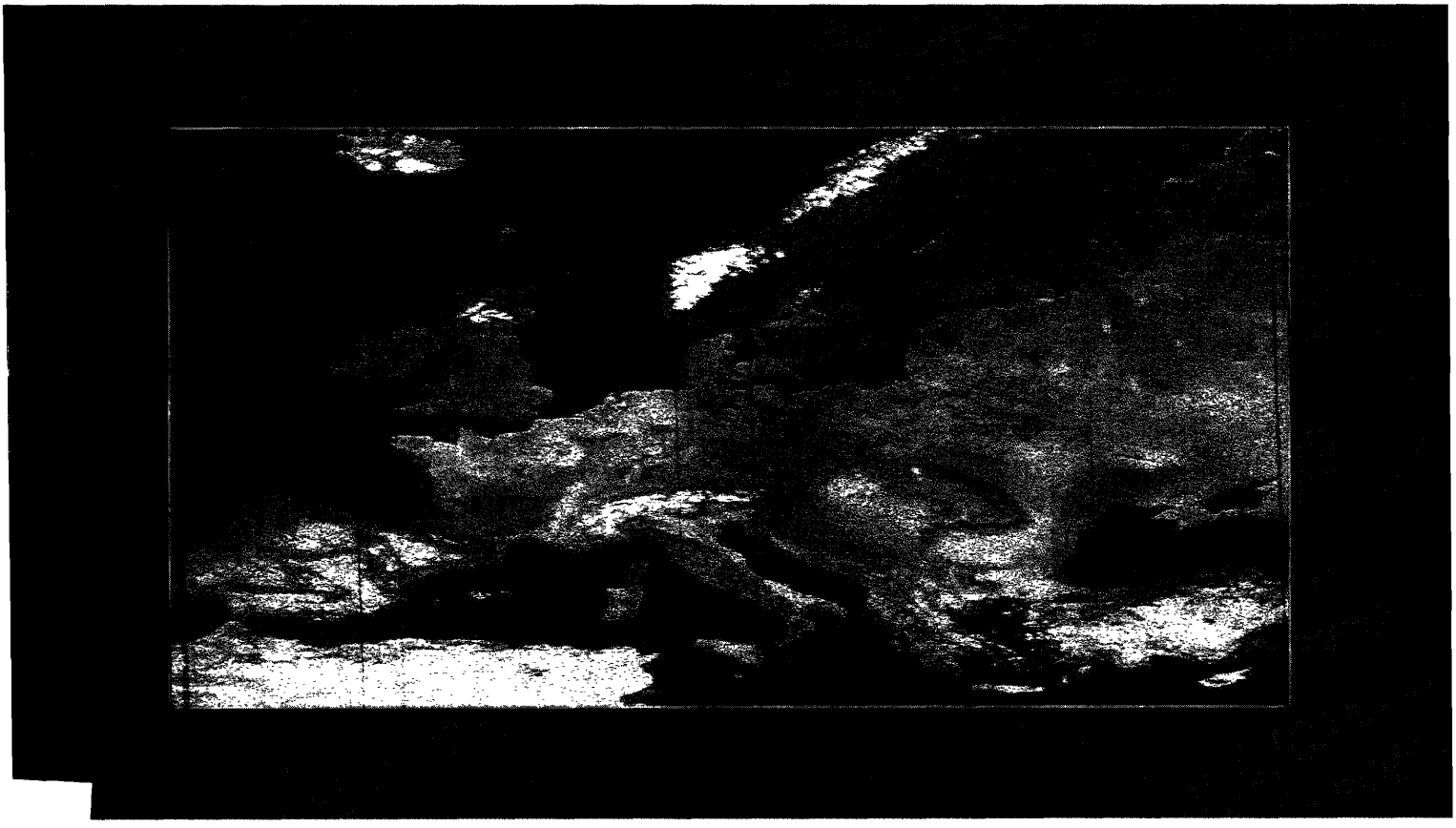
EN

COUNCIL OF
THE EUROPEAN UNION

GENERAL SECRETARIAT

DG H

EU
Schengen Catalogue



CEE: 30

SCHENGEN INFORMATION SYSTEM,

SIRENE:

Volume 2 | Recommendations and Best Practices

EU
Schengen Catalogue

Volume 2

SCHENGEN INFORMATION SYSTEM,
SIRENE:
Recommendations and Best Practices

December 2002

TABLE OF CONTENTS

Preface by the Danish Presidency

In accordance with the decision of the Council on 28 May 2001, the Working Party on Schengen Evaluation has initiated the drawing up of a Catalogue of recommendations for the proper application of the Schengen acquis and of best practice.

The purpose of the Catalogue is to clarify and detail the Schengen acquis and to indicate recommendations and best practices, in order to provide an example for those States acceding to Schengen and also those fully applying the Schengen acquis. The aim is not to give an exhaustive definition of the whole of the Schengen acquis but to put forward recommendations and best practices in the light of the experience gained through the continuous evaluation in the Schengen States of the correct application of the Schengen acquis.

