contact the NCPs and request that the agreed quota be exceeded for a certain period of time. Such requests are always approved immediately by all Member States. However, experts proposed to include a separate data category "important quota exceeding so as to avoid such contacts in the case of critical events". Even if the number of queries has already been reached on that day, query data records marked with this data category should not be rejected or retained for processing in a processing queue until the next day, but should be processed immediately in the requested partner state.

5.7 Encryption

Some Member States reported practical problems with encryption – particularly in the starting phase. The provision and also the change of the encryption certificates by possible storage on the Europol EPE server for download with prior notification of all operational partners via the defined NCPs works well. Nevertheless, communication problems may occur subsequently. These technical problems are mostly very small errors that are easy to fix but even such small problems must be analysed and found from technical experts. According to the experts, such problems can only be completely solved by setting up a central encryption service system. Such a service could easily be established by using a central router.

5.8 Central Data Router (eu-LISA?) with encryption-management

The possibilities of a central router service were only regarded as useful if they can contribute to a simplification of the current bilateral encryption management. They would also help to ensure that Member States would not have to gradually interconnect bilaterally by exchanging encryption data, but would be immediately connected to all operational Member States when they were connected to such a central service. Such a central router solution would also open up improved central statistical analyses.

For reasons of data protection, some participants emphasized that, when using a central router service on euLISA level, no decryption and no possibility of using the transmitted sensitive criminal investigation data content should exist on the central router service level. Clean data should be decrypted exclusively by designated recipients.

In-depth discussion on central router variants – meeting Lisbon and Wiesbaden

5.8.1 Simple central router solution or full decentralized routing solution

From a global perspective, a simple central router providing different functionalities has been identified as useful for compiling (technical) statistics or – from a technical point of view – to enable a smooth transition from SMTP to web service through this central transformation.

Nevertheless, some national experts voiced concerns related to data protection and data security. They stated that it should not be possible to decrypt the data of the transactions on a central level and also not to store transactions on a central site (e.g. eu-LISA as technical service provider should never have access or have the right to store operative data).

From a technical point of view, some participants confirmed the benefits of a central data router solution. Especially in terms of technical efforts, in terms of key management, server-availability or statistical reports, a central solution could reduce costs on national side. However, some participants voiced concerns related to data protection. The technical experts also agreed that there is no implicit need for a central router. Because of many remaining legal issues, this topic should be finally decided at political level. Experts of those Member States, which have a more neutral position on this question and may also accept a central router solution as a possible alternative, could only accept such a solution as a 'simple' message router and only if an EU agency (euLISA) would be entrusted with providing the responsible central router service and not a private company. Additionally, it has to be legally clear that such an entrusted EU agency would not be allowed to accede the very sensitive content of transmitted data and, furthermore, that the use of data would not be allowed for other purposes than technical and statistical support of Member States.

All experts agreed, however, that the use of such a simple central routing system would only offer a relatively small added value. It was therefore considered as not necessary in principle and rejected by the majority. Nevertheless, the working group did not yet close the issue, especially as not all EU MS are involved in the expert working group. It was therefore recommended to address this question again at DAPIX level with the involvement of experts from all Member States in order to commonly agree on a position.

5.8.2 Decentralized common router service solution

A possible alternative might be a “common router service” on national site to have a harmonized communication standard. National experts supported to have such standards but don’t see the benefit to develop such an application (conversion tools, etc.) as this means additional technical integration on the national level, which have often much better and state-of-the-art tools, than such simple common standard tools. However, those Member States, which do not have such comprehensive high technical standard solutions in place, could benefit from such a common standard router service. The preferred approach to find a solution might be that the standards and specifications on communication and functionality for web services should be defined in implementing acts in a comitology procedure. Member States might decide by themselves on how to implement or integrate while always focusing that a big bang scenario should be avoided.

euLISA (like in Eurodac) might develop the tools for those Member States which have not the need for a binding integration in their national infrastructure.

5.9 Refusal to start the operation despite the given conditions

Some Member States refuse presently to go live with other Member States despite their technical and legal readiness, or at least only agree very slowly and gradually to start operational exchange.

Of course, this contradicts the idea of Prüm cooperation and the principle of availability and has very negative operational consequences in the fight against international crime and terrorism.

The reasons given for such refusals to take operational action are usually the lack of existing national expert resources, which could also process the detected hits. This argument cannot be true, at least in the AFIS area, since the state requested only needs to have the technical resources in place (→ quota) as requests here are processed without any manual intervention by an expert. So personnel are only needed for requesting other Member States (→ verification of match results).

Nevertheless, such an argumentation is also prevalent in this AFIS area. A switch to a central router service would of course solve this problem. As soon as a Member State would connect to this central router, it would immediately be able to reach out to all already operational states. However, it would still remain the responsibility of every Member State to employ a sufficient amount of experts to conduct Prüm searches requested by its own national police forces.

