Council of the
European Union

Brussels, 8 October 2019
(OR. en)

12511/19

LIMITE

DAPIX 273
CRIMORG 131
ENFOPOL 417
ENFOCUSTOM 159
JAI 986

NOTE

From:	Presidency
To:	Working Party on Information Exchange and Data Protection (DAPIX)
No. prev. doc.:	14950/2/16 REV 2; 10649/19
Subject:	Prüm Decisions - dactyloscopic data exchange of the United Kingdom - Report of the evaluation visit (London, 10-11 September 2019)

The current report is based on the reply of the United Kingdom to the relevant questionnaire on data protection (14950/2/16 REV 2) and on an elaborated version of the reply to the questionnaire on dactyloscopic data exchange (10649/19), and includes the findings of the evaluation team during the visit.

In accordance with Council Decisions 2008/615/JHA and 2008/616/JHA, Germany, represented by experts of the German Federal Criminal Police Office (Bundeskriminalamt Deutschland - BKA) as partner state of the UK in the framework of implementing the provisions concerning dactyloscopic data exchange, made a visit to London from 10 to 11 September 2019.

The UK Home Office took great interest in the work and on-site findings of the evaluation team. The members of the German evaluation team received all requested information and were able to come into direct contact with the representatives who will apply the daily Prüm procedures in future.

The evaluation was carried out in line with the elaborated version of the questionnaire on dactyloscopic data exchange set out in Annex II. All points set out were explained in detail by UK delegates.

1. Participants of the evaluation and locations visited

The list of the evaluation team members is set out in Annex I.

The evaluation visit took place at the following location:

Metropolitan Police Service (MPS), Directorate of Forensic Services, 109 Lambeth Road, London, SE1 7LP, UK

2. Questionnaires

The UK has notified the General Secretariat of the Council of having implemented its relevant obligations prior to the evaluation procedure by means of the replies to the questionnaire on data protection (14950/2/16 REV 2) and the questionnaire on dactyloscopic data exchange (10649/19).

3. Pilot run / test run

The test run was performed between the automated fingerprint identification system (AFIS) test beds of the BKA Germany and the UK Home Office. The pilot run was performed in the operational (production) AFIS environments of both parties.

Each test was run as follows:

- Connection test over the TESTA NG network,
- Encrypted connection tests over the TESTA NG network,
- Data exchange procedures in accordance with Article 9 of Council Decision 2008/615/JHA using the Austrian Test Data Set Version 3.0

The results of the pilot run are set out in Annex III of this report.

4. Focal points

The following part of the report draws on the main aspects of the Prüm implementation by the UK law enforcement authorities. Chapters 4.1 to 4.5 give an overall view on the UK national Forensic Information Database Services, data processing, retention and protection. Chapters 4.6 to 4.8 describe the Prüm implementation in detail. All information given in the sub-chapters was provided by the UK administration to the German evaluation team members.

4.1 General overview – UK system landscape and responsibilities

The UK Home Office provides national fingerprint database services to several law enforcement authorities and other stakeholders. At present, there are two separate significant fingerprint systems in the Home Office sector. 'IDENT1' is the name given to the system supporting law enforcement, while the Immigration and Asylum Biometrics System (IABS) supports immigration. IDENT1 is used for verification and identification purposes. The system is used by trained practitioners to verify the identity of up to a million people each year taken into custody and arrested or detained. It is also used to identify suspects, witnesses and exclude innocent people through matching latent marks found at crime scenes or elsewhere by linking such marks to known persons. A discrete dataset is held within IDENT1 for national security purposes. IDENT1 is also set up to maintain the arrest history, closely coupled to the UK Criminal History System, which is the main criminal history database of subjects and the identity of offenders. Therefore, fingerprints are taken in every case of arrest to identify the subject.

IDENT1 comprises the UK national tenprint collection, which consists of fingerprint images obtained from people who have been arrested for a recordable offence within any UK jurisdiction, and unidentified finger marks obtained from scenes of crime. Police Elimination fingerprints (used for eliminating possible crime scene fingerprints from persons with legitimate access to a scene of crime), fingerprints from volunteers and vulnerable persons, and fingerprints relating to Schengen information system alerts and counter terrorism (CT) measures are also stored on IDENT1 and available for authorized searches.

The Metropolitan Police Service (MPS) Forensic Services is the processor for the CT fingerprint and DNA Databases and is accountable to both the Forensic Information Databases Strategy Board and National Security Biometrics Board (NSBB) for maintaining the integrity of the data held on the CT databases and for ensuring the efficient and effective provision of the database infrastructure, information, and services.

UK print sets from persons who are convicted will be available for search with the remaining UK data stock having separate governance and legislation.

To maintain the public confidence in these services, the UK Home Office is responsible for continuously examining whether the system is run under the conditions set out in the respective UK legislation and is in line with UK governance. To ensure the integrity of data held in the systems, it has set up a data assurance strategy, which controls the access and the use of law enforcement fingerprint records. Under this strategy the Forensic Information Database Services (‘FINDS’) is implemented. FINDS sets out the requirements for access and use of the national law enforcement fingerprint databases and services and maintains the data integrity between the systems.

4.2 Technical aspects related to the UK AFIS (IDENT1)

IDENT1 is physically run in two IT data centres and consists of more than 500 points of presence, among others 54 local bureau systems with 1,150 workstations attached.

Hosting and maintaining software applications and infrastructure falls into the responsibility of the Home Office.

IDENT1 holds fingerprint data of 9 million convicted individuals materializing in 23 million sets of ten prints and 13 million palm print pairs. Furthermore it holds 2 million unresolved crime scene marks.

The following friction ridge data is stored and searchable on IDENT1 AFIS for Prüm purposes:

- Tenprint rolled fingers
- Segmented plain (slap/flat) fingers
- Lower palm prints
- Writer's palm prints
- Latent finger marks
- Latent palm marks (lower palm or writers palm areas)

4.3 Organizational aspects

4.3.1 Service provider and stakeholders to IDENT1

The Home Office runs the immigration (IABS) and policing fingerprint databases (IDENT1). In doing so, its core objectives are to cut crime, prevent terrorism, control immigration and to support the UK's safeguarding agenda.

Concerning IDENT1, law enforcement agencies are responsible for

- loading print sets into the system obtained under UK legislation,
- searching latent marks recovered within their jurisdiction,
- loading unidentified latent marks into the national collection.

Law enforcement stakeholders to IDENT1 and their respective roles are

Stakeholder	Role
Home Office Digital Data & Technology	IDENT1 Product management
UK Visas and Immigration	Cross reference law enforcement fingerprints for immigration decisions
Immigration Enforcement	
Crime and Policing Group	Develop policy for biometric retention
International Criminality and Extradition Directorate	Develop policy for international biometric exchange
Office of Security & Counter Terrorism	Biometric use for counter terrorism and national security
The Forensic Science Regulator	Setting standards for forensic processes
Home Office Science	Home Office oversight of the use of UK forensic databases
The Biometrics Commissioner	Independent oversight of the use and retention of biometric samples.

External stakeholders to IDENT1 are

Stakeholder	IDENT1 related Role
National Crime Agency	Investigation and prevention of serious criminality across the UK, international exchange of biometric data.
National Police Chief's Council	Accountability for the IDENT1 law enforcement fingerprint data asset
Police & Crime Commissioners	Democratically elected Commissioner of a Police force ensuring police activity meets the needs of their electorate
The 43 Police Forces of England & Wales	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
Police Service of Northern Ireland	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
British Transport Police	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
HM Revenue and Customs	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction

Police Scotland	Investigation and prevention of crime and data controller for data collected and processed within their jurisdiction
The Scottish Government	Setting legislation relating to the collection and retention of biometric samples collected for the investigation and prevention of crime in Scotland
College of Policing	Setting the training standards and curriculum for Police Officers and Staff, specifically those involved in fingerprint processing and comparison
NPCC Criminal Records Office (ACRO)	UK central authority for international exchange of criminal records and provides national criminal record management and subject access services

4.3.2 IDENT1 and its relationship to the UK Criminal History System

To maintain the arrest history and the identity of offenders, IDENT1 is constructed as a subsystem to the UK Criminal History System on the PNC (Police National Computer). Each arrest event is given a unique arrest/summons number entry (AS) and recorded on the UK PNC. The linkage between IDENT1 and PNC ensures the proper retention of the whole criminal history data, including fingerprint data, as UK retention laws can be easily applied to fingerprints obtained for law enforcement purposes.

