Council of the
European Union

Brussels, 13 April 2018
(OR. en)

6130/01
DCL 1

SCH-EVAL 4
SIS 5
COMIX 108

DECLASSIFICATION

of document:	ST 6130/01 RESTREINT
dated:	9 February 2001
new status:	Public
Subject:	Draft report on the SIS evaluation visit to Sweden

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

6130/01

RESTREINT

SCH-EVAL 4
SIS 5
COMIX 108

NOTE

from:	the Survey Group - SIS
to:	Schengen Evaluation Working Group
No. prev. doc.	6360/00 SCH-EVAL 14 COMIX 183
Subject :	Draft report on the SIS evaluation visit to Sweden

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

TABLE OF CONTENTS

1. Introduction

1.1. Mandate

In consultation with the Swedish authorities, the Schengen survey group, 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 déf. of 1998 September 16th), visited Sweden between the 8th and the 10th of January 2001.

1.2. Members of the Survey Group

The group chaired by France consisted of 15 members:

- Mr Henri DELARUE - FRANCE (Chairman)
- Mr Jacques GRAFF - BELGIUM
- Mr Eckart BRAUER - GERMANY
- Mrs Judith BUCHHOLZ - GERMANY
- Mr Bruno RIDET - FRANCE
- Mr Jean-Marcel GUILLOT - FRANCE
- Mr Enrico Maria FALCONE - ITALY
- Mr Claudio BOLOGNESE - ITALY
- Mr Popko NOORDHOFF - THE NETHERLANDS
- Mr André VAN DER MEIJ - THE NETHERLANDS
- Mr Florian BILEK -AUSTRIA
- Mr Sebastião ALVES - PORTUGAL
- Mr Brian DONALD - UNITED KINGDOM
- Mr Phil DOUGLAS - UNITED KINGDOM
- Ms Chiara ADAMO - EUROPEAN COMMISSION

Observers from the Nordic countries :

- Mrs Mette TJALVE ***(8.01.2001)*** - DENMARK
- Mrs Liesbet JORGENSEN ***(9 and 10.01.2001)*** - DENMARK
- Mr Jan SEGERBERG - SWEDEN
- Mr Smari SIGURDSSON – ICELAND
- Mr Nils Erik EGGEN – NORWAY
- Mr Ole Tommy NYLAND - NORWAY

One member of the General Secretariat of the Council :

- Mr Gerrit HUYBREGHTS

1.3. Program of the visit

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

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

- 8 January 2001	National Police Board and N.SIS
- 9 January 2001	SIRENE and Arlanda airport
- 10 January 2001	Visit to the Police Headquarters and Operations Centre of Malmö Visit to Ystad Police District Visit to Skurup Police station

The visit was very well prepared by the host country. The survey group received very good support which enabled it to carry out its tasks in the most effective and efficient manner. All concerned authorities gave clear presentation of the tasks executed during the preparation phase and were ready to answer the questions of the group with obvious efforts of transparency and openness. The Swedish authorities and agencies visited gave clear and precise information both during the lead up to a visit of the survey group and during the evaluation visit itself.

2. Visit to the Swedish N.SIS

2.1. Organisation

The legal basis for the SIS in SWEDEN are :

- The Schengen Information System Act (2000:344), and
- The Schengen Information System Ordinance (2000:836).

The Minister of Justice holds responsibility for the Swedish Police. He exercises his authority through the National Police Commissioner who is the head of the National Police Board (NPB).

There are 21 police districts in Sweden. Each police district has a police authority headed by a County Police Commissioner.

The Police have the main responsibility for border control. The Customs, the Coast Guard and the Migration Board have assigned duties to assist in these activities.

The National Police Board is in charge of the N.SIS solution. There is one national IT supervision unit which is in charge of monitoring all Swedish IT systems including NSIS. It provides working 24h a day, 365 days a year cover. There is also one UNIX/Database unit working daytime (Monday to Friday), 8h a day.

There is a total of 41 people working in the IT supervision group responsible for the SIS.
The N.SIS is under the responsibility of the Development and Strategy Division.

The support consists of :

- Hardware contracts

HP	5 hours call to repair, 24 hours a day, 365 days a year.
IBM	Depending on severity of problem after examination by the engineer on duty, IBM will start working within 2, 4 or 8 hours, 24 hours a day, 365 days a year.

- Software contracts

HP	24 hours a day, 365 days a year (HP-UX)
IBM	24 hours a day, 365 days a year(AIX, DB2 and MQ-series)
IDA systems	24 hours a day, 365 days a year (Pax Enterprise)
Informix	Office hours, 5 days a week (Informix database)
BEA	Office hours, 5 days a week (Tuxedo, OSI/TP Gwy)

2.2. Security

The N SIS is located in the premises of the Swedish police data processing service at the Swedish National Police Board :
Polhemsgatan 30
Stockholm

The main entrance is open 24 hours a day and manned by two armed guards.
A second entrance is open during office hours and manned by one armed guard.
Several unmanned entrances are available for personnel. They provide controlled access by means of a smart card and an individual P.I.N. code.
The physical access to the computer room located underground is controlled by a separate and special smart card reader and P.I.N. codes.

