The Council also noted that since its competences for carrying out Schengen evaluations ceases on 1 January 2016, the continuation of the evaluation process must take place in the framework of the new evaluation mechanism. The Council therefore invited the Commission to carry out the recommended revisit under the new Schengen evaluation mechanism. On this basis and in line with the new evaluation and monitoring mechanism to verify the application of the Schengen *acquis*, as established by Council Regulation (EU) No 1053/2013[5] and an annual evaluation programme for 2017,[6] Commission and Member State experts and an observer from eu-LISA (the on-site team) carried out a Schengen evaluation revisit of the implementation of the SIS in the UK from 5 to 10 November 2017. This draft report has been established by the on-site-team on the basis of the UK's replies to the questionnaire,[7] on-site visits and additional information provided by the UK during the evaluation process.

In addition, in order to address the issues of the incorrect implementation of Council Decision on the establishment, operation and use of the second generation SIS 2007/533/JHA (hereinafter Decision 2007/533/JHA)[8] observed by the Commission during the evaluation of 2015, the Commission launched an own initiative EU-Pilot case against the UK (letter to the UK sent 3 August 2015). The Commission sought explanation from the UK on the unavailability of SIS at the primary border checkpoints, the copying of certain SIS alerts into the Warning Index database used by the UK Border Force, the de-synchronisation of the technical copy of the end-users caused by the proportionality test for checking the execution of European Arrest Warrants (EAW) and the fact that the UK has started to carry out the search functionality based on fingerprints although this was not legally provided for at the time. The latter question was clarified in the meantime, but the remaining issues are still pending as the Commission decided to suspend the procedure until the completion of the evaluation revisit.

2. THE REVISIT

The on-site team visited:

SIRENE Bureau (Warrington)

Hendon Data Centre

SIS (Semaphore) Local Technical Copy site

Metropolitan Police headquarters

Watchlist and Information Control Unit

National Border Targeting Centre

Folkstonejuxtaposed control checkpoint

---

5 OJ L 295, 6.11.2013, p. 27.

6 Commission Implementing Decision C(2016) 7387 establishing the first section of the annual evaluation programme for 2017 in accordance with Article 6 of Council Regulation (EU) No1053/2013 of 7 October 2013 establishing an evaluation and monitoring mechanism to verify the application of the Schengen acquis.

7 Schengen evaluation of the United Kingdom - Replies to the Schengen evaluation questionnaire (Document number 13484/13 SCH-EVAL 112 COMIX 490 RESTREINT UE/EU RESTRICTED).

8 Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generationSchengen Information System (SIS II) (OJ L 205, 7.8.2007, p. 63).

Coquelles juxtaposed border checkpoint

Heathrow airport

Southampton Airport

Edinburgh airport

Heathrow Police Station

Command and control Centre in Bilston Glen (Scotland)

Surprise visits:

Hendon police station

Hampshire Police Investigation Center (Basingstoke)

Hampshire police Operational Headquarters (Winchester)

ACRO Criminal Records Office

Police Hampshire Special Branch (Southampton)

British Transport Police (Edinburgh Waverley railway station)

Scottish Police (Wester Hailes police station)

Barnet Borough Police (Collindale Police Station)

Kent Police – Special Branch Command Centre Folkestone

3. FINDINGS OF THE ON-SITE TEAM

3.1. General introduction

The on-site team concluded that some major deficiencies in the legal, operational and technical implementation of SIS identified during the evaluation of 2015 were not effectively remedied and still persist.

The on-site team has identified several areas where it considers that the implementation of SIS in the UK is contrary to the core objectives and the legal framework of the system. Such implementation is also contrary to the reciprocity and mutual recognition which serve as a basis of the SIS cooperation and jeopardises the integrity of data stored in SISas well as the security of SIS data at the borders:

- **The use of SIS copies by the UK:**

  – The UK has a significant number of full or partial copies of the SIS database (listed in Section 3.1).Three of the SIS copies are administered by different private companies in their own premises or in rented premises. The UK authorities noted that the physical and data security of those copies is subject to the same level of security rules and controls as the copies that are administered by the Home Office. Nevertheless such set-up makes it much more

challenging to monitor the security of the data and prevent potential security breaches. Moreover, it creates difficulties for the synchronisation of the copies with the national copy as well as for the management and implementation of changes.

- The Warning Index (WI), which is available at first and second line border controls, is a watchlist which contains certain SIS alerts issued for arrest, alerts for missing persons and alerts on persons subject to discreet or specific check in accordance with Article 36 of the Decision 2007/533/JHA. The Warning Index does not contain "the full collection" of those alert categories but only those which are considered important by the UK (*e.g.* non-flagged alerts for arrest[9], vulnerable missing persons, etc.). This activity constitutes an unlawful copying of SIS data into a national database. Furthermore, the Warning Index is only updated once a day as a result of which none of the urgent SIS alerts uploaded to the SIS Central System (CS-SIS) are available at the UK border control up to 24 hours later.
- It was observed that the different technical copies of the SIS database are not fully synchronised. Examples were noticed whereAlerts, that were already deleted from CS-SIS,were still displayed in the various technical copies, such as the Police National Computer (PNC) available to police officers on the UK territory. The Warning Index also holds information on deleted SIS alerts.

These practices constitute serious and immediate risks to the integrity and security of SIS data as well as for the data subjects as the UK applies a selective approach in processing of SIS data for different purposes by splitting the database. This practice is contrary to Article 9(2) of the Decision 2007/533/JHAconcerning the requirement that a search carried out in CS-SIS must produce the same result as in the national or technical copies.It is also contrary toArticle 10 (1)(c) aiming to prevent unautoorised copying of SIS data.Moreover,it is very difficult to follow-up the data processing chain and it is uncertain whether the data is properly maintained and whether it is updated or deleted as required by the Decision 2007/533/JHA.

- **Selective approach to SIS data by the UK:**

  - The UK is applying a selective approach to the data contained in some of the copies. The Warning Index does not contain all categories of SIS alerts but only those categories which the UK considers to be important. Only alerts for arrest (except the ones issued by the Schengen Associated Countries), vulnerable missing persons and discreet and specific check alerts issued pursuant to Article 36 of the Decision 2007/533/JHAare displayed. This means that alerts on documents or persons sought for judicial purposes are not available at the UK borders. In addition, the UK also searches only non-flagged alerts for arrest within the SIS technical copy used by national Border Targeting Centre for checks on Advance Passenger Information (API) and Passenger Name Records (PNR). The UK was recommended to make available all categories of SIS alerts at its border already back in 2015, however, this recommendation was not implemented.

---

9 Flagging of an alert for arrest means that the Member State does not recognise the European Arrest Warrant issued by another Member State and it will not arrest the person subject of an EAW but it will only note and communicate the whereabouts of the person.

- **Limited reciprocity in the UK's SIS implementation:**

  - Alerts for arrest (extradition requests) issued by the Schengen Associated countries are systematically flagged in the UK.In accordance with the Decision 2007/533/JHAthe consequence of setting a flag is that the person cannot be arrested but only his/her whereabouts are noted. In the UK such alerts are not available at the borders.In line with the 2003 Extradition Act of the UK extradition requests from the Schengen Associated Countries can only be executed if the person wanted for arrest is known to be on the territory of the UK. Only if the UK authorities are informed that the person wanted for arrest by a Schengen Associated Country resides in the UK willthe Metropolitan Police actively search for him.
  - The UK still applies restrictions for the recognition of European Arrest Warrants (EAW) issued by a Member State and the corresponding alerts in SIS. All alerts for arrest issued by a Member State must undergo a validation process in the UK before they are released to the end-users. The SIRENE Bureau is carrying out this process which can last up to four hours; it is in fact an examination whether the arrest warrant fulfils all formal requirements and a proportionality test examining if the issued EAW is proportionate according to the UK as an executing country. During this period the end-users cannot see and find this alert.
  - The UK does not recognise a high number of EAW by adding a flag to the corresponding SIS alert.[10] Flagged SIS alerts are not available at the UK borders as they are not copied over either in the Warning Index or to Semaphoresystem used by national Border Targeting Centre. Moreover, flagged alerts for arrest are changed into alerts for criminal judicial purposes for the checks on the territory. Consequently, the end-user cannot see that the original alert is for arrest but he/she can only see that the person must provide his/her whereabouts for the purposes of a criminal judicial procedure. In this manner the UK changes arbitrarily the alert category without informing the alert issuing Member State.The numberof flagged alerts decreased since 2015, however the rate is still high compared to other Member States.
  - The UK also applies the aforementioned four hour validation process to discreet and specific check alerts issued for immediate reporting pursuant to Article 36 of the Decision 2007/533/JHA. Those alerts are only released to the end-users once the validation by the SIRENE Bureau is completed and the national security services have been notified.
  - The UK changes the discreet check or specific checks alerts issued pursuant to Article 36 with immediate reporting action into normal Article 36 alertswhen copying them into the Warning Index.
  - According to theUK's official College of Policing Guidance the UK officers are instructed not to seize objects subject to an alert issued pursuant to Article 38 of the Decision 2007/533/JHA. The officers are instructed to seize an item only if it relates to an offence committed on the UK's territory or it supports or forms part of a UK investigation or prosecution. Therefore, for instance, vehicles stolen on the territory of another Member State and located on the UK territory are not seized.