4.3.3 IDENT1 and its relation to the UK Forensic Information Database Services

The UK Forensic Information Database Services (FINDS) under the responsibility of the UK Home Office process fingerprint data to provide forensic matches which contribute to solving crime, including the facility to provide 24/7 support to the investigation of urgent crimes, most of which relate to serious offences. FINDS ensures that the records on IDENT1 (and in other systems) are accurate in order to support the criminal justice system and the principles of the data protection. It investigates and corrects all data errors on IDENT1 on behalf of the data owners.

It ensures that the database and its supporting policies are compatible with the current technology and developed to accommodate emerging technological advances. It contributes furthermore to wider business change within the forensic community by supporting the Home Office Biometrics Programme and the Transforming Forensics Programme and any other initiatives that require the skills and experience of the unit. Moreover, it supports the responsibilities defined within the Strategy Board governance rules.

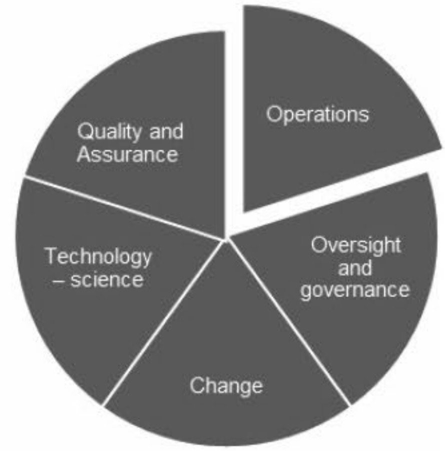


Figure 01: Overview FINDS responsibilities to IDENT1

4.4 Data retention

The retention periods for fingerprints and DNA profiles are specified in the UK Protection of Freedoms Act 2012 (POFA). DNA and fingerprint provisions are the same and are given in the tables below. The Act strikes a balance between protecting the freedoms of those who are innocent of any offence whilst ensuring that the police continue to have the capability to protect the public and bring criminals to justice.

For Prüm fingerprint data exchange only data of convicted persons are made available to the Member States. In that context it is to be noted that 98 per cent of individuals registered on Police National Computer for which the UK holds biometric samples have a conviction.

Retention for Convictions

Situation	Fingerprint and DNA Retention
Any age convicted (including given a caution or youth caution) of a recordable qualifying offence	Indefinite
Adult convicted (including given a caution) of a recordable minor offence	Indefinite
Under 18 convicted (including given a youth caution) of a recordable minor offence	1st conviction: 5 years (plus length of any prison sentence), or indefinite if the prison sentence is for 5 years or more. 2nd conviction: indefinite

Data retention for non-convictions

Situation	Fingerprint and DNA Retention
Any age charged with but not convicted of a recordable qualifying offence	3 years plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested for but not charged with a qualifying offence	3 years if granted by the Biometrics Commissioner plus a 2 year extension if granted by a District Judge (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Any age arrested for or charged with a minor offence	None (or indefinite if the individual has a previous conviction for a recordable offence which is not excluded)
Adult given a Penalty Notice for Disorder	2 years

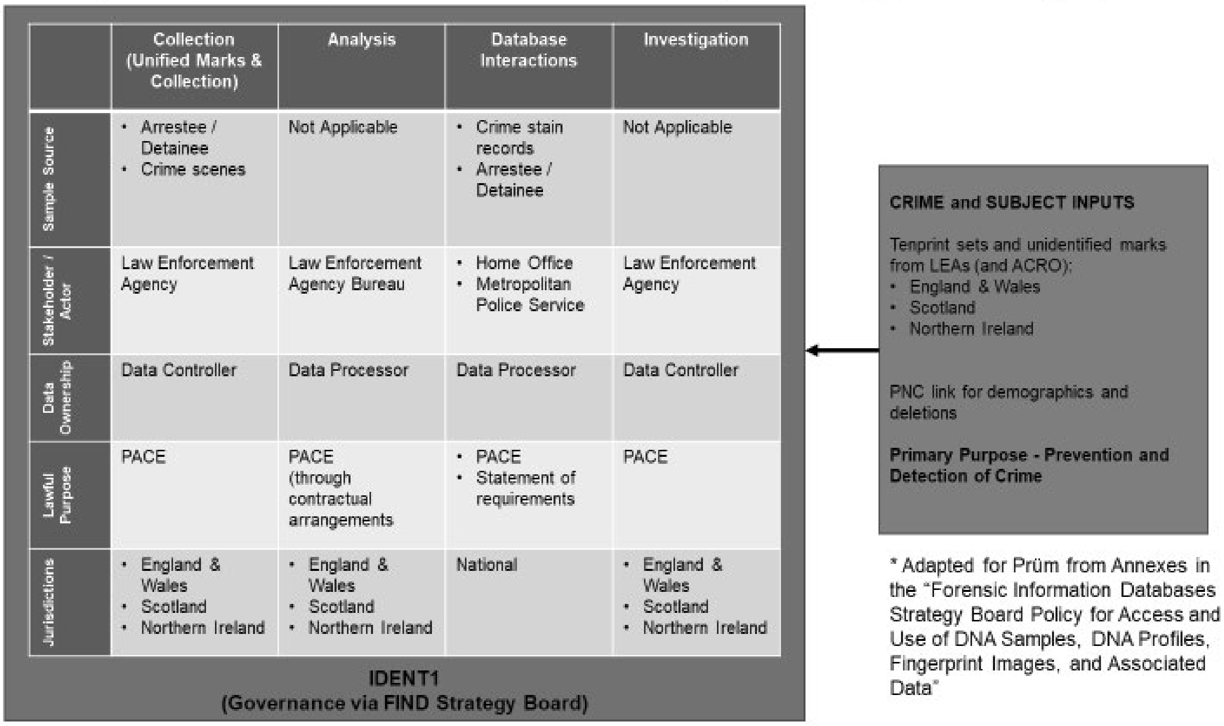
4.5 Data protection and data responsibility

The Forensic Information Databases Strategy Board was given a legislative footing in the POFA 2012. It is responsible for the overall strategic management of the databases, including IDENT1. It takes strategic decisions to balance the freedoms of the individual whilst making the tool operationally effective. It has a parliamentary accountability through POFA 2012 for the national DNA database (NDNAD) and IDENT1.

The Strategy Board comprises representatives of the National Police Chiefs Council, the Home Office, the Biometrics and Forensics Ethics Group, the Association of Police and Crime Commissioners, the Forensic Science Regulator (or representative), the Information Commissioner's Office, the Biometrics Commissioner (or representative), representatives from the police and devolved administrations of Scotland and Northern Ireland and such other members who may be invited.

The data on FINDS is owned by the Police (represented by the National Police Chiefs Council). The data held on IDENT1 is the property of the individual police forces – each chief constable is a data controller. The chair of the Strategy Board acts as joint data controller. The Home Office and each forensic service provider (organizations granted permission by the Forensic Information Databases Strategy Board to provide forensic services to law enforcement agencies) are data processors, whereby every organization has to have a data protection officer. The overall process is shown in the diagram below.