The first volume of the Catalogue regards external borders, removal and readmission. It was adopted and handed over to the candidate countries at the Council on 28 February 2002.

Denmark, which has held the Presidency of the Council of the European Union since 1 July 2002, considers it very important to continue the work on drafting the Catalogue. During the Danish Presidency a second volume of the Catalogue has been drafted. This Catalogue regards the Schengen Information System and the application of the SIRENE Manual.

The Danish Presidency would like to thank the Schengen States and the Commission for help and good cooperation in drawing up the Catalogue and in this connection addresses special thanks to Norway, the Presidency of the Mixed Committee, for helping the Danish Presidency by chairing the sub group, which has drafted the Catalogue.

The purpose of the Catalogue is explanatory and it has no legally binding status. It shows, set out in separate columns, on the one hand, the levels which should be required in order to comply with the Schengen acquis, and on the other hand, the best practices recorded in some of the Member States.

The Catalogue will be handed over to the acceding countries and the candidate countries. The Danish Presidency is confident that it will constitute a useful and additional instrument for ensuring the successful integration of the new Member States of the European Union in due time and in the appropriate manner.

December 2002

SCHENGEN CATALOGUE

INTRODUCTION

1. At its meeting on 28 May 2001, the Council set as an objective for further work by the Working Party on Schengen Evaluation the identification of "... best practices, particularly as regards border controls, so that they can serve as examples for those States acceding to Schengen but also those fully applying the Schengen acquis. These evaluations and the identification of best practices shall serve as inspiration for the establishment of standards defining the minimum application of the Schengen acquis (...) in the relevant working groups" (mandate for the Working Party on Schengen Evaluation) (8881/01 – SCH-EVAL 17, COMIX 371).

   On the basis of this mandate, the Working Party on Schengen Evaluation worked out the principles and procedure for drawing up the Catalogue of recommendations for the correct application of the Schengen acquis and best practices, hereinafter referred to as the Catalogue of recommendations and best practices, or Catalogue.

   The purpose of the Catalogue is to clarify and detail the Schengen acquis and to indicate recommendations and best practices, in order to provide an example for those States acceding to Schengen and also those fully applying the Schengen acquis. With this in mind the Catalogue gives a good indication to the candidate countries for accession to the European Union (hereinafter referred to as the "EU") (at their request) as to what is expected of them, particularly in practical terms, regarding Schengen. The aim is not to give an exhaustive definition of the whole of the Schengen acquis but to put forward recommendations and best practices in the light of the experience gained by the Working Party on Schengen Evaluation in verifying the correct application of the Schengen acquis in several countries.

   The text of the Catalogue does not seek to introduce new requirements but should also make it possible to draw the Council's attention to the need where appropriate to amend certain provisions of the Schengen acquis so that the Commission and, where appropriate, the Member States take the recommendations and best practices into account when putting forward proposals or formal initiatives. This exercise is inter alia the first stage of the process of defining minimum standards by the Council.

Moreover, the Catalogue will serve as a reference tool for future evaluations undertaken in the candidate countries. It will therefore also serve as an indicator for these countries of the tasks which they will be assigned and in this respect should be read in conjunction with the SIRENE Manual.

2. The Working Party on Schengen Evaluation adopted the following definitions to conduct this exercise:
recommendations: non-exhaustive series of measures which should make it possible to establish a basis for the correct application of the Schengen acquis and for monitoring it.
best practices: non-exhaustive set of working methods or model measures which must be considered as the optimal application of the Schengen acquis, it being understood that several best practices are possible for each specific part of Schengen cooperation.

3. Where the Catalogue mentions the Member States which apply the Schengen acquis, this is currently to be taken as meaning the thirteen Member States of the EU referred to in Article 1 of the Protocol integrating the Schengen acquis into the framework of the EU annexed to the Treaty on European Union and to the Treaty establishing the European Community (hereinafter the "Schengen Protocol"), to which must be added Iceland and Norway, pursuant to the Agreement concluded by the Council of the European Union, the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis, signed on 18 May 1999 (these 15 States are hereinafter referred to as the "Schengen States").

The United Kingdom and Ireland have expressed the wish to participate in certain provisions of the Schengen acquis. The arrangements for the United Kingdom's participation were adopted in the Council Decision of 29 May 2000 (2000/365/EC), those for Ireland in the Council Decision of 28 February 2002 (2002/192/EC). The Council has not yet decided on the implementation of the provisions in question.

The Schengen acquis and the other measures taken by the institutions within the scope of the acquis are, under Article 8 of the Schengen Protocol, regarded as an acquis which must be accepted in full by all States candidates for accession.

4. The Schengen acquis was integrated into the EU framework by the Schengen Protocol. The extent of the acquis is defined in Council Decision 1999/435/EC, published in OJ L 176 of 10 July 1999.