10 On 1 December 2017 there were 3000 alerts for arrest in SIS which were flagged by the UK. For comparison, Germany flagged 1166 alerts for arrest.

- The UK does not always take action on the alerts for arrest when the subject of the alert is located in the outbound area of the UK ports. While the UK authorities indicated that these situations arise due the insufficient timeframe to arrest the person, several Member States noted that they receive reoccurring information from the UK SIRENE Bureau about the impossibility to take the action while the subject is still present on the territory of the UK. In such cases the UK SIRENE Bureau warns the issuing Member State and the Member State of destination that a person subject to an EAW will land or arrive.
- As there is no physical border control upon exit in the UK, only non-flagged alerts for arrest are available at the external borders upon exit on the basis of PNR and API data. Other alert categories in SIS are not checked upon exit.
- The UK does not systematically add fingerprints and photographs to the alerts which it issues, even in situations where they are available.

- **Limited national end-user IT applications:**

- The end-user applications used by police and border force are outdated and display only limited information. The applications are not capable to accommodate binary data such as photographs or fingerprints. There is no reference to the existence of the EAW attached to the alert. Only the SIRENE Bureau has this data available. There is no procedure whereby the end-users would be obliged to send this data to the SIRENE Bureau for adding it to the alert or to contact the SIRENE Bureau to obtain this information.
- The Warning Index, the border control application used for first and second line border checks, displays even less information, essentially only the reason why the alert was inserted and who has to be contacted. This does not facilitate the situation of the border guards in identifying the subject of the alert or take the appropriate action as additional identification information such as photographs and fingerprints are not provided.
- Both the police and the border force applications use "fuzzy queries" which lead to a large amount of results. Officers monitoring the electronic border control gates (eGates) may face difficulties in matching the possible results to the person passing the eGate in case of a discreet check due to the numerous results returned by a fuzzy query and the lack of photographs and other identity details displayed by WI. Exact identification is only possible if the person is sent to a further check to the booth in case of ahit. The UK authorities explained that whenever a potential match is returned at the eGates which contain a non-stopping action, such as on discreet check alerts, WI will indicate that a discreet check is required. The list of potential matches will be presented to the monitoring officer for review. The monitoring officer checks the list of potential matches and if the passenger is the subject of an alert the officer will make a discreet note, take a printed copy, and allow the passenger to proceed. The monitoring officer will then report the hit through the back office systems. The problem with this practice is that the monitoring officer is not able to ascertain the identity of the person and consequently may report false hits or non-confirmed matches.
- Vehicle registration services do not have access to SIS.

The UK has presented a project of launching a completely new IT infrastructure for police and border control purposes. The project isto be finalised by 2020-2021, however according to the

presentation provided during the on-site visit the SIS developments do not form explicit part of the project.[11]

3.2. Statistics on the use of SIS in the UK

On 1 November 2017, the UK had 1 013 466 alerts, of which 31 867 (3.14%) concerned persons and 981 599 (96.86 %) concerned objects, mostly issued document alerts which the UK started to upload only recently. The UK has not inserted any alerts on banknotes, blank documents, license plates, vehicle registration documents or securities.

In 2016 the UK performed 514 160 087queries in SIS which is the second highest number among the Member States. In 2016 the UK reportedonly 9 542 hits on foreign alerts. This number of reported hitsis not considered to be commensurate to the high number of queries made by the UK. The UK also reported12 047 hits on its own alerts abroad.

The number of photographs and fingerprint records entered by the UKin accordance with Article 20 of the Decision 2007/533/JHAis very low compared to the number of person alerts (31 867) – on 1 November 2017 there were 174 fingerprint records and 321 photograph records in the system.

3.3. Applicable legislation

Several legislative and regulatory changes needed to be implemented to allow for the application of the SIS in the UK:

- the Extradition Act 2003 was amended to allow the certification of a warrant on the basis of an European Arrest Warrant or a SIRENE A form sent electronically, as set out in section 204;
- safeguards were introduced relating to the processing of personal data received from, or made available by, an authority in another Member State in Regulation 38 of the Criminal Justice and Data Protection (Protocol No.36) Regulations 2014;
- "Detention at Port" powers were introduced under the UK Borders Act 2007, allowing the Border Force to detain an individual for up to three hours at the border where they are liable to arrest, or formally subject to a warrant for arrest. This legislation establishes that individuals subject to a European Arrest Warrant who are encountered at the ports as a result of a SIS alert will not be held during the controls using immigration powers but will be detained according to the "Detention at Port" provisions. The police are responsible for executing any formal arrest.

3.4. Demonstration of integration of SIS into the national applications

3.4.1. National systems and applications for SIS queries

- **Police National Computer (PNC):**

[11] Following the on-site visit the UK authorities sent the following clarification: "SIS II forms part of the project plans for both the new border systems (Border Crossing, part of Digital Services at the Border), and the new police system (National Law Enforcement Database)." A timeline was not provided.

The Police National Computer (PNC) is the main front-line operational policing information system in the UK. It contains details of the national criminal records and convictions; national wanted/missing person reports; disqualified drivers; sexual offenders; firearms certificate holders; records of all vehicles registered in the UK and their insurance; records of all Great Britain's drivers' licences and certain categories of stolen property. PNC also queries Police National Database (PND). SIS alerts are made available to the end-users via a local technical copy which is referred to as PNC.SIS copy.

The PNC is also the main user application used for SIS queries by the police end-users. However PNC application provides only limited information to the end-user in case of a hit on a SIS alert:

- it does not display photographs, nor does it provide reference to the existence of fingerprints or an EAW. PNC does not indicate that pictures, fingerprints or EAW (together referred to as "binary data").are available at the SIRENE Bureau. The recommendation to introduce binary data was not implemented since the evaluation in 2015;
- there is no additional data for the purpose of dealing with misused identities. No "misused identity extension" is available in PNC; only the information that this is a "misused identity". as a consequence, it is nearly impossible to identify who is a victim and who is a perpetrator, since there is no possibility to distinguish to which identity the "misused identity" marker is related;
- the identity status as displayed in PNC as "confirmed by photograph, fingerprints or DNA" is misleading as it has a different meaning from "confirmed identity" in SIS. The end-users interviewed during the on-site visit (e.g. in Operational Headquarters of Hampshire) presumed that the identity of a person is indeed "confirmed by photographs, fingerprints or DNA", which is not always the case. The Evaluation Committee recommended the UK authorities to review the mapping from SIS to PNC already in 2015;
- when an alias is displayed in PNC, the ID status remains "confirmed by photograph, fingerprints or DNA" as this is attached to the main identity record. It may cause confusion for the end-users which may think that the identity is confirmed although it is an alias;
- the"immediate reporting" action is displayed in PNC, but only in the third alert information screen and it is not highlighted. This action was introduced in order to better address the foreign terrorist fighter phenomenon by ensuring that information in case of a hit will reach the relevant authorities as soon as possible, however, the display of the action in PNC does not put emphasis or draw the attention of the end-users.
- although links are displayed in PNC they cannot be opened directly via a hyperlink. Another search has to be performed in order to access the linked alert. Moreover, the link icons for the links on object alerts are highlighted, which makes them easily identifiable, but they are not highlighted for linked person alerts and as a resultmightbe missed by the end-users.
- It is not displayed in the query result whether a discreet check alert is created under Article 36(2) or 36(3) of the Decision 2007/533/JHA.