The use of such a central (simple) router service (message broker) would therefore be suitable for problem solving. Although from the experts' point of view it is unclear whether this political goal will really be supported by all Member States, because some are currently delaying such operational start-ups with above mentioned arguments.

5.10 Web-Service

The current Prüm SMPT (e-mail) communication is considered to be very well functioning, both in AFIS and especially in the DNA communication area, and must absolutely remain functional without possible restrictions. Nevertheless, faster, more modern web solutions can be expected, especially in the AFIS or /and Face Recognition cooperation through the development of additional web services.

The focus expert group is therefore encouraging the parallel development of web services. With a view to the most possible uniform communication platforms and interoperability, such a solution is recommended for all types of forensic data transmission, including accelerated 2nd step information exchange in all these forms of cooperation. It is essential that no big bang implementation should take place here so as to not disrupt the ongoing and well-functioning real operation. An open protocol has to be used as a future protocol service, which allows all transmission protocols in parallel and in interaction. For example, depending on the different technical development status and possible national updates of the systems, SMTP-SMTP, SMTP-HTTP and also HTTP-SMTP protocols for data transmission between the test states should be possible. In order to be able to implement such a technology with the least administrative effort, the experts would also consider the use of a central "simple router" or simple "message broker" on a central EU platform (e.g. euLISA server platform) as possible.

Even if the current technical architecture via SMTP is working fine, a web service solution gives more control on the communication, also keeping in mind that 2nd and 3rd step exchange on data and the exchange within DNA and FACE is/should be XML based. Seeing the architecture as a common approach for the exchange of data in all 3 fields, web service might be the preferred solution. Also from a security perspective, web service should be the technical architecture for future new and updated implementations.

A parallel WEB solution development for communication is therefore recommended. Irrespective of this, the existing SMPT solution must remain functional without interruption until all MS have switched to a new WEB solution.

Despite this, new technical developments such as new second step core data exchange solutions should not be planned and developed on different technical protocol systems but only in a new WEB service and XML based technical standards.

5.11 Workflow- functionalities Prüm AFIS 2nd step – Establishment of 2nd step NCPs for Prüm follow up data exchange.

Core Data exchange in case of confirmed hit, after online request from searching Member State.

Experts considered the establishment of a 2nd step national contact point (NCP) as very important. Unlike the current Prüm legislation, a potential new Prüm legislation should make mandatory such a contact point. It should depend exclusively on national organizational and legal regulations, which competent national 2nd step NCP carries out the follow-up correspondence, and the NCP should only be notified by the Member States. Of course, this NCP must also have access to secure electronic communication channels where this follow-up information can be transmitted in electronic and encrypted form.

These 2nd step data requests should be possible in three different cooperation levels, which will have different response timelines for these subsequent data.

Such a flexible approach is necessary because not all EU MS can shoulder technical developments equally quick and to the same extent. Due to different national legal bases, different authorities with different national data release processes and also with different contents in the Criminal Case Management Systems are involved in the second step data exchange.

All experts considered it to be very important that the results of the Prüm 1step matches are always checked forensically before initiating a 2nd step data request. Such clear checks and human intervention ensure not only data accuracy but also clear responsibilities. However, the requested Member State might implement an automatic data transmission to answer the 2nd step information request, if this is in line with national legislation.

5.11.1 First possible variant that must continue to exist (existing Prüm 2nd step process defined in future also as 3rd step process):

The 'classical' follow-up investigation correspondence, which should continue to exist, is carried out via the existing channels currently in use, i.e. Europol (Siena), Interpol (I-24/7), legal liaison officers network or SIRENE. It is not necessary for a national contact point to have direct access to these networks. However, it seems essential that a NCP should be able to forward and respond - if necessary also by secure routing on secure national networks - to the other Prüm 2nd step NCPsOnly verified data, that is data confirmed as 'hit' by the national experts, will be retrieved. Step 1 match candidates, which could not have been verified by fingerprint experts as 'hit', may not be subject to further information exchange in step 2.

Usually, such a method of transmitting follow up data means data provision within days or weeks. Nevertheless, in very urgent cases this process could also provide data within hours, especially when a request is followed up by telephone or other means of (parallel) communications to state the outstanding urgency and if partner offer 24/7 duty service (usual organization concept in Interpol cooperation).

5.11.2 Second possibility of a faster follow up data exchange of “core data” (two new alternative Prüm 2nd step procedures)

5.11.2.1 Core data exchange without prior authorization (fully automated answer)

(Automated) collection of core information about a person or a case in the national databases (compiled automated by a machine) available to generate a first response to a second step information request.

This first response would be approved by an authorized organization prior to the release to the requesting Member State. In addition to this existing possibility, providing certain important identification and case data on request should be implemented. These can be requested via the same secure network used to carry out the automated data exchange of the forensic 1step search, but with a separate interface and specific XML scheme. A forensic confirmation by a national expert, who confirms a possible “'match' in line with national fixed forensic quality standards as a real “hit”, is also essential here. An authorised follow-up data request must be made immediately in order to provide the 'core data' available in a country This core data should contain any identification data or crime case data and offence information available in the requested Member State and linked in a secure manner to the relevant forensic data of the hit file.

