



Council of the  
European Union

Brussels, 13 April 2018  
(OR. en)

6132/01  
DCL 1

SCH-EVAL 6  
SIS 7  
COMIX 110

## DECLASSIFICATION

---

of document: ST 6132/01 RESTREINT  
dated: 9 February 2001  
new status: Public  
Subject: Draft report on the SIS evaluation visit to Finland

---

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, 9 February 2001**

**6132/01**

**RESTREINT**

**SCH-EVAL 6  
SIS 7  
COMIX 110**

**NOTE**

---

from: the Survey Group - SIS  
to: Schengen Evaluation Working Group

---

No. prev. doc. 6347/00 SCH-EVAL 10 COMIX 179

---

Subject : Draft report on the SIS evaluation visit to Finland

---

This report is the result of the drafting committee of 9 February and includes the remarks of the Finnish delegation.

## TABLE OF CONTENTS

### **1. Introduction**

- 1.1 Mandate
- 1.2 Committee members of the Survey group
- 1.3 Program of the visit

### **2. Visit to the Finnish N SIS**

- 2.1 Organisation
- 2.2 Security
- 2.3 Installation
- 2.4 User Interface
- 2.5 Decentralised periphery
- 2.6 Training

### **3. Visit to the Finnish SIRENE**

- 3.1 Organisation and structure
- 3.2 Security and data protection at the SIRENE bureau
- 3.3 Installation
- 3.4 Recruiting and training of SIRENE officers
- 3.5 Tasks of the SIRENE bureau
- 3.6 Workflow and responsibilities for entry and deletion of records
- 3.7 Statistics on alerts and hits

### **4. Visits to the users of the SIS**

- 4.1 Visit to Helsinki-Vantaa International Airport
- 4.2 Visit to Vantaa Police District
- 4.3 Visit to Oulu Police District
- 4.4 Visit to Oulu airport

### **5. Remarks and conclusions**

## **1. INTRODUCTION**

### **1.1. Mandate**

In consultation with the Finnish authorities, the Schengen evaluation Committee for Finland, represented by the survey group (as mentioned in the note concerning the setting up of the above mentioned for candidate countries, SCH/Com-ex (98) 26 def. of 1998 September 16<sup>th</sup>), visited Finland between the 22<sup>nd</sup> and the 24<sup>th</sup> of January 2001.

### **1.2. Committee members of the Survey Group**

The committee chaired by France consisted of 17 members from the following countries:

- Mr Henri DELARUE – FRANCE (Chairman)
- Mr Jacques GRAFF - BELGIUM
- Mr Eckart BRAUER - GERMANY
- Mr Martin TUFFNER - GERMANY
- Mr José Luis MARIA DE FRUTOS - SPAIN
- Mr Ricardo LLORENTE HERNAN-GOMEZ - SPAIN
- Mr Bruno RIDET - FRANCE
- Mr Jean-Marcel GUILLOT - FRANCE
- Mr Enrico Maria FALCONE - ITALY
- Mr Marco DI STEFANO - ITALY
- Mr André VAN DER MEIJ – THE NETHERLANDS
- Mr Popko NOORDHOFF – THE NETHERLANDS
- Mr Florian BILEK - AUSTRIA
- Mr Sebastião ALVES - PORTUGAL
- Mr Brian DONALD – UNITED KINGDOM
- Mr. Geoffrey SONNENBERG – UNITED KINGDOM
- Mrs. Laura YLI-VAKKURI – EUROPEAN COMMISSION

One observer from the Nordic countries :

- Mr Jan SEGERBERG – SWEDEN

One member of the General Secretariat of the Council :

- Mrs Nathalie PENSAERT

### 1.3. Program of the visit

The survey group selected the locations they wished to visit and provided these details to the Finnish authorities. The Finnish authorities facilitated these visits by providing transport and other logistical support.