- **Warnings Index (WI):**

The WI is used at the UK borders primary check points (first and second line border controls) to check incoming travellers against the national lists of known criminals, terrorists or others that the

UK's government considers not to be admissible to the UK territory or should be thoroughly checked upon entry. It is managed by the Home Office, while the hardware and application are provided by, held and managed by the private contractor Fujitsu.

The on-site team considers that the Warning Index cannot be defined as a partial SIS copy for the following reasons:

(i) SIS data is not separated from other data stored in this database. The UK authorities were not able to demonstrate that SIS data is kept separately from the national data files, as required by Article 46 of the Decision 2007/533/JHA, once it is copied into this watchlist;
(ii) not all SIS alert categories are made available in the WI;
(iii) only selected alerts from the alert categories available in the SIS, are copied over;
(iv) SIS data is not deleted from Warning Index when the alert is deleted by the issuing Member State;
(v) the information is not displayed in line with the requirements of Decision 2007/533/JHA and does not follow instructions available in SIS alertspursuant to the "action to be taken" code table in Appendix 2 of the SIRENE Manual[12].
(vi) SIS alerts are not systematically deleted when they are deleted by the issuing Member State but may remain in the Warning Index.

A selection of certain categories of SIS alerts issued pursuant to Article 26, 32 and 36 of the Decision 2007/533/JHA are made available to border guards by copying the alerts into the Warning Index and merging them with other data during the "data amalgamation" procedure (*i.e.* newly uploaded data overwrites the old one and the possible discrepancies are checked manually).

More precisely, WI only contains information on Article 26 alerts for arrest that are not flagged, Article 32 alerts on vulnerable missing adults and missing minors as well as discreet and specific check alerts issued pursuant to Article 36 of the Decision 2007/533/JHA. Alerts on non-vulnerable missing adults, alerts on issued on documents, vehicles and other objects also on persons sought for judicial purposes pursuant to Articles 34, are not available at all at the UK borders. The UK authorities informed the on-site team that in 2018 there are plans to include also document alerts in Warning Index but only the alerts issued on documents invalidated for travel purposes would be available at the border crossing points. It has to be noted, however, that invalidated documents make only around 0.3% of all SIS document alerts.

Furthermore, flagged alerts for arrest under Article 26 of the Decision 2007/533/JHAare not available at the UK borders. This implies that none of the alerts issued for arrest by the Schengen Associated Countries can be seen by the UK Border Force. As a consequence persons sought for arrest for instance even for terrorism related activities by Schengen Associated Countries cannot be detected upon entry to the UK. The UK was recommended to review its processes of systematically

[12]Commission Implementing Decision (EU) 2017/1528 of 31 August 2017 replacing the Annex to ImplementingDecision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II) (notified under document C(2017) 5893) (OJ L 231, 7.9.2017, p. 6).

flagging Article 26 alerts for arrest issued by the Schengen Associated Countries already in 2015.

The information available to border guards in the Warning Indexconsists of only the number of the relevant articleof Decision 2007/533/JHAunder which the alert was created and the reason why the alert is requested. The "action to be taken"is not in line with the "action to be taken" code table in Appendix 2 of the SIRENE Manualas it only indicates if a match is "green" or "stop" and "report". It is also indicated which institution should be contacted (Watchlist and Information Control Unit - WICU) in case of a hit. The application does not, however, provide any of the following mandatory elements of the SIS alerts:

- complete action to be taken, including "immediate reporting" action;
- type of offence;
- photographs, existence of EAW and fingerprints;
- type of identity and aliases;
- links;
- "misused identity" extension;
- warning markers are displayed on the first screen, however only as "v" (violent) regardless of what is the actual warning marker displayed on the second screen.

The lack of the visualisation of the relevant identification information in a SIS alert adds a challengefor the border guards to identify if a person is subject to a SIS alert and also to take the appropriate action as the complete instruction concerning the "action to be taken" is not displayed.

In addition, the Warning Index operates with fuzzy query parameters without additional measures to make the received result precise. As a result a high number of possible matches are returned to the end-user. Although the system displaysan accuracy rating of potential hits (how likely the result could be an actual hit) in percentage points, given the limited information provided, it is still challenging for the border guards to decide which alert should be acted upon and to know whether the person is the subject of that alert. Since the eGates are also operating with the fuzzy query parameters, the identification at eGates in case of a discreet check can produce false positive matches.

The UK authorities informed the on-site team that a new Warning Index application is launched in six airports across the UK as a pilot project (e.g. Southampton and Edinburgh). The on-site team noticed that the new Warning Index application has the same shortcomings regarding the display of SIS hits. One of the improvements of the applications is that next to accuracy rating the age of the subject of the alert will be displayed to simplify the identification process for the border guards. This, however, does not eliminate the fact that none of the mandatory elements of SIS alerts are displayed in the new version of the application.

The UK authorities reassured the on-site team that the "Five Eyes" law enforcement cooperation partners (Australia, Canada, New Zealand and the US) have no access to SIS data stored in the Warning Index or the Semaphore application.

- **Semaphore**

Semaphore is an application used by the National Border Targeting Centre (NBTC) to capture inbound and outbound passenger information supplied by airlines and shipping companies who are forwarding the Advance Passenger Information (API) and Passenger Name Record (PNR) data as well as the data available in the machine readable zone of an ID document or passport as scanned by the carrier (Eurostar or Eurotunnel). This data is then checked against various watchlists included in the Semaphore application.

Semaphore also contains a partial online technical copy of SIS which is separated from other data sources used within Semaphore. This partial technical copy does not contain alerts on industrial equipment and containers as the application is not used for customs checks.

The passenger information is not checked against all the relevant categories of SIS alerts, but only against a sub-set of (non-flagged) Article 26 alerts for arrest.

Semaphore displays limited information in case of a SIS hit, however the officers at NBTC have direct access to the Police National Computer (PNC) where they can further verify the hit. However,photographs, fingerprints or availability of EAWare neither displayed in Semaphore nor in PNC. If a hit is confirmed and a person is identified, the NBTC directly contacts the port of arrival or exit as well as the SIRENE Bureau. As indicated by several Member States, many times the person will not be detained upon exit from the UK by the UK authorities. Instead the UK SIRENE Bureau informs the SIRENE Bureaux of the issuing Member State and the Member State of arrival that the person cannot be arrested, despite the fact that the person is still present on UK territory. Although the UK authorities stated that they do not detain and arrest someone only if the time is too short for boarding, other Member States confirmed that in many cases they receive the information very well in advance of the arrival of the person. In fact there is no clear procedure which determines the period of time needed for arresting the person. It is left to the discretion of the NBTC operator.

The NBTC informed the on-site team that in the future it is planned to include also alertsfor discreet or specific check issued pursuant to Article 36 where the type of offence is indicated as "terrorism related activity" in the Semaphore for the check of the passenger information. It has to be noted that all alerts issued for discreet or specific checks should be available to the NBTC pursuant to Article 9(2) read in a conjunction with Article 46 and Article 40 of the Decision 2007/533/JHA. A selective approach whereby the UK would make available only certain alerts from an alert category is contrary to the principles of the SIS. Also since it is not mandatory for the issuing Member State to indicate "terrorism related activity" in the alert, the security services in certain countries prefer not to disclose this type of information due to serious operational reasons. Due to such selective approach towards SIS by the UK some of the important alerts can be missed.

- **IDENT1:**

IDENT1 is the UK's central national database (UK national Automated Fingerprint Recognition system - AFIS) for holding, searching and comparing dactyloscopic information on those who were arrested by police. Information held in IDENT1 includes fingerprints, palm prints and scene of

crime marks. IDENT1 is kept in a separate location administered by the Crown.

Fingerprint records attached to SIS alerts are matched against the national fingerprint records held in IDENT1. All fingerprint records in the form of NIST[13] files are stored in the UK's national copy and in the SIRENE local technical copy. Moreover, they are also collected and sent as a single daily load file to IDENT1. These NIST files are enrolled into a separate SISII Collection on IDENT1 and are matched against national fingerprints also stored in IDENT1. On this basis fingerprint records attached to alerts are stored in three different copies.