Automated data provision is possible between Member States which have implemented automated links to agreed 'core data' information in their national databases. In accordance with Article 4 of the Framework Decision 2006/960/JHA, these data have to be made available in certain time limits as soon as they are stored in databases, which are accessible by a law enforcement authority (LEA).

A human interface for an upstream forensic confirmation is a prerequisite in the requesting state in which the decision has been taken to query simultaneously with own 'core data'. However, the supply of data by the requested state is no longer dependent on an additional decision of an officer of the 2nd step NCP. If the requested data comply with the specified minimum data quality, which could be checked automatically by IT systems (e.g. required names, crime description, etc.), the follow-up data will be provided immediately in an automatic way to the requesting country. Only those data will be retrieved which have been confirmed as a 'hit' by the national experts and not also matching data of other match candidates.

This method of transmitting follow up data means a 2nd step data provision within seconds or minutes even if a partner country could not offer 24/7 duty service.

5.11.2.2 Core data exchange with prior authorization (only partially automated answer)

Authorization of a core data set (compiled automatically by a machine) by a competent human being of the competent authority (2nd step NCP) before releasing the compiled information to the requesting country must be always be possible.

This first response would be approved by an competent authority prior to the release to the requesting Member State.

Replying to such a follow up request may be subject to a supplementary authorisation in the requested Member State on the basis of national legislation or organisational concepts. However, the data transmission shall always been carried out in a structured, electronic and encrypted form on the same data network as the 1step data comparisons.

Such a solution allows for manual addition of core data elements by 2nd step NCP officers, as such data may be stored in databases not searchable or not available in a structured manner for example, to add extended but relevant content to the answers that is stored in other databases on the person concerned (e.g. a known residential or residence address, conviction data, etc.). However, such data content should always be transmitted in a structured form and in data fields available for this purpose. However, the advantage of possible more extensive data provision is, of course, offset by the longer processing time until possible data transmission.

This method of transmitting follow up data means data provision within hours or days.

5.12 Content of 2nd step core data

Which data is suitable and necessary as 'core data' for rapid data transmission will depend on the type of data concerned. The exact definition of this core data should be defined in the future legal act according to the respective data type of the cooperation and the technical possibilities.

The data types can differ according to the type of search and will consist of mandatory necessary data contents and also possible data types, which can only be provided if they are also structurally stored in a database in the requested state.

In an intensive discussion, the experts defined a set of 'core data' which should be exchanged in all biometric data types. The amount of information needed deferred on the transaction type (Reference or Latent). The core data set includes information on:

- Alphanumeric Personal Data,
- Relevant police information (convictions and/or suspicions, curent investigations)
- Information of biometrics acquisition,
- Additional biometric data information ,
- Identity documents,
- Additional data (e.g. Technical, Alert or Warning Information etc.)

For reference databases, some data fields like e.g. family name, first name, date of birth, place and country of birth and gender, should be mandatory. Without this information, no core data will be transmitted. All other information may be provided if available and also legally permissible.

The discussion of national experts on a meaningful scope of 'core data' showed that the data content, with reference to technical solutions, may vary according to the type of transmission used. For example, data on convictions of a data subject in the national Criminal Record databases are in most states currently not directly linked to the identification databases in which the biometric data and the core data of the data collection are stored. In this area, the ECRIS - TCN application will soon have to make technical – organizational changes at national level in all EU MS, otherwise biometric data transmission to ECRIS-TCN and EU Interoperability database platforms will not work, but this will still take some time. A similar situation also applies to other data that are important for the initiation of criminal investigations, such as national databases of prisons, residence registration data or also wanted person databases on national and also EU level (SIS). However, if such data can be edit manually ('core data' exchange with prior authorization), core data set can be supplemented with additional information.

For this reason, it makes sense to include in the legal framework really all data contents useful for the initiation of criminal investigations, even if not all of them are currently suitable for fully automated data provision.

In the subsequent necessary drafting of the implementing acts, it must be defined which data contents or data fields are to be defined as mandatory, as mandatory if available (complementary) or only as optional data if available.

The detailed information on the Core Data fields for law enforcement purposes will be provided as Annex to this document.

5.13 Usage of a common penal code table and common language for automated 2nd step core data transmission

The experts agreed that when such standardized data contents of 'core data' are used, a uniform offence code should be used. Such a uniform and constantly updated offence code already exists at EU level. These are the ECRIS offence lists for which uniform offence descriptions have been fixed and to which the respective national Ministries of Justice (ECRIS NCPs) always have to assign different national offence descriptions before ECRIS transmissions are carried out.

In order to make such data content easier to understand, it will also be necessary to consider fixing data content to an international working language. If such an approach - which is also suitable for the acceleration of messages - is desired, here only the English language would be suitable, since this language is the only language, which can be accepted by all NCPs in each case and worked on immediately without further translation work.

