Council of the
European Union

**Brussels, 28 May 2018
(OR. en)**

**6353/06
ADD 1 DCL 1**

**SCH-EVAL 15
COMIX 158**

DECLASSIFICATION

of document:	ST 6353/06 ADD 1 RESTREINT UE/EU RESTRICTED
dated:	13 March 2006
new status:	Public
Subject:	Answers to the additional questionnaire addressed to the new Member States related to - Schengen Information System - Prior consultation

Delegations will find attached the declassified version of the above document.

The text of this document is identical to the previous version.

COUNCIL OF
THE EUROPEAN UNION

Brussels, 13 March 2006

6353/06
ADD 1

RESTREINT UE

SCH-EVAL 15
COMIX 158

NOTE

from :	the Maltese delegation
to:	the Schengen Evaluation Working Party
No. prev. doc. :	9820/1/05 REV 1 ADD 1 SCHEVAL 36 COMIX 380
Subject :	Answers to the additional questionnaire addressed to the new Member States related to - Schengen Information System - Prior consultation

On 1 July 2005 the Schengen Evaluation Working Party adopted the questionnaire for the Schengen evaluation of the new Member States - doc. 9820/1/05 REV 1 SCH-EVAL 36 COMIX 380 of 30 July 2005.

It was also agreed that the part on SIS was supplemented by an additional questionnaire, including a paragraph on Prior Consultations and some questions on visa, for which a separate document was prepared and sent to the new Member States - doc. 9820/1/05 REV 1 ADD 1 LIMITE SCH-EVAL 36 COMIX 380 of 19 September 2005.

Please find below the answers to the additional questionnaire on Schengen Information System and Prior consultation.

SCHENGEN INFORMATION SYSTEM

I. Schengen Information System

Note : Questions included in the following chapter are based on the current SIS, but are equally valid in relation to SIS II.

1.1. Legislative and regulatory provisions adopted or to be adopted to set up the national system.

The legislative and regulatory provisions to be adopted are currently under review. The final drafts of the legislation will be ready after the adoption of the SIS-II legal basis in the Council.

1.2. Have you already made preparations on the practical modalities or created National Information Systems for the purpose of issuing and accessing the following categories of alerts:

a) alerts on persons who should be refused entry to the Schengen area;
b) alerts on persons wanted for arrest (in view of surrender or extradition);
c) alerts on persons to ensure protection or prevent threats;
d) alerts on persons wanted for judicial procedure;
e) alerts on persons and objects for discreet surveillance or specific checks;
f) alerts on objects for seizure or use as evidence in criminal proceedings.

Yes. These are being catered for in Malta's police national system. A new system is being developed so as to cater for the new requirements.

Are these systems set up with the future data structure of the SIS II in mind?
Yes. The future structure of the SIS-II is being in-built into the national system.

If yes, what is the level of progress achieved?
System development is in progress. These are expected to be completed in time for integration testing with SIS-II.

If not, please describe the relevant projects/plans.

N/A.

- **Organizational conditions**

1.3. Geographical location of the future access points or national interfaces of the SIS II (if known).

The main Police data centre is located in Floriana (Malta) and the Police back-up data centre is located in Gudja (Malta).

1.4. Describe the structure, hierarchy and organisation of the future SIS II national office.

A technical unit in the Malta Police Force will be responsible for the operational aspects of SIS II service and will be provided on a 24 hours/7 days a week basis through the implementation of necessary service level agreements to ensure the smooth operation of SIS II.

Such structures are currently being defined and implemented.

1.5. General presentation of the organisation of the services responsible in future for police functions in relation to the SIS II.

All members of the Malta Police Force will be instructed on the use of the system in so far as their duties require. Access to the SIS II will be restricted according to deployment necessity.

1.6. Which tasks under national law shall necessitate access to SIS II by the judicial authorities?

These tasks are currently being assessed at national level.

1.7. List of services or authorities which will be authorised to process SIS II data including access to it.

This list will include, but not be limited to:

- *The Customs Division within the Ministry of Finance;*
- *National Judicial Authorities;*
- *Malta Police Force, International Relations Unit Europol and Police Immigration Section within the Ministry for Justice and Home Affairs;*
- *Office of the Attorney General and the Eurojust Office;*
- *Consular posts and Diplomatic Missions within the Ministry for Foreign Affairs;*
- *Citizenship and Expatriates Directorate (residents permits) within the Ministry for Justice and Home Affairs;*
- *The Malta Transport Authority (Vehicle Registration and Driving Licences) within the Ministry for Urban Development and Roads;*
- *The Office of the Refugee Commissioner;*
- *The Land and Public Registry Division (Passports) within the Ministry for Justice and Home Affairs;*
- *Malta Police Force (Identity Cards) within the Ministry for Justice and Home Affairs.*

Access will be strictly limited according to specific functional requirements and based on defined user roles.

- **Technical conditions**

1.8. How many terminals are or will be made available for input and consultation of data by:

(a) Law enforcement services, including those with a control function

There will be approximately 400 terminals throughout the Malta Police Force.

(b) the border control authorities;

There will be approximately 50 terminals assigned to border control authorities.