- *The Finnish N.SIS*
- *The Finnish SIRENE Bureau*
- *The operational use of the SIS*

- 22 January 2001            visit to N.SIS in Vantaa  
                                 visit to Vantaa Police District
- 23 January 2001            visit to Oulu Police District
- 24 January 2001            visit to SIRENE bureau  
                                 visit to Helsinki Vantaa International Airport

The visit was very well prepared by the host country. Cooperation with the Finnish authorities was excellent. The survey group has been given all facilities to carry out its tasks in the best conditions possible. All concerned authorities gave a clear presentation of the work carried out during their preparation phase, in an open minded spirit of cooperation. The visit was conducted in total transparency and in a climate of mutual trust.

DECLASSIFIED

## 2. VISIT TO THE FINNISH N.SIS

The surveys conducted during the visits to the Finnish N.SIS were directed primarily at IT infrastructures, organisational structures, personnel training and overall security.

### 2.1. Organisation

In Finland there is only one centralised police organisation, which comes under the direct responsibility of the Ministry of the Interior.

The Police Department of the Ministry of the Interior, acting as the Supreme Police Command, coordinates police operations across the whole country as well as the operations of the National Police Units (NPU).

Within, the Police IT Management Agency (PTHK) is responsible for the IT management and all data and telecommunications systems of the police.

The police have their national IT systems in computers located in a computer room in the premises of the National Bureau of Investigation (NBI). The systems are managed by police personnel.

In the NBI, there are three engineers who work entirely for the SIS.

Seven operators take care of the N.SIS and its technical copy as part of their normal responsibilities. There is always at least one operator in the computer room.

Maintenance and support is arranged by the company TietoEnator Oyj, which has developed the Schengen Search File (cf. chapter 2.3.2 – national applications).

DECLASSIFIED

## 2.2 Security

The N.SIS is located in the premises of the National Bureau of Investigation at the following address: **Jokiniemenkuja 4, VANTAA** (city next to HELSINKI)

This is a three-year old building, which has been constructed to the highest security specifications. The outer shell of the building has been constructed with specially reinforced concrete and is fitted with ballistic- and bomb-proof glass. The computer room is located in the centre of the ground floor. It was explained that because of the high level of the ground water, it was not possible to site this computer room in the basement.

Entry and access is controlled by electronic pass-key and user ID number. Externally the building is protected by closed circuit TV with infrared capability, with a monitor also located at Vantaa police station.

During office hours a guard and pass system is in operation for visitors, who must be collected, escorted at all times and returned to the main entrance. Each employee is responsible for his/her visitors.

Outwith office hours the building is secured against unauthorised access during this period and access is restricted to members of staff, who must use their electronic key and user ID. Outside office hours, members of staff are only allowed access to their department. Full audit facilities are available to monitor such access.

The number per unit of electronic keys in use inside the building is restricted and controlled. Only authorised persons with the appropriate access entitlement are permitted entry to the computer room.

The SIS falls into the category of the highest security level of the Finnish Government.

The Security Police check, in general, the background of persons recruited by the police and other security authorities.

User access to different data systems are based on the needs of the employee and are confirmed by his/her superior.

Personal user IDs and passwords are used, and the systems require that users change their passwords regularly.

The computer room is equipped with uninterrupted electricity supply as well as with double reserve power and carbon dioxide fire prevention equipment. It is protected against Electro Magnetic Pulse (EMP) and there is a direct link with the nearest fire brigade.

Since the visit of the data protection survey group, the Data Ombudsman has been consulted on data security, visited the premises recently and is preparing his report.