Overall process, defining stakeholders, data ownership, authority, and lawful purpose*



	Collection (Unified Marks & Collection)	Analysis	Database Interactions	Investigation
Sample Source	• Arrestee / Detainee • Crime scenes	Not Applicable	• Crime stain records • Arrestee / Detainee	Not Applicable
Stakeholder / Actor	Law Enforcement Agency	Law Enforcement Agency Bureau	• Home Office • Metropolitan Police Service	Law Enforcement Agency
Data Ownership	Data Controller	Data Processor	Data Processor	Data Controller
Lawful Purpose	PACE	PACE (through contractual arrangements	• PACE • Statement of requirements	PACE
Jurisdictions	• England & Wales • Scotland • Northern Ireland	• England & Wales • Scotland • Northern Ireland	National	• England & Wales • Scotland • Northern Ireland

IDENT1
(Governance via FIND Strategy Board)

CRIME and SUBJECT INPUTS

Tenprint sets and unidentified marks from LEAs (and ACRO):

- England & Wales
- Scotland
- Northern Ireland

PNC link for demographics and deletions

Primary Purpose - Prevention and Detection of Crime

* Adapted for Prüm from Annexes in the "Forensic Information Databases Strategy Board Policy for Access and Use of DNA Samples, DNA Profiles, Fingerprint Images, and Associated Data"

Figure 02: Overall UK Data Protection Processes

The UK data protection legislation consists of

- the General Data Protection Regulation (GDPR) (EU) 2016/679
- the UK Data Protection Act (DPA) 2018, which was enacted on 25th May 2018. (This includes the Police Directive (EU) 2016/680, which was incorporated as Part 3 of the DPA 2018)

GDPR and DPA 2018 together make up the UK 'data protection legislation':

- Part 2 covers general processing
- Part 3 covers law enforcement processing
- Part 4 covers intelligence services processing

4.6 1st step information exchange (AFIS-interconnection)

4.6.1 Technical Architecture

The UK technical solution for connecting to the Prüm network and for processing incoming and outgoing requests consists of three major systems, interconnected with IDENT1 AFIS.

a) UK Government E-Mail, which is part of the UK governmental IT infrastructure, used for encrypted communication over TESTA NG with Prüm partner states.

b) The Prüm landing zone, where messages from the Prüm partner states are received, signature validation, message decryption and anti-virus scanning is performed. Also, this gateway is responsible for transforming incoming requests from the technical standard compliant with the Prüm interface control document (ICD) to the IDENT1 internal technical standard HONE-1 (Home Office NIST Exchange) for further processing.

c) The Biometric Services Gateway (BSG), where incoming messages are aggregated, queued and audited before processing through IDENT1 AFIS. For outgoing messages, message separation and transformation (to Binary) as well as message signing and encryption is performed by this part of the system. The data transformation is needed as, for example, some of the Prüm types of transactions (TOT) differ from the internal Home Office TOTs for processing in IDENT1. Nevertheless, all Prüm TOTs and the required areas of friction ridge detail, as defined in the Prüm ICD, are supported by the UK solution.

d) The Prüm Gatekeeper Service will authorize outgoing Prüm requests to ensure that the maximum allowable number for the target Member State is not breached (→ quota management). To provide an equitable basis for authorizing search requests there will be two cut off points during the day. Each will be allocated 50 per cent of the available search capacity.

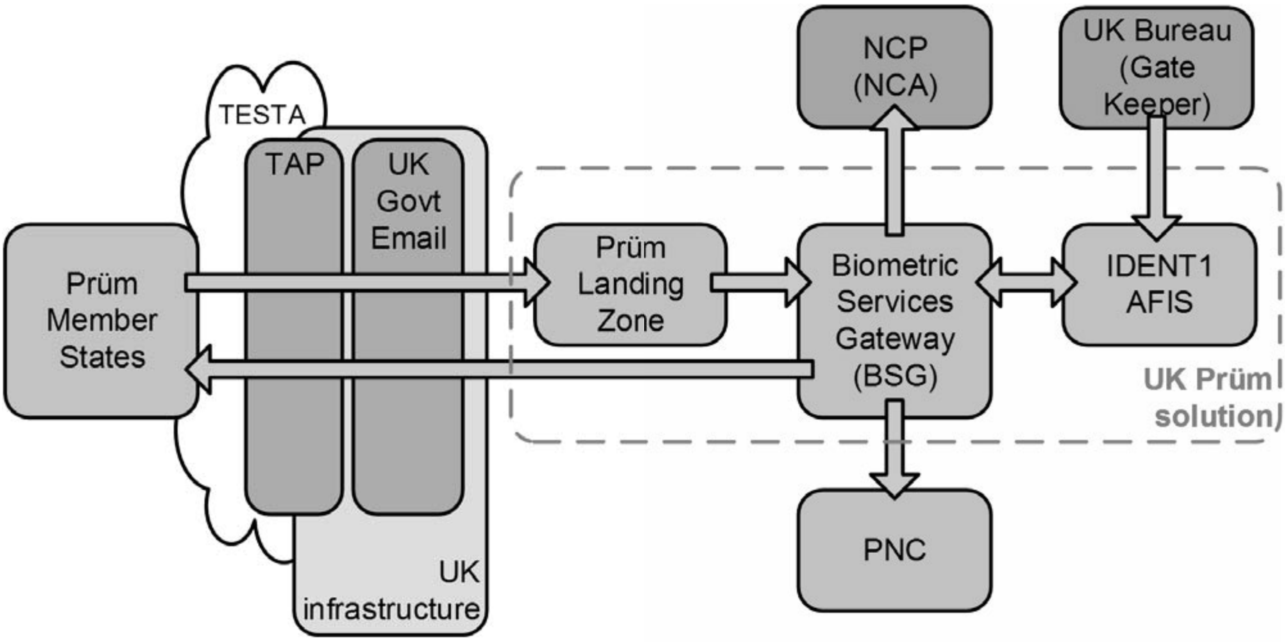


Figure 03: Overview UK Prüm technical solution

4.6.2 Prüm data processing and priority levels

The BSG and IDENT1 are designed to deal with volumes of transactions of many thousands per day pertaining to UK law enforcement processing, and deal with requests, in most cases, within a few minutes. The introduction of Prüm transactions has been incorporated into this existing high volume solution. All Prüm transactions will be processed within minutes rather than hours.

A high priority level can be set in an incoming Prüm request and the UK solution will accept this high priority request (as well as any priority code set in the Prüm NIST message). All Prüm requests will effectively be treated as high priority due to the processing speeds that will be provided by HO systems. Prüm requests will not be batched or placed in queues behind standard search requests to IDENT1 made from within the UK.

4.6.3 Auditing and logging

The UK Prüm implementation utilizes existing audit functions in the BSG. The BSG is the primary audit store for Prüm messages and meets the Prüm logging requirements. All messages (in and out) are audited. Key identifiers are inserted into specific columns to facilitate searching. Prüm entries are flagged to distinguish them from other audited messages.

All Base64 encoded images relating to original Prüm NIST records are hashed using MD5.

A daily process runs to identify Prüm audit entries older than 24 months. At 24 months the Type-2 is also hashed. The only audit remaining after 24 months is meta-data reflecting that there was an exchange, but no detail about that exchange.

The core AFIS has also been designed to meet Prüm requirements and ensure that business data in audited records are overwritten after 24 months.

4.6.4 Operational Security

HO has adopted several processes to assure the Prüm fingerprint service:

Physical security – Prüm services are hosted in secure locations in accordance with Police assured secure facilities (PASF) requirements.

Personnel security – All support personnel hold national security vetting to Secure Check (SC) and Non-Police Personnel Vetting Level 3 (NPPV3).

Independent IT health checks (ITHC) – All services are subject to independent ITHCs in accordance with the National Cyber Security Centre (NCSC) CHECK Scheme.

Monthly security reviews – A monthly operational security report is produced for discussion at a security working group (SWG) that focusses on any security incidents, vulnerabilities and status on remediation of technical debt (where applicable).

4.6.5 Support Service

For any issues encountered with Prüm fingerprint requests addressed to the UK, a service desk solution has been installed for 24/7 monitoring, which operates as depicted in figure 04.

Planned or/unplanned outages will be communicated to the Prüm partner states.