IDENT1 matches SIS fingerprints against the national fingerprint records stored in IDENT1 and provides a numerical 'score' based on a specific algorithm. The score is either categorised as "low", "medium" or "high" confidence numerical range, for instance if several matches are returned it would qualify as a "low" confidence match, whereas if an exact match is achieved it would qualify as "high" confidence match. If a match occurs the information is automatically sent to the SIRENE Bureau. When comparing the UK IDENT1 fingerprint collection with the SIS fingerprint collection there have been 569 high confidence hits, since the go-live of the project in September 2016.

- **Automatic Number Plate Recognition (ANPR):**

The ANPR in the UK is available on mobile and fixed cameras. Currently, however, it queries only PNC and not SIS. The UK authorities informed the on-site team that it is planned to connect the ANPR to SIS in 2018.

There isa possibility to indirectly achieve a hit in SIS on the basis of an ANPR hit. All the ANPR hits are automatically displayed in the "back-office", a service dedicated to processing all the ANPR hits. The officers in the back-office verify those hits against the PNC application on a workstation which also queries the SIS. Therefore a hit in SIS can be achieved in the back-office on the basis of a hit in the PNC, however, of course no hit in SIS would be achieved if there is no PNC record on the vehicle or license plate.

4. ON-SITE VISITS

4.1. N.SIS and technical architecture

The UK has several full or partial copies of the SIS database:

- **EU Connector (SIB)** – a full national copy of the SIS, which is used for the Data Consistency Checks (DCC) with the Central system.The SIB copy is located in the Hendon data centre and is operated under the responsibility of the Home Office.
- **A SIS technical copy** -located in Hendon data centre that is operated under the responsibility of the Home Office.
- **PNC SIS** - a technical copy of the SIS where all the queries made via PNC by the police end-

[13] American National Standard for Information Systems / National Institute of Standards and Technology.

users are directed. It does not contain any binary data (photographs, fingerprints and EAW). The copy is located in Hendon data centre and is operated under the responsibility of the Home Office.

- **SIRENE SIS** – technical copy of SIS used by SIRENE Office. This database also contains binary data (photographs, fingerprints and EAW) and this is the only copy through which the binary data can be retrieved. This technical copy is managed by a private contractor CGI (US-Canadian company).
- **Semaphore** – a partial technical SIS copy used by NBTC. This copy contains different categories of SIS alerts with the exception of industrial equipment and containers. Only alerts for arrest are checked against inbound and outbound passenger information supplied by airlines and shipping companies. This technical copy is managed by a private contractor IBM inthe premises of another private contactor – ATOS.
- **IDENT1** – this database contains a copyof all fingerprint records that are stored inCS-SIS (converted from type 14 (SIS II compliant) to type 4 (UK AFIS compliant)). The SIS fingerprints are kept in a separate SISII Collection on IDENT1. This technical copy is managed by the Crown.
- **Warning Index** – although the UK authorities label the Warning Index as a partial off-line technical copy of SIS, it is in fact a national database containing some selected SIS alerts that are copied into this database. It contains only Article 26 alerts for arrest that are not flagged, Article 32 alerts on vulnerable missing adults and missing minors and discreet and specific checkalerts issued pursuant to Article 36 of the Decision 2007/533/JHA. The WI is updated daily with an "insert & delete" file provided by N.SIS and this is loaded electronically. The daily update is followed by a manual "data amalgamation process" which is applied for the data that are stored in the national databases and SIS during the daily upload, *i.e.* the data that is uploaded to the Warning Index is run against national and SIS data existing in Warning Index. In case any potential matches are identified by the system, the data is manually merged (amalgamated) by the ICU operator. Such a procedure poses a risk for the integrity of the data. Some of the data is also changed by the UK in a unilateral manner, for instance all discreet and specific check alerts with "immediate reporting" action are changed to normal Article 36 alerts, something which is contrary to the provisions of Decision 2007/533/JHA. Deleted SIS alerts are sent daily by N.SIS and this may mean a delay of up to 24 hours before they are changed on the WI. The on-site team even noticed some alerts that had beendeleted from the CS-SIS longer than 24 hours ago but still available in the Warning Index. This database is managed by the Home Office, while the hardware and application for the system are provided and managed bythe private contractor Fujitsu.
- **Back-up laptops** - Warning Index, including the SIS data, is also stored on numerous laptops at the airports and ports as a business continuity solution in case of emergency.

The UK authorities could not provide any reasonfor the necessity of maintaining such a significant number of technical copies.

Locations where the technical copies are stored are isolated and unknown to the public. The facilities, including the ones administered by private contractors, are highly secure. The on-site team concluded that the physical security of the data centre in Hendon and the ATOS data centre is

state of the art.

Nevertheless, the on-site team considers that the practice of entrusting the management of the SIS technical copies to private contractors poses increased risks in terms of physical and logical data security, especially since the private contractors in the UK are not only hosting the systems, but also implement changes to the system under the change management process and have system administrator access rights. Such practice is contrary to the recommendation set out in the Catalogue of the Recommendations and Best Practices for the correct application of the SIS[14], which specifically provides that '[...] neither the operational management of N.SIS II nor any technical copies should be entrusted to third parties'.

The on-site team also enquired the UK authorities about the safeguards available in the contracts concluded with the 'US parented' private companies hosting SIS technical copies, namely IBM and CGI, in order to ensure that SIS data is not shared with the US authorities for law enforcement purposes in case the US Government would request this data under the USA PATRIOT Act[15]. The UK authorities reassured the on-site team that neither IBM and CGI would be obliged to comply with the US request, since:

- IBM operates the service for the Home Office but the Home Office owns the hardware, the intellectual property of the System and the data on the System;
- In the case of IBM, the production service operates from a data centre that is not owned by IBM – it is an ATOS data centre rented by the Home Office.

As regards the business continuity of the various technical copies, namely PNC.SIS, N.SIS and SIB managed by the Home Office, and Semaphore and WI operated by the Border Force, they are fully replicated in a disaster recovery site which is situated in a separate location from the main site.

The SIRENE.SIS technical copy and the CIMS (software used by SIRENE Bureau) are not replicated in a disaster recovery site, something which constitutes 'a single point of failure' as the SIRENE Bureau would not be able to access any data at all in case of a major disruption. Moreover, only the SIRENE Bureau has access to all the binary data which is provided to the end-users in case of a hit. In addition, all recently inserted alerts for arrest and for discreet or specific check with immediate action issued under Article 36 of the Decision 2007/533/JHAwould not be made available to UK end-users in case of the failure of SIRENE.SIS technical copy as the validation process could not take place and the alerts concerned would not be released to the end-users.

The UK authorities informed the on-site team that the SIS technical copies are synchronised online in real time with the national copy (N.SIS) and controlled through a Data Consistency Check mechanism. The Data Consistency Checksare performed between the N.SIS and all other technical copies are only incremental. They are performed on a daily basis only with regard to new or

[14] Commission Recommendation establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS II (C(2015)9169/Final).

[15] An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

updated alerts ("high level Data Consistency Check"). No full Data Consistency Checks are performed. Full Data Consistency Checks are only performed by eu-LISA concerning the copy included in SIB.

The on-site team noticed several times during the visit that some of the SIS copies are not fully synchronised. The on-site team observed that an alert that was displayed in PNC (PNC.SIS) as active although it was deleted on 31st October from CS-SIS (one week before the visit). The on-site team was also informed that the Warning Index returns several results concerning the same alert issued by the same Member State, something which can only happen if the same Member State issues a new alert for the same person. Such situation poses a serious risk that an action, such as arrest, will be taken on the basis of expired alert. This issue persists since the UK has joined the SIS. The Evaluation Committee recommended the UK to complete the synchronisation between the different copies as soon as possible, including performing end-to-end data consistency checks already in the 2015 evaluation.

As regards the Security Plan provided by the UK authorities, the on-site team concluded that the categorisation of what is the actual national copy (N.SIS) is misleading. Based on the Security Plan the actual N.SIS is the SIB and not the Master Test Copy (MTC) as described in the Security Plan. Moreover, the Security Plan has to be reviewed and all the local technical copies have to be added, including the copies of the Warning Index on the emergency laptops.