## 2.3 Installation

### 2.3.1 N.SIS

a) The Finnish N.SIS integrated towards C.SIS has several components:

- A communication system, the actual **N.SIS** that is identical to the Austrian solution. This system is implemented on two IBM RISC/6000 machines running the communication stack (including the X.400 UA and MTA) and a data base system holding the reference N.SIS database for storing the broadcasts from the C.SIS.
- This system is connected via the X.25 modem to the C.SIS.
- Furthermore, several other data systems form the so-called SIS-Net:
  - Schengen Record File  
The competent authorities record their SIS alerts in this file. After SIRENE checked the alerts, they are then further transmitted via the N.SIS to the C.SIS. The alerts come from several national applications. It passes the information along to SIRENE workflow system when processing requires to do so,
  - Schengen Search File  
This file contains all valid SIS broadcasts. It is an **identical** technical copy of the reference database in the N.SIS and handles all queries from the end users. It is implemented in such a way that the system is able to handle peaks of searches as effectively as possible. These peaks may occur e.g. when a high number of passengers from outside of Schengen territory arrive in the country. The searches in the Schengen Search file are made from the national applications (see below) and by means of a webbrowser interface.

b) The installed software of the N.SIS is at the same maintenance level as in Austria:

- Operating System: IBM AIX Version 4.3.3
- X.400 MTA: ATOS MXMS 88
- X.400 UA: Common Schengen portable UA
- RDBS : IBM Universal Database Version 5.3
- Control Software: N.SIS Application "CHARON"

c) The N.SIS configuration is set up with one operational and one combined backup/test machine ("COLD standby").

Each of the machine racks houses a IBM SSA disk array containing the N.SIS database. The disk array in the operational machine is the active image of the database while the other one in the backup/test machine is the mirror to recover from a hardware failure of a disk. The SSA disk arrays are configured in RAID1 mode.

d) To ensure a safe separation between the operational and test environment, the following measures have been taken:

The hardware architecture of the SSA in combination with the disk controllers in the RISC machine guarantees that only the operational machine has access to it. It is therefore technically not possible to access the disk array from the test system.

In case of a failure of the operational machine, the test system has to be stopped and an image of the production system has to be started. This image is stored on internal disks of the computer and cannot be accessed while the test system is running. The hardware boot sequence of AIX ensures this.



The activation procedure for the backup system, the “TAKE OVER” procedure, is easily executable from an operator and enables Finnish authorities to have close to 100% up time of the N.SIS.

According to the Finnish Head of N.SIS, a study will be carried out to consider to install a separate Test environment, which would then allow to use the current infrastructure as Cluster, which would significantly improve the availability of the system.

- e) The N.SIS is exchanging update requests and SIS broadcasts with the Schengen Record File and the Schengen Search File via a queuing system. The queuing system, a standard product of IBM, MQ-Series, is responsible to ensure that none of the messages will get lost on the way between the N.SIS and the Schengen applications. At regular intervals, a database comparison between the N.SIS and the technical copy.

### 2.3.2 National systems

Data that has to be sent to the SIS is entered in the Finnish national systems. There exist several of them:

#### **Data System for Police Matters**

The data system for police matters plays a two-sided role in relation to the Finnish national SIS. Alerts are made in this system by the competent authorities except those based on article 96 and those on 99 concerning State security.

Searches can be made in this system **AND** in the Schengen Search File (SIS) simultaneously using restricted search criteria.

#### **ULKONET**

Ulkonet is a search engine maintained by the Frontier Guard. It enables simultaneous searches in data files of various authorities including the Schengen Search File.

It is indented specifically for making simultaneous swift mass searches in those files. Firearms and Banknotes cannot be queried from this system.

#### **Data system of the Directorate of Immigration**

Art. 96 records (Prohibitions of entry to Schengen territory) are recorded first on this system by the Directorate of Immigration and then transferred into the Schengen Record File. Only the Directorate of Immigration may issue prohibitions pursuant to article 96. Because the system does not allow searches to the SIS data, the Directorate of Immigration can make searches in the SIS either by means of the ULKONET, by means of the Data system for Police Matters or by means of the direct interface.

#### **Visa Data System**

The Visa Data System is a data system maintained by the Ministry for Foreign Affairs used by all authorities dealing with visa matters like Ministry of Foreign Affairs, embassies and consulates issuing visas, Frontier Guard, Police, Customs Directorate of Immigration. It is possible to see only SIS alerts pursuant to article 96 by means of this system.