(c) diplomatic missions and consular posts;

Diplomatic Missions and Consular Posts will not have direct access to the SIS II data. Requests to verify visa applicants on the SIS database will be done through other authorised authorities.

(d) the authorities responsible for aliens and asylum;

As these functions fall, in their majority, within the overall police functionality the terminals that will be made available in 1.8.a will also be accessible to authorities responsible for aliens and asylum.

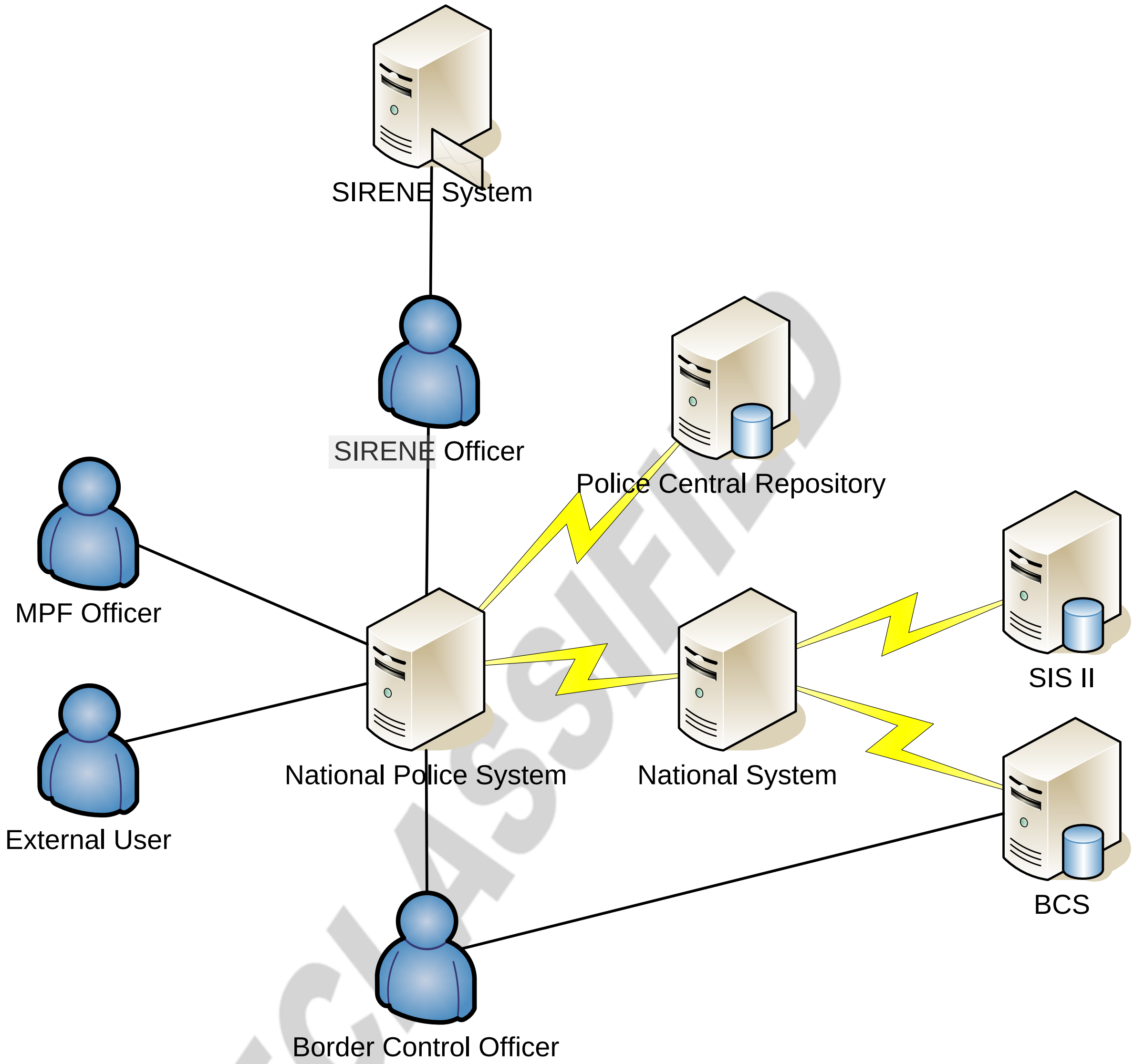
(e) customs authorities

This information is not currently available.

(f) others ?

