COUNCIL OF THE EUROPEAN UNION

Brussels, 5 February 2002

5968/02

LIMITE

SIS 6
COMIX 78

NOTE

from :	Presidency
to :	Working Party on SIS (EU/Iceland and Norway Mixed Committee)
No. prev.doc.	14790/01 SIS 107 COMIX 767 14094/01 SIS 100 COMIX 742 13269/01 SIS 95 COMIX 693 6164/5/01 REV 5 SIS 11 COMIX 114
Subject:	Requirements for SIS

1. Introduction and summary

On 7 December 2001, the Ministers of Justice and Home Affairs had a debate on the future requirements for SIS, which built upon the discussions held in the SIS Working Group and the Article 36 Committee during the whole of 2001.

Taking into account the timing and the complexity of the task, it is thought useful to divide the work, set priorities and continue accordingly. The discussions held until now and notably the outcome of the Ministers' debate are taken as a basis for setting these priorities.
A proposal to this end, and by the same token, for the way to go forward is submitted in chapter 5, based on the description of each of the requirements as set out in chapters 3 and 4.

Chapter 2 sets out some general questions such as methodology, timing and implementation, the involvement of the JSA, etc.

2. General questions

2.1 General comments

Setting out and deciding upon the requirements for SIS is a complex task because it is a multi-pillar and multi-disciplinary matter, covering a wide variety of subjects and involving many actors. This follows from the fact that the SIS is a support tool, both to the free movement of persons and police co-operation.

When the SIS was first created, its only purpose was to be a compensatory measure for the opening of the borders. Ever since, and not in the least because the SIS has proven to be a useful and efficient tool, recognition has grown that the potential of the SIS could be maximised, mainly within the frame of police cooperation.

The most clear examples for this are those requirements that aim at extending the access to SIS data to other authorities than those initially foreseen. They are mostly authorities that will not be able to take the concrete measures for which the alerts have been introduced (arrest, refusal of entry to the territory, communication of the whereabouts, surveillance, …) but for whom the information that a person is inserted in the SIS can be an asset in their work and improve their efficiency. Obviously, such access should be carefully considered, not only because of the very evident data protection reasons but equally to avoid that by granting a too large access to the SIS, the SIS data would become less valuable and the SIS less efficient. Nevertheless, the idea of using the SIS data for other purposes than those initially foreseen, and especially for police *information* purposes in a broad sense, is now widely agreed upon and even follows from the Council conclusions after the events of 11 September 2001.

2.2 Timing and implementation

Concerning timing and implementation, the list of requirements for SIS can be divided, as was done originally, into two main parts: the proposals to extend the access to SIS and the proposals for new functionalities.

This stems from the fact that extending access to the SIS is a matter of national implementation[1] and does not affect the technical implementation of the C.SIS or N.SISes. It is therefore independent from the technical development of SIS II and can be done at any time, providing that the legal conditions are fulfilled. The drafting and approval of the necessary legal instruments is therefore the only condition for the implementation of these proposals.

The implementation of the new functionalities depends both on the legal and technical conditions being in place. For most, if not all, of the functionalities, the technical implementation will be done in the development of the SIS II because it is either technically impossible with the current system or so cumbersome that the costs do not outweigh the benefits and/or political priority.
However, in order for the technical specifications of SIS II to be as accurate as possible, it is necessary to have very soon a clear view on the politically desired functionalities for SIS II. The legislative acts implementing them, which will also contain the exact details for implementation, should be ready at an early stage of the development of SIS II.

2.3 Involvement of the JSA

The Joint Supervisory Authority (JSA) will be involved in the decision-making process about the new requirements for the SIS. The practical arrangements of this involvement will be discussed at the meeting of the Presidency with the JSA at the end of February.

2.4 Methodology

Depending on the degree of support they have, requirements will be treated differenty:

a) once there is an agreement in principle about a requirement, a legislative initiative can be proposed;
   - the Presidency has described in chapter 3 those requirements it considers ready to be submitted in a legislative proposal;
   - further details (legal basis, grouping of certain requirements in the same legislative act, exact wording of the proposal, data protection measures, etc.) can then be discussed and agreed upon in the negotiations about these initiatives;

[1] The practical and organisational consequences of giving access to Europol and/or Eurojust have not yet been examined in detail.

b) requirements concerning which there are still major objections or that require more study before a principle decision can be taken, should be further discussed:
   - the Presidency has set out these requirements in chapter 4 and has tried to describe the status of the discussions as well as the "open questions";
   - the SIS Working Group should further discuss them with the aim of submitting an advice to the higher groups, which should take a principle decision;
   - following such a decision, either a legislative initiative should be prepared or the requirement should be abandoned/postponed indefinitely;

c) requirements that do not require legislative changes can be passed on to the technical experts once they have been agreed upon in the SIS Working Group, the requirements concerned are the possibility to carry out searches on the basis of incomplete data; transliteration rules, search criteria for issued documents.