Since its integration into the EU, the Schengen acquis has undergone developments and amendments which lend it an evolutionary character.

The Schengen acquis has also taken on board the results of the evaluations which have been conducted within the framework of the Standing Committee for the application and evaluation of the Schengen acquis, now called the "Working Party on Schengen Evaluation". Under the Working Party's mandate, reports are submitted to the Council to establish whether the conditions required for the entry into force of the provisions of the Schengen acquis in a country wishing to participate in those provisions (or in some of them) have been met and, secondly, to monitor the correct application of the Schengen acquis by the Schengen States, in particular by detecting problems and proposing solutions.

5. The first volume of the Catalogue, which was handed over to the candidate countries at the Council of 28 February 2002, dealt primarily with issues of borders and removal. The current second volume of the Catalogue deals with the Schengen Information System, notably the application of the SIRENE Manual. Free movement within the territory of the Schengen States is a freedom which as a counterpart requires not only the strengthening of the common external borders and a policy for the removal of illegally resident third-country nationals, but also the rapid and efficient exchange of information in the context of border controls and police co-operation. Accordingly, the measures adopted in this context seek to strengthen European integration and in particular to enable the EU to become more rapidly an area of freedom, security and justice.

6. The current volume of the Catalogue comprises the chapter on the SIS/SIRENE. A short general section describes the basic concepts underlying the recommendations and best practices set out. These are presented in tabular form, with recommendations on the left and best practices on the right, alongside the relevant recommendations.

* * *

PART III : THE SCHENGEN INFORMATION SYSTEM

DETAILS OF RECOMMENDATIONS AND BEST PRACTICES

GENERAL SECTION

The list of recommendations and best practices set out hereunder has been compiled mainly on the basis of the outcome of different evaluations carried out over the last years, both evaluations of the SIS in different countries and more specific evaluations of the SIRENEs.

The content of this Catalogue has been drafted in such a way that it is independent from the underlying technical system, i.e. SIS 1+ or SIS II. It is indeed meant to be used in the setting up of national databases which will provide the information for the SIS as well as in the preparation of the national section of the SIS, whatever form this may take with the SIS II architecture.

It is recalled that, in any event, to the extent that EU classified information is handled by the users of Schengen IT systems, Council Decision 2001/264/EC adopting the Council's security regulations is applicable (OJ L 101, 11.4.2001, p. 1).

Concerning the introduction of alerts in the SIS, the underlying basic principle is to find a balance between inserting as much as possible alerts in the SIS, within the framework of the provisions of the Convention, and ensuring that the alerts inserted in the SIS are of good quality. Both are an essential condition for the efficiency and usefulness of the SIS. Every national alert that is "Schengen-relevant" should in principle be introduced in the SIS. However, in order to be able to execute the alert, it is necessary that the alert is correct, as complete as possible and traceable. Finally, it should be borne in mind that when a Schengen State executes an alert, it has the right to expect that the issuing Schengen State will follow up the hit. Not doing so without a valid (legal) reason will negatively impact on the willingness of (local) authorities to use the SIS and maximise its potential.

The role of the SIRENE in the working of the SIS is absolutely essential. Whereas it is not expected or necessary that the SIRENE is responsible for every single action in relation to the SIS, the SIRENE is the human interface of the SIS. This implies that it has a role of first-line contact both for the other SIRENEs and for national authorities and end-users. Depending on the case, SIRENE must be able to deal with it independently or to refer it to the competent authorities or agencies. SIRENE staff should therefore be competent and well-trained and have established good contacts with national and foreign authorities.

RECOMMENDATIONS/BEST PRACTICES

RECOMMENDATIONS	BEST PRACTICES
1. National section of the SIS	
1.1 systems and organisation	
- a national section for the SIS must be set up providing 24/7 operation with sufficient engineer support at all times - guarantee data integrity between N.SIS and any national technical copies, where these exist	- maintenance and service level commitments for hardware and software should be provided for to ensure the 24/7 operation - real-time synchronisation of copies - regular database comparisons
1.2 communication infrastructure	
- there should be a stable national network	- appropriate maintenance and service level commitments should be provided to guarantee a high availability of the network
- a rapid response time to queries should be ensured	- the response time should be less than 5 seconds
- SIS data available at consular posts must be updated regularly	- at best, consular posts should have on-line access to the relevant SIS data - where only off-line access can be provided, updates of the database should be sent every second week and additional phone check should be made