To get access to the data of the Swedish Police computer system you need a personal smart card and a BasA PC. Only the operational- and UNIX/Database staff have the root access to the production and test servers in the N.SIS solution.

The root password is kept locked in a "security box".

The electrical supply has a dedicated generator back up facility in case of a power cut.

The computer room is equipped with a fire extinguisher system which uses Inergen gas.

2.3. Installation

2.3.1 N.SIS

The N.SIS and the SIRENE solution are running in the same network (the closed Swedish police data network).

The Swedish N.SIS integrated towards C.SIS has two main components :

A communication system, the actual N.SIS, is identical to the Austrian solution. This system is implemented on two IBM RISC6000 machines running the communication stack (including the X.400 UA and MTA) and a database 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.

Further more, there exists a second component, the Operational SIS (**O.SIS**), implemented on a HP UNIX machine. This subsystem has various tasks :

1) It collects the SIS Update requests coming from various sources inside the national applications and forward them to the N.SIS.
2) It passes the information along to the SIRENE workflow system when the processing requires doing so.
3) It maintains an **identical** Technical Copy of the N.SIS database.
4) It is the "engine" for processing queries on the SIS database of the end-users. It is only via the Technical Copy that the end-users have access to the SIS data. It is built on an Informix Database Management System (DBMS).

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"

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 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, in the backup/test machine, is the mirror to recover in case there would be a hardware failure of a disk. The SSA disk arrays are configured in RAID1 mode.

To ensure a safe separation between the operational and test environments, 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 by an operator and enables Swedish authorities to have close to 100% up time of the N.SIS.

The Swedish Head of N.SIS is currently considering whether to install a separate Test environment. This would allow them to use the current infrastructure as a "Cluster" which would significantly improve the availability of the system.

The N.SIS is exchanging update requests and SIS broadcasts with the O.SIS via a queuing system. The queuing system, a standard product of IBM, MQ-Series, is responsible for ensuring that none of the messages get lost on the way between the N.SIS and the O.SIS.
At regular intervals a database comparison will be done between N.SIS and O.SIS.

2.3.2 National systems

To transfer the data from the Swedish national system into the SIS standard software, Tuxedo servers, is used.

Data that have to be sent to the SIS are entered first in the following Swedish national systems.

- Central police systems

* EPU	system containing national person alerts (searches)
* EF	system containing lost/stolen vehicles
* STAMM	system containing persons subject to refusal-of-entry decisions
* DAR	work-flow system for the SIRENE bureau
* Gods	system for stolen goods
* Pass	passport system

Those applications run on a Unisys mainframe. Only the EPU and the pass applications send their requests via a Tuxedo online interface.
Data from the other registers are loaded onto the O.SIS via batch File Transfer Programs once per day.

- Other national systems

* Migration Board	records according art. 96
* Stolen vehicles	records of vehicles coming from the Swedish Road Administration

Data are loaded only via FTP batch jobs once a day.

According to those responsible, the frequency of the batch jobs could be increased on demand. In the future, there will be an on-line connection of the EF application to the O.SIS in order to speed up the entry of vehicle requests.

2.4. User Interface

The users access the system through a Windows-based client-server application running on the BasA system, which is the standard equipment for the police. The end-users have access to the SIS data by means of this client program.
In its current version it implements queries against each category separately except for Wanted Persons. There is a combined query for WP and stolen passports (only ID category, no DB).
There exists also a mobile terminal solution, the so-called MoBasA, that includes the same functionality of the BasA workstation but accesses the police network via encrypted GSM link.

2.5 Decentralised periphery

A lot of attention has been devoted to ensure communication encryption reaches a high standard.

Authorised staff have access to SIS as well as to other police registers via BasA terminals.

- 17000 work-stations are available to the police
- The Coast Guard and the Customs plan to have at least one work-station with access to SIS available at each of their stations.
  Mobile work-stations with applications supporting access to the SIS were purchased during 2000 thus enabling mobile control- and surveillance teams to have immediate access to SIS.
- For border control, a standard workstation (BasA) is used.
  Border controls at major border crossing points will be equipped with a scanner function (Border Guard System), which scans the passport and forwards information for search in the SIS-system. The result of the search will be presented in the end-user application.

  If communications between the border control and the SIS-system are disrupted, the border control can still use the mobile workstation, MoBasA.