3. Requirements for which there is general agreement[2]

Access for governmental vehicle registration authorities to certain categories of SIS data

The need to allow vehicle registration authorities access to certain categories of SIS data has long been recognised so as to enable the recovering of stolen vehicles.

The legislative act allowing for this access will have to determine in detail:

- to what categories of data these authorities can have access: data on stolen, misappropriated or lost vehicles, blank (and issued[3]) stolen, misappropriated or lost official documents relating to vehicles;
- for what purpose they can use the data: to refuse the registration of such vehicles and to inform the competent authorities of any hit in order for the vehicle or document to be seized; and
- what data protection guarantees need to be provided: capacity of the personnel, no access to personal data, ...

When determining the legal basis for the legislative act to allow for this access, account should be taken of the opinion of the Legal service, set out in document 9731/99 JUR 249 SIS 20 CATS 10, and notably Council Directive 1993/37/EC of 24 April 1999[4].

Consideration should be given to the fact that in some countries, the vehicle registration authority is not a governmental body. Taking into account the objections against granting non-governmental bodies access to the SIS, it would appear that non-governmental vehicle registration authorities should not get access to the SIS. The concerned States could consider setting up, in as far as possible under national law, a system of indirect access, whereby police officers could on a regular basis check lists of vehicles that were presented to be registered against the SIS.

Extended access for authorities issuing residence permits

In the context of combating illegal immigration, it seems useful and justified to extend the access of authorities issuing residence permits to data on identity documents.

[2] This does not imply that the reservations of some delegations on certain issues have been lifted.
[3] This is not foreseen in the Schengen Acquis as it currently stands.
[4] Published in OJ L 138/57 of 1.6.1999

The legislative act allowing for this access will have to determine in detail:

- the categories of data these authorities can have access to: data on stolen, misappropriated or lost (blank and issued) identity documents;
- for what purpose they can use the data: to refuse a residence permit and to inform the competent authorities of any hit in order for the document to be seized;
- what data protection guarantees have to be provided: capacity of the personnel, ….

Access for Eurojust

When adopting the proposal for a Council Decision setting up Eurojust (foreseen for 28 February 2002), the Council intends to adopt *i.a.* the following declaration[5]:

> *"The Council agrees to adopt, as a matter of urgency and in accordance with the principles laid down in Article 101(3) of the Schengen Convention, no later than 15 June 2002, arrangements whereby the national members of Eurojust will have access to certain data in the Schengen Information System, in particular those referred to in Articles 95 and 98 of the Schengen Convention."*

Such access will allow Eurojust to be more complete and accurate in its coordination of and cooperation in operational cases of investigation and/or prosecution.

If this declaration is adopted, a legislative act should be prepared, which should determine in detail:

- what categories of data Eurojust can have access to: data referred to in Articles 95 and 98 of the Schengen Convention;
- for what purpose Eurojust can use this information: coordination of and cooperation in international operational cases of investigation and/or prosecution;
- what data protection guarantees need to be provided: capacity of personnel, applicable law and competent data protection authority, …;
- how such access will be organised in practice.

[5] Cf. document 14766/1/01 REV 1 EUROJUST 14

New categories of objects

It is generally recognised that it should be possible to introduce additional types of objects into the SIS, for the purposes of seizure, use as evidence in criminal proceedings or surveillance.

The legislative act setting out these new categories will have to determine in detail:

- what categories of objects are allowed: boats, aircrafts, containers, invalid and counterfeit identity documents, other issued official documents apart from issued identity papers (including issued residence permits, vehicle registration certificates, ...), "credit documents" (cheques, bonds shares), works of art, animals etc
- what criteria have to be fulfilled to insert these objects to make sure that the data are of a high enough quality to be useful: is some kind of serial number required or any other means that allows an (easy and) unequivocal identification of the object, which type (technical specifications) of boats, aircrafts and containers are meant, …
- what purpose the data are introduced for: to seize invalid or counterfeit documents, or stolen, misappropriated or lost objects and/or use them as evidence in criminal proceedings, to put boats and aircrafts under surveillance, …
- which authorities would get access to these new categories of data;
- what data protection guarantees need to be provided: capacity of the personnel, no access to personal data, ...