In order to avoid problems with different national alphabets or spellings (e.g. cyrillic letters, diacritical characters), the 2nd step core data content at national level should always be transcribed into ICAO standard (Latin-based letters ISO 1073-2) for transmission. Such requirements already exist in the Prüm Eucaris solution.

5.14 Necessary 3rd step information exchange

All these possibilities for the acceleration of data supply for identification should not prevent a 3rd step information exchange which might take place in practice. In such a 3rd step information exchange, further detailed and investigative information may be made available either in classical police cooperation or also in classical judicial administrative assistance. However, delivering such information is not as urgent as the initial identification and subsequent use of personal data of identified suspects. If need be, exchanging such information should be possible at any time in the future via classical police and judicial cooperation.

In-depth discussion 2nd & 3rd step– meeting Lisbon

The results and proposals of the first meeting with three different parallel possibilities of standardized core data transmissions to be created and an unchanged possibility to exchange further non-standardized information in a third step on classical police communication channels were confirmed. National authorities are currently overloaded with work and have to wait days and weeks to receive data on which they might decide on how to process the case. To speed up the process and to optimize their cases this core data could be given to MS after confirmed hit.

Some MS requested that there is the need to have – as a possible proof – the fingerprints included within the 2nd step exchange again. Thus, they are able to confirm/to be sure that the personal data is really linked to this person/fingerprint. Particularly after latent searches the provision of the whole TP/PP dataset is necessary anyway for further forensic checks and confirmations.

In the case of semi-automated or also alternative possible full-automated 2nd step data provision processes, also the full dactyloscopic data set and a current image of the confirmed hit candidate could be transmitted to the requesting state in addition to the alphanumeric personal / case data when answering the requested in the answer file.

5.15 Remark to proposals of Deloitte study to define Europol (Siena) as binding 2nd step channel for Prüm follow up exchange

The proposal of the feasibility study to determine the response speed by the mandatory use of one of the classic police communication channels, i.e. the Europol channel, was strictly rejected. Such a demand does not speed up the response, but significantly worsen it.

It is also of considerable importance that for the classical existing channels of unstructured data transmission, which in the future will concern mainly further 3rd step information exchange procedures in the Prüm cooperation, the free choice of channel is left to the EU MS.

This free choice of channel selection was an essential and important point of Council Framework Decision 2006/960/JHA for classical police and justice cooperation. The competent national authorities will always use the channel according to the individual task and the most suitable and best functioning way and must not be forced to use less suitable and slower channels.

The 3rd step is outside the scope of Prüm and belongs to classical police cooperation. Therefore, the choice of the relevant communication channel (Interpol, Europol) is not in the scope of Prüm.

5.16 Technical Helpdesk

The possibilities for obtaining technical support are currently considered insufficient. The initiative to set up such a Europol Helpdesk was considered to have failed by all experts. The established EPE server, however, performs an important function for the provision of the encryption certificates. However, all other support functions, in particular the intention to provide always up-to-date information or documents, did not function sufficiently.

In this context, however, the support provided by the GSC working group was considered very important. These documents always reflect the current status and are always kept up to date by the GSC. Of course, the GSC is also dependent on reliable feedback from the MS in order to carry out the updates.

Purely technical support can currently only be provided bilaterally by experienced Member States, which, of course, also places a considerable burden on their limited personnel capacities. Fortunately, there are hardly any problems in the daily cooperation. The establishment of the central NCPs has proven very successful. If there are problems, they are always solved in an uncomplicated way with direct contact. The most frequent problems concern communication problems due to non-operational ability, which is not always immediately apparent.

The establishment of a central router could also contribute to solving this problem, which is not frequent but which does occur. According to the experts , only euLISA should be considered as a service provider for such a router, , since a 24/7 operation of an EU agency is required here in any case. However, some experts considered restricted access rights to data content to be of great importance.

5.16.1 Possible role of EU-Lisa

For technical topics related to Prüm exchange, euLISA should develop an implementation guide and create also benchmark test-set and perform benchmark tests together and with the support of national experts. To that end, a Member States' expert Advisory Board within euLISA should be established.

5.16.2 Possible role of Europol

The function of the Europol Prüm Helpdesk has not proven as successful as originally planned. There are several reasons for this. On the one hand, Europol technicians, who are not themselves familiar with the decentralized Prüm systems and forensic needs, cannot provide sufficient technical support and advice. Established information platforms on the EPE server are in fact also unused and unhelpful due to the non-availability of useful and up-to-date information by the Member States, which do not provide regularly such information to Europol. The only really relevant added value of the Europol Helpdesk EPE server is the possibility of setting and downloading the encryption keys within a secure network.

Purely technical support services and advisory boards should therefore be shifted better to euLISA in the future. The lack of up-to-date legal information and never working organizational Prüm coordination at Europol level does not constitute a shortcoming, as these tasks are excellently performed by the GSC. This proven support for the MS coordination and updating of all legal documents should continue to be provided in this proven way by the GSC in the future.