RECOMMENDATIONS	BEST PRACTICES
2. SIRENE	
2.1 national structure	
- a SIRENE must be set up and designated as the single point of contact for each Schengen State in respect of SIS alerts and post-hit procedure	- all offices responsible for international police co-operation, should be accessed through a single point of contact, be contained within the same management structure and located at the same site
- the principle that Schengen alerts take precedence over Interpol alerts should be respected and enforced	- the Interpol alert should include a note for the Schengen States indicating the Schengen ID-number of the alert
2.2 organisation and system	
- the SIRENE must provide 24/7 cover for communication with all other SIRENEs and national authorities	- continuity of management, staff and technical aspects
- all staff, including those who are assigned to work out of office hours, should have the competence and experience to provide the necessary service to other SIRENEs and deal with any incoming alerts	- flexibility of working arrangements
- in addition to administrative and operational staff, there is a defined need for IT support staff	- maintenance and service level commitments for hardware and software should be provided for to be ensure the 24/7 operation
- the SIRENE must be equipped with an efficient and effective workflow system	- an electronic workflow/case management system for SIRENE operators has been found to enhance the quality of work and reduce the possibility of mistakes

RECOMMENDATIONS	BEST PRACTICES
- the SIRENE should have the possibility to quickly and efficiently transmit images, such as photographs and fingerprints	- the electronic workflow/case management system should interact with the N.SIS application and national systems in respect of the management of incoming and outgoing alerts; this should include automatic indications • of whether a requested flag has been added or deleted • of when an alert has changed • of the arrival of a new Article 95 alert - electronic transmission of images is preferred to ensure the transmission of useable images - for such electronic transmission, the ANSI/NIST-CLS 1-1993 standard or later revisions should be used
2.3 recruitment and training	
- the SIRENE should have a workforce able to function on their own initiative, in order to ensure an efficient handling of cases - all operators should have a good knowledge of national legal issues, national law enforcement (including a theoretical knowledge of police activities), national judiciary and immigration administration system and as a minimum a basic knowledge of international legal issues	- there should be management support, including access out-of-hours to legal and other expert advice, to enable devolved responsibility - special attention should be paid to human resources management to ensure continuity of personnel, which is an asset for enhancing the quality of the SIRENE work - a training system of the SIRENE workflow should be available

RECOMMENDATIONS	BEST PRACTICES
- legal expertise should be available with a good knowledge of national and international law, a thorough knowledge of the Schengen Convention and related regulations and a theoretical knowledge of police activities - staff with a law enforcement background are needed in order to provide experience which has been shown to be significantly advantageous and reduces the time of training	- legal expertise can be provided through the recruitment of in-house legal advisors or organising legal training for SIRENE staff
- establish common standards and common understanding	- common training, at least once a year - regular exchange of operators, starting prior to the operational use of the SIS
- recruitment levels should take account of number of national alerts and the re-examination of these alerts at end of their validity period as well as of the number of hits on the national territory - the SIRENE recruitment strategy should provide for the validation of the existing Article 95 files prior to the operational use of the SIS	
- staff should have sufficient linguistic skills	- this should be a key element in the recruitment process and ongoing training for SIRENE staff - SIRENE staff should get priority in language training
	- the standard practice is to exchange forms in the language of the issuing country and English

RECOMMENDATIONS	BEST PRACTICES
- for utmost efficiency in bilateral communication, languages familiar to both parties shall be used	- it is clearly desirable that operators are knowledgeable in the most commonly spoken languages, both for direct communication and the ability to manage documentation in the absence of translation support

RECOMMENDATIONS	BEST PRACTICES
3. End-users	
3.1 querying and user interface	
- there is a need for querying or searching that goes beyond exact match searching	- examples of this include phonetic queries, wildcard queries, fuzzy logic, soundex
- single query for both national and international systems is the most efficient way to guarantee systematic consultation of the SIS	- it should be ensured that such a single query is not prevented by national legislation - it should be ensured that single query is quick and easy
- direct access is preferable	- the largest possible number of data querying devices should be provided to end-users to allow direct queries
- information both on national and international alerts should be shown simultaneously - information that the person is considered dangerous and/or armed should be available to the end-user on the first screen	
- when introducing national alerts, the insertion of the alert in the SIS should be set as a default function so that this insertion does not require an additional action on the part of the end-user	- alerts should be pre-checked at the national database and from there be transferred to the N.SIS in an automated way
- pre-existing national data should be checked on their Schengen-relevance and correctness before the initial data-loading of national alerts in the SIS	
- display clear information and instructions about the actions the end-user has to carry out in case of a hit	- in the case of misused identity, clearly display on the screen the procedure for dealing with a hit on a misused identity and the subsequent investigations that should be carried out to establish the whether the person is the victim or the perpetrator of the misuse

