Council of the European Union

Brussels, 2 March 2016
(OR. en)

6720/16

SIRIS 33
DAPIX 30
ENFOPOL 54
COTER 22
VISA 55
FRONT 106
COMIX 174

COVER NOTE

From:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	29 February 2016
To:	Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2016) 93 final
Subject:	REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)

Delegations will find attached document COM(2016) 93 final.

Encl.: COM(2016) 93 final

EUROPEAN
COMMISSION

Brussels, 29.2.2016
COM(2016) 93 final

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II)

1. INTRODUCTION

It is becoming increasingly difficult to establish the identity of a person due to changing names and the use of aliases or fraudulent documents. The use of document fraud is an increasing modus operandi to illegally enter and move around within the Schengen area. The *Frontex Annual Risk Analysis* for 2015 reported that in 2014 there were around 9 400 detections of document fraud cases on entry to the EU/Schengen area from third countries, which represents a slight decrease compared to the previous year. By contrast, cases reported on intra-EU Schengen movements showed a marked increase from 7 867 in 2013 to 9 968 in 2014 (+27%).

Document fraudsters not only undermine border security but also the internal security of the EU. Often persons, sought by the police, are evasive about their identity and use multiple aliases. Some persons subject of an entry ban to the Schengen area can legally change their identity in their country of origin to avoid detection. In this context, a reliable method to establish identity is needed. The use of fingerprints would be an efficient way for both border guards and law enforcement officials to identify persons sought by the authorities and to detect cases of document fraud.

The fraudulent use of travel documents in connection with the recent terrorist attacks in Paris also confirms the necessity for a tool that provides the possibility of identification of persons on the basis of fingerprints. In this context the Council Conclusions of November 2015 underlined the importance of strengthening controls and performing systematic checks. To date there is no EU-wide system which would allow the checking of persons on the basis of fingerprints.

The second generation Schengen Information System (SIS) entered into operations on 9 April 2013. A new feature is the storage of fingerprints in the central system. At present, prints are used to *confirm* the identity of a person located as a result of a search, usually on name and date of birth. This is a "one-to-one" search - the person's prints are compared to one set of prints stored in SIS. However the possibility to *identify* a person on the basis of his/her fingerprints requires an evolution to the present law enforcement practice: the comparison of a person's prints to all sets of prints – a "one-to-many" search – to identify the person solely on the basis of fingerprints. This functionality requires the implementation of an Automatic Fingerprint Identification System (AFIS).

AFIS has been successfully used in numerous national and cross-border cooperation databases. For the E.U. the obvious examples are the Visa Information System (VIS) and EURODAC.

Articles 22 (c) of the SIS II Decision[1] and the SIS II Regulation[2] provide a legal basis for using AFIS. Before this functionality is implemented, the Commission must present a report on the availability and readiness of the required technology, on which the European Parliament shall be consulted. The objective of this report is to address this requirement and to confirm that fingerprint identification technology is available and ready for its integration into SIS-II.

[1] COUNCIL DECISION 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

[2] REGULATION (EC) No 1987/2006 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II).

The level of readiness and availability have to be assessed in the context of the unique situation and characteristics of SIS II which present a series of technical and organisational challenges requiring appropriate and customised solutions. This report, supported by a study conducted by the Commission's Joint Research Centre (JRC)[3], also outlines the technical and organisational requirements in the context of SIS, describes the type of scenarios where fingerprints are used operationally and includes recommendations for the successful implementation of AFIS functionality.

2. THE JRC STUDY AND ITS FINDINGS

The *Horizon 2020 EU Research and Innovation Framework Program* describes the readiness and availability of technology using a nine-point scale[4]: level 1 represents the observation of basic principles, level 9 the proving of actual systems in an operational environment. AFIS technology has already achieved level 9 with many systems working world-wide.

2.1 Overview of AFIS technology

2.1.1 Performance

JRC provided an overview of the most significant independent performance evaluation campaigns, identifying the relevant initiatives for the context of SIS. Three key concepts emerged:

- The accuracy of an AFIS is fully dependent on the data used for its evaluation and on the quality of that data.
- Other factors that can affect the performance of an AFIS are size of the database in which searches take place, number of prints used for the search and expected response time.
- Given good quality data and 10 print to 10 print searches, evaluation campaigns show that the accuracy of AFIS technology is very high, with error rates around 0. 1%

2.1.2 Quality

Many studies and benchmarks have shown that the performance of biometric systems depends on the quality of the input samples. Improvement of the quality can be technical, standards-related or even linked to the method for acquiring the prints, i.e. electronic scanning ("live-scan") or manually-taken inked prints. Electronic scanning, supervised by an experienced operator, is the preferred method for obtaining the best quality. However, inked prints which are scanned into the database still exist. Systems should incorporate processes to detect poor quality prints.