A decision on the new objects to be inserted in the SIS should avoid an overlap between the SIS and existing systems and the cost/benefit ratio should take account of the (main) users of the SIS. When deciding about the necessity of including photographs in the SIS to allow for unequivocal identification of objects, regard should be given to the decision about wether or not photographs on persons will be included into the SIS, as including photographs is a major technical change compared to alerts consisting only of text.

Addition of certain particulars concerning a wanted person or object

With a view to maintaining public order and security, protecting the officials performing checks on the SIS and increasing the use of the SIS, it is considered useful to include additional information on a wanted person or object.

The legislative act setting out these new categories will have to determine in detail:

- what particulars can exactly be added: the type of offence, the fact that the person is a fugitive, the fact that the person is in psychological danger, covert markers and intelligence markers related to alerts entered pursuant to Article 99 (the fact that a person is a suspected drugs dealer, suspected people trafficker), information on objects owned, held or used by offenders, …
- what criteria have to be fulfilled to insert these particulars and what other data protection guarantees need to be provided
- which authorities would get access to this additional information: a distinction can be made between information that should be visible for the on-the-spot officers and other information that rather belongs to what is now known as the SIRENE files but which could in the SIS II be included in another part of the alert, only visible to the SIRENE bureaux for example;
- if necessary, any additional procedures to be followed when certain particulars are used.

As the Schengen Convention does not describe what kind of information can be entered in the SIS concerning wanted objects, it is possible that no legislative text is necessary to determine what information can be added in alerts on vehicles, vessels and aircrafts (such as indications on the class of risk, for example that the vehicle is being used to transport explosives / chemical or biological weapons / nuclear material).

Interlinking of alerts

It is widely recognised that the possibility of linking alerts will improve the use and efficiency of the SIS.

The legislative act allowing such interlinking will have to determine in detail:

- which categories of data can be linked to which, thereby also taking into account the current proposals for new categories;
- what criteria have to be fulfilled to interlink certain alerts;
- what data protection guarantees are necessary, *i.a.* to avoid that certain authorities with limited access would get, through the interlinking, access to categories of data to which they are not allowed access.

Simplifying procedures for introducing Article 99 alerts

Cf. document 5969/02 SIS 7 COMIX 79

Determining the storage period for SIRENE files

Determining the storage period for SIRENE files after deletion of the relevant alert is an operational measure but it has to have a basis in law. This period is currently governed by domestic law but, since the files include data from other States, it would be useful to draw up common rules. In doing so, it will probably be necessary to determine what the SIRENE files are and possibly even what the SIRENE bureaux are.

Consideration might be given to setting only a maximum deadline, taking into account domestic legislation, limiting the applicability of this rule to information coming from another State and differentiating between information in cases where a hit has occurred and those where the alert has expired.

If it is agreed that these rules be included in the SIRENE Manual, this requirement would be taken care of in the legislative act modifying the SIRENE Manual.

4. Requirements that require further study

Access to the SIS for security and intelligence services

Cf. document 5969/02 SIS 7 COMIX 79

Restricted access terrorist database

Cf. document 5969/02 SIS 7 COMIX 79

Access for Europol

Cf. document 5970/02 SIS 8 COMIX 80

Incorporation of identification material in alerts on persons

It is widely recognised that it should be possible to include identification material in SIS II, such as photographs, fingerprints and possibly even other material.

However, more study is necessary to determine:

- the type of identification material that can be included: photographs, fingerprints, useful elements for the unequivocal identification of persons;
- the authorities having access to it: as with the addition of certain particulars to an alert, a distinction could be made between identification material that should be visible for the on-the-spot officers (such as photographs as it clearly helps the officer with the identification of the person) and other information (such as fingerprints and other elements that require more time to be used as means of identification) that rather belongs to what is now known as the SIRENE files but which could in the SIS II be included in another part of the alert, only visible to the SIRENE bureaux for example;
- the type of alerts to which such material could be added;
- the data protection guarantees that need to be provided.

It has also been proposed to foresee the (technical) possibility to link SIS II to national databases for facial/iris recognition, number plate recognition and fingerprint identification, without for the moment deciding on whether to actually set up this link.

The technical, legal, organisational and data protection conditions for creating this possibility should be further analysed.