Aside from all the aforementioned integrated query facilities exists a separate web based search facility, the so-called “Direct interface”. This interface allows very fast searches in the Schengen Search file. Insertions of data by means of this interface are not possible.

## 2.4. User Interface

The main interface for police forces are the queries against the PATJA system. There is also an implicit function for querying the SIS. No special action has to be taken for querying the SIS. In case of a hit, the national record is presented first and in the lower half of the screen the findings in the SIS are displayed.

During the inspection it was noticed that, especially in case of querying the big amount of ID documents, the search in the SIS database took longer than the time-out function foreseen in the PATJA system. This led to an interruption on the query. The end user was asked to continue the search. In case of a positive answer, the system could not establish a connection to the database engine anymore. The system did not show any result and the user had to log out of the whole application in order to submit another query.

For these reasons, users of the PATJA system tend to avoid the double query and choose to repeat the transaction to query the SIS via the web browser, which has better response times.

The survey group feels that this duplication of these efforts will reduce the number of SIS transactions as it is recognised that a check against a national database will tend to take priority.

The ULKONET provides a very user-friendly interface. Searches in the various registers are performed very fast. Despite the fact, that the user had to know about transliteration characters, all tried searches in the SIS resulted in a hit. This interface will be used especially at the border control.

The alternative possibility to query information of the SIS is the so-called DIRECT QUERY. This interface appears as WEB based solution, allowing the end user to query any kind of information in the SIS database.

The observed behaviour of this application showed very fast answers of queries. This is the preferred interface for doing searches independently from searches in the national registers. However some technical problems were encountered during the search of known cases. Especially in case of a hit on an alias record in the Wanted Person category, there was no display of the associated main record and the other corresponding aliases. Also the search with names containing special national characters worked not satisfactory. The user had to enter the transliterated character according to the Schengen rules in order to find the record. Aside from this noted problems the application worked satisfactory and can be considered as easy to use.

Clarifications were sought from the Finnish authorities whether it was possible to use the web browser simultaneously for direct access to the SIS and Internet.

The Finnish authorities confirmed that such concurrent use was possible but not recommended, nor a used practice or taught feature. Only 20% of the users have access to the Internet. Measures are being taken to separate SIS and police applications from the Internet. The survey group recommends to implement these measures as soon as possible.

## **2.5. Decentralised periphery**

The police has a secure intranet for data communication purposes. All SIS searches are made inside this network. The other competent Schengen authorities have their secure networks and they use SIS inside these networks, connected to the police network through a firewall.

### **The police:**

In Finland, there are some 8,500 work stations located all over the country in police stations and connected to the data communication network of the police. All of them can be used for consulting the SIS, depending on the access rights that a user has. Entering data is possible on all terminals whose users have a right to enter SIS alerts. The access rights of police users, as with all other users, is validated by PATJA.

Patrols in Finland do not have mobile terminals and take radio/telephone contact with their control room, which will do the searches. There are 600 remote access terminals to the police network, with portable computer that accept just one smart card. 300 policemen have such access to, for example, PATJA or SIS, via a secure server. The connection of the remote accesses is encrypted.

### **The border control authorities:**

The Frontier Guard has 450 working stations, each with access to the SIS. Approximately 1,000 officers will have access rights.

Remote access technology is being studied by Nokia, so that ULKONET might in future be accessed via such new palmtop-type devices.

### **Customs**

The Customs have 500 working stations, each with access to the SIS.

Remote access technology is being studied by Nokia, so that ULKONET might in future be accessed via such new palmtop-type devices.

### **Ministry of Foreign Affairs:**

There are in total 200 users work stations in the Ministry for Foreign Affairs, the missions (88) and other authorities subjected to it with a possibility to query data pursuant to Article 96 in the SIS and get a yes or no answer. 59 of the embassies and consulates have direct access, via the private network of the Ministry of Foreign Affairs, which is restricted to authorised users, a firewall at the Ministry and via the police network to the Schengen Search File through the Visa Information System. Connections to the 14 biggest embassies is encrypted. The Ministry of Foreign Affairs wants to encrypt connection to the other embassies by the end of 2002.