There should be an end-to-end concentration on quality in:

- Taking the prints

[3] http://publications.jrc.ec.europa.eu/repository/handle/JRC97779

[4] https://ec.europa.eu/research/participants/portal/doc/call/h2020/common/1617621-part_19_general_annexes_v.2.0_en.pdf
http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf

- Technical assessment of their quality
- System-based solutions for ensuring matching
- Using the best samples
- Monitoring the performance of the system and the people using it

As the study was comprehensive it also addressed the most challenging area concerning quality: "latent" prints found at crime or incident scenes.

Latents will exclusively be used for consultation. It is anticipated that only full 10 print sets from known persons will be stored in SIS.

In most Member States visited, quality is also managed through "multiple datasets". When a person has been fingerprinted on several occasions, e.g. each time he is arrested, the prints are stored. The individual prints in the sets can be compared according to their quality score and a composite set can be compiled of the highest quality 10 prints. Such an approach could also be used in SIS.

A critical issue is the inclusion of quality measurement mechanisms in an AFIS to boost performance. Regarding quality six key concepts must be considered:

- The performance of an AFIS is fully dependent on the quality of the data (i.e. print samples) it runs on.
- Many factors can affect the quality of prints. Some are controllable (e.g. cleanliness of the sensor), others are not (e.g. eroded fingertips due to manual work).
- Automatic fingerprint quality mechanisms play an essential role in controlling the quality of data entered in an AFIS.
- Different types of prints present different quality levels. The main types an AFIS has to deal with are: inked/live-scanned, rolled/flat/latent.
- The most challenging data in terms of AFIS performance are latents as there is no control over their quality.
- Although there is no standard way of measuring print quality, *NFIQ* and *NFIQ-II* (American National Institute for Standards and Technology (NIST) Fingerprint Image Quality) have become de facto standards due to their proven very high performance and availability.

2.2 Common usage of national AFIS

The study set out the typical use-cases concerning fingerprints. The most significant for SIS purposes concern a person who is present at the time of print acquisition, e.g. a suspect who has been arrested. Two parameters must be defined:

- Minimum expected accuracy of the matching process
- Maximum permitted response time

As an example, an arrested suspect is taken to a police station where he is fingerprinted. The set of 10 prints is used to search the central fingerprint database. A matching set of 10 prints is found, taken when he was arrested on a previous occasion. The person was present when each set of prints was taken, so high quality can be expected. As the person is in custody for possibly several hours a rapid response time is not a necessity.

As a contrast, when a rapid check is required, e.g. at an airport control booth, perhaps only two fingers are scanned.

The expected accuracy of the check is lower but there is still considerable control over the taking of the two prints and the full sets of 10 prints used for comparison. As the person is not under arrest a rapid response time is expected, probably a matter of seconds rather than minutes. If a match is achieved a second-line check can be carried out using a full 10 print search.

2.3 EURODAC and VIS

To learn potential lessons for SIS the two existing E.U. systems using AFIS were studied.

As set out in the eu-LISA Annual Report for 2014, EURODAC held 2.7 million fingerprint records (10 print) and a total of 756 368 transactions took place. Due to in-built quality procedures the rejection rate for sub-standard prints was 4.49%, necessitating the re-taking and re-submission of the prints. The size of the database is close to the potential for SIS but the volume of transactions is much smaller and the response times much slower than would be required for SIS – an urgent comparison in EURODAC is carried out within an hour, in SIS the expected time would be seconds due to the very different operational scenarios.

VIS holds around 20 million fingerprint records (10 print). Generally VIS conducts verifications at borders, i.e. is this person the original visa applicant? However, VIS also carries out one-to-many searches on new visa applicants and at second-line border checks using a full 10 print set. An average of 20 000 to 30 000 such identifications take place every day with a peak rate of 3000/hour. The expected response time for an identification is less than twenty minutes (less than three seconds for a one-to-one verification using one to four fingers for a typical border check).

2.4 Member States' and third country AFIS

The study identified that a national criminal police AFIS in the Member States can be larger than the anticipated size of the SIS AFIS due to the retention of extensive records. The two systems studied in the USA contain tens of millions of records. SIS can only hold prints in person alerts. On 1 January 2015 there were just under 800 000 person alerts in SIS.