However, there is a common understanding at expert level that Europol - at least if Europol so wishes - could be granted a better operational use of the Prüm system for dactyloscopic data or also for potential future face recognition comparisons. With such solution Europol would o be able to carry out independent comparisons like a further additional "Prüm State".

Of course, it makes no sense that Europol checks the biometric data stored by Member States at Europol against national databases. Member States and their forensic experts, who have to prove with their expertise the results also in their courts, can do this check efficiently by means of the existing Prüm online access.

Nevertheless, Europol also receives biometric data from third countries - such as biometric data on suspected terrorists or internationally active criminals. It may make sense for Europol to be able to compare such data with the national reference data or with the central EU databases of the interoperability system, once they would have established own biometric systems and hired own forensic experts for such data processing.

Granting Europol direct access rights to Member States' databases for the purpose of checking such data against the national databases is not a question that can finally be answered by the expert group. It is a political and legal question which must be assessed by the Member States, European Parliament and also by Europol itself. Of course, it would also have to be ensured that follow-up personal and case information data would never be sent from Europol to third countries without the prior information and consent of the Member States whose data would be concerned.

5.17 Statistics

For years, demands have been repeatedly made for more comprehensive and coherent statistics.

It should be pointed out that more extensive statistics such as the type of offence concerned cannot be compiled with anonymized data and that this is therefore not a technical issue but a legal and organizational one.

Only NCPs for 2nd step information exchange are in the position to provide information on concerned offences, existing wanted person records etc. in rapid manner and sufficient data quality. This is currently not provided for in Prüm cooperation. The forensic institutes that handle mainly the Prüm 1step cooperation usually have very rare and never complete information about background of crimes.

The current Prüm statistics correspond fully to the legally possible statistical contents and were fixed after years of discussion in DAPIX in best possible manner.

However, the fact that even here - especially in the DNA area - there are always inexplicable differences between the cooperating Member States is difficult to explain and can probably be traced back to different technical system settings or software solutions in use with sometimes limited functionalities.

At least, such technical differences could be avoided in the future by using a central message router service. Search queries and their results could also be read centrally. It should be noted, however, that even such superficial statistical evaluations by a central office (euLISA simple router? – hub in the middle) require access to the content data of the messages. If, for example, the central router cannot read out whether the data type is a latent or a reference data, no meaningful statistics can be created.

As already mentioned above, however, some experts had considerable reservations about providing content data in LEA cooperation to a central EU agency, which, however, would be a pre-requisite of allowing for more detailed statistics. In addition, it is never possible to determine with present Prüm ICD functions, whether a detected match could be confirmed as an actual hit by the searching fingerprint experts afterwards in the AFIS area.

For this reason, the extension of the Prüm ICD should also be examined in which these forensic expert decisions are reported back to the requested state with a further transaction if more meaningful statistics are desired. This would become evident anyway with the implementation of a 2nd step online data exchange requirement but could be also realized with a forensic additional 'hi' notification to relevant searched partner country system. This would not only improve statistics, but would also improve the national AFIS quality setting, for example by adjusting the threshold values if they provide too often wrong candidates e.g. after TP/TP search transactions.

As a conclusion, with a central routing server, not only improved technical communication support but also at least transaction statistics could be kept uniformly but further discussions are necessary.

The current statistical contents in the first step are very good and also meaningful.

Today statistics are annually transmitted to the GSC. As an alternative, an automated electronic process for transmission of statistical information could be implemented. Such kind of process would especially avoid copy and paste errors that appear today when national statistics are consulted to fill in the statistic template.

Often required statistical detail, such as information on clarified types of offences, can only be provided if such information is also exchanged electronically in a standardized/harmonized form and centrally via the above mentioned standardized 2nd step processes. Such statistics would, however, have to be regarded as separate follow-up statistics and therefore have to be defined separately as 2nd step exchange statistics.

5.18 Number of maximum candidates per transaction type should be stay as presently fixed

The fixed number of possible candidates in the various search transactions has proved its worth and should not be changed. In addition, already today every Member State may introduce rules to their national experts on how many candidates may be requested for certain search types, crime types or urgency levels.

Prüm latent searches are only triggered for criminal offences. This makes it all the more important that possible hits can also be identified by providing potential match candidates.

It is not a problem, but an important prerequisite, that after a TP/TP request a candidate for a match is sometimes offered by 15 states. TP/TP hits are - if the national thresholds are set seriously - almost always correct hits. This only proves that an internationally active offender has been recorded in numerous EU MS. Usually, not only numerous different false identities and also existing search alerts become recognizable, but also the composition of criminal organizations. Restrictions of hit candidates as they have already been considered (e.g. by a subsequent comparison on a central eu-LISA service only the first 10 candidates of all EU MS to display) are therefore to be strictly rejected.

The same also applies to such ideas from the area of trace comparison. In the latent comparison area, of course, much higher match candidate numbers can be provided. For example, up to 200 match candidates could be offered for a query of a crime scene latents against 20 MS, which must be checked by the national fingerprint experts. Here too, however, the same basis applies as for personal checks. The greatest added value of the Prüm cooperation is the large reference databases of EU MS with biometric data of criminals. Comparison results must never be arbitrarily restricted for quality reasons alone.