The Ministry for Foreign Affairs will make a check against the SIS for the 29 missions that do not have an on-line connection to the visa system of the Ministry for Foreign Affairs and will provide a yes or no answer to the mission in question.

### **The authorities responsible for aliens and asylum:**

The Immigration Unit and the Refugee and Asylum Unit of the Directorate of Immigration have some 80 users in total with a possibility to consult the SIS and enter alerts pursuant to Article 96. All queries are made on Schengen Search File and do not have their own copy of the SIS database.

## 2.6 Training

The police training program contains several courses with the aim to introduce full implementation of the Schengen acquis to the police staff.

In relation to the SIS, a group of trainers of police, customs and frontier guards has been given the necessary training in the summer of 2000. The training lasted 4,5 days and covered the following topics:

- the Schengen Convention
- the SIRENE activities
- the Schengen police co-operation
- the SIS
- the Finnish national SIS architecture
- the use of the Schengen search file and
- the national SIS alerts.

These were planned to train all future users of the SIS on regional level before the system coming operational. In December about 50% of the police staff had been trained, all should be trained by March 2001, but this is a regional responsibility. For Customs and Frontier Guards, the figure is about 80 to 90%.

Because of the regional responsibility, there are no national profiles for different training sessions (from a couple of hours to some days).

The survey group was pleased to note that a national manual had been made available to all staff through the electronic Bulletin Board of the police.

DECLASSIFIED

### **3. VISIT TO THE FINNISH SIRENE**

#### **3.1. Organisation and structure**

The SIRENE bureau is also located in the premises of the National Bureau of Investigation.

The Finnish SIRENE bureau is thus situated both organisationally and physically in the context of the National Bureau of Investigation where all other critical functions of the police administration are situated also (NSIS for example). Therefore, the security level of the SIRENE bureau and the data systems is the same as the highest security level of the police administration. (Cf. chapter 2.3).

The National Bureau of Investigation acts also as a judicial authority in some cases, which makes international co-operation much easier.

The Frontier Guard and the Customs sent their liaison officers to work in the SIRENE bureau in 1999. These members of staff also work as SIRENE desk officers.

The working stations of the employees of the SIRENE bureau are connected to the national police data communications network.

The Finnish SIRENE was available 24h/7d from October 2000 onwards.

There are 5 members of staff on duty during office hours. At peak days (i.e. Mondays and Fridays) 8 officers are occupied. Shifts have been organised in such a way that the office hours of all Schengen countries are covered by the day shifts.

Two persons work on the night shift: one police officer and one civilian member of staff. Three persons are on duty at weekends.

All officers speak Finnish, Swedish and English. Some of them speak also the other Schengen languages except for Greek or Dutch. Support can be asked from the translation team of the intelligence unit during office hours.

The NBI commanding officers on duty for international operations are also available to the SIRENE Bureau.

The whole SIRENE staff has been trained to use the Schengen Workflow system connected to the SIS as well as all other means of international telecommunication. Processing of other international matters (Interpol, Europol) takes place by the staff in the various Sections of the Criminal Intelligence Division.

The personnel of the SIRENE Bureau have access to all SIS data.

The employees have at their service SIRENE Workflow system, Schengen Record File and Schengen Query File. They also have access to the data systems of the police and other relevant authorities and they can use the Fast Query System. (This tool links together data systems of the Police, the Frontier Guard, the Customs, the Ministry for Foreign Affairs and the Directorate of Immigration.)

There seems to be a problem to reach the SIRENE because of the number of telephone lines at the SIRENE. It is recommended to either have a dedicated phone line for contact with the other SIRENE bureaux or have more accesses to the one number.