The UK incident contact point for : Prüm partner states is

ITNOWSERVICEDESK@homeoffice.gov.uk

A technical contact point is available under

spoc_fp_admin@fp.pruem.gb.testa.eu

The Service Manager contact details are

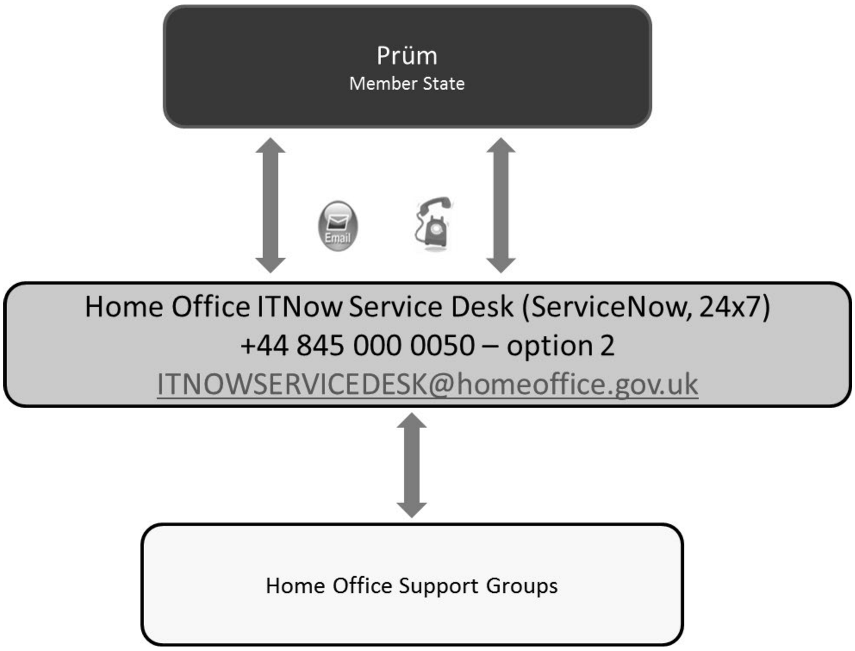

Prüm
Member State
Email
Home Office ITNow Service Desk (ServiceNow, 24x7)
+44 845 000 0050 – option 2
ITNOWSERVICEDESK@homeoffice.gov.uk
Home Office Support Groups

Figure 04: Flow chart depicting UK's Service Desk solution

4.7 Initiation of outgoing Prüm searches

The Prüm fingerprint data exchange is solely processed by the Metropolitan Police Service (MPS) for all UK LEA stakeholders. All outgoing search requests are authorized through the Prüm gatekeeper function which consists of a dedicated team within MPS that utilises the secure UK communication network to receive and respond to outbound Prüm search requests from UK LEAs.

Incoming search results are processed by MPS as depicted in figure 05 and figure 06 below and in line with the forensic policy (cf. chapter 4.7.1 of this report).

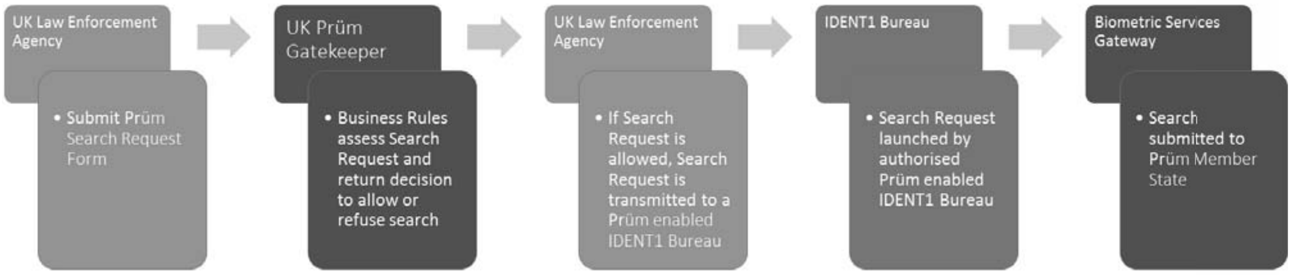

UK Law Enforcement Agency
• Submit Prüm Search Request Form
UK Prüm Gatekeeper
• Business Rules assess Search Request and return decision to allow or refuse search
UK Law Enforcement Agency
• If Search Request is allowed, Search Request is transmitted to a Prüm enabled IDENT1 Bureau
IDENT1 Bureau
• Search Request launched by authorised Prüm enabled IDENT1 Bureau
Biometric Services Gateway
• Search submitted to Prüm Member State

Figure 05: Flow chart – Prüm 1st step search initiation

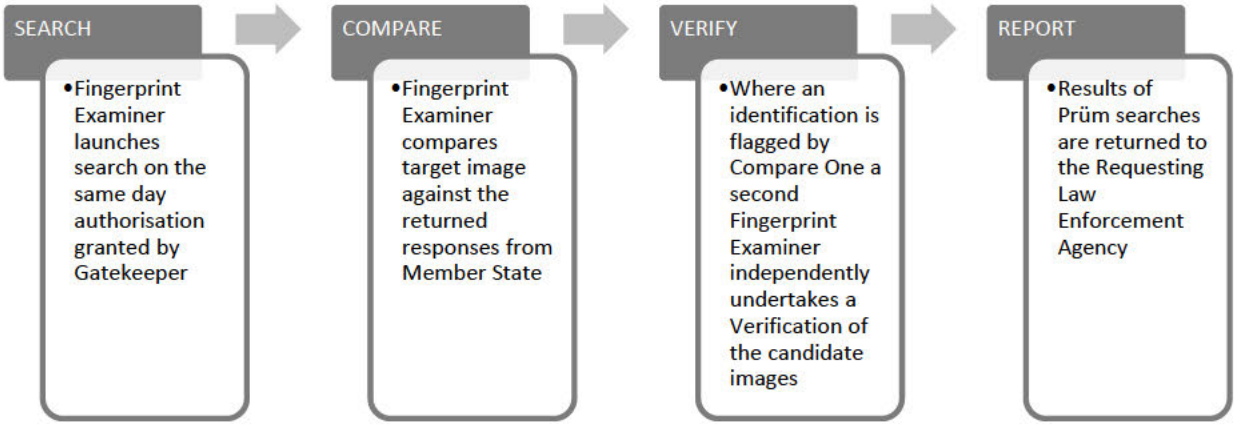

SEARCH
•Fingerprint Examiner launches search on the same day authorisation granted by Gatekeeper
COMPARE
•Fingerprint Examiner compares target image against the returned responses from Member State
VERIFY
•Where an identification is flagged by Compare One a second Fingerprint Examiner independently undertakes a Verification of the candidate images
REPORT
•Results of Prüm searches are returned to the Requesting Law Enforcement Agency

Figure 06: Flow chart – Prüm 1st step outgoing search verification

4.7.1 Fingerprint examination accreditation and Forensic Policy

All forensic services within the MPS (as the legal entity) that fall within the Codes of Practice and Conduct of the Forensic Science Regulator will be delivered through a single corporate Quality Management System that is accredited to international standards, subject to external third party accreditation and operated by the Directorate of Forensic Services.

The Director of Forensic Services will on behalf of the Commissioner be the Senior Accountable Person for ensuring that the MPS meets the quality standards set by the Forensic Science Regulator and that all forensic staff who give evidence as an expert witness comply with their duty under the Criminal Procedure Rules.

Fingerprint Accreditation covers

- Codes of Practice and Conduct for Fingerprint Comparison
- Guidance for Validation: Friction Ridge Detail Search Algorithm
- Codes of Practice and Conduct for Fingerprint Examination – Terminology, Definitions and Acronyms

4.8 2nd step information exchange (police cooperation / follow up correspondence)

Within the National Crime Agency (NCA), the UK International Crime Bureau (UKICB) provides the UK National Central Bureau for INTERPOL, the UK Europol National Unit and the UK SIRENE Bureau. The workflow for processing incoming and outgoing 2nd step information exchange requests are depicted in figure 07 of this report.

The UKICB uses a case information management system (CIMS) to research review and assessment of relevant information and intelligence data associated with people, objects, locations and events for a policing purpose to

- identify and prevent operational compromise and conflicts of interest,
- assist in mutual cooperation where two or more parties have an active interest in the same entity,
- provide a signpost for strategic and tactical information which may support the assessment of serious and organized crime in the UK as described in legislation.