RECOMMENDATIONS	BEST PRACTICES
- applications should be developed in a user-friendly way, allowing for speedy and effective means of carrying out SIS tasks	- where appropriate, querying the SIS could be combined with querying existing systems - when entering a name during a query, the system should check both the data on persons and on documents - the user interface should allow and encourage that the name and, where applicable, the document number are entered simultaneously and the application should check both in the same query
3.2 training	
- ensure awareness of interested parties in SIS: police and other (law enforcement) agencies, magistrates and prosecuting authorities	- provide for permanent training of these parties - make a training system available to end users - ensure close contact of the interested parties with SIRENE through liaison officers - promote awareness via the relevant working groups (police co-operation, border control, police chiefs task force, judicial co-operation, terrorism working group) or via CEPOL - authorities responsible for public security could be made (more) aware of the possibility of introducing alerts under Article 96(2)(b)
- the training on SIS should be included in the end-users' initial training as well as in continuous training, already before the operational use of the SIS	- explain what effect the lifting of the internal border controls has on police work - explain the use of SIS as day-to-day police tool - the training should cover both querying the system and introducing alerts - SIRENE staff should participate in police schools' SIS training

RECOMMENDATIONS	BEST PRACTICES
- handbooks on internal procedures should be developed - updated instructions reflecting new functions should be issued - before Schengen start, cascade training should be organised - refresher courses should be provided once the end-users have gained a certain experience	- manuals, including the SIRENE manual, information, training and refresher materials should be available on the police intranet or other media - before the operational use of the SIS, a newsletter informing the end-users on the status of the project can ensure and guarantee their interest - the implementation of SIS should be a seamless extension of current national querying methods so as to reduce the need for training

RECOMMENDATIONS	BEST PRACTICES
4. Data handling	
4.1 entry / modification / deletion of alerts	
- at insertion, all alerts should satisfy the criteria to ensure that a hit will be followed up	- inform the authorities which introduce alerts in the SIS about the consequences of such introductions and notably the obligation to follow up a hit - establish national procedures defining the responsibilities for full submission of extradition requests or for retrieving stolen vehicles ...
- examine the files on existing alerts pursuant to Article 95 before they are available to the end-user	- ensure that the SIRENE workflow system emits an automatic warning when a new alert pursuant to Article 95 is entered - if it has not been possible to pre-validate all files on alerts pursuant to Article 95, these alerts should nevertheless be made available to the end-users as soon as the system is open to the end users, without waiting for the result of the examination of the A-form by SIRENE; in this case, procedures must be established to ensure a swift examination of the file if the alert is executed
- the priority and incompatibility rules should be respected	- SIRENE operators should be allowed to manually delete alerts that do not respect the priority and incompatibility rules - "secondary" alerts on a person should be kept available so that they can be inserted when the first alert on this person, with which the "secondary" alert was incompatible, expires

RECOMMENDATIONS	BEST PRACTICES
	- national legislation should allow for all actions, notably "specific checks" pursuant to Article 99
- before extending an alert, its on-going validity and relevance should be re-examined - Schengen ID-numbers should not be re-used - the time between the incident and the introduction of an alert in the SIS should be minimised - alerts that fulfil the Schengen criteria should, insofar as possible, be entered in the SIS in an automated way: if the SIRENE has to manually copy such alerts from national systems to insert them in the SIS, this often causes delays	- the entry of alerts should preferably be done in real time - decentralise entry of alerts (especially on objects) as much as possible to avoid delays due to internal administration procedure, such as posting the alerts to data input centres - where direct introduction is not possible, quick means of transmission should be provided to send the information from the local level to the level where the data are inserted, in particular for alerts on missing children and stolen vehicles

RECOMMENDATIONS	BEST PRACTICES
- data quality measures should be set up to avoid that SIS alerts affect persons unconcerned with the alert	- a vehicle registration number should not be re-issued for use as long as it is a subject of an SIS alert - it is standard practice that an alert is deleted from the SIS and kept only in the national database when it is established, where this is provided for under national law, that a stolen vehicle has been lawfully obtained by a bona fide owner
- the systematic input of alerts in the SIS should be enhanced as much as possible and national criteria should be set for such introduction - at insertion, it should be checked whether there is no double alert	- the system should automatically check for possible double alerts through searching that goes beyond exact match searching
4.2 follow-up of hits	
- the SIRENE must be the single point of contact and the conduit for the transmission of all information in relation to the post-hit procedure - for alerts pursuant to Article 95, the SIRENE must be the single point of contact and is responsible for the post-hit exchange of information until at least the formal extradition procedure starts	- the exchange of all information not requiring a rogatory letter should be sent through SIRENE - where possible and/or appropriate, the SIRENE may facilitate any further exchange of information subsequent to the arrest

RECOMMENDATIONS	BEST PRACTICES
- a reply, or at least a preliminary answer on the status of the case, should be sent within the set time periods	- it should be ensured that also the authorities responsible for dealing with third country nationals' are available 24/7 or organised in such a way that deadlines for giving additional information can be respected: the SIRENE could be given access to the database of these authorities
- an alert should be deleted from the SIS once the need for the alert does not exist anymore	- alerts pursuant to Article 95 should be deleted once extradition has taken place - alerts pursuant to Article 96 should not be deleted after a hit - alerts on adults pursuant to Article 97, not requiring to be placed under protection, should be deleted upon a hit - other alerts pursuant to Article 97 should be deleted when the protective measures are executed - an alert on a stolen vehicle (including the double alerts) should be deleted rapidly after the hit to avoid problems when returning the vehicle
- procedures should be established to ensure that actions on lost objects are rapidly carried out - provide statistics on hits	- define the roles and responsibilities of the concerned parties - a hit is a positive response found in a Schengen State to an alert issued by another Schengen State - every hit should be accurately registered, including those on alerts pursuant to Article 96 - hits should be categorised per article