The National Bureau of Investigation is the national authority responsible for international co-operation in police matters. It acts as the national centre for Interpol and Europol, and it is responsible for the SIRENE Bureau.

The Schengen co-operation takes priority over the Nordic co-operation channels and the SIS data have automatically priority over the Interpol data. If an Interpol alert is still needed, it is made after the SIS alert in the national NCB.

DECLASSIFIED

### **3.2 Security and data protection at the SIRENE bureau**

The SIRENE bureau being in the same premises as the N.SIS the same high level security rules apply.

Only SIRENE staff can only log onto SIRENE computers.

The SIRENE archives are kept in the general archives room situated outside the SIRENE room but within the building.

Inspections by the Data Ombudsman found the system to be satisfactory. There will be further regular inspections in future.

DECLASSIFIED

### **3.3 Installation**

The SIRENE work-flow application, the SIRENE Case File, is based on Lotus Notes and the X.400 communication subsystem, running both on an IBM RISC/6000 machine.

The SIRENE Case File is a versatile workflow system designed and implemented for the purposes of SIRENE activities relating to article 95 – 100. The most important features of this system are:

- Processing alerts made in Finland before they are sent to the C.SIS
- Preparation and transmission of SIRENE forms to other SIRENE Bureaux.
- Reception of alerts from abroad and SIRENE forms from other SIRENE Bureaux
- Recording measures relating to processing the alerts
- Processing hits
- Compilation of necessary statistics

Special searches from SIRENE Case File can be made in the Schengen Search File for checking of multiple alerts in the SIS.

DECLASSIFIED



### **3.4 Recruiting and training of SIRENE-officers**

The Security Police checks the background of personnel of the SIRENE Bureau before their recruitment.

The training of the SIRENE Bureau key personnel began with a thorough examination of the Schengen Convention and the SIRENE manual.

The personnel has also analysed the handling of the alerts referred to in Articles 95-100 and participated in planning the SIRENE data flow system.

In addition, they have made study trips to Austria, the Netherlands, Italy, France, Spain and Germany and participated in a one-week course in the Dutch and the German SIRENE Bureau.

The exchange of civil servants was carried out in a way that each of the staff members was in practical training in two SIRENE Bureaux for a period of up to one week in each of the Bureaux.

The aim of the training organised in Finland has been to familiarise the personnel with the operation of the co-operation partners, i.e. the Customs, the Frontier Guard and the Directorate of Immigration.

The key personnel has also familiarised themselves with the work done within the SIRENE Working Group in Brussels.

A part of the personnel took part in a seminar organised for SIRENE Bureau personnel in Spain in April 2000, as well as in an exchange programme for civil servants.

Six staff members also took part in a course arranged in Oslo.

When all staff was recruited, the personnel would be provided with training in international affairs. This course discussed the different forms and channels of international co-operation, and it was carried out in accordance with the plan made in advance.

### **3.5 Tasks of the SIRENE bureau**

The SIRENE Bureau operates as the national and international contact point in Schengen matters and particularly, in matters relating to the SIS.

On a national level, the SIRENE Bureau also acts as a Helpdesk for the SIS for all officers in the field. About 5 to 10 such calls are received per day.

All Article 95 files have now been received and about 65% of them have already been examined. The files are checked at the SIRENE bureau by police inspectors (middle rank). A lawyer is available at the SIRENE bureau to answer questions and equally a liaison officer at the Ministry of Justice.

At the start, several problematic cases have been solved in close co-operation with the Ministry of Justice so that certain guidelines have been set out.

SIRENE is also the designated authority for police co-operation (art. 39 and 46 Schengen Convention).

DECLASSIFIED

### **3.6 Workflow and responsibilities for entry and deletion of records**

(Cf. also chapter 2.3.2 – national systems)

#### **Art 95- Art 97- Art 98- Art 99-**

The alerts are introduced by the local police forces but are checked by the SIRENE bureau on their legality.