4.2. SIRENE Bureau and procedures

Since the last evaluation of 2015 the UK has made considerable efforts to improve the functioning of the SIRENE Bureau in accordance with the recommendation of the Evaluation Committee. The training efforts were intensified and some of the operating procedures were redefined in order to ensure the effectiveness of the processes.

The on-site team observed that the UK SIRENE Bureau has strengthened the co-operation with the counter-terrorism (CT) authorities which has led to entering of approximately 1350 alerts on discreet check alerts on persons related to national security. Moreover, when providing an M form pursuant to Article 36(3) of the Decision 2007/533/JHA, the UK SIRENE Bureau adds also further information; in particular they systematically provide the number of the identity document when available. However, despite the active efforts of the SIRENE Bureau to promote the use of SIS among the CT authorities, so far only one Article 36(3) alert on a vehicle was issued and very limited number of photographs and fingerprints is provided.

Some serious issues persist since the evaluation of 2015 in the SIRENE processes. Most importantly, the UK SIRENE Bureau still carries out the validation process of all incoming alerts for arrest ("proportionality check") before making them available to the end-users. The impact of this validation process is that the UK does not make the incoming alerts for arrest searchable to its end-users as long as the proportionality check is in progress. The Evaluation Committee in its evaluation report of 2015 and the Commission (in the EU-Pilot letter to the UK dated 3 August 2015) stated that such procedure is contrary to Decision 2007/533/JHAand infringes Article 9(2)

read in conjunction with Article 46(2) of that Decisionwhich sets out the requirement of equivalence of results which means that a search in a technical copy must produce a result equivalent to that of a search in the SIS database.

The UK authorities informed the on-site team that they intend to change the procedure for validation of all incoming alerts for arrest. At the moment however the immediate circulation of alerts for arrest is still not possible due to technical reasons and the necessary training of the SIRENE staff on the new procedure. As an interim solution pending the technical rebuild, a prioritisation of the validation workflow has been introduced. This is a manual process due to which alerts will be made available faster. The instant circulation of the alerts for arrest will only be introduced as of June 2018.

The on-site team also noted that the UK applies a validation procedure for all incoming discreet or specific check alerts under Article 36(2) and Article 36(3) with "immediate reporting" action, which means that they are not displayed to the UK end-users before the SIRENE Bureau validates them. Such procedure completely undermines the purpose of the measure which was introduced to better address challenges posed by the foreign terrorist fighter phenomenon by ensuring that the information on the most serious cases would be circulated without any delay. Such process is contrary to Article 9(2) read in conjunction with Article 46(2) of the Decision 2007/533/JHA.

Another issue is the flagging procedures for alerts for arrest. The UK introduced very rigid procedures on the validation of incoming EAWs and the possible flagging. The Evaluation Committee in its report of 2015 and the Commission (in the EU-Pilot letter to the UK dated 3 August 2015) pointed out that in accordance with Article 25 of the Decision 2007/533/JHA, a flag shall only be added to alerts for arrest when the competent judicial authority has refused execution of the EAW, or if it is obvious that the execution of the European Arrest Warrant will have to be refused; they thus questioned the proportionality and effectiveness of the UK practice.

The UK has now confirmed that as a result of the recommendation it has lowered the validation requirements of EAWs, which resulted in significant reduction of flag requests. In July 2017 there were 76 flag requests compared to 666 in May 2015 alone, although the situation in 2015 was rather extraordinary due to the fact that the UK just joined the SIS and a large bulk of alerts under Article 26 was to be validated by the UK. It has to be noted that to date there are 3000 alerts for arrest in SIS to which the UK has requested a flag. It is about 9 % of all such alerts.

Another related issue concerns the systematic flagging of alerts for arrest (extradition requests) issued by the Schengen Associated Countries. This issue was also raised in the 2015 evaluation and has not been resolved yet.

Most importantly, in the UK alerts for arrest under Article 26 where a flag was requested are automatically changed to Article 34 alerts on persons sought to assist with a judicial procedure. The UK changes the alert category without even informing the issuing Member State. This is done immediately when the UK requests the flag and generates the F form ahead of the Member Statesetting the flag. Such implementation is not in accordance to the Appendix 2 of the SIRENE

Manual and also Article 9(2) of the Decision 2007/533/JHA. Although in essence the action to be taken is the same for flagged Article 26 alerts and 34 alerts (to determine the place of residence or domicile of the person), the reason for the request must remain 'for arrest'. The implementation poses serious issues for the Schengen Associated Countries as all their Article 26 alerts are flagged and judicial (Article 34) alerts are not at all available at the UK borders.

In addition, the on-site team observed that once the UK SIRENE Bureau requests an issuing Member State to add a flag , it automatically changes the alert category from an alert for arrest (Article 26) to a judicial alert (Article 34) at national level, there is no procedure whereby the UK SIRENE Bureau would ensure that the requested flag has indeed been added by the issuing Member State. The on-site team witnessed a case where a request for a flag was sent by the UK to the issuing Member State, however, the latter did not consider that the flag was to be added in accordance with the provisions of Article 25 of the Decision 2007/533/JHA. As a result, the flag was not added by the issuing Member State, however the alert remained as issued for the purposes of Article 34 in the UK.

The on-site team noticed that the SIRENE Bureau is not adequately involved in the training of end-users and in other activities to promote the correct use of SIS among other police forces, e.g. within the "peer review" evaluations performed by Home Office.

The on-site team also considered that the information provided to the end-users by the SIRENE Bureau is not always clear. For example, when the picture of the victim of the misused identity was sent to the end-user, the SIRENE Bureau did not provide a clear explanation whether it was a victim or the perpetrator of the misused identity.

4.2.1. SIRENE workflow

Several improvements were introduced in the SIRENE case management system (CIMS) since the evaluation of 2015:

- modifications to the "SIS Loaded Search" suite;
- technical changes implemented to assist the ability to provide attachments to front-line officers by sending them straight to the end-users instead of to the single points of contact;
- automatic detection of alerts in the CIMS workflow where the action to be taken requiresan immediate response.

Nevertheless, the on-site team considers that CIMS still needs further improvements:

- although an automatic detection of the alerts with the "immediate reporting action" was introduced in CIMS, they are automatically displayed as such but the "immediate reporting" marker must be added manually to the case title;
- the "misused identity" is not highlighted in red automatically but only if the misused identity marker is added manually;
- not all SIRENE operators have the special shortcut to be able to perform searches on industrial equipment;

– it is not possible to directly open the linked alerts in CIMS from "links screen". The Schengen ID (SID) has to be copied and searched individually, which delays access to important information. When the links were found by the SIRENE operators they were easily mixed with manually created links between the files in the case management system.

The on-site team also noticed that in order to find out whether there is a photograph or fingerprints attached to the alert, the operator has to open numerous files and bookmarks. Despite the fact that the SIRENE Bureau is the only source of photographs and fingerprints for end-users, the process to retrieve them and to provide them to end-users is cumbersome. First the operator has to find the alert by typing in Schengen ID of the alert or finding the Schengen ID via PNC, then he/she has to check all different folders by opening them one by one, and scroll through them to find the biometric data. The data which is retrieved must be copied in an e-mail message to which the biometric data are to be manually attached.

The on-site team noticed when dealing with misused identity casesthat the photographs of the victim of the misused identity were not available in three cases in CIMS. In two other cases even the photograph of the perpetrator was not available despite the fact they are all available in the alert and consequently in CS-SIS. It points at a serious desynchronisation between CIMS, the SIRENE technical copy and SIB (the national copy).

Another observed issue is that the CIMS case management automatically creates the case name with special characters, but which have to be transliterated and added manually by the operator. However when a case is searched in CIMS with simple characters, it might not be found because CIMS does not search in transliterated values.

Based on the above examples the on-site team concluded that overall the workflow system does not provide a sufficient level of automation to manage the daily workflow. It is labour-intensive and not user-friendly or clear and it may miss important information. Thus it needs significant further improvements. It is also questionable why the SIRENE officers access SIS alerts via CIMS and PNC when the SIRENE technical copy contains the full data set available in SIS alerts, including the binary data, whereas CIMS and PNC only contain limited information as described above.