Crime scene traces are very often of inferior forensic data quality both in the DNA and in the dactyloscopic area. Therefore the following forensic expertise work, which could confirm such match candidates as correct or also incorrect hit is very essential in this LEA cooperation. If the number of candidates is limited to a certain number, for example only on the basis of the highest ten or twenty best threshold values from all EU MS candidates, exactly the right hit candidates could not be displayed. In this case, the entire Prüm cooperation would have to be questioned, since classical matching requests that cannot be processed from the workload would again be necessary. It is therefore important that all match candidates are fully available for such searches.

5.19 Possibilities of reducing of number of latent search candidates list by usage of national micro matcher solutions on national side – National Ranking

EU MS can limit the forensic expert checks in their own area if they want. Such limitations could be realized, for example, by the use of a national “micro matcher” process. By usage, the two hundred incoming candidates of above mentioned example are compared again with their own national match algorithms against the searched latent data set (2nd micro matcher record 9 / record 13 search process) with provision of found minutia information on AFIS search results before forensic verification by the fingerprint experts will start. Such micro matching functionalities also makes it possible to rank all 200 candidates according to threshold values of 1 - 200 and it is then up to the national fingerprint experts to decide which of the 200 candidates they consider relevant for an expert test. Such micro matcher solutions could work by use of in Record 9 or Record 13 provided template information or alternative / additional also with automated national coding procedure by usage of own AFIS algorithm software solutions. In important criminal cases, this could be all 200 candidates, and in less important criminal cases perhaps only those candidates who exceed a certain national threshold set in the light of experience with confirmation of 'hits'.

5.20 Possibilities of reducing of number of latent search candidates list by usage of national micro matcher solutions on central side (hub in the middle router) – Central Ranking

Of course – from a technical point - such a micro matcher quality ranking would also be possible in a central router solution. However, such a central solution would also immediately open up numerous problems. As already mentioned, there could be no restrictions on the provision of candidates accepted from EU MS. In the case of a central adoption of such quality rankings by a uniform EU micro matcher, for example at euLISA level, the transmitted data at this level would have to be decrypted and decoded for possible data processing at any way, which is viewed very critically by some MS. In addition, problems are to be expected if, for example, one or more requested systems of an MS do not respond immediately. In this case, it will not be possible to establish a quality ranking of all files in a timely manner. There must not be any significant delays in the provision of data. For this reason, the use of such quality checks at national level is to be preferred, should it be deemed necessary at all from concerned EU MS , which is not the case.

5.20.1 Verification of results

The general approach is to have an optimized verification process for all candidates. Thus, a central service as a router on central level could collect all candidates – after automated dispatching of an initiators request – and perform a micro matching process over all candidates.

EU MS see also constraints concerning the access of the data. To perform such operations on central level, the data has to be decrypted. To avoid this maybe a reduced visibility on the data like minutiae data only and no fingerprint images could be implemented for the central routing service. It has been stated that this process on a central level might be difficult as the data protection protocol should as well be on central level (logging of candidates; logging on reduced list [cut] of candidates).

Also, a timing issue might be an issue if not all candidates are transmitted for this verification process or if there are operational issue on this router this will delay the whole process.

The members of the focus group recommended therefore, that such a micro matcher solution should only be an optional tool (add-on) on national side.

5.20.2 Quality check - threshold value

In today's Prüm exchange, it has been experienced that a few EU MS transmit candidates – especially with TP/TP transactions - which are obviously below a recognizable threshold value.

Experts recommended that quality control should be deactivated for Prüm searches.

5.21 New biometric dactyloscopic data categories in ICD – finger tips / writer palms

A possible requirement to include specific types of data that are only processed in very few MS was also being discussed (finger tips and writer palms). Whether such data extensions are necessary could not be answered amicably, since such data have hardly been processed nationally and do not show any relevant added value in practice also on national side. Nevertheless, with a possible definition of such specific partial data, at least those states that process such data could enable a targeted search in partner states that also process such data. This point needs to be discussed in more detail.

Writers palms are already described in the ICD and should also be in included in the future. For counter terrorism processing some MS see the need to include finger-tips in future ICDs. Footprints have been discussed but it was decided not to include this category in the Prüm exchange. So only finger-tips should be included in ICD if some MS like to do so and can use it.

6 Proposals from Commissions (EC) study contractor in 3rd expert meeting Brussels particularly to data quality

The study contractor firm proposed several proposals for the alleged improvement of data quality. From the point of view of the national experts, all these proposals are unsuitable for forensic cooperation in the Prüm area and were discussed and rejected.