Police personnel can get access to the SIS data only after they attend the approved training.
The decision on authorisation to access the SIS data is given by the County Commissioner on a "need to know" basis. A very few, non-operational Police staff, will be the only ones not granted access to the SIS.

Art. 96 records will be consulted by embassies either on-line or on CD-ROM which are updated every 2 weeks. The Migration Board will access these data through the WILMA application which is a Web-based application with a PKI client.

2.6 Training

All police personnel and civilian staff concerned have received a basic Schengen-training during year 2000.
During 2001 the above mentioned personnel will receive further training in using the SIS.
On March 25th 2001 the following number of persons are expected to be trained in SIS-procedures.

LEVEL	PERSONNEL	TOTAL NUMBER	SHARE
1	Border control staff	1 600	100 %
2	Duty officer, staff in Communication centers etc.	1 200	100 %
3a	Traffic officers	800	100 %
3b	Uniformed police	8 000	60 % *
4	CID-officers	5 000	60 % *

* Full training is expected by the month of June.

3. Visit to the Swedish SIRENE

3.1. Organisation and structure

The national SIRENE Bureau headed by Mr Sören Clerton is an integrated part of the International Liaison Office(ILO) within the National Criminal Investigation Department.
The ILO includes units for Interpol and Europol and has about 65 staff members.
Within the International Liaison Office there is a Duty officer who is in charge of the Front Desk. This person is responsible for generating an immediate response to incoming requests. As needed, requests are allocated to either the Front Desk or the back office which is specialised in the handling of alerts, Art. 95 as well as translations.
Liaison officers from the Swedish Coast Guard and Customs are seconded to the International Liaison Office.
25 persons (police officers as well as civil staff) have been recruited in order to meet the expected resource needs of the SIRENE bureau.

The SIRENE bureau is located in the Swedish National Police Board´s premises at :
Polhemsgatan 30
Stockholm

4 senior officers within the NCIS have a legal qualification.

The following languages are spoken by the operators : English, French, German, and Spanish.
The International Liaison Office also includes knowledge of Dutch and Finnish.

The SIRENE office is manned 24 hours a day
The night and weekend shifts are overseen by one police officer.

A set of manuals and guidelines is available in the SIRENE office to cover all relations with the Schengen countries as well as with the national authorities.

3.2. Security and Data protection at SIRENE Bureau

Effective security measures have been taken to ensure that SIRENE work will be kept separate from other international relations channels.
The security of the SIRENE office is ensured by restricted access through smart card and P.I.N. code.
Video surveillance manned by the duty officer is available to control entry.
The PCs are accessed through a smart card and a P.I.N. code.
Security clearance of the personnel is verified every 5 years
All visitors names are kept in a register and visitors are escorted at all times during their visit of the SIRENE. The premises include a locked archive room

All documents will be stored under electronic format and deleted as soon as the alert is deleted. If, however, Sweden dealt with the matter, the papers are kept for 3 years according to Swedish archive regulations.

3.3. Installation

The SIRENE support system is implemented as two components :

- The X.400 communication subsystem, running Microsoft Exchange on Microsoft WINDOWS NT
- The SIRENE workflow application, named DAR (**Diarie- och Ärendehanteringssystem**).

The DAR application was developed by a software company IDA system AB.
It runs on a HP-UNIX system with Informix as DBMS. The application is a customised version of a standard workflow system named PaxEnterprise.

For the communication between the O.SIS and SIRENE a standard software called Tuxedo is used.

The SIRENE server set-up consists of one operational and one "HOT standby" solution delivered by HP.

3.4. Recruiting and Training of SIRENE-officers

During late spring and early autumn in year 2000, a specialised training programme was given to the SIRENE staff. The training programme included inputs on the SIRENE manual, the use of standard forms, security and register issues and utilisation of the supporting IT-solutions including the SIS and the new work-flow-system.
Personnel recruited to the SIRENE also attended several courses and participated in each programme:

- Training course in Madrid in April 2000: 5 participants
- Training course in Oslo in November 2000: 7 participants
- Exchange program (study visits at SIRENE Bureaux) Autumn 2000 with :

  - ✓ France: *2* participants
  - ✓ Germany: 3 participants
  - ✓ Spain: 2 participants
  - ✓ Netherlands : 3 participants
  - ✓ Austria: 2 participants
  - ✓ Belgium 3 participants

As part of the project implementing the SIRENE , the head of SIRENE designate and an assistant to gain first hand experience visited the SIRENE Bureaux in Austria, Germany, the Netherlands and Spain.

3.5. Tasks of the SIRENE bureau

The SIRENE office is involved in the semiautomatic and manual procedures for entering data in the SIS for alerts concerning art. 95, 96, 97, 98, 99 and 100 (firearms).
The duty officer who is informed of all hits will first check the information and dispatch the case to the appropriate desk according to the type of case and time of the day.