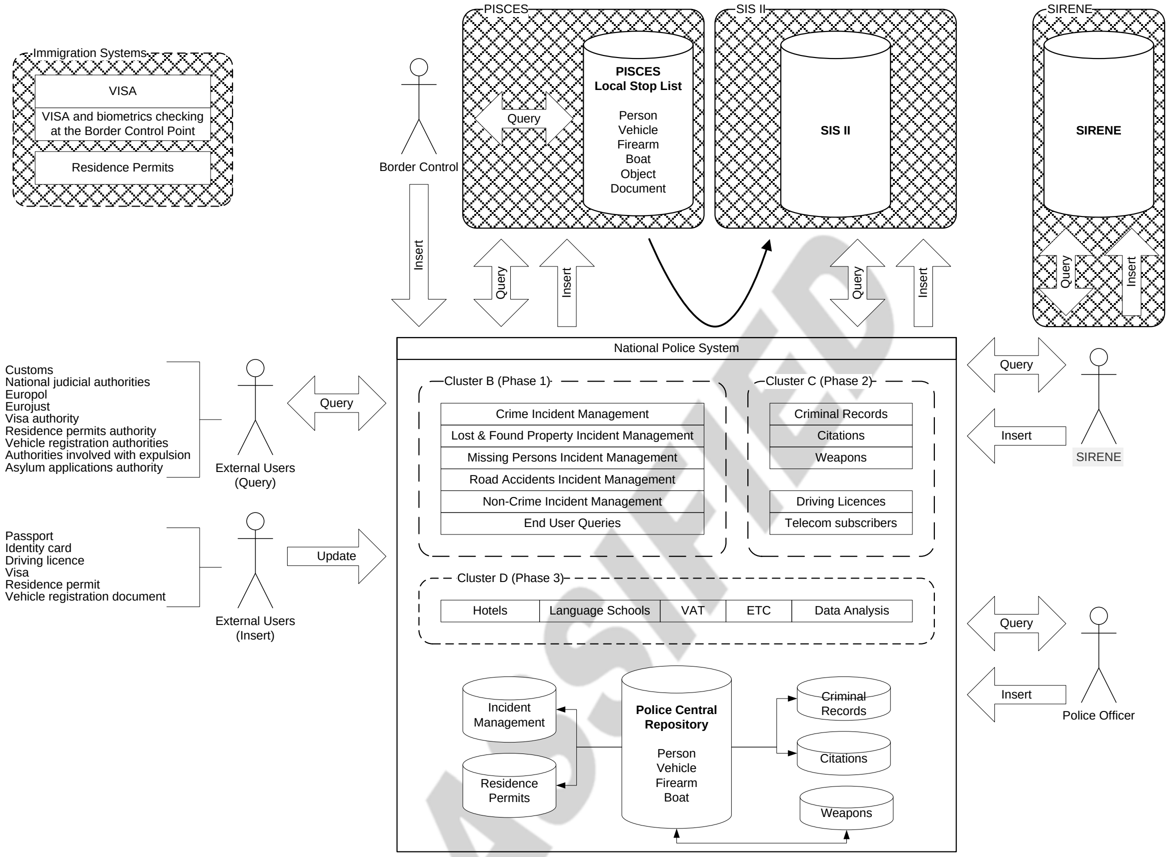
This information is not currently available.

1.9. Presentation of the computer architecture of national systems which will be connected to the SIS II.



The National System (N-SIS) as shown in the diagram above will be the only system that will have direct access to SIS-II. The Police National System, the SIRENE system and the Border Control System (BCS) will in turn access the SIS-II via the N-SIS.

1.10. Description of the future data flows between national systems and the SIS II in connection with input of data according to each of the aforementioned category of alerts



The data flows between the national systems and the SIS-II in the input of data for each of the alerts listed above will be as follows and will take place via the National System. These are depicted in the above diagram.

Every interaction within the national system be it for an incident report at a police station or at a border control point, will have the following data flows between the national systems and the and the SIS-II database in connection with the following alerts:

- *Alerts on persons who should be refused entry to the Schengen area*
  Checks on persons entering the Schengen area will be carried out at the border control via the Border Control System (BCS).

For every third country national crossing the borders a full identity check and visa check will be carried out against the national stop list, the SIS-II database and the Visa database. Should there be a hit or the visa is found to be invalid or revoked, the person is removed from the queue and further checks will be carried out. Interaction with the SIRENE office will take place in requesting the relevant documentation in relation to the alert.

For EU nationals crossing the borders, checks will only carried out if there is reasonable suspicion. Should there be a hit on the SIS-II, interaction with the SIRENE office will take place in requesting the relevant documentation in relation to the alert.

- *Alerts on persons wanted for arrest (in view of surrender or extradition)*

  Checks on persons will be carried out on the national stop list and the SIS-II database on every interaction with the national law enforcement authorities and other authorities authorised to access the SIS-II data. Should there be a hit detailing the person being wanted for arrest, interaction with the SIRENE office will take place in requesting the relevant documentation in relation to the alert.
- *Alerts on persons to ensure protection or prevent threats*

  Checks on persons will be carried out on the national stop list and the SIS-II database on every interaction with the national law enforcement authorities, other authorities authorised to access the SIS-II data and as the need may arise in the course of investigations. Should there be a hit detailing the person for protection or for the prevention of threats, interaction with the SIRENE office will take place in requesting the relevant documentation in relation to the alert.
- *Alerts on persons wanted for judicial procedure*

  Checks on persons will be carried out on the national stop list and the SIS-II database on every interaction with the national law enforcement authorities, other authorities authorised to access the SIS-II data and as the need may arise in the course of investigations. Should there be a hit detailing the person as wanted for judicial procedure, interaction with the SIRENE office will take place in requesting the relevant documentation in relation to the alert.