4.3 data quality measures	
- automated introduction of SIS data, via a link between the relevant national databases and the N.SIS database - automated introduction of alerts should be accompanied by a real-time automated change/deletion in the SIS following a change/deletion in the national system	- this is satisfied where the introduction in the SIS is set as a default option, as recommended in chapter 3.1
- alerts should be as complete as possible	- the data of the alert should be checked, preferably in an automated way, against national registers - alerts should be updated with additional information, as it becomes available, such as the document number of an issued document or VIN of a stolen car - the SIRENE of the country of origin of a stolen object should provide supplementary information to update the alert

- SIRENE should act as data quality assurance manager - the SIRENE must validate every alert pursuant to Article 95	- the SIRENE should have the national competence as well as the operational and technical means to ensure data quality, including having access to national databases, and dip-sample all categories of all alerts - the SIRENE should be involved in users' training - the lists of hits should be checked against the lists of deleted alerts - the alerts/hits ratio should be reviewed and studied - it should be regularly checked with the local authorities whether it is necessary to maintain an alert on a missing minor
- the transliteration rules should be respected	- specific information on transliteration rules should be made available to the end-users
- the end-users should be trained in data quality measures	- introducing untraceable information is not allowed, e.g. filling in "unknown" in mandatory fields, leaving optional fields blank instead of filling in "unknown" or "?"

RECOMMENDATIONS	BEST PRACTICES
5. Security	
5.1 Planning of data security work	
- the determination of a security policy for the Schengen IT systems (N.SIS, C.SIS, SIRENE and end-users systems) should be an integral part of the definition of the overall security policy of the authorities concerned with these systems - the security policy adopted has to be documented in writing by the competent authorities - it is vital to allocate the necessary resources for preparing and maintaining security measures - at the national level, procedures and areas of responsibility should be established to ensure that all security measures are continuously updated and revised - the updating or revision should, as far as practible, be carried out once every year so that they are constantly adequate and reflect existing conditions - in addition, updating and revision should take place following significant/serious incidents or following system changes that have an impact on data security	

5.2 Security organisation	
- efforts to ensure data security should – whenever appropriate – be planned within the framework of a security organisation, which may comprise one or more authorities	
- responsibilities and authority delegated to persons involved in data security work should be clearly defined, possibly in connection with job specifications for the persons concerned - it will normally be appropriate to provide documentation of the organisation of security work by means of an organisational chart	
5.3 Asset control	
- it has to be ensured that all important parts (assets) of the systems are known, so that they can be protected in accordance with their importance - a register of relevant IT equipment should therefore be maintained on an ongoing basis - in addition, updated network and systems documentation, showing for instance the connection and functionality of the specific system elements, ought to be available	
5.4 Personnel security	
- only persons with specific authorisation may have access to SIS data and to equipment used to process SIS data - SIS may only be accessed when this is required to carry out the tasks for which the user is responsible	- screening of personnel as part of the recruitment procedure and repeated every 5 years

- job descriptions for personnel with access to SIS data and to equipment used to process SIS data should include information on security responsibilities	
- staff recruitment practices should attach importance to knowledge of data security - this personnel have to take the necessary user-training programme, which has to include all current rules on data security - confidentiality and secrecy agreements have to be made with all persons who do not belong to any national authority - these persons must have the necessary clearance or certification - they should only get access to SIS data where this is required for the execution of their tasks - chains of command and procedures have to be defined, ensuring that security incidents or suspected security incidents are reported as quickly as possible - the procedure must be known by all internal personnel and external contractors - feedback processes have to be implemented to ensure that information about the results is communicated, once the incident has been dealt with and terminated - any contravention of security rules has to be disciplined to the extent necessary, in conformity with national legislation	

5.5 Physical security	
- SIS data processing facilities (N.SIS, C.SIS and SIRENE) and other critical or sensitive resources, such as media storage areas, must be housed in secure areas, each one protected by a defined security perimeter with appropriate physical barriers and entry controls	- a class 2 security area as defined by the Council Decision of 19 March 2001[1] is desirable in relation to the handling of all SIS data (to the extent that SIS data processing facilities handle EU confidential information, at least a class 2 security area is necessary anyway) - computers located underground - different security zones - access cards - guards - monitoring by CCTV
- the area has to be appropriately protected against any form of intrusion - the external walls must be of solid construction and the access doors must be suitably protected against unauthorised access, e.g. by control mechanisms, bars, alarms and locks - a building or site containing SIS data processing facilities must have an attended reception area or other means to control physical access	
- access to the secure areas containing the SIS data processing and media storage facilities must be controlled and restricted to authorised persons	- monitoring of entries and exits

[1] Council Decision 2001/264/EC adopting the Council's security regulations, published in OJ L 101, p. 1 of 11.4.2001.