A step 2 Prüm response covers the following data (where available):

- Nominal Data (Demographics)
- Criminal history (Disclosure Print)
- Custody Photograph (if available)
- Fingerprints (NIST and JPEG if available)
- Warning markers (if available)
- Current Location and associated intelligence entities
- UK Crime Information / Investigation (crime stains)

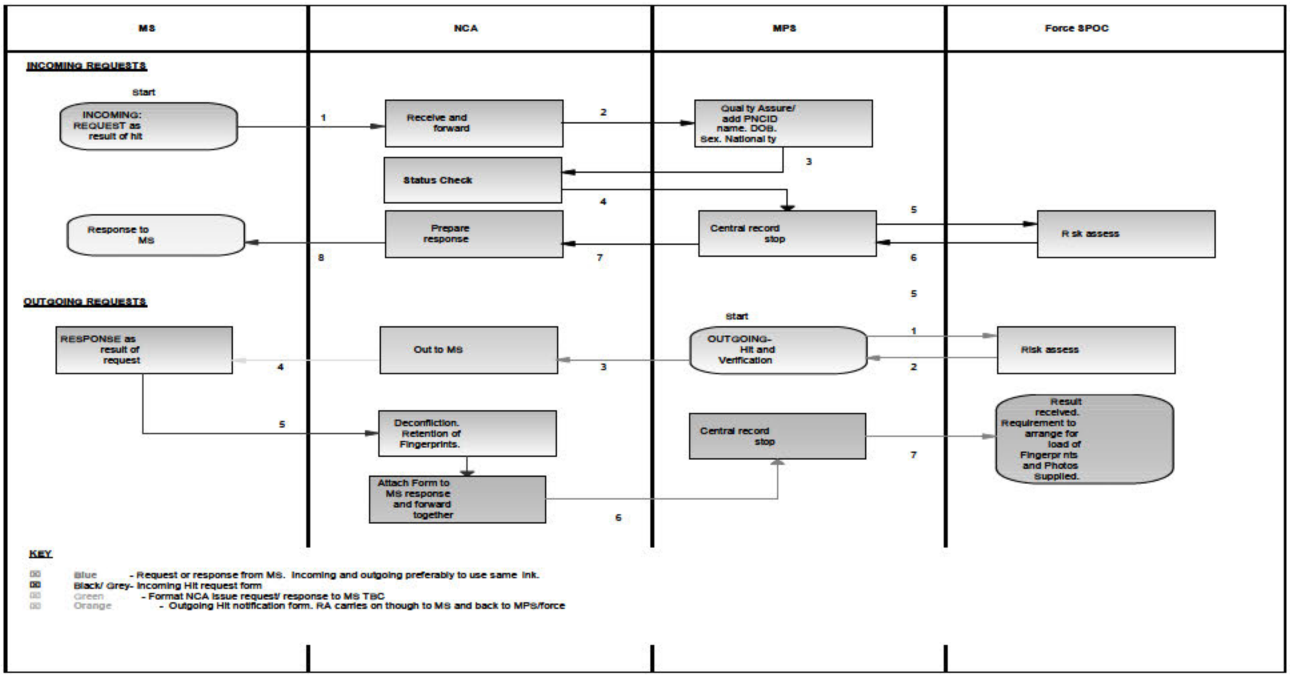

MS
NCA
MPS
Force SPOC
INCOMING REQUESTS
Start
INCOMING: REQUEST as result of hit
1
Receive and forward
2
Qual ty Assure/ add PNCID name. DOB. Sex. National ty
3
Status Check
4
Central record stop
5
R sk assess
6
7
Prepare response
8
Response to MS
OUTGOING REQUESTS
5
Start
OUTGOING- Hit and Verification
1
Risk assess
2
3
Out to MS
4
RESPONSE as result of request
5
Deconfliction. Retention of Fingerprints.
Attach Form to MS response and forward together
6
Central record stop
7
Result received. Requirement to arrange for load of Fingerpr nts and Photos Supplied.
KEY
Blue - Request or response from MS. Incoming and outgoing preferably to use same ink.
Black/ Grey- Incoming Hit request form
Green - Format NCA issue request/ response to MS TBC
Orange - Outgoing Hit notification form. RA carries on though to MS and back to MPS/force

Figure 07: Flow chart incoming/outgoing 2nd step information request

The National Contact Point for Step 2 is

NCB Manchester

UK International Crime Bureau (UKICB)

National Crime Agency

+44 (0) 207 238 8115 (operated 24hrs)

5. Recommendations given to the UK authorities

Whilst none of the points raised below impact on the technical evaluation, they capture some broader observations made by the BKA experts during the pilot and the visit. They should be considered by the UK and have been included for completeness of the report.

5.1 Data stock made available by UK for Member States in the context of Prüm

As described in chapter 4.4 of this report, the UK will only make available data of convicted subjects to the Member States in the context of Prüm. This was already subject to discussions on the automated Prüm exchange of DNA data subsequent to the evaluation visit conducted by Austria, Germany and France on 1 - 2 August 2018. Several Member States claimed this to be a violation of the principle of availability of law enforcement information (cf. Council Framework Decision 2006/960/JHA), which is considered a corner stone of European law enforcement data exchange.

The Council concluded on the successful implementation of the general provisions on data protection of Chapter 6 of Council Decision 2008/615/JHA by UK with the following mandatory requirement:

"*Furthermore, the Council requests that, within 12 months from the launching of the automated data exchange, the United Kingdom review its policy of excluding suspects' DNA data files, in the light of operational experience with Prüm DNA data exchange and of the explanations in the evaluation visit report (11545/18). If, by then, the United Kingdom has not notified the Council that it makes available suspects' DNA data files, the Council will, within three months, re-evaluate the continuation or termination of the automated DNA data exchange with the United Kingdom.*"

Because both DNA and fingerprint provisions refer to the UK Protection of Freedoms Act 2012 (POFA), the Home Office is therefore recommended to align the provisions on dactyloscopic data exchange and to agree on the timeline set in Council Implementing Decision (EU) 2019/968.

5.2 2nd step data exchange – Choice of channel

During the evaluation visit the representatives of the NCA stated that current the UK policy determines that the INTERPOL route is used for international biometric exchanges. Note – this is for UK governance for control, measuring and reporting purposes.

As on European level it is recommended but not mandatory to use the Europol channel respectively the SIENA tool for 2nd step information exchange in the context of Prüm (cf. Strengthening law enforcement cooperation in the EU: The European Information Exchange Model (EIXM); COM(2012) 735 final), the use of the Interpol channel does legally not affect the operational data exchange. Nevertheless, all incoming requests, which are sent via the SIENA tool by the requesting Prüm partner state and which are answered by NCA through Interpol, may lead to organizational or even technical problems in the requesting Member States. The UK is considering a review of this policy at the same time as the review on the use of suspects fingerprints takes place.

The UK Home Office is therefore recommended to review the current policy for the processing of 2nd step information requests that are not communicated via Interpol to NCA as proposed above.

5.3 Legacy NIST-files in 2nd step information exchange

During the evaluation visit, the NCA representatives stated that electronic fingerprints which are usually added to biographical data as answer to 2nd step information requests are transmitted in the format of NIST respectively as so called NIST-files. That is fully in line with international biometric data exchange rules. However, some records held in IDENT1 contain fingerprint and latent images that are compressed with jpeg algorithms (as WSQ compression was not available when IDENT1 was initially implemented). Although still compliant with NIST standards, the use of JPEG compression for print or latent images is considered legacy. Today, biometric services would rather expect NIST-files containing fingerprint images that are compressed by jpeg2000 or WSQ algorithms. This output may be possible depending on whether an internal conversion is provided in the solution between IDENT1 and NCA and prior to data being provided in the 2nd step information.

The UK Home Office is therefore invited to check whether this internal data conversion can be implemented so that fingerprint data may be provided to requesting Member States in WSQ format where a NIST-file is part of the 2nd step information provided by the NCA to a Prüm partner state. This would ensure the proper handling of such legacy NIST-files in the receiving country.