- *Alerts on persons and objects for discreet surveillance or specific checks*
  Checks on persons and objects will be carried out on the national stop list and the SIS-II database on every interaction with the national law enforcement authorities, other authorities authorised to access the SIS-II data and as the need may arise in the course of investigations. Should there be a hit detailing the person as wanted for judicial procedure, interaction with the SIRENE office will take place in requesting the relevant documentation in relation to the alert. Alerts on objects will be handled in accordance with national procedures.
- *Alerts on objects for seizure or use as evidence in criminal proceedings*
  Checks on objects will be carried out on the national stop list and the SIS-II database on every interaction with the national law enforcement authorities, other authorities authorised to access the SIS-II data and as the need may arise in the course of investigations. Alerts on objects will be handled in accordance with national procedures.

1.11. Description of the future computer processing of SIS II data from the remote workstation of an end user.

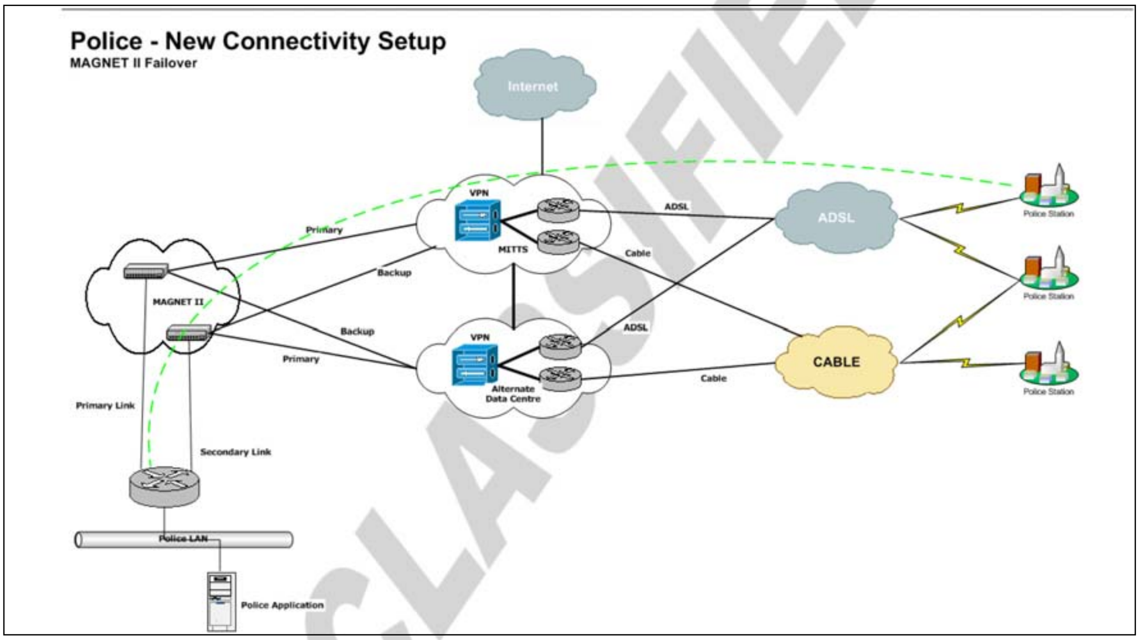
The processing of SIS-II data from the remote workstation of an end user will take place via a combination of technologies. The National Systems (NS) will be all interlinked and on-line and all processing will take place in real time.
There are two fundamental types of users; one type of users will be using web-based or browser-based technology while the other type will use client-server technology. The former will be used in the more widely distributed processing applications such as the National Police System (NPS) which will operate in all police stations, and also from mobile services in future. The latter will be used in enterprise-type systems such as the border control applications that will require more intense processing of data due to the capture of information from travel documents.
<u>Web-Based Services</u>: The web-based services will be used from the remote police stations that will be connected to the main government data centre via ADSL or Cable VPN lines. The critical police stations will have both types of connections as a back-up to each other.

The connection from the main government data centre to the police data centre will take place by using the secure Malta Government Network (MAGNET-II). The final connection to the servers within the police data centre will take place via the Police General Head Quarters Local Area Network (PGHQ-LAN).

The transmission of data from the server to the end-point computer will use a secure version of the Hyper Text Transfer Protocol using encryption (HTTPS).

The processing of data will take place within the servers in the police data centre. The computers of the remote police stations will only be used to display information and allow for data entry.

The process described can be seen in the diagram below.



<u>Client-Server Services</u>: Client-Server Services will only be used where there is a direct connection from the file server to the end- user terminal.

Very few applications will be using this technology, the main application being that at the border controls points where the computers will be connected via a secure local area network to file servers within the data centre. There will be localised variations of this where a local data centre is not possible.

1.12. Does the national system allow for phonetic queries?

Yes, in new systems with the SIS-II scripts once issued by the Commission.

1.13. How will the competent authorities on the ground have access to end-user terminals (by radio, only by telephone, via mobile terminals fitted in vehicles, only in person, only in writing)? Are there differences between the various national authorities?

Police to Police by radio, AFM to AFM by Radio and Interpol by telephone.