- visitors to secure areas should be supervised or cleared - visitors should only be granted access for specific, authorised purposes - third party support services personnel should be granted restricted access to secure areas only when required - this access must be authorised and monitored	
5.6 Equipment security	
- all equipment used to process or store SIS data must be protected against accidental damage or loss and unauthorised access	
5.6.1 SIS data processing equipment	
- SIS data processing equipment must be located in an area to which access is minimised - continuous monitoring must be carried out to minimise the risk of potential threats, including criminal or terrorist assaults, fire, overheating due to climate control failure, structural collapse after explosion, and penetration of water - in order to achieve continuity of power supplies, the following equipment must be ready and regularly checked and tested: • an uninterruptable power supply (UPS), that keeps the essential functions running • a backup generator for continued processing in case of a prolonged power failure	- fire, heat and smoke detection systems - automatic fire extinguishing system - sufficient air-conditioning
- telecommunications cables must be protected to the necessary extent	

- electronic network equipment must be installed in locked rooms or locked cabinets	
- only authorised maintenance personnel may carry out repairs and equipment maintenance - separate back-up system, regular check of the switch between the back-up and operational system	- cold/hot standby or mirrored sites - in remote location so that a disaster affecting one site does not affect the other
5.6.2 Terminals and PC workstations	
- terminals, PC workstations and printers must be placed so as to ensure that unauthorised persons cannot read data thereon - procedures should be established to monitor printing from screen and SIS data listing - PC and terminal sessions must be automatically terminated after a period of no activity and they must be protected by locking devices, passwords or other control measures whenever they are out of use - terminals, PC workstations and printers that are installed in rooms to which there is access for the general public must be monitored constantly	
5.7 Communications and operating management	
5.7.1 Operating procedures and responsibility	
- the operating procedures established by the individual Schengen States must be documented and continuously updated - they must as a minimum, comprise the following:	
• procedures for day-to-day operating measures such as back-up, anti-virus updating, network monitoring, etc.	

• procedures for handling data media and other assets • procedures concerned with access restrictions • instructions on how to handle errors or other exceptional conditions • support contacts in case unexpected operating or technical difficulties arise • procedures for restarting and restoring the system after any system failure - satisfactory control of all modifications of SIS data processing facilities and systems should be ensured, including hardware, software or procedures - there need to be clear responsibility instructions and procedures for handling them	
5.7.2 Procedures for incident management	
- there must be emergency plans and escalation procedures to be used to remedy incidents that may potentially interrupt the operation of the system and make the Schengen IT systems fully or partly inaccessible - if an incident occurs which will not render the entire system inaccessible but will compromise data security, procedures must have been defined for detecting and handling such incidents	

5.7.3 Protection against malicious software	
- to protect the integrity of software and data, a range of security measures should be taken to prevent and detect the intrusion of malicious software and contribute to restoring systems afterwards - these should include control measures for protection against viruses, worms, Trojan horses and other malicious software - as a minimum the following elements should be included: • a formal policy requiring compliance with software licenses and prohibiting the use of unauthorised software • anti-virus detection and repair software is to be deployed across all PC's with regular virus definition updates and scanning across servers, PC's and laptop computers; exceptions, if any, should be documented • any electronic mail attachments and downloads will be checked for malicious software before use; it should be stated where this check will be carried out: e.g. at electronic mail servers or when entering the network • formal procedures for reacting against virus-related incidents have to be available	- forbid attachments which are exe.files, encrypted, contain macros or passwords, ...
5.7.4 Backup	
- backup copies of SIS data, configuration files and applications must be taken regularly	- make daily copies

- all backup systems must be tested regularly to ensure that they conform to the requirements of the operating plans	
- backup data must be subject to the physical protection required and placed in different geographical locations	- keep copies in at least two different locations
- restoring procedures must be checked and tested regularly	- twice a year
5.7.5 Network management	
- national transmission of SIS data may only use networks which are protected against unauthorised access	- encrypted network / radio / fax
- networks must be constantly monitored	
- measures have to be taken to protect the confidentiality of SIS data during transmission via communications networks	- secure communications between the SIRENE and field offices / operational officers for the exchange of personal data
- access to SIS data from public networks such as the Internet must not be possible	- avoid that access to the Internet is possible through the police network
- transmission of passwords and other security elements must be protected by encryption methods	
5.7.6 Handling of data media	
- the number of technical copies of SIS data must be restricted to the minimum necessary (see Article 102(2))	
- procedures must be established for handling and storing SIS data in order to protect such data against unauthorised retransmission or misuse	
- such procedures should comprise	

