Council of the European Union

NOTE

From:	Presidency
To:	Working Party for Schengen Matters (SIS/SIRENE)/Mixed Committee (EU-Iceland/Norway and Switzerland/Liechtenstein)
No. prev. doc.:	7045/18
Subject:	Automated Fingerprint Identification System (AFIS) component of the Schengen Information System (SIS)
	- Implementation of a multiple identity dectector (MID)

I.   INTRODUCTION

In accordance with point (c) of Article 22 of Regulation (EC) No 1987/2006 of the European Parliament and the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)[1] and point (c) of Article 22 of Council Decision 533/2007/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II)[2], the European Commission submitted in February 2016 a report to the European Parliament and the Council on the availability and readiness of technology to identify a person on the basis of fingerprints held in the Schengen Information System (SIS)[3].

---

[1]   OJ L 381, 28.12.2006, p. 4.
[2]   OJ L 205, 7.8.2007, p. 63.
[3]   6720/16.

The Member States (MS) and their end-users will be able to use a fingerprint search functionality to search for a person in SIS not only by their name and date of birth, but also by their fingerprints. In this way, law enforcement authorities can locate people with false identities, missing persons, people trying to escape justice with forged identity documents and so on.

Fingerprints could only be used to verify and confirm the identity of a person already identified by name. This security gap enabled individuals subject to an alert to use fraudulent documents to avoid an exact match in SIS.

The implementation of this new technology will make Europe a safer place. Gradually it will become impossible for individuals like the terrorist who carried out the Berlin attack and who was known in SIS to have used 16 different identities (aliases) to operate.

The Commission confirmed that, to address this critical weakness, a fingerprint search functionality would be added to SIS in the form of an Automated Fingerprint Identification System (AFIS), as provided for in existing legislation[4].

Once developed, the AFIS would also be accessible to Europol and would therefore run alongside Europol's systems for criminal investigation and counter-terrorism and the fingerprint exchanges performed under the Prüm framework. The relevant 2015 studies by the Joint Research Centre and the eu-LISA Agency, endorsed in the Commission's February 2016 report, established that with the help of the relevant stakeholders, including all Member States and the Commission, the AFIS functionality could be up and is running since 5 March 2018[5].

The requirements established during the preparation and design phase, in particular include that all newly created or amended fingerprint records are to be checked against AFIS and a function applicable to all Member States a consultation mechanism on duplicate fingerprints in the SIS records.

---

[4]   Articles 22, point (c), of Regulation (EC) No 1987/2006 of the European Parliament and the Council of 20 December 2006 and of Council Decision 533/2007/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 381, 28.12.2006, p. 4 and OJ L 205, 7.8.2007, p. 63, respectively).

[5]   The eu-LISA Agency implemented AFIS in SIS via the long-anticipated Release 9.0.0 on the evening of 5 March 2018.

For the remainder of the Member States, AFIS in its current state includes a search of SIS for previous alerts about the same person from other Member States, when uploading the NIST-compliant fingerprints to the alerts.

For SIRENE officers, the procedures involving AFIS-related notifications, matches and hits are described in the latest update of the SIRENE Manual from 31 August 2017[6].

In view of this new search functionality and the potential problems associated with it, a common approach should be established and taken into account.

To that end the prescribed steps to be taken in the processing of such hits are outlined below and reference is made to the corresponding points in the SIRENE Manual, in particular Sections 1.15 and 2.5.

II. PROCEDURE SET OUT IN THE SIRENE MANUAL

The reporting procedure for matches on fingerprints when carrying out the initial upload of fingerprints or when carrying out searches using fingerprints is set out in Section 2.5 of the SIRENE Manual.

Point (a) of Section 2.5 says that where a possible match in SIS II is achieved from a search of a person's fingerprints against the fingerprints stored in SIS II, national law and procedures apply for the verification of the match.

Point (b) of Section 2.5 provides that once the match has been verified, the SIRENE Bureau in the Member State achieving the match must inform all other affected SIRENE Bureaux, using an L form, about the match and the possible need to update alphanumeric data in SIS II.

---

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

Point (d) of Section 2.5 describes a further provision to be observed. The provision says that SIRENE Bureaux receiving such information must check the data for which they are responsible and take the necessary measures to ensure the updating of alphanumeric data, as described in Section 1.15.

The last paragraph of Section 1.15 of the SIRENE Manual also applies in this context. In order for the data in SIS to be kept up-to-date, in line with the outcomes of SIS-AFIS matches, the SIRENE Bureau must take the necessary measures to ensure the prompt updating of alphanumeric data in alerts; either by the SIRENE Bureau itself or by liaising with the relevant authority which created the alert. This covers activities such as inclusion of aliases or correction of identity details.

III. QUESTIONS ABOUT THE PROCEDURE

These steps to be performed raise the following questions, which will have an impact in particular on the steps to be taken by the end user:

a) How are the MS currently implementing the provisions of Section 2.5 of the SIRENE Manual, in particular with regard to a possible verification of matches under the relevant national laws and procedures (e.g. 24/7 availability)?

b) If verification of matches takes place, it should be clarified to what extent and if applicable in which time sequence the verification of a SIS AFIS match is performed before the match is communicated to the other Member States. Point (b) of Section 2.5 of the SIRENE Manual says that the other MS are to be informed once the match has been verified. In this context, pursuant to Section 1.15 those Member States then have an obligation to update the alphanumeric data promptly.

c) If MS rely exclusively on automated data matches given the high probability of a hit and so no verification is performed, should the MS affected still be notified under Section 2.5 of the SIRENE Handbook?