1.14. Procedure planned to be followed by a user in the field to consult the SIS II database. Will the SIS II and the national system be consulted at one and the same time, or do both systems have to be consulted separately?

The consultation with the SIS II database and the national system will be simultaneous and transparent to the end- user.

1.15. Volume of data to be transmitted to the SIS II database

The following is the expected annual volumes of alerts that will be transmitted to the SIS-II database from the national systems:

Alerts:	*Data currently not available*
Missing Persons:	*300 p.a.*
Missing vehicles:	*900 p.a.*
Missing Objects:	*3,000 p.a. (documents only)*
	50 p.a. (seacraft)
EAW:	*Data currently not available*
Interpol:	*Data currently not available*
Extradition:	*Data currently not available*
Aliens (96):	*Data currently not available*

The above data is for inserts, not queries.

1.16. Have you already created a contingency centre/separate backup centre? If so please give further details about location, functions etc.

A back-up data centre is in the process of being set up. It will be located in Gudja, Malta and will be able to offer full support for all police and immigration functions.

1.17. Will checks be made of the switch between the backup and the operational system (BP 5.6.1)?

Yes.

1.18. What measures are you planning to take to guarantee 24/7 operations? How will the engineer support be organised?

A Service Level Agreement (SLA) is being drafted with the government agency responsible for centralised and strategic IS/IT systems to provide monitoring, maintenance and support on a 24 hours/7 days a week basis. The Police IT services support will provide the back-up support and network equipment which is required.
Both sites will be manned on a 24 hours/7 days a week basis.

1.19. How will the backup system be organised?

Daily, weekly, monthly: father / son generations. All copies will be kept offsite.

Will you take daily copies?

Yes, daily copies will be taken.

On what media will backups be kept? If so describe the location and its protection.

Back-ups will be kept on tape cartridges (DAT type). Back-ups will be taken daily of critical databases from servers at the Police data centre / back-up data centre.
The back-up tape cartridges will then be stored in an offsite location using a secure container. At the offsite location, the tape cartridges will be stored in a data safe. Details of the actual location of the offsite storage are classified as EU Confidential.

Will they be transported to other locations?

Tape cartridges will be transported and deposited in the data safe at the offsite location under secure escort.

How will the media be labelled and protected during support?

The tape cartridges will be labelled with adhesive labels on which there will be sufficient information for their identification. These cartridges will also be protected in portable data storage containers and a handover procedure shall be put in practice.

Will backup systems regularly be checked?

Yes, back-up systems will be checked on a regular basis.

Will restoration procedures be checked and tested? If so, how often?

Yes, procedures will be in place in relation to data control and restoration. These checks will be carried every 6 months in the presence of the designated data controller.

1.20. Have you already prepared an emergency plan relating to situations where it is impossible for users to search the SIS due to problems of the national systems or network inaccessibility? What are its main elements?

A plan is currently underway in order to ensure the continuing of border control checks in case of problems with the national systems or network inaccessibility. It is foreseen to have in place procedures which will enable access for the users to the SIS data even in emergency situations. Such plan will also provide for the setting up of a complete back-up data centre that can be accessed in all situations by the border control / immigration officers at the airport.

A contingency plan will also be put in place to allow accessibility in case of network inaccessibility.

1.21. How will the consular posts of your country access the SIS II?

Consular posts will not have direct access to SIS II data. Requests to verify visa applicants on the SIS database will be done through other authorised authorities.

- **Data**

1.22. Are there any plans to introduce methods for collecting statistics on system down time?

A Service Level Agreement (SLA) is being drafted with the government agency responsible for centralised and strategic IS/IT systems which foresee the provision of monitoring system accessibility and system down time. A guaranteed uptime will be part of the SLA.

1.23. Management/review of SIS II alerts

(a) How will deletion of the data be guaranteed if action has been taken in response to an alert?

The deletion of data after action has been taken in response to an alert will be part of an automated process when closing a report.

(b) What kind of checks will be carried out?

An internal audit function is in the process of being set up.

(c) At what stage of implementation will an alert be deleted?
(e.g. immediately after notification of an arrest, after notification of a person's whereabouts, after the reported discovery of an object, or after all measures have been taken, e.g. actual extradition, dispatch of documents to the place of residence, retrieval of the object)

An alert will be deleted when the report / incident is closed and the data retention period has expired.

(d) How will the authority responsible for central or local management carry out its duty of preventing the data files from becoming clogged with data (non-deletion of alerts after a hit)?

The Internal Audit function is in the process of being set up.

(e) What measures will be taken to cope with such a situation if it is detected?

In such cases, a consultation process with the data owner will be engaged to remedy the situation.

1.24. Which concrete steps will be taken by the end-user when it is proven that there is a case in the SIS II of misused identity?

If an error has occurred from the part of the end-user part, the original alert is deleted and the correct alert is entered. The entry procedure is defined in draft legal framework for misused identity.

- **Security**

1.25. Security measures to ensure the control of future access to SIS II data? Measures put or which will be put in place to ensure that each user has access only to the categories of data for which he or she is authorised.