5.4 IDENT1 not capable of displaying unsegmented flat finger prints

During the pilot run, it was noted by HO that IDENT1 is currently not capable of displaying non-segmented flat fingerprints (NIST position codes 13 and 14) to its fingerprint expert users when comparing responses to MPS requests. This was unexpected and had not manifested during internal testing carried out by the UK using the Austrian data set. The UK had originally not anticipated that non-segmented flat fingerprints would be returned as part of a mark to print search (MPS) response search result (SRE). However, as this kind of data may be returned from other PRÜM AFIS (like Germany) as part of the MPS search result, the UK solution will need to be able to receive and process it. This issue only affects outgoing searches conducted by the UK. All incoming transactions are processed according to the Prüm ICD (2008/616/JHA) in IDENT1.

During the evaluation visit, the Home Office stated that the problem has been identified and is being tackled already, and that a technical solution is currently being agreed between the Home Office and the IDENT1 AFIS contractor.

The UK Home Office is therefore invited – for information purposes only – to report to the Member States when the issue is closed.

5.5 Display of national ID of fingerprint data in IDENT1

During the evaluation visit, it was noted by the evaluating experts that in IDENT1 all search results (fingerprint data received by EU partners' AFIS) are assigned a UK internal Prüm ID in the main respondents panel of the AFIS verification screen. The reason for this is due to legacy restrictions on the behaviour of this particular respondents panel and the allowable number formats that it can support. The national ID of the data set assigned by the sending Member State can be seen by opening a dedicated additional window ("More Details" dialogue box) in the user interface. Without adequate user training, this may lead to the circumstance that the MPS fingerprint experts report the UK internal Prüm ID to its NCA partner who may ask for additional information via a 2nd step information request to the respecting Prüm partner state with the incorrect reference.

As it is impossible for the current system behaviour of IDENT1 to be changed to display the reference of the fingerprint data assigned by the Prüm partner state in the main respondents panel, the UK Home Office is therefore invited to emphasize the procedure and need to look up the correct external ID within the training procedures of MPS experts that operate the Prüm service.

6. Conclusions

Based on the outcome of the relevant questionnaires, the results of the pilot run and the evaluation visit, the evaluation team considered the implementation of the Prüm dactyloscopic data application and the related Prüm dactyloscopic data information flow as successfully concluded both on legal and on technical level in the UK. However, the experts strongly advise the UK to follow the recommendations given in chapter 5 to use the Prüm fingerprint data exchange to the full extent both in the UK as well as in the Member States taking part in the data exchange.

The evaluation team proposes that the Working Party on Information Exchange and Data Protection (DAPIX) discuss this report and subsequently inform the Council that for the purposes of automated searching of dactyloscopic data, UK has satisfactorily implemented the provisions of Council Decision 2008/615/JHA and Council Decision 2008/616/JHA.

ANNEX I

List of participants

DE participants			
Mr		BKA Germany	Department IT 26 – Biometric Systems
Mr		BKA Germany	Department ZI 21 – AFIS Management
UK Participants			
Ms	Cressida Dick	Metropolitan Police Service	Commissioner
Ms		Metropolitan Police Service	
Mr		Metropolitan Police Service	
Ms		Metropolitan Police Service	Quality Lead
Mr		Metropolitan Police Service	
Ms		Home Office Biometrics Programme	
Ms		Home Office Biometrics Programme	Project Support
Mr		Home Office Biometrics Programme	Security
Mr		Home Office Biometrics Programme	Data Protection
Mr		Home Office Biometrics Programme	Service Support
Mr		National Crime Agency	UK International Crime Bureau
Mr		National Crime Agency	
Mr		Home Office Biometrics Programme	Technical Architect
Mr		Home Office Biometrics Programme	Technical Architect
Mr		Home Office Biometrics Programme	Business Analysis
Ms		Home Office	Policy Lead
Mr		Home Office	Police National Computer
Mr		Home Office	Forensic Information Database Service (FINDS)

Questionnaire on exchange of dactyloscopic data pursuant to Article 9 of Council Decision 2008/615/JHA (as set out in EU Doc 6661/09 REV 3)

1. Organisational

1.1. Please provide the details of your Member State's national contact point for incoming requests been designated.

Home Office

2 Marsham Street

London SW1 4DF

Tel: +44 845 000 0050

Email: ITNOWSERVICEDESK@homeoffice.gov.uk

1.2. Does your Member State intend to use a central national contact point for the follow-up consultation procedure after hit notifications (2nd step consultation procedure)?

National Crime Agency

UK International Crime Bureau

PO Box 58345

London NW1 9JJ

Tel: +44 207 238 8115

Fax: +44 207 238 8112

e-mail: Manchester@nca.gov.uk

2. Technical

2.1. Can the national contact point connect onto the TESTA-network?

The UK Home Office will provide the national contact point for "step 1" of the Prüm process. The Home Office is connected to the TESTA-network and will use the spoc_fp_admin@fp.pruem.gb.testa.eu email address

2.2. Has your AFIS been connected to a sMIME v.3 compliant mail server?

The core Law Enforcement AFIS communicates with external requestors via the Biometric Services Gateway (BSG). The BSG has been expanded with the implementation of dedicated inbound and outbound mail servers specifically for Prüm transactions, compliant with sMIME v3.

2.3. Does your mail server follow the processing rules defined in chapter 1.5.4 of the Annex to Council Decision 2008/616/JHA?

The UK solution uses two different groups of mail servers – one group for inbound and one group for outbound traffic

All clauses / rules are met in the UK implementation for both mail servers, operating over TESTA-NG.

2.4. Is the configuration of your mail server compliant to chapter 1.5.7.4 of the Annex to Council Decision 2008/616/JHA?

As an existing user of TESTA the UK already has IP addresses on the TESTA network

In addition, to support the Evaluation pilot (and ongoing system validation), the UK's AFIS has been seeded with the 'Austrian data set'

2.5. Is your AFIS capable to process requests in a fully automated way?

Prüm request processing by all components of the UK 'AFIS solution' (Mail Landing Zone, BSG and Law Enforcement core AFIS) is designed to be fully automated as required.

2.6. Is your AFIS compliant to the data format specified in the "Interface Control Document (ICD)" defined in chapter 2 of the Annex to Council Decision 2008/616/JHA?

The boundary of the UK solution, provided via the BSG and Landing Zone, ensures full compliance with the Prüm ICD format.

Due to transformation into the Home Office ‘internal’ NIST format prior to routing via the BSG, the core AFIS does not use the Prüm ICD format itself. However, it complies with all of the processing requirements of the Prüm ICD.

2.7. Is your AFIS capable to process within 24 hours all incoming requests defined and agreed in the table with maximum daily searches?

The BSG and core AFIS are designed to deal with volumes of transactions of many thousand per day pertaining to UK law enforcement processing and deal with requests, in most cases, within a few minutes. The introduction of Prüm transactions has been incorporated into this existing high volume solution. All Prüm transactions will also be processed within minutes rather than hours.

2.8. Is your AFIS able to handle requests with high priority?

A high priority level can be set in an incoming Prüm requests and the UK solution will accept this high priority request (as well as any priority code set in the Prüm NIST message). Further to the response in 2.7, all Prüm requests will effectively be treated as high priority due to processing speeds that will be provided by HOB systems.

2.9. Is your AFIS able to handle requests linked to fingerprint searches (transaction types CPS, PMS, SRE ERR)?

All Prüm TOTs and the required areas of friction ridge detail, as defined in the Prüm ICD, are supported by the UK solution.