6.1 EC study contractor proposal - Standard Quality Metric from NFQ1 to NFQ2

The study contractor explained that MS use one of the two NFQ standards for data collection. This statement was incorrect. The two NFQ standards are standards that are used exclusively for flat fingerprints when capturing live scans with in maximum 500 dpi resolution. They are therefore typically only used in the field of civil AFIS data acquisition (e.g. in visas or border control areas) due to their low possible data quality. Such data quality is also only sufficient for simple TP/TP search procedures but never in forensic area. Reference data acquisition for police authorities is always carried out in police quality with flat and rolled fingerprints as well as palm data acquisition. With this considerably higher data quality, the ever poorer trace qualities secured by crime scenes (latents) can also be used in AFIS in much better form and particularly in latent data acquisition very often with 1000 dpi resolution.

Thus, while much higher quality standards are usual for data storage in national police AFIS , conversely poor latent qualities for processing are also necessarily permitted for latent search and storage procedures in forensic police systems.

The still permissible latent qualities are based exclusively on forensic principles, which are also subject to EN/ISO 17025 accreditation in each EU MS. The permissible quality standards vary from country to country, but in most countries they are between 10 and 12 minutes fixed as minimum quality. Automated rejections or the determination of excessively high latent forensic qualities are always counterproductive in this forensic investigation area.

Criminals try to leave neither good quality of dactyloscopic data nor of surveillance camera photos nor of biological traces at crime scenes because this enables their identification. The data qualities of biometric latent are therefore only ever rejected as inadmissible for storage in forensic biometric search systems to the extent that their use, even in the event of a hit, would require the creation of an expert.

The data qualities of latents are therefore only rejected as inadmissible for storage in forensic biometric search systems to the extent that their use would no longer make it possible to draw up an expert opinion even in the event of a match.

Beside of this, data quality control will be organized on national level also always on a two level approach. On first level (data acquisition local police level) only the quality during data acquisition will be checked and monitored (e.g. via software of livescan). On second level, the more important data quality check will be handled from the central AFIS systems. On this level also corrections of minutia information with manual coding procedures possible by fingerprint experts if quality is detected from AFIS as possible not sufficient in line with national fixed quality strategy.

Prüm works exclusively with possible quality control on second line level because there is never a new data acquisition from persons on police stations with direct data transmission for checks in Prüm partner countries. Furthermore, exclusive data transmission and processing from existing files of national criminal AFIS systems started after performed national search and storage procedures.

In the Prüm context, however, as already mentioned in this report before, such quality controls / refusals for data processing processes are generally not meaningful. Prüm does provide for comparison procedures but not for storage. Data quality controls only make sense for storage data, since they can be used to maintain a minimum quality standard. Pure searches do not deteriorate any data pool, but are regularly possible with poor data quality in the forensic area of perpetrator identification without problems.

Finally, a common processing standard (M1-378) was developed for Prüm, which was used by all systems. Essential for a meaningful trace processing is also the possibility of the usability of the Record 9 templates which are possible over this standard. Trace processing, especially for important criminal offences, always takes place in individual case coding procedures by forensic experts, where the minutia are also checked individually and corrected before they are coded and sent to the matcher from the national AFIS.

6.2 EC study contractor proposal - Usage and accuracy reporting and improve candidate lists

This proposal also has no discernible added value. The national AFIS work with different match algorithms and completely different GUI and reporting tools.

The transmission of different score values from national systems does not offer any added value in the work of other experts. If meaningful rankings should be implemented by the MS, this is only possible via the micro matcher solutions already defined by the expert group.

6.3 EC study contractor proposal – Priority Based Scheduling

The proposal of different processing levels according to importance ranging between 12, 24 and 28 hours has no added value. The current check functionality already has functioning Prüm AFIS priority levels. However, these are usually never needed. The maximum processing time of the agreed quotas of 24 hours is completely sufficient. In practice, TP/TP searches are carried out within a few minutes in all states and latent searches usually within maximum 30 minutes in all Prüm partner states, even if no higher priorities are defined.

In the forensic area, the processing time of latent data is usually of completely subordinate priority. It usually takes days until dacty latents can be used for AFIS processing after securing at the crime scene and often needed time consuming chemical latent visualization methods processed from experts in dactyloscopic labs.

The TP/TP search process also does not have the same processing time requirements as e.g. a border control process which must be completed within seconds. In the forensic area, for example, subsequent investigations are carried out or, in the case of urgent queries, the persons concerned are usually detained.

More important than speed in the forensic area is the possibility to search and find hits with very poor latent data quality and following validation / verification process performed by forensic fingerprint experts.

Essential is not an acceleration of the Prüm 1 step processes that function excellently with the presently fixed data quality, but the acceleration of the subsequent data provision.

6.4 EC study contractor proposal - Pooled Quotas

The study contractor recommended a pooling of the quota for which unused queries of a partner could be used by other partners in order to make better exploit of the daily possible search quantities. As already mentioned in this document before, the agreed quota restrictions are not a problem in principle. According to the current state of knowledge, only a smaller EU MS cannot fully meet the quota requests of other partners due to a very small AFIS. Of course, it would be much less costly for such a Member State to substitute these relatively low costs for expansions by financing problems with EU subsidies than to develop a very complicated and costly quota-polling system that also cannot function operationally. It is not possible to deprive a state of its rightful query quantities up to a time of day that must necessarily be fixed, as this could then sometimes no longer carry out important queries of its own crimes and criminals.