Access to SIS data will be controlled by a Personal Identification System (PIDS) and a full audit trail.

All data terminals situated in police premises and with access to SIS-II will be equipped with an authentication device that will be supplemented by a user code and password. This will ensure that the user identity code in the audit trail will actually pertain to the person accessing the SIS-II data.

1.26. What security measures at the future national systems (physical and logical security and security organisation)

Adequate security measures to ensure compliance with both national and SIS-II legislative requirements.

1.27. Control of physical access to the premises of the future national systems , where applicable including paper archives storage rooms.

Physical access will be controlled by an access control system with a personal identification device. Every access to the premises is authenticated and logged. Logs are then audited.

Physical access will be further controlled by security doors with access control and CCTV systems.

The physical access to paper archives is currently under review.

1.28. Level of protection and protection measures applied to computerised national applications – and in connection to this which special measures will be taken in relation to the SIS II application?

Protection measures to computerised national applications will include:

- *Personal Identification Devices and user codes and passwords for access to computer terminals carrying out business processes. All access will be logged and audited on a sample basis;*
- *Personal Identification Devices for physical access with logs and audit trails supplemented by CCTV and security doors for centres housing data processing and communications equipment.*

- **Training and information**

1.29. Description of the specific training given to future operators and to those responsible for the national systems in future.

Training programmes on the use of national systems are currently being held. The programmes are currently being reviewed to include the processes required for SIS-II and SIRENE. Twinning light programmes will commence shortly on SIRENE procedures and processes and data protection.

1.30. Training and information for end users. In particular:

- **Will newly-recruited user (e.g. policemen) be given training in the use of SIS? If so, what will be the content of this training and how many hours will it last?**
- **Will continued training take place in the form of courses, seminars, conferences etc? If so, how many hours?**
- **If continued training will be provided, i.e. courses, seminars, conferences, how many hours.**

A training needs analysis programme is currently being carried out to establish the content and duration of such training for new recruits and as refresher courses / seminars for existing officers.

1.31. What measures are being or will be taken to ensure the level of competence of new users?

Measures will include minimum attendance requirements and examinations. This will then be followed by a continuous professional learning programme.

1.32. Alert procedures for the judicial authorities and procedures following a hit:

(a) How will judges and public prosecutors be informed about the SIS (awareness of the SIRENE Bureaux, the role of the SIRENE Bureaux, differences between SIS and Interpol searches)? (by specific training, in the course of ordinary training, multiplier effect from trainers, publications, through specific brochures, through general public relations work)? Will they be informed regularly, just once or not at all? Are there regional differences?

(b) Will the future SIRENE Bureaux have any influence (by information and training measures)?

A twinning light programme will be carried in 2006 covering the relevant areas of the SIRENE bureaux.

The future influence of the SIRENE Bureaux is to be reviewed.

II. SIRENE (will certainly need to be updated on the basis of the result of the discussions of the SIS II legal proposals)

1.33. Have you already set up your SIRENE bureau?

If yes, what level of progress has been achieved ?

If no, please describe the relevant projects/plans.

Malta has commenced the setting up of its SIRENE bureau and a limited number of officers have been assigned. It is envisaged that considerable progress will be registered once the two twinning light projects will commence.

Two twinning light projects are scheduled to be carried out in 2006/2007, covering the relevant areas of the SIRENE bureaux.

The Twinning Light 1 programme will be carried out in 2006 and will include:

- *the development of a plan for the setting up and proper running of the SIRENE Office in connection with Interpol and Europol Office;*
- *the development of a training strategy for the staff at the SIRENE Office;*
- *training Police staff, including the SIRENE staff, on the effect of the lifting of the internal borders on police work.*

The Twinning Light 2 programme will be carried out between 2006 and 2007 and will include:

- *Training on Data Handling in the SIRENE Office for SIRENE staff*
  - *Training in IT skills on the SIS II to support the SIRENE office for IT staff*
- *Training in the daily use of the SIS II on a ‘train the trainer’ basis, including SIRENE staff*
  - *Preparation of the Handbook re Standard Operating Procedures of SIS II*
  - *Links with SIRENE Office: visit for selected Police personnel to SIRENE office site in Italy to familiarise themselves with operations at a SIRENE Office.*

- **Organizational conditions**

1.34. Geographical location of the future SIRENE Bureau.

SIRENE MALTA will be one of the constituent offices of the International Relations Unit. The other offices that currently constitute the International Relations Unit (IRU) are Europol's National Unit and National Central Bureau (NCB) Floriana, Malta as well as the Anti-Terrorist Unit . New offices are currently being specifically built for the IRU. These are located at the Police General Headquarters in Floriana.

1.35. Administrative organisation of the future SIRENE Bureau and practical organisation of the work of the SIRENE Bureau (staff, administrations represented, day and night teams, specialisation of operators…).
What about language skills availability? Will they all cover at least English and/or French during night time and on weekends? If not, what will they do with urgent information in foreign languages at those times?