2.10. Is your AFIS able to handle requests linked to fingerprint latent searches (transaction types MPS, MMS, SRE ERR)?

Cf. answer to question 2.9

2.11. Is your AFIS able to handle requests linked to palmprint searches (transaction types PMS, SRE, ERR)?

Cf. answer to question 2.9

2.12. Is your AFIS able to handle requests linked to palmprint latent searches (transaction types MPS, MMS, SRE, ERR)?

Cf. answer to question 2.9

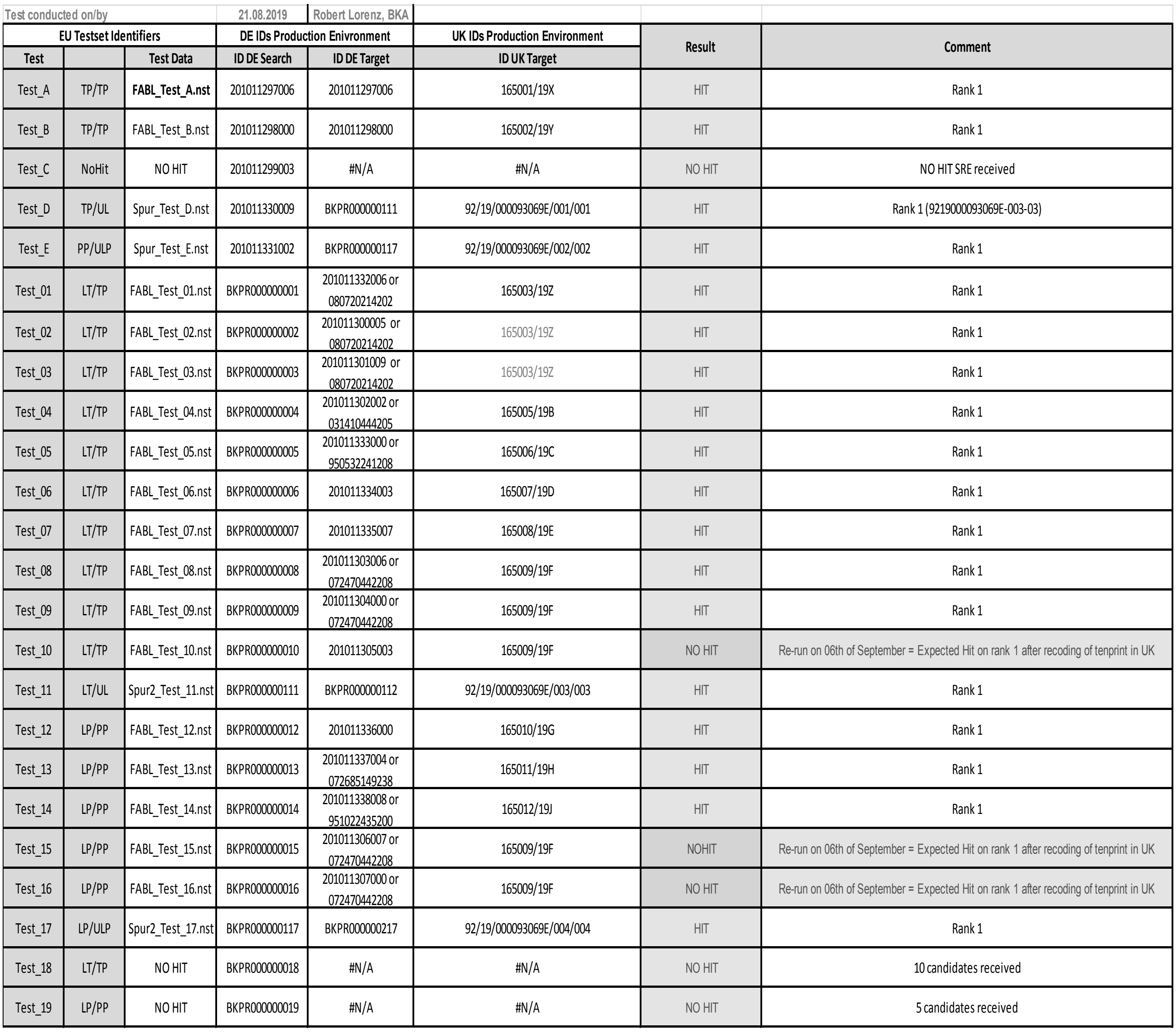
2.13. Does your national technical workflow ensure that you will not exceed the maximum number of requests defined and agreed in the table with maximum daily searches?

The UK process for Prüm requests requires outgoing requests to be authorised through a gatekeeper function that will ensure the maximum allowable number for the target Member State is not breached.

ANNEX III

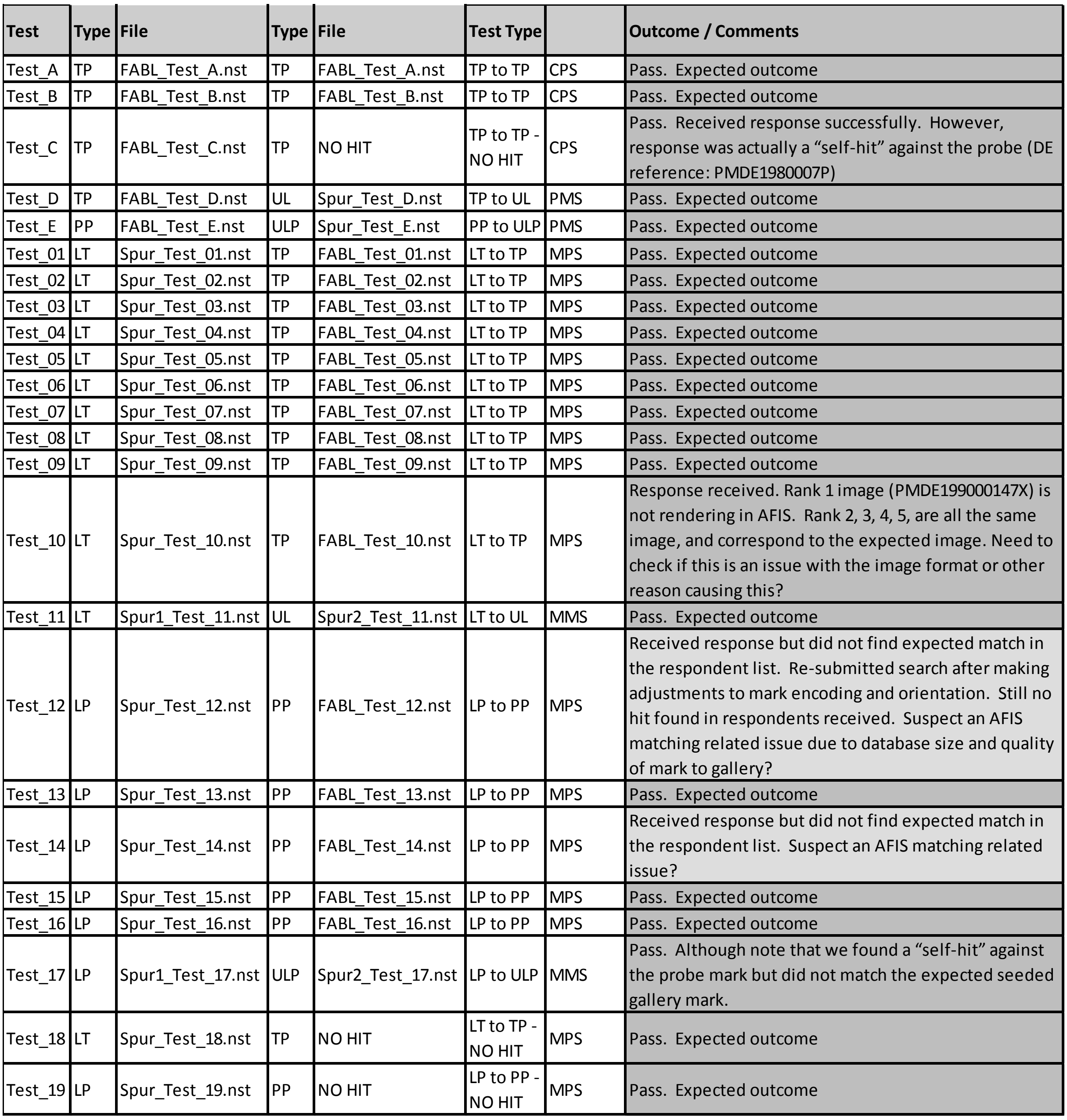
Report of the pilot run between Germany and UK from 21st to 23rd of August 2019