Such a proposal was strictly rejected by the expert group.

6.5 EC study contractor proposal - feature data exchange (templates)

Of course, the current NIST or also other forensic and technical standards are always used for new developments which are state of the art during definition of new ICD anyway. However, the versions of NIST standards mentioned by the study contractor differ from older standards - because of the always necessary back value compatibility - mostly only in additionally possible data contents or transaction types. From very comprehensive NIST standards, only the tools will be used which are really needed in Prüm cooperation.

As to the suggestion of the study contractor use a direct template in Prüm search procedures, such a template is already given with the latent comparisons (record type 9 comparison) where it is already necessary.

When using TP/TP data, they are not desired, since the automated coding processing of the image information in these procedures works with better quality and results, since the specific own AFIS coding and match algorithms of the system that performs the search are always used. This makes it possible to achieve higher match accuracies. Whether the search process with template use is minimally accelerated does not play any role in the Prüm context as stated. This proposal was rejected.

7 Verification

7.1 Human Intervention for forensic conformation and Core Data exchange

Legislation regarding data exchange requires expert verification. There is need for human intervention before starting any case of follow-up data exchange (even for core data exchange). This is necessary because of data protections rules and ensuring correct results before further investigation work should be started. Experts could be located in different organization units of the requesting Member State.

The responsibility for forensic verification always lies with the respective state, which then also requests the subsequent data. These national forensic services provider have been subject to the accreditation Directive since November 2015 and are therefore quality-assured.[3]

For possible follow up data provision after such human verification, see the explanations above.

8 Data format communication

Technical formats for communication platforms should be harmonized. One File Format for all Prüm data types (DNA, Dacty, Face Recognition) maybe split over different verification processes. The use of a standard format shouldn't change the whole Prüm system and no complex changes in the national systems are needed. The latest generation of NIST / Interpol standard formats for the transmission of biometric data should still be examined by the technical experts for a possible suitability of a new data format solution that is as uniform as possible. More details on the data format and metadata will be discussed in the next focus group meetings.

All 3 areas should use the same standard (AFIS, FACE, DNA).

It has also been agreed that UMF3+ should not be part of Prüm 1step data categories and exchange because in this area specific standards exists. Instead it should be stated that UMF3+ is a technical standard for the exchange in the general police cooperation or could be used in maximum for planned 2nd step core data structure.

[3] COUNCIL FRAMEWORK DECISION 2009/905/JHA of 30 November 2009 on Accreditation of forensic service providers carrying out laboratory activities

9 Annex

2nd Step Core Data / REFERENCE DATABASE / All Biometric Data Types

- **Alphanumeric Personal Data**
  - Family Name (m)
  - First Name (m)
  - Name of birth
  - Former names
  - Date of birth (m)
  - Place and country of birth (m)
  - Gender (m)
  - Nationality
  - Alias/Nickname
  - Status of Identity (Identity confirmed or not)
  - Further identity information (e.g. description, marks, tattoos)
  - CRN – Criminal Reference Number
  - National Identification Number
  - Address/Contact Information
  - First Name of Parents
  - Information about convictions/suspicions, current investigations

- **Information of biometrics acquisition (Face Image, Dactyloscopic data, DNA-Profile)**
  - Date of biometric acquisition
  - Place of biometric acquisition
  - Reason of biometric acquisition (e.g. type of crime etc.)
  - Source of biometric (Database)
  - File Number (s) (CRN)
  - Responsible Authority

- **Additional Biometric data information (depends on request)**
  - Additional Face Images
  - Dactyloscopic data
  - DNA available yes/no/unknown
  - DNA – Profile (Match report after DNA-Hit)
  - Information on additional DNA-Data (e.g. Y-DNA, mt-DNA etc.)
  - DNA-Kit Information
  - EN/ ISO 17025 accreditation status

- **Identity documents (**e.g. number, type of document, issued authority, scan/image of document**)**

- **Other data**
  - Technical information (e.g. hash-value etc.)
  - Alert information (e.g. arrest warrant etc.)
  - Warning information (e.g. weapons, twins etc.)
  - Prior Convictions
  - Free text

2nd Step Core Data / LATENT / All Biometric Data Types

- Date of biometric acquisition
- Place of biometric acquisition
- Reason of biometrics acquisition (e.g. crime, dead body)
- Source of biometrics (database)
- File number (CNO, SQN, MID)
- Responsible authority
- Free text

Additional Biometric data information (depends on request)

- Additional Face Images
- Dactyloscopic data
- DNA available yes/no/unknown
- DNA – Profile (Match report after DNA-Hit)
- Information on additional DNA-Data (e.g. Y-DNA, mt-DNA etc.)
- DNA-Kit Information
- EN/ ISO 17025 accreditation status