4.3. Airports

4.3.1. Heathrow airport

More SIS alerts are now available at the UK's border crossing points than in 2015 on entry, however, only alerts for arrest (but not from Schengen Associated Countries or any other flagged alerts), alerts on vulnerable missing persons as well as discreet and specific check alerts issued pursuant to Article 36 of the Decision 2007/533/JHAare made available in WI. Alerts on documents or persons sought for judicial purposes are not available at the UK borders. Unlike during the evaluation of 2015, when no possibility was granted to the Evaluation committee to have a closer look at WI at Heathrow airport, this time the on-site team was able to see the application and perform queries.

In the case of a SIS hit in the first line border control booth, the border guard who achieved the hit will proceed to the control room for further checks (except for discreet check alerts). The information provided to the border guard in the border control application (WI) is extremely limited, it does not provide a complete action to be taken, or any binary data that could help to identify the person subject to the alert. Border guards therefore are instructed to always contact the Watch List and Information Control Unit (WICU) and not the SIRENE Bureau in case of a SIS hit. This unit performs the query in PNC on behalf of the border guardto obtain more detailed information which is available in the alert, since there is no access to PNC at the first or second line border controls. Although PNC provides more information than WI, it does not contain binary data either. Therefore in order to receive, for instance, a photograph attached to the alert to identify a person, the WICU will need to contact the SIRENE Bureau, which will then send the photograph. The WICU also fills in the hit reporting form on behalf of the border guards and sends it to SIRENE Bureau.

Since the action to be taken is not displayed in full in the WI application, it adds a challenge for the border guards to take an appropriate action on discreet check alerts in accordance with Article 37 of the Decision 2007/533/JHA. A hit on a discreet check alert should display, in accordance with section 2.1.5. of the Appendix 2 of the SIRENE Manual, a list of itemswhichthe border guard mustreport on the alert subject. This list is not displayed to the UK border guards, therefore relevant information might not be gathered. In addition, since no binary data is displayed in WI it ismuch more challenging toidentify the person correctly. Interesting to observe that neither the border guard nor the WICU have the complete information available in the alert, only the SIRENE Bureau; the border guard is not in direct contact with the SIRENE Bureau, only with the WICU. A rather long chain of calls is necessary to receive the information which should be immediately available to the border guards during the first line control.

All Article 36 alerts for discreet or specific check with "immediate reporting" actionare changed into simple discreet check alerts when they are uploaded to the WI. Consequently, the this application does not display the "immediate reporting" action and does not allow the real time communication which is the main objective of the alert. Border guards would not be aware that this information should be passed to relevant authorities without any delay and the hit reporting will not take place instantly. This completely undermines this measure which was introduced to better address the foreign terrorist fighter phenomenon by ensuring that information in case of a hit will be forwarded to the alert issuing authorities without any delay. The border guards interviewed by the on-site team were not aware of the existence of the "immediate reporting" action.

Hits on alerts for arrest, which are achieved on the basis of API and PNR data, processed by the NBTC are sent to the unit of the Metropolitan Police located in Heathrow which is in charge of aviation policing in Heathrow and London City airports. This means the Heathrow police unit will be informed on the expected arrival of the person subject to the alert for arrest and will take measures to meet the passenger at the gate. As the majority of airlines are submitting the API and PNR data to the NBCT, the biggest part of alerts for arrest are processed by the latter and not directly by the Border Force at the Heathrow airport.

There is no physical outbound check of passengers in the UK. The outbound checks are performed by the NBTC only on the basis of passenger data which are compared against alerts for arrest (except flagged ones).

There is no access to lost, stolen, invalidated document alerts in SIS at the UK Border. As a compensatory measure the UK Border Force has access to Interpol's Lost and Stolen travel document database (SLTD). The on-site team was informed that the Border Force is seizing all documents for which there is a hit in SLTD.

The on-site team noticed that the computer screens in the first line border check booths at Heathrow were not protected and therefore the data was clearly visible to the passengers. This situation was also observed in Southampton, Edinburgh airports and Coquelles juxtaposed border checkpoints. The Evaluation team recommended to the UK installing privacy screens already in 2015, but this recommendation was not implemented.

The on-site team witnessed a clear example in WI of how SIS alerts are not correctly displayed because of the daily manual amalgamation of the data whereby new data is merged with the existing data in WI and the discrepancies are solved manually. The border-guard was asked to perform a search person who is a subject to discreet check alert under Article 36(3)issued by Germany. As a result, two hits were achieved for discreet checks concerning two personsfor whom only the day and month of birth were different. Both hits indicated the same reason for request and the same actions to be taken but there were references to three different Schengen IDs – one form Germany, the second from France and a third one from Sweden, even though only one alert (i.e. Schengen ID) was active and valid. This phenomenon was also observed when querying the same personin Southampton airport. This proves that deleted alerts are still available in WI.

4.3.2. Southampton airport

In Southampton airport the on-site team had the possibility to observe the piloting of the new WI application which is to be launched by 2021. However, in terms of the SIS queries, this new application has the same shortcomings as the existing version of the application and displays only very limited information to the border-guards. i.e. only the relevant Article under which the alert was created and the reason why the alert is requested. The action to be taken does not mirror the SIS action and no binary data is provided.

The on-site team also had a chance to review the on-line SIS training module (Border Force Operations Manual) available to the border guards on an intranet platform. The on-site team noticed that although it provides useful information on SIS post-hit procedures, it does not contain information on certain important aspects. The Manual does not make any distinction between Article 36 alerts with "immediate reporting" and simple discreet check (as this distinction is also not available in WI), nor does the Manual explain which further information could be retrieved from the SIRENE Bureau, such as for instance binary data. Therefore, the interviewed end-users were not aware of possibility to receive this data.

4.3.3. Edinburgh airport

The on-site team had the possibility to observe border controls in Edinburgh airport. The on-site team noticed that due to the fact that WI is using a fuzzy query algorithm without additional measures to precise the received result, many similar results are returned. A hit was achieved on a person who had the same first name, surname and date of birth as the subject of the alert, only the nationality indicated in the alert differed from the passport provided by the passenger. It was, however, almost impossible to establish whether the person was indeed the subject of the alert, as only very limited data and no photograph is available to first line border guards.

In Edinburgh airport the on-site team also learned that WI (including SIS data) is stored on laptops as a business continuity solution in case of emergency.

4.4. Border Crossing Point(s)

4.4.1. Coquelles Juxtaposed border checkpoint

There are around 5 million passengers per yeartravelling through the Coquelles Juxtaposed border checkpoint.The checks are performed via WI since PNC is available only for police end-users. According to the statistics provided to the on-site team, there were42 hits on alerts for arrest, 915 hits on discreet check alerts and 146 on missing person alertsin 2016.

The on-site team noticed when visiting the premises for checks of bus passengers that the Border Force terminals did not have any screen protection, so that the data was visible to the passing passengers.

The on-site team also observed that the police officer present in the control booth could easily retrieve an alert containing a misused identity via the PNC,the officer was however not able to identify that this is a misused identity case. The officer was not aware of the post-hit procedure or the possibility to receive any additional information. The officer finally stated that the case would be handed over to the migration service.

4.5. The use of SIS by the police end-users

As regards the use of SIS by the police end-users, the on-site team noticed that overall the end-users were not well familiar with the SIS procedures.

The on-site team considers that the PNC application is outdated and not user-friendly. This has a significant influence on the processing of SIS alerts. First of all, PNC does not display binary data – photographs, existence of an EAW and fingerprints. Moreover, PNC does not even indicate that photographs, fingerprints or an EAW could be available at the SIRENE Bureau. Therefore, the majority of the interviewed end-users were not aware of the possibility to receive this data from the SIRENE Bureau. In the Operational Headquarters of Hampshire (Winchester), the 24/7 intelligence unit, the operator was not aware of the fact that the SIRENE Bureau could have binary data attached to the SIS alert and tried to retrieve it from Interpol alerts and even said that the embassy of the

relevant country could be contacted for this purpose.