• only authorised personnel should have access to computer-based storage media containing SIS data • all media containing SIS data must be marked appropriately and adequately protected during their transportation • media that are obsolete or no longer required must be rendered unusable, or when they are reused, be treated in such a way as to eliminate all SIS data - archives should be secure - access to archives should be controlled and restricted to designated staff - such access should be monitored and registered - archives should be managed to ensure that deletion policies are followed	- updates of the SIS database that are sent to consular posts should be sent on encrypted media and through diplomatic carrier - prevent the erroneous distribution of data by inappropriately recycling material, including paper - replacement of media by competent authorities or agreed/screened company - procedures for storing and destroying material/ clean desk policy - electronic archives provide the best security guarantees including logging of access to and use of the files and audit facilities - electronic archives can include automatic weeding and deletion functions - in the case of physical archives, a combination of a magnetic card and a personal code to access the archives was thought to be the best solution - print-outs in respect of electronic archives should be avoided and in any case destroyed after use
5.8 User access control	
- there must be a user registration and de-registration procedure of users for granting access to the different systems and services - this procedure must include:	- validation of queries on sample basis

• using unique user IDs, so that actions of individual users can be accounted for and users can be made responsible for their actions; therefore, the use of group IDs must not be allowed • each user must only have the minimum set of access rights needed for the normal execution of their jobs	
• immediately removing access rights to SIS data whenever the respective users cease to exercise functions that imply the necessity to have such an access • periodically checking that the level of access granted is according to the user profile	- the application may include a technical function to automatically close a user account when it has not been used for e.g. two weeks
• periodically checking for, and removing, redundant user IDs and accounts	- the user ID and account can be automatically linked to the personnel status
- the allocation and administration of passwords must be controlled by a formal procedure ensuring that: • users are informed and aware of their obligations in respect of their passwords • passwords are communicated to users in a safe way	
• users are required to regularly change their passwords and reuse of passwords is rejected, • passwords are never stored in the computer system without any protection	- a password should be changed every 60 to 90 days
- a procedure has to be established to ensure regular revision of all user access rights	

5.9 Monitoring system access and use	
- the national use of the Schengen IT systems must be monitored in order to ensure detection of unauthorised activities - the transmission of personal data shall be recorded in accordance with Article 103 of the Schengen Convention - a log of the user's log-on, and, as far as possible, log-off; attempts to connect or failed connections and attempts of unauthorised use of data should be kept for the period as set out in Article 103 - the data recorded should include user ID, date and hour of the incident and, if possible, the identity and location of the terminal	- logs and audit trails in respect of SIRENE files should be pro-actively monitored and retained for a sufficiently long period in accordance with domestic law - electronic workflow/case management systems provide the best means of securing that every action taken on a SIRENE file is logged and audited
5.10 Development and maintenance	
- to minimise the risk of damage to operational systems, security control measures have to be established for data and programs	
- it should be ensured, for example, that the updating of operational systems, including program libraries, is only executed subject to prior approval - before approval is granted, it has to be ensured that the updating has been tested and documented satisfactorily	

- a test system must be available separately from the production environment, so that changes can be tested before they are made operational and no test data are introduced in the operational system - any use of real SIS data for testing purposes should be avoided unless they have been anonymised	
5.11 Emergency planning	
- each Schengen State must establish and implement suitable emergency planning measures, taking account for example of the following situations: • a N.SIS or network inaccessibility is noted • some or all users are unable to search SIS data due to problems in the national IT infrastructure - the emergency plans have to be based on a risk assessment of the threats that may lead to inaccessibility of the system and the impact of the threats on the other Schengen States - emergency plans must, at a minimum, include the following:	
• criteria for implementing the plans and measures to be taken immediately to assess the situation	
• escalation procedures, in accordance with the procedures agreed upon for the Schengen States, with a view to informing the national management authorities, C.SIS and other Schengen States	

• emergency procedures describing the measures to be taken after an incident that interferes with the accessibility of the system • fallback procedures describing the measures to be taken to shift essential N.SIS operations to alternative temporary servers • restoring procedures describing measures to be taken to restore normal operation - emergency plans must be updated and staff routines tested regularly	
5.12 Control	
- procedures have to be established which ensure ongoing control of the compliance with all applicable EU and national rules and regulations	- regular security audits done by persons external to the IT-department

The purpose of the Catalogue is to clarify and detail the Schengen acquis, to provide an example for those States acceding to Schengen and to those already fully applying the Schengen acquis.
The first volume of the Catalogue was published in February 2002. It dealt with External borders control as well as with Removal and readmission.
This second volume of the Catalogue addresses specifically the Schengen Information System and SIRENE. It gives a good indication to candidate countries for accession to the European Union as to what is expected of them, particularly in practical terms, regarding Schengen.