The police co-operation pertinent to art 39 to 46 is dealt with by the SIRENE.

3.6. Workflow and responsibilities for entry and deletion of records

On January 1st 2001 approximately 11000 art 95 alerts were present in the SIS. Sweden has so far checked about 2000 of the received A-forms Nevertheless, all the A-forms related to existing art. 95 alerts will be examined before March 25th.

No flag will be requested on article 95 alerts issued by other countries on the basis of citizenship of another Nordic country.

Alerts regarding inadmissible aliens according to article 96 are created by the Swedish Migration Board (Migrationsverket) which sends them to the N.SIS and the SIRENE bureau.
The SIRENE Bureau will act as "a mail-box" in respect of article 96. According to current plans an encrypted electronic mail system between the SIRENE Bureau and the Migration Board will be introduced later this year.

The workflow for the introduction of alerts in the SIS system is explained in Annex 1.

3.7. Statistics on alerts and hits

The Swedish authorities have given the following estimations for data to be loaded in the SIS. On 8 January, only 10 alerts had been introduced in the SIS.

Article	Estimated total amount	Amount on 8/2/2001
95	140	70
96	The migration board has not yet taken position on the historical data loading	
97 to 99	3000	
100		
vehicles	15 000	13 918
weapons	8 000	3 120
id-documents	280 000	77 411
blank documents	1 000	
bank notes	3 000	

At the time of the visit no hits were recorded by the SIRENE.
The query system was disrupted until January 5th by a technical problem.

According to information received by the Swedish authorities on the 8th of February, the number of searches made on the system since the 1st of January is 11400, at a rate of 500 a day.
On the 6th of February there had been a total of 13 hits.

4. Visits to the end-users of the SIS

ARLANDA Airport, MALMÖ Police Headquarters, YSTAD Ferry Terminal and SKURUP police station have been visited by members of the survey group on the 8th and 9th of January 2001.

The SIS application was found to have a very good response time.
In practice the query application searches against one category of data at a time i.e. persons or objects. The Survey group is of the opinion that, especially for the purpose of border controls, there should be an option to automatically run a combined query against data concerning persons and documents, including passports and Identity Cards.

In ARLANDA, only two workstations had access to the SIS data.
For the County of SKÅNE only 5 had that function (2 at the Headquarters, 1 at YSTAD Ferry Terminal and 2 at STURUP Airport)

A total of 500 officers will have access rights to the SIS data.

According to the Swedish authorities, there are two main reasons for the delay in founding the access to the SIS data in Sweden :

- Granting of access rights to SIS data is linked to the specialist training which has not yet been given to all police officers. It seems that the last half day dedicated to the SIS usage (from the 5 days Schengen training) has not yet been given, but should be completed by the end of February 2001 for staff belonging to levels 1 and 2 (border control personnel, patrolmen, traffic police, neighbourhood police and detectives).
- A technical problem within the security environment delayed distribution of the client functionality to the work-stations for several days until the 5th of January.

For the Coast-Guards, access to the SIS data will be made by six officers at the regional Headquarter upon request by radio.
For the Customs, authorised Customs officers will have access to SIS data through mobile terminals (MoBasA).

According to information received on the 8th of February 3500 persons would be trained by the end of the following week, 1500 of them are considered as key personnel working in command centres and border controls. This allows field officers who have not yet been trained indirect access to SIS data.

An **impromptu visit** was made to the local police station of SKURUP. Although the SIS is not yet accessible, the personnel rated level 3 (occasional need to query the SIS), had received a basic Schengen training, and showed an appropriate level of awareness.

5. Remarks and conclusions

The visit took place in the very early days of the application of the SIS in Sweden from 8 to 10 January 2001.

The visit showed a good functioning of the N.SIS and SIRENE as well as the communication infrastructure.

It has been noted that the training program is concentrated on the query of the system. The survey group considers that end-users should also have a better information on the conditions of introduction of records in the system and the advantages of it in all domains of police activity.

Concerning the access to the SIS by the end-users, there are general shortcomings which require immediate attention as the Swedish authorities have stated they intend to do.

It was noted that operational, back-up and test systems for the N.SIS were next to each other so that in case of major incident the three systems would be out of order, leaving the N.SIS without any fallback solution. Therefore the survey group recommends to study and implement a safer solution such as having at least the back-up systems in a separate computer room, if not in a separate site.

Through all presentations, conversations and contacts the visiting group could have, it appears that the SIS is mainly considered as a tool to be used for border controls and police checks made on foreigners and/or foreign cars. Therefore the survey group is of the opinion that training of the end-users should be enhanced so that the SIS plays its full role as compensatory measure.

Appendix

Annex 1: chart related to introduction of Swedish alerts in the SIS