LARGE SCALE E-JUSTICE INTEROPERABILITY:
The case of the Schengen Information System,
the technological backbone of the European Arrest Warrant
and surrender procedures.

Marco Velicogna
IRSIG-CNR, Bologna, Italy

Project coordinator
Research Institute on Judicial Systems, National
Research Council of Italy (IRSIG-CNR)

In partnership with
Law Faculty, Central European University (CEU),
Budapest
ICT Department, Italian Ministry of Justice, Rome
Institute of Law and Technology, (IDT) Autonomous
University of Barcelona
Department of Political Science (DSP), University of
Bologna
Interdepartmental Research Centre on European
Law (CIRDE), University of Bologna
Centre for Social Studies (CES), University of
Coimbra

With the financial support of
European Commission, Directorate General Justice
Freedom and Security,
Specific Programme Civil Justice, Grant
JLS/2009/JCIV/AG/0035
Large scale e-justice interoperability:
The case of the Schengen Information System, the
technological backbone of the European Arrest
Warrant and surrender procedures.

Author:
Marco Velicogna IRSIG-CNR
Marco.Velicogna@irsig.cnr.it

Report prepared for the
Building interoperability for European civil proceedings online
JLS/2009/JCIV/AG/0035

May 2012
Executive Summary.......................................................................................................................... 5
0. Introduction................................................................................................................................. 10
1. Institutional Background............................................................................................................. 13
  1.1 European Union: integration, security and criminal Justice Cooperation................................... 13
    1.1.1. European Union Law....................................................................................................... 14
    1.1.2. The Area of freedom, security and justice................................................................. 16
  1.2. The Schengen Agreement, Convention and Schengen Area ................................................ 17
    1.2.1. The Schengen Area expansion..................................................................................... 18
  1.3. The European Arrest Warrant Framework Decision............................................................. 19
    1.3.1. The EAW Roadmap...................................................................................................... 22
2. The Schengen Information System .............................................................................................. 25
  2.1. SIS Legal Basis....................................................................................................................... 27
  2.2 Some Governance elements ................................................................................................... 28
    2.2.1. SIS I ................................................................................................................................ 29
    2.2.2. SIS II ............................................................................................................................. 30
  2.3. Some technical and organizational features ........................................................................... 32
    2.3.1. The Data ...................................................................................................................... 35
    2.3.2. The Forms .................................................................................................................... 39
    2.3.3. The Network .................................................................................................................. 43
  2.4. SIRENE Bureau .................................................................................................................... 45
  2.5. A long evolution path .......................................................................................................... 49
    2.5.1. The first step, from SIS I to SIS I+ ............................................................................... 49
    2.5.2. SIS II ............................................................................................................................. 49
    2.5.3 Some new functions for SIS I+ ..................................................................................... 54
    2.5.5. SIS II and SIS I+R(evolution) .................................................................................... 57
  2.6. Outside of the box: e-CODEX EAW and Secure communication in cross border criminal matters ............................................................................................................................... 62
    2.6.1. e-CODEX High Level Architecture .......................................................................... 64
3. The EAW in action in Italy .......................................................................................................... 72
  3.1. Issuing an EAW in Italy ....................................................................................................... 72
  3.2. Executing an EAW .............................................................................................................. 78