2.5 The challenges in implementing AFIS technology

The challenges in implementing AFIS technology can be summarised as:

- Use-cases
- Performance
- Quality
- Speed (response time)
- Size of the database
- Matching capacity
- Number of transactions/matches at peak demand times
- Strategy to manage the queries
- Exchange formats
- System architecture: centralised or at several sites
- Type of data being processed – print format

- Latent prints

2.6 Conclusions

As stated in the introduction of this chapter, the technology is available and ready. The Commission has also highlighted challenges to be addressed. The recommendations for successful implementation and to address these challenges are described in chapter 4.

3. THE AFIS IN SIS

The SIS AFIS must handle all the types of fingerprint records that will be generated. This will include:

- flat and rolled prints
- fast checks where only two fingers, for example, are scanned
- latents collected from a crime scene

3.1 Data protection

Any processing of fingerprints within SIS II, including storage and use for identification purposes must comply with the relevant data protection provisions of the SIS II legal instruments and applicable national provisions on data protection implementing Directive 95/46/EC[5] and Framework Decision 2008/977/JHA[6]. Both legal instruments apply to the processing of fingerprints of third country nationals as well as Union citizens. Any use of the fingerprints must be authorised by Union or Member State law. In line with the principle of purpose specification, the purpose and means of using the fingerprints in SIS II must be clearly defined. Processing of fingerprints shall not go beyond what is necessary for the objective of the general interest pursued, and if necessary be subject to appropriate safeguards. The implementation of such new functionalities in SIS II should respect data protection by default and by design principles.

3.2 Scenarios for the use of fingerprints in SIS

Two types of fingerprint transaction can be foreseen in SIS:

- An alert is created/updated with the attachment of prints
- The SIS database is consulted using prints instead of name and date of birth. This consultation will also take place prior to the introduction of a new alert to check if the person is already in SIS under another alert

Prints must be attached to SIS alerts when available. The circumstances when prints can be encountered in SIS are set out in the sub-sections below. Each case was compared to similar "use-cases" already processed in Member States' AFIS. Depending on the scenario, the cases are broadly covered by the use-case in the JRC study describing "10 print to 10 print" checks.

Except where a case highlights an operational challenge, in general the quality of the prints is high as both the newly acquired prints from the person and the set of prints stored in the database

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[6] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters.

are taken in controlled circumstances with the option to reject poor quality prints and re-acquire them.

Where a Member State creates an alert but does not have prints to complete it, another Member State which has already dealt with the person may hold prints in its national AFIS. The SIRENE Manual[7] describes the sending of such prints to be attached to the alert. As prints may have been taken in another system it should be ensured that the prints hold a record of their "quality score" so that any use of the prints takes place in an informed context.

3.2.1 Refusal of entry or stay (Regulation, Article 24)

This person alert is by far the most common. Assuming that the issuing Member State has access to the person who is the subject of an alert in SIS (alert subject), 10 prints will be collected, added to the alert and compared with the 10 print cards already in SIS. This might identify links with other alerts.

3.2.2 Arrest for surrender or extradition (Decision, Article 26)

The alert subject might not be accessible at the time of the issue of the alert and prints will not be available. However, the alert-issuing Member State may already have the person's prints in its national AFIS and can complete the alert. 10 prints will be collected, added to the alert and compared with the 10 print cards already in SIS for other alerts.

3.2.3 Missing persons (Decision, Article 32)

The prints of such persons are not always available when the alert is created. However, in certain cases, if a national registry exists and legislation allows it, prints can be transferred to the alert.

In the course of the investigation, latent prints of the person may be used to query SIS (but these prints would not be retained and stored in the database). If this takes place it is not an alert creation but a case of consultation.

3.2.4 Persons sought to assist with a judicial procedure (Decision, Article 34)

Prints might not always be available; however a Member State can complete the alert with prints from its national AFIS, where permitted.

3.2.5 Discreet or specific checks (Decision, Article 36)

There may be cases where prints are not available. The nature of the checks implies that prints are not likely to be accessible at a later stage. However, the alert-issuing Member State may already have the person's prints in its national AFIS and can complete the alert. Police/border checks may offer the possibility to carry out a search against these prints.

3.2.6 Misused identity (Regulation, Article 36; Decision, Article 51)

With the consent of the victim whose identity has been misused, Member States can add his prints to the alert on the person who misused this identity. This measure will lead to an alert "update", not a "creation". It allows authorities to identify both impostor and victim, as the victim can prove his identity when necessary. After a hit from a search on name and date of birth at the first-line border control, the identity of the victim can be verified at the second line.