#### **Art 96-**

The Directorate of Immigration introduces the alerts, these are not checked by the SIRENE Bureau. The SIRENE bureau does, however, deal with the technical aspect of the matter.

#### **Art 100-**

The alerts are automatically forwarded to the SIS after they have been entered in the national system. The local police fills in the forms in accordance with the instructions (these instructions include e.g. the national “SIRENE Manual”).

It is recommended to take as soon as possible a decision on the number of historical data to be introduced and the way for doing this.

At the time of the visit, Finland requested a flag for article 95 records concerning citizens of the Nordic countries to change the action to be “gathering of information” instead of arrest for extradition. However, the Ministry of Justice is examining whether to reconsider its opinion in view of the position of the other Nordic countries.

According to a statement of the Finnish SIRENE bureau of 29 January, the Ministry of Justice has meanwhile changed its position and such a flag will not be requested anymore in future.

When receiving a message on the imminent expiry of an alert, the SIRENE will check whether and how long the alert can be extended according to national legislation. It will then contact the local police force that introduced the alert so that they can extend the alert if they wish to do so.

Deleting a national alert is not possible, unless the SIS alert is deleted first. An alert is deleted from the system when all measures relating to it have been taken.

On 1 January 2001, approximately 11.000 alerts pursuant to article 95 existed in the SIS. So far, Finland has checked around 7.000 of the relating SIRENE-files.

The files corresponding to alerts will be deleted at the moment the alert is deleted, except when the hit has occurred in Finland.

Documents concerning hits are stored for 25 years, in accordance with national legislation.

Documents concerning an alert issued by Finland are stored by the local authority that made the alert.

### **3.7 Statistics on alerts and hits**

The workflow system compiles statistics concerning the SIS automatically.

On 23 January 2001, there were 249 Finnish alerts in the SIS.

The numbers of historical alerts that Finland foresees to enter in the SIS are as follows:

- about 10,000 firearms;
- 1,000 – 2,000 vehicles;
- between 10,000 and 20,000 other records relating to article 100.

Between 1 and 23 January 2001, there have been 72.675 queries on the SIS.

The SIRENE bureau reported that since 1 January 2001, there have been 2 hits on article 95 alerts, two hits on vehicles of article 100 and at least 2 on article 96. The hits on article 96 are not executed but information is passed on to the Directorate of Immigration.

It is not clear whether the Frontier Guard will pass the information on hits on article 96 alerts to the SIRENE bureau.

DECLASSIFIED

#### **4. VISITS TO THE END-USERS OF THE SIS**

##### **4.1. Visit to Helsinki-Vantaa International Airport**

The visit of the survey group to the Vantaa airport confirmed the impression received at Oulu airport. Checks are mainly, if not only, done via ULKONET, but direct access is also available. The response time for the ULKONET browser is good and users seem very knowledgeable and professional.

DECLASSIFIED

## 4.2 Visit to Vantaa Police station

On 22 January 2001, following the visit to the Finnish N.SIS at Vantaa, the opportunity was taken to include an impromptu visit to the Vantaa police station.

On arrival members of the survey group were welcomed by Detective Chief Inspector Seppo Kujala, who headed the local drugs squad. He was joined by two of his colleagues who were responsible for overseeing SIS and Schengen training.

Using the computer training facilities, the survey group was given a demonstration of both the dual function query on PATJA and the browser. Hits were achieved using both types of search.

Thereafter, during a visit to the police control room, staff demonstrated SIS searches.

It was noted that performance is degraded by wildcard queries and it would therefore be necessary to take the appropriate measures to improve the response time.

DECLASSIFIED

### **4.3. Visit of Oulu Police District**

On 23 January 2001 the survey group visited the police district of Oulu, the command centre for one of five police commands in Finland.

Following a presentation by the local police chief Veli-Erkki Wäre on the structure, organisation and manpower of the Oulu police district, a question and answer session with senior police officers and representatives of the Customs and Frontier Guards was held.