a) Test protocol DE BKA



Test conducted on/by			21.08.2019	Robert Lorenz, BKA			
EU Testset Identifiers			DE IDs Production Enivronment		UK IDs Production Environment	Result	Comment
Test		Test Data	ID DE Search	ID DE Target	ID UK Target		
Test_A	TP/TP	**FABL_Test_A.nst**	201011297006	201011297006	165001/19X	HIT	Rank 1
Test_B	TP/TP	FABL_Test_B.nst	201011298000	201011298000	165002/19Y	HIT	Rank 1
Test_C	NoHit	NO HIT	201011299003	#N/A	#N/A	NO HIT	NO HIT SRE received
Test_D	TP/UL	Spur_Test_D.nst	201011330009	BKPR000000111	92/19/000093069E/001/001	HIT	Rank 1 (9219000093069E-003-03)
Test_E	PP/ULP	Spur_Test_E.nst	201011331002	BKPR000000117	92/19/000093069E/002/002	HIT	Rank 1
Test_01	LT/TP	FABL_Test_01.nst	BKPR000000001	201011332006 or 080720214202	165003/19Z	HIT	Rank 1
Test_02	LT/TP	FABL_Test_02.nst	BKPR000000002	201011300005 or 080720214202	165003/19Z	HIT	Rank 1
Test_03	LT/TP	FABL_Test_03.nst	BKPR000000003	201011301009 or 080720214202	165003/19Z	HIT	Rank 1
Test_04	LT/TP	FABL_Test_04.nst	BKPR000000004	201011302002 or 031410444205	165005/19B	HIT	Rank 1
Test_05	LT/TP	FABL_Test_05.nst	BKPR000000005	201011333000 or 950532241208	165006/19C	HIT	Rank 1
Test_06	LT/TP	FABL_Test_06.nst	BKPR000000006	201011334003	165007/19D	HIT	Rank 1
Test_07	LT/TP	FABL_Test_07.nst	BKPR000000007	201011335007	165008/19E	HIT	Rank 1
Test_08	LT/TP	FABL_Test_08.nst	BKPR000000008	201011303006 or 072470442208	165009/19F	HIT	Rank 1
Test_09	LT/TP	FABL_Test_09.nst	BKPR000000009	201011304000 or 072470442208	165009/19F	HIT	Rank 1
Test_10	LT/TP	FABL_Test_10.nst	BKPR000000010	201011305003	165009/19F	NO HIT	Re-run on 06th of September = Expected Hit on rank 1 after recoding of tenprint in UK
Test_11	LT/UL	Spur2_Test_11.nst	BKPR000000111	BKPR000000112	92/19/000093069E/003/003	HIT	Rank 1
Test_12	LP/PP	FABL_Test_12.nst	BKPR000000012	201011336000	165010/19G	HIT	Rank 1
Test_13	LP/PP	FABL_Test_13.nst	BKPR000000013	201011337004 or 072685149238	165011/19H	HIT	Rank 1
Test_14	LP/PP	FABL_Test_14.nst	BKPR000000014	201011338008 or 951022435200	165012/19J	HIT	Rank 1
Test_15	LP/PP	FABL_Test_15.nst	BKPR000000015	201011306007 or 072470442208	165009/19F	NOHIT	Re-run on 06th of September = Expected Hit on rank 1 after recoding of tenprint in UK
Test_16	LP/PP	FABL_Test_16.nst	BKPR000000016	201011307000 or 072470442208	165009/19F	NO HIT	Re-run on 06th of September = Expected Hit on rank 1 after recoding of tenprint in UK
Test_17	LP/ULP	Spur2_Test_17.nst	BKPR000000117	BKPR000000217	92/19/000093069E/004/004	HIT	Rank 1
Test_18	LT/TP	NO HIT	BKPR000000018	#N/A	#N/A	NO HIT	10 candidates received
Test_19	LP/PP	NO HIT	BKPR000000019	#N/A	#N/A	NO HIT	5 candidates received

b) Test protocol UK Home Office



Test	Type	File	Type	File	Test Type		Outcome / Comments
Test_A	TP	FABL_Test_A.nst	TP	FABL_Test_A.nst	TP to TP	CPS	Pass. Expected outcome
Test_B	TP	FABL_Test_B.nst	TP	FABL_Test_B.nst	TP to TP	CPS	Pass. Expected outcome
Test_C	TP	FABL_Test_C.nst	TP	NO HIT	TP to TP - NO HIT	CPS	Pass. Received response successfully. However, response was actually a "self-hit" against the probe (DE reference: PMDE1980007P)
Test_D	TP	FABL_Test_D.nst	UL	Spur_Test_D.nst	TP to UL	PMS	Pass. Expected outcome
Test_E	PP	FABL_Test_E.nst	ULP	Spur_Test_E.nst	PP to ULP	PMS	Pass. Expected outcome
Test_01	LT	Spur_Test_01.nst	TP	FABL_Test_01.nst	LT to TP	MPS	Pass. Expected outcome
Test_02	LT	Spur_Test_02.nst	TP	FABL_Test_02.nst	LT to TP	MPS	Pass. Expected outcome
Test_03	LT	Spur_Test_03.nst	TP	FABL_Test_03.nst	LT to TP	MPS	Pass. Expected outcome
Test_04	LT	Spur_Test_04.nst	TP	FABL_Test_04.nst	LT to TP	MPS	Pass. Expected outcome
Test_05	LT	Spur_Test_05.nst	TP	FABL_Test_05.nst	LT to TP	MPS	Pass. Expected outcome
Test_06	LT	Spur_Test_06.nst	TP	FABL_Test_06.nst	LT to TP	MPS	Pass. Expected outcome
Test_07	LT	Spur_Test_07.nst	TP	FABL_Test_07.nst	LT to TP	MPS	Pass. Expected outcome
Test_08	LT	Spur_Test_08.nst	TP	FABL_Test_08.nst	LT to TP	MPS	Pass. Expected outcome
Test_09	LT	Spur_Test_09.nst	TP	FABL_Test_09.nst	LT to TP	MPS	Pass. Expected outcome
Test_10	LT	Spur_Test_10.nst	TP	FABL_Test_10.nst	LT to TP	MPS	Response received. Rank 1 image (PMDE199000147X) is not rendering in AFIS. Rank 2, 3, 4, 5, are all the same image, and correspond to the expected image. Need to check if this is an issue with the image format or other reason causing this?
Test_11	LT	Spur1_Test_11.nst	UL	Spur2_Test_11.nst	LT to UL	MMS	Pass. Expected outcome
Test_12	LP	Spur_Test_12.nst	PP	FABL_Test_12.nst	LP to PP	MPS	Received response but did not find expected match in the respondent list. Re-submitted search after making adjustments to mark encoding and orientation. Still no hit found in respondents received. Suspect an AFIS matching related issue due to database size and quality of mark to gallery?
Test_13	LP	Spur_Test_13.nst	PP	FABL_Test_13.nst	LP to PP	MPS	Pass. Expected outcome
Test_14	LP	Spur_Test_14.nst	PP	FABL_Test_14.nst	LP to PP	MPS	Received response but did not find expected match in the respondent list. Suspect an AFIS matching related issue?
Test_15	LP	Spur_Test_15.nst	PP	FABL_Test_15.nst	LP to PP	MPS	Pass. Expected outcome
Test_16	LP	Spur_Test_16.nst	PP	FABL_Test_16.nst	LP to PP	MPS	Pass. Expected outcome
Test_17	LP	Spur1_Test_17.nst	ULP	Spur2_Test_17.nst	LP to ULP	MMS	Pass. Although note that we found a "self-hit" against the probe mark but did not match the expected seeded gallery mark.
Test_18	LT	Spur_Test_18.nst	TP	NO HIT	LT to TP - NO HIT	MPS	Pass. Expected outcome
Test_19	LP	Spur_Test_19.nst	PP	NO HIT	LP to PP - NO HIT	MPS	Pass. Expected outcome

Additional notice: Test 12 and test 14 were re-run several times after the formal pilot run, but the expected candidates were not retrieved in the German AFIS in these tests. The subject was still under investigation while this report was produced. As all other tests have been accomplished successfully, there seem to be specific problems with the encoding (placement of minutiae or ridge details) in the German AFIS. Although these issues occurred, the pilot run was seen as successfully conducted by both Member States.