Full recording of all system searches

There seems to be a general agreement on the usefulness of recording all system searches in order to improve the possibilities to check the correctness and legal appropriateness of searches in the SIS to allow more effective controls by the data protection authorities. This should ideally be supported by software capable of analysing/interrogating the record of system searches making it easier to identify if the system is being abused and affording the opportunity to develop an "intelligence search capability" of this aspect of the system.

When considering these proposal, it should therefore be considered which authorities are allowed, and/or even obliged to check these audit trails and for which purposes they can be used (audit and investigative / intelligence purposes).

Furthermore, it has been proposed that, without prejudice to national legislation, it should be possible to keep the audit trails for more than 6 months, notably with regard to the discovery of illegal queries.

In as far as searches on the SIS are done on the N.SIS, this is a matter of national implementation.

Persons precluded from leaving the Schengen area

Although the need for a category of persons precluded from leaving the Schengen area is recognised in some respects, there are still many questions about which persons would be concerned (e.g. inmates who have been granted a conditional release, persons under criminal investigation but also minors subject to custody decisions), the action required when finding such a person, the implications under domestic law, etc.
Due account should be taken of the right of free movement and in particular Directive 64/221/EC.

The persons envisaged to be included into the category of "persons precluded from leaving the Schengen area" could vary widely:

- children whose parents are in a dispute over a claim to custody or who are at risk of abduction and who, under a judicial or administrative order, may not leave the Schengen area,
- inmates who have been granted a conditional release by the prison (e.g. the chance to spend a weekend or Christmas at home), or
- persons subject to criminal investigations.

Several delegations have supported the idea of introducing an alert on children who may not leave the Schengen area, especially if this is done further to a judicial or administrative order.
As to the other proposals:

- it has been stated that the repercussions introducing prisoners into the SIS would not be in reasonable proportion to the potential benefits, since the number of prisoners allowed on conditional release failing to return is not very high,
- and, it has been pointed out that persons subject to criminal investigations could be introduced as an Article 95 or Article 99 alert.

Further study is therefore necessary.

Access for public prosecutors and possibly other judicial authorities such as magistrates

Since Article 101 of the Schengen Convention allows access for "authorities responsible for (…) police and customs checks carried out within the country, *and the coordination of such checks*", it would seem that public prosecutors have a right to direct access to the SIS based on this provision. This can, however, depend on each State's legislation and the definition of powers under domestic law.

Where public prosecutors are not responsible for the coordination of police and customs checks, it should be carefully considered for what purposes they would need access to the SIS and under which conditions. The same is true for other judicial authorities, also in view of the security considerations that have to be taken into account.
However, there is a need to ensure that the authorities responsible for the European arrest warrant have the necessary access to the SIS and taking account of national legislation, it should be examined whether an amendment of the Schengen Acquis is necessary to allow this.

Access for asylum authorities

In the context of combating illegal immigration, it seems useful to allow asylum authorities access to alerts pursuant to Article 96 with a view to better determining which State is responsible for an asylum application case under the Dublin Convention. However, it was recognised that once Eurodac would start operating, the access for asylum authorities to the SIS might be re-considered. In view of the fact that Eurodac should start operating during the year 2002, it should be examined whether it is (still) worthwile to draft and negotiate a legislative act for this purpose.

If it is considered opportune to draft a legislative proposal, the act allowing for this access will have to determine in detail:

- the categories of data these authorities can have access to: alerts pursuant to Article 96;
- for what purpose they can use the data: to determine the responsibility for asylum applications and possibly to inform the competent authorities of any hit in order for them to take the necessary measures to remove the person from the Schengen territory and
- what data protection guarantees have to be provided: capacity of the personnel, ….

Extending the duration of alerts in the SIS and replacing maximum deadlines by review deadlines

Most delegations consider that the rules of the Schengen *acquis* concerning the duration of alerts and the possibility of renewing the alert when it is still valid under national law offer enough flexibility and cover operational needs. The added benefit, in terms of management and workload, of extending the duration of SIS alerts and/or replacing maximum deadlines with review deadlines does not outweigh the significant data protection problems that this would involve.
Some delegations still want these proposals to be examined further.
A principle decision should be taken.

Access for government departments such as Benefits Agency

In the context of combating cross-border financial crime, it seems useful to allow government departments such as the Benefits Agency access to SIS data on stolen, invalid, counterfeit etc. identity documents.