The SIRENE Office in Malta will be administered by the Malta Police Force and will operate on a 24 hours/7dats a week basis. It is to be noted that Malta has only one Police Force. It is envisaged that outgoing traffic will not be significant; however the incoming traffic is expected to be the same as in the other Bureaux across the Schengen Area. The SIRENE Office will be manned by an adequate number of officers.
All personnel posted at the SIRENE Office will be fluent in the English language. In total, the SIRENE personnel will have language capabilities to cover other languages. Senior officers in the Unit will cover the legal knowledge required.

1.36. Are you planning to hire civilian personnel?

Persons not belonging to any national authority

- **will such persons work on your premises?**
- **if so, what measures will apply/will these persons have the necessary clearance or certification?**
- **will non-disclosure/confidentiality agreements be made?**

This possibility has not been ruled out. However, if civilian personnel are to be deployed at the SIRENE Office, they will undergo all the appropriate security screening.

1.37. The limits of the respective spheres of competence of operators and end users.

The competence of operators and end users depends on the respective tasks entrusted to be carried out in accordance with their place of deployment.

1.38. What practical steps have been or will be taken to issue alerts on persons wanted for arrest (in view of surrender or extradition)? Do agreements exist with the judicial authorities, particularly with a view to ensuring that SIS alerts take priority over Interpol alerts?

Council Framework Decision on the European Arrest Warrant and the Surrender Procedures between Member States (2002/584/JHA) provides that an issuing judicial authority may issue an alert for the requested person in the SIS. The alert must conform to Article 95 of the Schengen Convention. Such an alert is equivalent to a European Arrest Warrant accompanied by the information set out in Article 8 of the Framework Decision. It is expected that under SIS II an Article 95 alert will have all the required information. In Malta, all incoming European Arrest Warrants are received by the Attorney General who must certify that the formal requirements are satisfied. Upon doing so, the European Arrest Warrant is executed by the Police in accordance with the Extradition (Designated Foreign Countries) Order (LN320/04) that transposes the European Arrest Warrant Framework Decision. The Attorney General, as the receiving authority, will have access to the SIS II. Alerts on SIS will take priority over Interpol alerts.

1.39. How will the activities related to alerts for the purpose of refusing entry and Articles 5 and 25 of the Convention be performed?

Since Malta is in the early stages of establishing this Office and assessments relating to work procedures are still in progress, the activities are still being identified. However, note is being taken of the specified procedures contained in the SIRENE Manual related to such alerts.

a) **Which authorities in your country will issue the alerts for purposes of refusing entry?**

This will be the combined duty of the SIRENE Office within the Police and the Police Immigration Service.

b) **Which authority will perform the role of the national SIRENE Bureau with regard to these alerts? Will clearly defined channels of communication be in place between the national authorities involved?**

Almost certainly, it will be the SIRENE Bureau. Any secure means that leaves a record of the communication is appropriate (fax or mail).

▪ **What measures will be taken as regards the availability for the SIRENE Bureau of background information (e.g., a decision for expulsion/ ban on entry) which is not recorded in the SIS?**

This matter requires to be regulated through legislative and administrative provisions. Whatever the measure, sufficient safeguards for data protection must be ensured. The SIRENE Office would only have the right to use the information for the purposes delineated above.

▪ **Which national authority will liaise with the Schengen partners for purposes of sending and receiving of requests for consultation under article 25 of the Convention?**

The SIRENE Bureau will be the national authority which will liaise with the Schengen partners for purposes of sending and receiving of requests for consultation under Article 25 of the Convention.

1.40. The Sirene Bureaux' position and margin for manoeuvre at national level

(a) **Will the Sirene Bureau have the possibility to directly consult and enter data in the national police system when running SIS searches, or initiate procedures for this to be done, (such as on indications concerning an abductor in an alert on a missing minor)? If not, are steps being taken to this end?**

The SIRENE Bureau will have access to the national police system. Access for consultation and/or data entry will be strictly controlled by access control, user rights and roles.

(b) **Will the Sirene Bureau be able to access and enter data into other databases (vehicle registration databases, aliens' registers, population register), is there coordinated and effective cooperation with the corresponding departments?**

The SIRENE Bureau must be given access to data, which is required for the performance of their function. Cooperation with other departments must be established and regulated.

(c) **Will the Sirene Bureau have the possibility to give instructions or will it have any other ways of influencing cooperation? Does national authorities training cover the future Sirene Bureau?**

The SIRENE Bureau or at least some of the personnel must have the authority to give instructions. National Authorities' training covers the SIRENE Office.

(d) **Will the Sirene Bureaux be empowered to conduct investigations (?) or act as coordinators? (such as in Articles 39 and 41).**

The SIRENE Bureau will not be conducting investigations. Investigations will be conducted by other sections from the IRU or other Police Specialised Branches, as necessary.

- **Technical conditions**

1.41. **Technical arrangements made to enable to operate the future SIRENE Bureau without interruption in exceptional situations such as natural disasters, power cuts, disturbance or interruption of traditional telecommunications systems, etc.**

The premises will be provided with a back-up power supply. A back- up structure will be set up at a secondary site.