4. Preliminary conclusions ............................................................................................................. 84
5. Some lessons for the creation and evolution of an EU scale interoperability infrastructure ............... 86
  5.1. About Norms ....................................................................................................................... 86
  5.2. About Organization ............................................................................................................ 87
  5.3. About Technology .............................................................................................................. 88
  5.4. About Semantic .................................................................................................................. 88
  5.5. About Governance............................................................................................................. 89
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFSJ</td>
<td>Area of freedom, security and justice</td>
</tr>
<tr>
<td>C-SIS</td>
<td>Technical support function of the Schengen Information System- central site containing SIS reference database</td>
</tr>
<tr>
<td>DG</td>
<td>Directorates-General</td>
</tr>
<tr>
<td>e-CODEX</td>
<td>e-Justice Communication via Online Data Exchange, the first European Large Scale Pilot in the domain of e-Justice</td>
</tr>
<tr>
<td>EAW</td>
<td>European Arrest Warrant</td>
</tr>
<tr>
<td>EDPS</td>
<td>European Data Protection Supervisor</td>
</tr>
<tr>
<td>EIF</td>
<td>European Interoperability Framework for European public services</td>
</tr>
<tr>
<td>EPO</td>
<td>European procedure for Payment Order</td>
</tr>
<tr>
<td>EIS</td>
<td>European Interoperability Strategy for European public services</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EURODAC</td>
<td>EURODAC is an information system created to support the comparison of fingerprints of asylum applicants and illegal immigrants</td>
</tr>
<tr>
<td>Eurojust</td>
<td>European Union's Judicial Cooperation Unit</td>
</tr>
<tr>
<td>Europol</td>
<td>European Police Office</td>
</tr>
<tr>
<td>FD</td>
<td>Framework Decision</td>
</tr>
<tr>
<td>Frontex</td>
<td>European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union</td>
</tr>
<tr>
<td>JSA</td>
<td>Schengen Convention Joint Supervisory Authority</td>
</tr>
<tr>
<td>MS</td>
<td>Member State</td>
</tr>
<tr>
<td>N-SIS</td>
<td>National section of the Schengen Information System</td>
</tr>
<tr>
<td>OST</td>
<td>Operational Systems Test</td>
</tr>
<tr>
<td>PJSA</td>
<td>Schengen Convention provisional Joint Supervisory Authority</td>
</tr>
<tr>
<td>PWP</td>
<td>Permanent Working Party</td>
</tr>
<tr>
<td>s-TESTA</td>
<td>Secured Trans-European Services for Telematics between Administrations</td>
</tr>
<tr>
<td>SIA</td>
<td>Schengen Implementation Agreement</td>
</tr>
<tr>
<td>SIRENE</td>
<td>Supplementary Information Request at the National Entry</td>
</tr>
<tr>
<td>SIS</td>
<td>Schengen Information System</td>
</tr>
<tr>
<td>SIS I+</td>
<td>Updated version of the Schengen Information System</td>
</tr>
<tr>
<td>SIS I+RE</td>
<td>Schengen Information System I+ Renewal and Evolution</td>
</tr>
<tr>
<td>SIS II</td>
<td>Second Generation Schengen Information System</td>
</tr>
<tr>
<td>SIS One4All</td>
<td>Modified version of SIS I+ offered by Portugal to new MS to allow the enlargement of the Schengen Area over the SIS I+ limits</td>
</tr>
<tr>
<td>SIS Steering Committee</td>
<td>Schengen Information System Steering Committee</td>
</tr>
<tr>
<td>SIS-TECH WG</td>
<td>SIS-TECH Working Group</td>
</tr>
<tr>
<td>SISNET</td>
<td>SIS virtual private network</td>
</tr>
</tbody>
</table>
Executive Summary

The Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA) was introduced with the purpose of replacing the extradition procedure between EU Member States with a faster and simpler surrender procedure. The European Arrest Warrant (EAW) is a judicial decision that can be issued by a Member State judicial authority “with a view to the arrest and surrender by another Member State of a requested person, for the purposes of conducting a criminal prosecution or executing a custodial sentence or detention order”. Once issued, the EAW is valid throughout all European Union Member States. This new procedure removes the political and administrative phases from the decision-making process. According to the Commission “in general, the EAW is operating efficiently. The basis for this conclusion is the increasing volume of requests, the percentage of them that result in effective surrender and the fact that the surrender deadlines are generally met. The improvement is even more striking when these variables are compared with those existing under the previous extradition regime”. ¹

This report focuses its attention on the features of an Information Infrastructure, the Schengen Information System (SIS), which supports the implementation of the EAW Framework Decision. SIS is the European “largest shared database on maintaining public security, support police and judicial co-operation and managing external border control”². The Schengen Implementing Convention of 1990 introduced SIS as a ‘compensatory measures’ to the increased risks associated to the abolishment of obstacles to the free movement of goods, persons, services and capital between Schengen States.