[7] Annex to Commission Implementing Decision 2013/115/EU on the SIRENE Manual and other implementing measures for the second generation Schengen Information System (SIS II).

3.3 Quantifying the size of the SIS AFIS and the number of transactions

At the time of carrying out the study there were around 5 500 fingerprint records in SIS. Member States confirmed that the lack of AFIS functionality was a limiting factor in uploading prints to SIS.

3.3.1 Size

The number of person alerts in SIS is relatively stable. This may increase with proposals to add alerts on return decisions and related entry bans. Even with an increase, the size of the SIS AFIS is expected to be below that of a large Member State and therefore does not present technical problems on sizing.

3.3.2 Volume of transactions

There are three types of transaction to be taken into account:

- **Queries/consultations.** The largest demand on SIS will be caused by queries/consultations. In 2014 almost two billion queries, on all alert categories, were sent to SIS, either in national copies or to the central system. This will include consultations, already sent to SIS, which will be supported by the introduction of an AFIS. Visa applications via VIS should be checked against SIS. Up to 20 000 to 30 000 identification queries/day are conducted. EURODAC processed 750 000 transactions in 2014. Prior to these transactions, VIS and SIS must be consulted for the prevention, detection and investigation of terrorist and other serious criminal offences. It is anticipated that fingerprint checks will also be conducted. Checks at Schengen borders are carried out using name and date of birth. In future, for third country nationals, it is envisaged that fingerprint checks will be carried out. Not all alerts contain prints, so not all person queries can be carried out in this way; many checks will continue to be on name and date of birth. Not all SIS access points can carry out queries based on prints.

- **Create/update/delete (CUD) of alerts.** There were 1.4 million CUD transactions in 2014. Of these 780 000 involved the creation and update of person alerts and could therefore involve the addition of prints. Deletion should be an automated process upon deletion of an alert but naturally the processing demands should be accommodated.

It is important to ensure that accurate statistics are available for the correct sizing of the SIS AFIS. Expertise gained in the development of national AFIS can be used in the context of SIS.

3.3.3 Standards for exchange of fingerprints

The NIST standards and best practice guide from Interpol provide an appropriate basis for such exchange.

3.3.4 Architecture

The architecture of SIS comprises:

- A central system handling 20% of transactions – five Member States use the central system directly
- National copies (80% of transactions) which can be:

- "partial" (only data formed of words and numbers - nine Member States have such copies) or
- "full" (data formed of words and numbers plus photos and prints - 16 Member States have such copies)

A central AFIS is needed to provide service to Member States without a national copy, Member States with a partial national copy or even Member States facing technical unavailability of their full national copy.

All alert CUD transactions involve the central system. Adding prints to an alert will require an AFIS quality check at the central system.

CUD transactions sent to the central system are broadcast within three minutes to the national copies. A central AFIS will be necessary to support these transactions.

According to the SIS II legal instruments, a search in a national copy must produce a result equivalent to a search in the SIS database. Compliance with this concept for searches carried out on names and numbers will have to be applied to fingerprint searches.

If a Member State implements its own AFIS as part of a national copy it will have to offer the same identification performance as the central AFIS. It is technically and legally possible to have an AFIS as a part of a national copy but equivalence of results will be a challenge.

Centralised architecture is easier to manage from a quality point of view but must be able to handle the demands placed on it. An architecture comprised of a central AFIS together with other AFIS in full national copies would distribute the demands but would face the challenge described above. This could be managed through all such AFIS using the same software.

Once an overall architecture has been decided it should be considered if use-cases should be handled in the same way or differences in volumes or response times would favour parallel work-streams or sub-systems within the AFIS.

Some law enforcement or border control operations will require a response time below 30 seconds but at a consular post the response time might only need to be below five minutes.

In controlled situations at a police station a response time below 10 minutes might be required. It is important to assess the workloads provided in these use-cases and the definition of priority in handling demands. The use of filters, such as age and gender can reduce the number of records against which comparisons are made thereby improving the response time.

Finally, the SIS AFIS will have to enter the evaluation and reporting procedures set out in the SIS II legal instruments.

4. RECOMMENDATIONS

The previous chapters confirm the readiness and availability of AFIS technology. In addition, the Commission considers that the implementation of the following 19 recommendations should be considered to support the successful deployment and use of an AFIS in SIS.