The procedure to retrieve data from the SIRENE Bureau is also rather lengthy due to the "dual level" of reporting. All the end-users in the UK are first instructed to contact the local 24/7 intelligence unit in the case of a SIS hit. 24/7 intelligence units (i.e. the PNC Bureau or PNC unit) are the designated services to provide guidance to the end-users on post-hit procedures, they fill in the hit-reporting forms on behalf of the end-users and also issue certain categories of SIS alerts. However, in order to receive binary data for example, the end-user will need to contact the 24/7 unit first which will then contact the SIRENE Bureau and the same procedure has to be followed for dispatching the actual data. The on-site team witnessed that it took around 20 minutes for the SIRENE Bureau to send the binary data (photograph) to the end-user at the Command and control Centre in Bilston Glen (Scotland). Hence, hit reporting might be delayed by the additional level of information flow, especially for the alerts with "immediate reporting" action when the SIRENE Bureau should be contacted directly.

As regards the hit reporting procedure, one of the helpful functionalities of the PNC is the hit-reporting forms which are created and sent to the SIRENE Bureau directly via the PNC application.

Since the PNC does not support any binary data, photographs and fingerprints are also not attached to the alerts issued by the UK end-users even if they are available. There is no officially established mandatory procedure or guidelines for end-users to contact the SIRENE Bureau to add those data. SIRENE will also not request those data proactively.

The on-site team also witnessed desynchronisation issues of PNC.SIS technical copy. When making queries in the PNC application in Southampton Special Branch Police station and at the Coquelles Juxtaposed border checkpoint, an alert was displayed in the PNC as active although it was deleted on 31 October from CS-SIS (one week before time of the visit). Moreover, when the end-user at the Hampshire Police Investigation Centre contacted the 24/7 unit at the Operational Headquarters of Hampshire to provide further information on a SIS hit, the officer was informed that thePNC was unavailable for queries and the error message was displayed *"SIS link unavailable"*.In another location, Barnet Borough Police (Collindale Police Station),the officer was not able to access the PNC application because, according to the officer, there were too many users using it at the moment.

The "immediate reporting" action is displayed in the PNC application, but only in the third screen of the alert information and it is not highlighted, therefore the end-users may not notice it. Although the interviewed end-users were overall familiar with the concept of discreet checks, they were not aware of the differences between simple discreet check alerts and alerts with "immediate reporting" (Heathrow police station, Hampshire Police Investigation Unit, Scottish police command and control centre Edinburg).

There is also no misused identity extension available in PNC. Only the information that this is a 'misused identity' is displayed, however, it is almostimpossible to identify who is the victim and who is the perpetrator of the misused identity, since there is no possibility to distinguish to which

programme. The programme consists of visits (evaluations) to review how each force uses the SIS, how they are using different types of SIS alerts and how they respond to the alerts. Each visit is followed by detailed recommendations. To date 39 out of 43 forces in England and Wales have been reviewed and the Police of Scotland and the Police Service of Northern Ireland. This awareness raising and training activities led to an increase of SIS alerts issued by the UK.

5. GENERAL ASSESSMENT AND SUMMARY:

The on-site team concludes that the UK has not effectively incorporated the use of SIS into their working procedures. Due to the UK's selective approach toSIS data, the high number of full or partial copies of the SIS database and their synchronisation problems as well as the limited reciprocity concerning the execution of the actions requested by the alert issuing Member States and the technical constraints of the end-user IT applications, the on-site team considers that these constitutes **very serious deficiencies**in the implementation of SIS at national level.

The UK implemented the recommendations of the previous evaluation report (document No 11780/15 SCH-EVAL 20 SIRIS 57 COMIX 381), dated 8 September 2015, related to Section 5 of the Report (Recommendations on training); the UK also implemented the recommendations to carry out the following:

- to complete the back record conversion of Article 38 from PNC to SIS without further delay;
- to implement an integrated query encompassing all different systems atScotland Police;
- to delete all pre-SIS international alerts entered manually in PNC;
- not to introduce and use the fingerprints to identify the person on the basis of his biometric identifier before the report from the Commission has been finalised and the opinion of the European Parliament is sought on the matter;
- to allow the Evaluation Committee to perform simulated queries during the visits;
- to display warning markers more clearly on the PSNI Portal;
- to allow documents to be queried by use of the family name and date of birth, and to allow a combined query on persons and documents;
- to allow for queries based on VIN numbers;
- to ensure that all hits at the border are followed up, processed and eventually send to the respective Member State;
- to keep the Joint Operational Authority (JOA) in place.

However,all the remaining recommendations of the previous report were not implemented.

5.1 Compliant and points of particular interest:

- Statistical reporting tools and the availability of the detailed statistical reports is considered as best practice.

- The "peer review" programme initiated by the Home Office consisting of visits (evaluations) to

review how each force uses the SIS is considered to be a best practice.

5.2 Compliant but improvement necessary:

- Information provided by the SIRENE Bureau to the end-users is not always complete, especially in cases of misused identity.
- The SIRENE Bureau is not actively involved in SIS processes in the UK, such as providing clear information to the end-users, giving training to the end-users on SIS related matters.
- The CIMS workflow and case management system does not provide a sufficient level of automation to manage daily workflow; it is labour intensive, not user friendly and not clear.
- The CIMS workflow and case management system automatically creates the case name with special characters. However, it is not possible to retrieve such case when searching in CIMS with simple characters as CIMS does not search in transliterated values.
- The misused identity is displayed in red in CIMS only if the misused identity marker is added manually.
- The PNC application does not provide for differentiation between Article 36(2) and 36(3) of the Decision 2007/533/JHAwhen displaying an alert.
- Not all SIRENE operators have a special shortcutto be able to perform searches for industrial equipment in CIMS application.
- The "immediate reporting" action for discreet check alerts is displayed in PNC, but only in the third information screen and is not highlighted.
- Links between alerts are displayed in PNC, but cannot be opened directly.
- In PNC only the links for objects are highlighted but not for persons.
- The mapping of the identity status "confirmed by photograph, fingerprints or DNA" is different from the concept of "confirmed identity" in SIS and therefore it is misleading. The end-users may think that the identity of a person is indeed confirmed by photographs, fingerprints or DNA while the confirmation of the identity can be carried out in other ways as well.
- Hit reporting might be delayed with additional level of information flow via the 24/7 Intelligence units, especially for the alerts with "immediate action" as the reporting is not carried out by the end-user but by the24/7 Intelligence units. It should be ensured that in case of immediate reporting the end-users would contact SIRENE Bureau directly.
- The SIRENE Bureau is not involved in the end-user training, including the "peer review" programme.

- More end-user training is needed on misused identity, linking functionality, possibility to retrieve pictures and other binary data from the SIRENE Bureau, also the new actions in the SIS such as "immediate reporting" and invalidated documents.

5.3 Non-compliant:

- The practices applied in the UK concerning the high number of partial and full technical copies constitute serious and immediate risks concerning the integrity of SIS as well as the SIS data security at the borders as the UK is processing SIS data for different purposes by splitting the database. It is hardly possible to follow-up the data processing chain and it is uncertain whether the data is properly maintained and whether it is updated or deleted as required by the SIS legal provisions.

- The Warning Index cannot be considered as a partial technical copy of the SIS and therefore constitutes an unlawful copying of SIS data for the following reasons:

  i. SIS data is not separated from other data stored in this database. The UK authorities were not able to demonstrate that SIS data is kept separately from national data files, as required by Article 46 of the Decision 2007/533/JHA, once its copied to this watchlist;
  ii. only selected alerts are copied over within a particular alert category;
  iii. not all alert categories are made available in the Warning Index;
  iv. SIS data is not deleted when the issuing Member State deletes it but kept in this database;
  v. the displayed information does not follow the information and instruction available in SIS alerts
  vi. SIS alerts are not systematically deleted when they are deleted by the issuing Member State but may remain in the Warning Index.

Therefore the Warning Index does not comply with the requirements of Article 46 of the Decision 2007/533/JHAon processing the SIS data and cannot be considered the SIS technical copy.
The data amalgamation procedure applied to the SIS data in the Warning Index constitutes an unlawful copying of the SIS data and is contrary to the requirements set out in Article 10 (1)(c) and Article 46(2) of the Decision 2007/533/JHA.