During this session it was established that of the 244 police officers, 98% had been trained. Oulu police district had one police trainer of the 80 trained nationally. Specialist investigators were given training of approximately 6 hours, while non-specialist officers, which included control room staff, received training of 4 to 5 hours. Nevertheless the survey group learned that some officers had been trained for no longer than 2 hours. The training officer confirmed that his program would be complete by the end of February. Customs and Frontier Guard both reported that a similar level of training had been achieved.

It was confirmed that all police officers working in Oulu district had access to the SIS. This access could be achieved either through use of a workstation or by radio/telephone to the area control room (alarm centre).

It was established that Frontier Guard had direct access to the SIS at their airport unit. Customs would have direct access from their base at Oulu harbour, however, the computer equipment had not yet been installed. Both services have alternative indirect access by radio or telephone to their own command centres.

Following this session, the group was divided and separately visited the specialist investigation department, the alarm centre and the Foreign Affairs unit. During the visit at the investigation department and the control room several members of staff displayed their ability to complete searches and follow up hits on the SIS. Although obviously new to the system, staff appeared comfortable with both web browser and dual query search functions on PATJA. The role of the SIRENE bureau was clearly understood by all staff.

An officer in the control room showed that the on-line version of the national Schengen manual was available and personal paper copies of this Manual were seen in offices of several members of staff.

Following the visit at the Oulu police headquarters, an impromptu visit was made to the Frontier Guard and Customs units at Oulu airport.

At the Frontier Guard unit, the system ULKONET proved to be fast in response time and efficient for the queries. The member of staff demonstrating the queries seemed very well trained and knowledgeable about Schengen.

At the Customs unit, the querying is done using a web browser, which functions quickly. However, the user interface of an SIS alert does not display the action to be taken.

The Customs use the SIS while profiling foreign flights prior to their arrival based on the passenger list.

The answers given by the members of staff met by the survey group at the airport showed an encouraging knowledge of SIS.

## 5. REMARKS AND CONCLUSIONS

Overall, the performance of the SIS was found to be good, response times being short. Users seemed well trained and aware of the possibilities of the SIS, which is demonstrated by the number of queries already made.

However, the performance problem on PATJA should be solved to enhance the quality of the searches and promote dual queries. For example, searching the SIS via PATJA for a stolen document, the record was not found, probably because of the time-out function and the lack of processing power to check the big documents file within the time lock.

During the visit at the Vantaa police station, some connection problems were encountered. According to the Finnish authorities, this was due to the installation of a training program, and this problem was solved on the next day.

During the checks, the survey group found a problem concerning the accessibility of the main record when an alias was searched for. In a message of 5 February, the Finnish authorities state that this problem has been identified and will be solved within a month.

Another issue was also detected: when querying an article 95 alert on which the Finnish authorities had requested a "flag", the end users still receive a reply indicating that it concerns an article 95 record but the "action to be taken" is "communication of whereabouts". In such a case, confusion may arise and the end users should only see the alternative "action to be taken". This problem is being investigated and would be solved in the near future.

The N.SIS and its technical copy are located in the computer room of the National Bureau of Investigation, where there is also the hardware of the other national data systems of the police. For the moment, the back-up tapes are also stored in the computer room, but they will be stored at another building from February onwards.

It is planned to move the back-up machine to another building in about 2-3 years' time. The survey group recommends doing this as soon as possible.

The same applies for the SIRENE computers.

The survey group found that there is a need for enhancement concerning the transliteration rules. The querying technique must be changed so that a query checks the normal letter and the transliterated character. Alternatively, staff could be trained on using the wild card queries better and quicker, provided that the adequate measures are taken to improve the response time.

Throughout the visit, it appeared that the SIS is mainly considered as a tool to be used for border controls and police checks made on foreigners and/or foreign card. Therefore, the survey group is of the opinion that this issue should be addressed in future training courses and could be solved by promoting a combined query of the national and SIS databases.

-----