It will have to be determined:

- exactly which authorities would get access;
- to which data these authorities could have access;
- for what purpose they can use the data: to refuse granting benefits and possibly to inform the competent authorities of any hit in order for the documents to be seized and
- what data protection guarantees have to be provided: capacity of the personnel, ….

Access for non-governmental authorities

There are many reservations about giving non-govermental authorities access to SIS data.
A certain need for it is recognised, f.i. to allow access by central credit agencies in connection with the fight against cross-border financial crime. However, it is also generally agreed that further study would be necessary to ensure that such access is only indirect, always subject to governmental control and limited to non-personal data.

Possibility of introducing multiple alerts on the same person by the same State

Different States are allowed to introduce (compatible) alerts on the same person.

In order to allow the judicial authorities greater leeway to conduct criminal investigations, it has been proposed that a State be allowed to introduce several (compatible) alerts on the same person. There are, however, practical objections to this, notably that this might lead a display of confusing search results for the officer-on-the-spot.

As the Schengen Convention does not prohibit this possibility for one State to introduce multiple alerts on the same person, there is no need to amend it.
If it would be agreed to allow for this possibility, only the SIRENE Manual would have to be adapted, as additional procedures would have to be drawn up, notably to establish an order of priority avoid the risk of double data and to guarantee data quality in general.
If agreed upon, this requirement would thus be taken care of in the legislative act modifying the SIRENE Manual.

Network for information exchanges concerning visas issued

In its conclusion n° 26 of 20 September, the Council invited the Commission to submit proposals for establishing a network for information exchanges concerning visas issued.
As the Commission will do a feasibility study for the technical implementation of SIS II, it proposes that the possibility of using the SIS for such a network for information exchanges be examined in this technical study.

It should therefore be considered whether the SIS is the appropriate tool for storing and exchanging large volumes of information on delivered (and refused) visa taking into account that the majority of these data need not to be visible for the SIS end users, as these persons are not "wanted".

Persons likely to be violent troublemakers at certain events

Following the Council conclusions of 13 July 2001, a new category could be created in the SIS to include data on persons likely – in the context of certain international events, especially those linked to demonstrations in the context of European summits or comparable events or to sporting events – to be violent troublemakers, posing a threat to public order.
This proposal begs questions as to the right of free movement (cf. Directive 64/221/EC), other civil liberties and data protection, as these persons would only be "wanted" for limited time periods and in connection with certain events. Alerts concerning these persons should therefore not be permanently visible or included in the SIS, requiring a very careful and cumbersome management of such alerts.
While there is no doubt about the fact that there should be an information exchange between European law enforcement agencies concerning violent troublemakers in view of mass events, and this was also recognised by the Council on 13 July 2001, the main question is whether the SIS is the most appropriate tool for such an information exchange.

In case of a positive answer to this last question, it will be necessary to determine what criteria have to be fulfilled in order to include people in this new category, which authorities will have access to the data, what action is required when such persons are discovered, and what data protection guarantees need to be provided.

5. Conclusion

The SIS Working Group is invited to agree on the following conclusions and submit them to the Article 36 Committee.

The following proposals are agreed and are therefore submitted to the Commission to be taken into account in the development of SIS II:

- the possibility of carrying out searches on the basis of incomplete data (in as far as this is technically relevant for other systems than the national systems)
- general and easily applicable transliteration rules
- search criteria concerning issued documents.

As functional discussions on the following proposals have advanced well enough, it is proposed that they be further discussed only once they are subject of a legislative proposal:

- access for governmental vehicle registration authorities
- extended access for authorities issuing residence permits
- access for Eurojust
- new categories of objects
- addition of certain particulars concerning a wanted person
- inter-linking of alerts

The following two proposals will be included in a legislative act modifying the SIRENE Manual:

- simplifying procedures for introducing Article 99 alerts
- determining the storage period for SIRENE files

In the short term, the SIS WP should submit to the higher groups a final advice on the following proposals:

- access for security and intelligence services
- restricted access terrorist database
- access for Europol
- incorporation of identification material
- full recording of system searches

- persons precluded from leaving the Schengen area
- access for public prosecutors and other judicial authorities
- access for asylum authorities
- extending the duration of alerts in the SIS and replacing maximum deadlines by review deadlines

The other proposals could be discussed at a later stage:

- access for government agencies such as the Benefits Agency
- access for non-governmental agencies
- possibility of introducing multiple alerts on the same person by the same State
- network for information exchanges concerning visas issued
- persons likely to be violent troublemakers at certain events