- The use of the back-up laptops which contain the copy of the Warning Index database including also SIS data is considered as the unlawful copying of SIS data, therefore non-compliant with the principles enshrined in Article 10 (1)(c) and Article 46 of the Decision 2007/533/JHA.

- Contrary to the principle of equivalence of results which is enshrined in Article 9 (2) read in conjunction with Article 46 (3) of the Decision 2007/533/JHA, the Warning Index does not provide any of these mandatory elements of the SIS alerts:

  i. complete action to be taken, including "immediate reporting" action;
  ii. type of offence;

iii. photographs, existence of EAW and fingerprints;
iv. type of identity and aliases;
v. links;
vi. "misused identity" extension;
vii. warning markers to be displayed on the first screen, however only as "v" (violent) regardless of what is the actual warning marker displayed on the second screen.

- Technical SIS copies and the Warning Index are not fully synchronised with the CS-SIS contrary to the provisions of Article 9(2) read in conjunction with Article 46 of the Decision 2007/533/JHA; moreover in case alerts deleted by the issuing Member State remain in technical copies or in the Warning Index they do not respect the retention period for alerts defined in Art. 44 and 45 of Decisions 2007/533/JHA.

- Only the incremental Data Consistency Checks (DCC) are done on the SIS technical copies but no full DCCs are performed on those copies in accordance with the requirements of Article 9(2) of Decision 2007/533/JHA.

- Contrary to Article 9(2) of Decision 2007/533/JHAand Appendix 2 of the SIRENE Manual all alert under Article 36 of Decision 2007/533/JHAwith "immediate reporting" action are changed to simple discreet check alerts in the Warning Index.

- The Semaphore SIS technical copy only checks passenger information against non-flagged alerts for arrest (Article 26 of Decision 2007/533/JHA)which is not in accordance with Article 9(2) read in a conjunction with Article 46 and Article 40 of Decision 2007/533/JHA.

- Contrary to Article 26(2) of Decision 2007/533/JHAalerts for arrest (extradition requests) issued by the Schengen Associated countries are systematically flagged in the UK.

- All flagged alerts for arrest are automatically changed into Article 34 alerts on persons sought to assist with a judicial procedure in PNC, which is contrary to Article 9(2) of Decision 2007/533/JHAand the principle of equivalence of results as well as to Appendix 2 of the SIRENE Manual.

- Contrary to the provision of Article 24 of Decision 2007/533/JHA, all alerts for arrest are automatically changed to Article 34 alerts on persons sought to assist with a judicial procedure as soon as the UK SIRENE Bureau requests an issuing Member State to add a flag without waiting until the flag will be added by the Member State which entered the alert.

- As soon as the UK SIRENE Bureau requests a flag from the issuing Member State by sending an F form it automatically changes alerts for arrest to judicial alerts at national level. There is no procedure for the UK SIRENE Bureau to follow up and verify if the requested flag has indeed been added to the alert by the issuing Member State contrary to the provision of Article 24 of the Decision 2007/533/JHA.

- Photographs and fingerprints are not attached to the alertsissued by the UK end-users even if

available because there are no officially established mandatory procedures or guidelines for end-users to contact the SIRENE Bureau to add those data. The SIRENE Bureau will also not request those data proactively. This is contrary to Article 20 of the Decision 2007/533/JHA.

- Alerts for arrest are not available immediately to the end-users before the validation of the SIRENE Bureau. This is contrary to the principle of equivalence of results which is enshrined in Article 9 (2) read in conjunction with Article 46 (3) of the Decision 2007/533/JHA.

- Alerts for discreet or specific check with "immediate reporting" action pursuant to Articles 36(2) and 36(3) of the Decision 2007/533/JHAare not available immediately to the end-users before the validation of the SIRENE Bureau. This is contrary to the principle of equivalence of results which is enshrined in Article 9(2) read in conjunction with Article 46(3) of the Decision 2007/533/JHA.

- The PNC does not display binary data such as photographs, existence of EAW and fingerprints which is contrary to the principle of equivalence of results which is enshrined in Article 9(2) read in conjunction with Article 46(3) of the Decision 2007/533/JHA.

- There is no misused identity extension in PNC. Only information that this is a 'misused identity' is displayed, however no information on who is a victim or perpetrator is provided nor is the data related to the victim available. This is contrary to Article 9(2) read in conjunction with Article 46 (3) and Article 51 of the Decision 2007/533/JHA.

- An alert was displayed in PNC as active although it was deleted on 31st October from CS-SIS. This is contrary to Article 9(2) read in conjunction with Article 46 (3) and Article 45 of the Decision 2007/533/JHA.

- When the information on the alias is displayed in PNC, the ID status remains "confirmed by photograph, fingerprints or DNA". This is not correct and contrary to Article 9(2) read in conjunction with Article 46 (3) of the Decision 2007/533/JHA.

- The photographs of the victim of misused identity were not available in three cases in CIMS application. In two other cases the photograph of the perpetrator was not available. This is contrary to Article 9(2) read in conjunction with Article 46 (3) and Article 51 of the Decision 2007/533/JHA.

- There is no back-up available for the SIRENE technical copy, although it is the only source of the biometric data for the end-users. This is seriously risking the availability of binary information to the end-users as it can be made available only from this copy.

- The UK officers systematically do not seize items subject to an Article 38 SIS alert. The officers are instructed to seize an item only if the item is connected to the offence committed on the UK territory or it supports or is part of a UK investigation or prosecution. This is not in accordance with Article 39 of the Decision 2007/533/JHAand the Appendix 2 of the SIRENE Manual.

- Contrary to Article 10 and Article 40 of the Decision 2007/533/JHAthe information displayed

on the computer screens in the first line border controls at the UK ports can be read by passing passengers.

- Contrary to security measures enshrined in Article 10 of the Decision 2007/533/JHAthe complex password requirements are not implemented in NBTC.

- Only selected SIS alerts are available for the passport controls, e.g. information on lost/stolen/invalidated travel documents are not available at all which is not in accordance with Article 9(2) read in a conjunction with Article 46 and Article 40 of the Decision 2007/533/JHA.

identity the 'misused identity' is related. As a result the end-users in Barnet Borough Police (Collindale Police Station), Southampton Special Branch Police station, Coquelles Juxtaposed border checkpoint,the Scottish police command and the control centre in Edinburgh, Hampshire Police Investigation centre, Heathrow police station, Scottish Police (Wester Hailes police station) were not able to clearly establish who is the victim or the perpetrator in misused identity case. Not only the improvement of the functionality in the PNC but also further end-user training is needed in this regard.

The on-site team was also informed that as a general rule the UK end-users are instructed not to seize objects subject to an alert issued pursuant to Article 38 of the Decision 2007/533/JHA. The officers are instructed to seize an item only if it relates to an offence committed on the UK territory or it supports or is part of a UK investigation or prosecution. This is provided for in the UK's official College of Policing Guidance *'[...]officers should seize the item if it supports or is part of a UK investigation or prosecution (including offences overseas that will be prosecuted in the UK).'* If officers are not investigating an offencecommitted in the UK, they should not seize the item. Therefore, for instance, vehicles stolen on the territory of another Member State and located on the UK territory would not be seized.

The end-users throughout the country were not familiar with the transliteration rules and did not have the transliteration table available to them. The officers from the British Transport Police in Edinburgh Waverley railway station were not aware of the possibility to perform a query with special characters.

Overall the on-site team considered that not only the functionalities of the PNC application should be significantly improved but also more training should be provided to the end-users on SIS procedures.

The on-site team took note of the interface called "PUMA app" for PNC and SIS queries used by the Police Service of Northern Ireland. This application is available on the workstations as well as on mobile devices which are distributed to each officer in Northern Ireland. The on-site team considers that the application is more user-friendly and clear than the PNC interface. Although the binary data from the SIS could be available via this application, currently it cannot be retrieved due to the limitations of the PNC which is queried in the background.

4.6. Training

The UK authorities have stepped up their efforts in providing training on SIS to the end-users since the last evaluation. SIS is now included in the National Training Curriculum. The on-site team also had a chance to observe that the guidelines on SIS procedures were available in the police stations. Despite the efforts stepped up in the field of training the on-site team experienced a significant lack of awareness of SIS functionalities and procedures.

In order to further raise awareness on SIS, the Home Office has initiated a "peer review"