How is the provision 'once the match has been verified' under point (b) of Section 2.5 of the SIRENE Handbook to be interpreted? Should a verification be performed or can it be dispensed with on the basis of national rules? In the latter case, would the MS affected no longer need to be notified? Specifically, the added value of SIS AFIS in this area should be examined.

d)   Where there is no verification, but a notification is sent to the relevant MS(s), how can this be squared with Article 22 of the General Data Protection Regulation ('GDPR') and Article 11 of the Data Protection Directive for Police and Criminal Justice Authorities? Both of those articles contain specifications concerning automated database checks and the use of the results of such checks against the interests of the person concerned. It should be stressed, in that regard, that pursuant to the GDPR, verification need not be performed only through the use of fingerprint checks; other verification methods could be used, such as photo comparisons.

e)   How should hits be handled as regards the rules on incompatibility, in particular where SIS AFIS matches have not been verified in advance but notified? In principle, the SIRENE Manual provides the option of derogation from incompatibility rules, in particular for national security purposes. The use of the term 'in particular' indicates that this is not an exhaustive list, so that the option may also be utilised in the context of serious crime.

IV.   IMPLEMENTATION OF A MID FUNCTION IN THE SIS

The new SIS legislation (the three Regulations to be adopted in Autumn 2018[7]) has no clear rule governing SIS AFIS matches and the associated procedures, except for latent prints from crime scenes.

---

[7]   See 9146/18 + COR 1.

In the context of the draft regulations on interoperability[8], a discussion is also being held on the underlying issues relating to the verification procedure following a biometric match. This concerns both the future interoperability model and the associated concerns of combating cross-border crime, protecting external borders and, of course, preventing the use of false or falsified identities by potential criminals or other suspicious persons, thereby greatly facilitating the recognition of such persons.

One potential model for addressing the underlying issues, which may be used as a basis for discussion, is included in the proposed draft regulations on interoperability. They provide for a multiple-identity-detector (MID). Within the MID, the corresponding links between alerts (identities) from the different major systems are automatically established. The connotation (colour) of the links can be changed after the corresponding verification.

It would also be desirable to have a similar MID function in SIS, so as to provide an operational solution for the following scenario in SIS AFIS:

- A SIS AFIS match triggers a link and a notification is sent, based on the current procedure, from CS.SIS to the MS that has obtained the match.

- The MS performs the verification and the link can then be seen in another colour as a verified match.

- MS would not need to correct/supplement the alias identities as the alerts have been linked by the MID. So there is no more uncertainty about where added alias data has come from.

- The workload of the SIRENE Bureaux would be significantly reduced by this linking process.

- This procedure also brings advantages in relation to the data protection provisions as it is no longer a question of 'hits' but 'matches'.

---

[8] See 9670/18.

- This procedure would be fully compliant with the future SIS regulations, where AFIS is to be compulsorily implemented and its usage will be further extended to FRONTEX and Eurojust, in addition to Europol.

This model could add value, mainly as it would comply with the future regulations on interoperability and would considerably reduce the workload as the addition of alias data would no longer be necessary.

As regards verification as a 'hit' the following points are mentioned, for information. At EU level there is currently a binding legal requirement for fingerprint matches in the EURODAC system to be verified by an expert (applicable to all results provided from EURODAC). The quality of the expertise must of course meet the relevant quality management requirements. Since November 2015 all MS have had to comply with these requirements in their central forensic laboratories and the work is routinely subject to external evaluation. All MS have this type of central forensic contact centres which also handle all the Prüm data exchange work.

In addition, the final amount of data in the EU's biometric matching service (BMS) is expected to reach some 300 Million biometric data sets.

Above all, the fingerprint data quality planned for the Entry/Exit System, with only four fingers on one hand, will in any case lead to an increased number of false hits. Even in those circumstances, however, individual fingerprint testing of cases giving rise to concern can result in reliable identification or, indeed, rule out such candidates. But such cases always require follow-up procedures and would need technical, staffing and organisational arrangements that enabled them to be performed in a few minutes 'around the clock'.

V. CONCLUSION

The Presidency wishes to provide clarity on the underlying issue and invites the MS to engage in the discussion process on the basis of the questions set out under point III with a view to reaching a common approach in the SIS/SIRENE Working Party aimed at solving the underlying problem with the solution set out under point IV. The objective of SIS AFIS must always be to make use of the available information in a legal manner and over the long term.

The Member States are therefore requested to express their position as regards the above-mentioned issues with respect to the differing procedures used in MS when verifying fingerprints and to interoperability.

On that basis the Presidency intends to establish a common approach with regard to the implementation of a MID function in SIS AFIS, that could be forwarded to the JHA Counsellors meeting on 19 July 2018, with a view to being incorporated in the draft regulations on interoperability.

———————————