- **Data**

1.42. Follow-up action

(a) Will hits following alerts be recorded manually or automatically?
(b) If they will automatically be recorded, how this will be done?
(c) Will the actions taken after a hit occurred, f.i. the results of an investigation, be recorded? If so, this will be done centrally or locally?
How long the results of an investigation will be retained?

Hits following alerts will be recorded automatically. Hits will automatically be recorded at central level independent of user intervention. Records will be retained according to the parameters of national legislation.

- **Data protection and other legislation**

1.43. Legislative and regulatory provisions adopted or to be adopted to set up the SIRENE Bureau, including subsequent legislative measures.

Legislative and regulatory provisions to be adopted by the SIRENE Bureau still need to be drafted and will probably be in the form of regulations. Circulars may also be used to regulate administrative aspects.

1.44. Foreseen security measures at the future SIRENE Bureaux (logical and physical security, security organisation)

Some security measures are delineated in the SIRENE Manual.

1.45. Control of physical access to the premises of the future SIRENE Bureau, where applicable including paper archives storage rooms.

Access to the SIRENE Bureau will be restricted to SIRENE Officers and certain other personnel. The handling and storage of documents will take place according to the procedure established for EU documents.

1.46. Level of protection and protection measures applied to computerised police applications – and in connection to this which special measures taken or to be taken in relation to the Sirene application

Adequate security will be implemented for IT infrastructure and applications, including SIRENE.

1.47. Who is in your country the national supervisory authority regarding data protection issues?

The national supervisory authority regarding data protection issues is the Data Protection Commissioner.

1.48. Measures taken or which will be taken to ensure that SIRENE files are destroyed after withdrawal of the alerts to which they relate. Who will be responsible for controlling implementation?

This will be provided for by legislation. The act of withdrawal will probably be the responsibility of the SIRENE Office. Control will be carried out by the Police Data Audit Unit (Legal Office) and, where necessary, even the Data Commissioner.

- **Education and information**

1.49. Description of the specific training given or planned to future operators and to those responsible for the SIRENE Bureau in future.

This is provided for in the Twinning Light Programme. The Maltese SIRENE Officers will be trained by Italian SIRENE Officers both nationally and abroad.

1.50. Training and information for end users. How will you organise the training when the SIS is implemented ?

This will be determined during the Twinning Light Programme. It will be established in consultation with Malta's Italian Counterparts.

1.51. What measures are being taken to ensure the level of competence of new users?

The level of competence of new users will be determined in accordance with the standards set in the SIRENE Manual.

1.52. How will police officials on the ground be informed about the SIS and the SIRENE Bureaux (by specific training, in the course of ordinary police training, multiplier effect from trainers, articles published in police journals, through specific brochures, through general public relations work)?

Police officials on the ground will be informed about the SIS and the SIRENE Bureaux by specific training offered in the Twinning Lights, in the course of ordinary police training and through the train the trainers' concept which is to be applied.

1.53. Which procedures have to be followed at the future SIRENE Bureaux once informed about a misused identity alert?

This will be settled in accordance with the SIRENE Manual.

1.54. What procedures will be put in place following a hit?

Please refer to Malta's reply to question 1.42. The SIRENE Manual already provides for such procedures.

1.55. Relationship of the SIRENE bureau with prosecuting authorities

The prosecuting authorities before the Courts of Magistrate are the Executive Police while the prosecuting authority before the Criminal Court is the Attorney General. The Malta Police Force has a very good working relationship with the Office of the Attorney General. Moreover, due to the special circumstances in Malta whereby there is only one Police Force, there is a close cooperation between all Units within the Police Force.

III. Under chapter "Visa"

1.56. What provisions have been made to ensure that permanent consular posts will only issue Schengen visas in the future?

Provisions ensuring that diplomatic missions and consular posts will issue only Schengen visas in the future are being made in accordance with the recommendations and best practices as outlined in the Schengen Catalogue Vol. III on the issuance of visas.

1.57. Is any specialised training given in the detection of false documents?

Prior to posting, consular officers and staff attend a three-hour training programme on forged document detection at the Police HQ (Fraud Section).

1.58. Are there any manuals of specimen documents to check that the documents presented are genuine?

Manuals/journals are available at border control check-points. All diplomatic missions and consular posts are supplied with copies and updates of the Interpol Identity Checker (Keesing Reference Services).

IV. Prior Consultation

1.59. How are other States consulted? What technical means are implemented?

Other States will be consulted through VIS and SIS II systems.

1.60. What is the estimated response time for consultation?

The estimated response time would be determined once both systems have been rolled-out and tested.

1.61. Under which circumstances do the consuls of your country consult their central authorities?

Consular posts will not have direct access to SIS II data. Requests to verify visa applicants on the SIS database will be done through other authorised authorities.

1.62. What criteria are applied?

Honorary Consulates are not entitled to issue visas.

1.63. Under which circumstances do other States consult them? (What is the number of national and international consultations?)

There is currently no consultation with other States.

Do you intend to include third countries in Annex V B for prior consultation? How many?
No decision has yet been taken on which and how many third countries are to be included in Annex V B. However, Consular cooperation agreements have been signed with other Member States for representation in the majority of these third countries.