1. **Need for complementary statistics** - on the number of consultations/year on persons and their operational context in order to correctly assess the size and processing power of the AFIS

2. **Promotion of best practices** - for the SIS AFIS based on expertise acquired during the development and management of national AFIS

3. **Common exchange standard** - NIST containers provide an appropriate basis for the exchange of fingerprint data. An automatic check on implementation should be developed

4. **Prüm and SIS II complementarity** - the complementary nature of the Prüm mechanism and the SIS AFIS should be clarified to avoid overlap[8]

5. **Dedicated sub-systems** – due to the different use-cases, especially on volume and response time, there should be consideration of parallel work streams or dedicated sub-systems

6. **High-quality enrolment process** - the enrolment phase should favor the use of live-scan devices and experienced operators

7. **Storage of multiple datasets** - to support a composite matching strategy

8. **Controlled transfer of datasets** – the SIS AFIS should accept prints produced in other systems, as long as the parameters of these systems are retained in the dataset included in the alert

9. **Quality of capture points**

    a. **Supervision by an operator -** appropriate training for enrolment

    b. **Adequate sensor** - live-scan devices should be favoured

    c. **Enhanced graphic user interface (GUI)** – to provide real-time feedback on acquired data

    d. **Proper user interaction** - the enrolment process should be user-friendly

    e. **Adequate environment** - in terms of illumination, temperature and background

    f. **Sensor maintenance** - should be regular and systematic

10. **Quality assessment algorithms**

    a. **Adherence to standards** – the use of recognised quality metrics

    b. **Corrective actions** – to obtain satisfactory quality prints

[8] The fingerprints stored in SIS II are attached to alerts and access to SIS II takes place in the course of border controls and checks by law enforcement authorities. Based on Decision 2008/615/JHA, the Prüm mechanism provides the possibility to query national criminal AFIS. Unlike SIS II, the Prüm mechanism does not provide for real-time access of fingerprint records and can be used only in individual investigation cases.

11. **Quality of identification systems**

    a. **Quality-based processing** - including the use of supplementary tools such as alternative feature extraction functions and process-specific matching algorithms

    b. **Quality based fusion** - the combination of different samples so as to be able to conduct composite checks

    c. **Template substitution/update** – the use of best samples when generating templates for an AFIS

    d. **Monitoring** – producing statistics for each type of application; sites, devices and operators

12. **Children cases** – especially in relation to missing persons, the SIS AFIS should be able to tune the matching process where it is clear that the child will have grown since the prints were acquired

13. **Quality check central service** - to check print quality against the SIS AFIS quality metrics

14. **Reporting on lower quality fingerprint card** - when a dataset, proposed for enrolment or addition to an alert, does not have the quality level required for the SIS AFIS either in an alert or in the dataset card itself

15. **Integrity of the database** - use of best practice to reduce the risk of inconsistency or erroneous data, including prints, recorded in the database

16. **Consultation**

    a. **Enhanced resolution (1000dpi[9])** - to provide the possibility to store prints at higher resolution where Member States have upgraded their scanners

    b. **Flat and rolled fingerprints** - Member States should be allowed, for consultation only, to limit fingerprint collection to flat prints

    c. **Two prints fast check** - the possibility to carry out quick consultations

17. **Appropriate response times** – to cope with three indicative response times based on the different operational scenarios: (a) very short (i.e. below 30 seconds); (b) medium (i.e. below five minutes); (c) longer (i.e. up to ten minutes)

18. **Queries priority** - the definition of priority levels for processing queries in order for the SIS AFIS to better manage the workload of the system

19. **Performance benchmark** – early consideration of the scheduling of performance evaluations of the SIS AFIS

[9] Dots per inch.

5. THE NEXT STEPS - ACTION PLAN

The completion of the study and the submission of this report for consultation to the European Parliament are the first steps towards the provision of AFIS functionality in the SIS environment. In practical terms, the high-level description of activities which must now take place, with eu-LISA and the Member States, can be summarised as follows:

(1) Establish the requirements for the special quality check to ascertain the fulfilment of a minimum data quality standard. The specifications should be included in a Commission Implementing Decision

(2) Finalise the user requirements and the sizing of the required system

(3) Define the architecture of the required system. This should be included in a Commission Implementing Decision

(4) Define the technical specifications and the timeline for implementation

(5) Carry out the project leading to the implementation of the SIS AFIS

6. CONCLUSION

AFIS functionality has already been intrinsically linked with law enforcement and border databases. SIS constitutes one of these databases and alerts related to persons will not deliver their full capacity and usefulness without the support of an AFIS.

In the light of the analysis and observations summarised in this report, the Commission concludes that AFIS technology has reached sufficient levels of readiness and availability in order to be integrated in SIS. This report also provides an overview of the Commission's suggestions which will be addressed in the implementation and use of the SIS AFIS in an operational environment.