SIS contains data (alerts) on people (wanted, to be controlled or with refusal of entry) and goods (i.e. vehicles to be placed under surveillance or subjected to specific checks, objects sought for the purpose of seizure or use in criminal proceedings) that is entered and accessed by the authorized personnel of the participating States. The system is used by immigration, border control, judicial and police authorities with objectives ranging from

border control, to “issuing of visas, residence permits, driver's licenses, customs regime, police and judicial activities, and also to guarantee public order, national and European security”.\(^3\)

From a normative perspective, after the EAW FD has been implemented within the Schengen area, if a person is “wanted for arrest for extradition or surrender purposes (Schengen Convention, Art. 95) -the alert in SIS is equivalent to a European Arrest Warrant or a request for provisional arrest pursuant to the European Convention on Extradition”.\(^4\) At the same time, until the SIS is capable of transmitting all the information described in Article 8 of the EAW FD, the alert is the equivalent to a European arrest warrant only “pending the receipt of the original in due and proper form by the executing judicial authority”.\(^5\)

As SIS predates EAW FD, the fit between the two is not seamless. As an example, not all the elements provided for by the EAW form find their equivalent in the SIS database structure. Furthermore, the scope of the SIS is broader than that of the EAW, including for example 'third-country nationals' who should in principle be denied entry to any of the Schengen States, missing persons and persons to be placed under police protection.

In order to investigate the complex evolution trajectory of the Schengen Information System, as the information infrastructure backbone that enables the EAW to operate, the report explores in depth:

1. The institutional context, including the creation of the Schengen Area and the rise of the European Arrest Warrant.
2. The Schengen Information System’s features and its changes over time from a normative, technological and organizational perspective.
3. The SIS in action throughout the EAW procedure in one Member State, Italy.

The analysis of the story of the Schengen Information System allows to see how the system, while ‘making the EAW performative’ (in other words, allowing it to perform its function), has changed in a non always parallel

\(^3\) [https://www.privacyinternational.org/article/austria-privacy-profile](https://www.privacyinternational.org/article/austria-privacy-profile)


\(^5\) Art. 9 EAW FD, 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision
path. Indeed, the system has evolved over time, as the Schengen area expanded, institutional settings modified and risks and their public perception changed, in part in response to the needs to find a better fit with the EAW, but also to address other needs.

So for example:

- The number of States sharing SIS database has grown from the initial seven in 1995 when the system became operational, to 26 at the time of the writing of the report, including four States (Iceland, Norway, Switzerland and Liechtenstein) that are not members of the European Union and to which the EAW FD does not apply.
- The number of SIS records has increased from almost 3,9 millions "alerts" in 1995\(^6\) to over 35 millions in 2010 and is rising of an average of 3% per month.\(^7\)
- Functions have increased: from alerting authorities of other Schengen countries on certain categories of people and goods in order for them to take ‘concrete measures’ to support investigation.
- Organizational units, the SIRENE Bureaux, have been created as single point of contact for each Schengen State, to respond to coordination needs. They are now “an essential feature of the SIS system, without which it could scarcely function.”\(^8\)
- From a technological perspective, newer versions of the system have been developed and implemented, in order to keep up with geographical, functional and data requirements (SIS 1+, SIS One4All). At the

---

\(^6\) http://database.statewatch.org/article.asp?aid=2662  
\(^8\) HOUSE OF LORDS, (2007) "Schengen Information System II (SIS II)", Report with Evidence
same time, the attempt to develop a second generation SIS, which, between the other improvements, should be capable of transmitting all the information described in Article 8 of the EAW FD, has not been very successful so far.

- From a normative perspective, the articles of Title IV of the Convention on the Implementation of the Schengen Agreement have undergone a number of amendments (not all of them applicable given the two pillars nature of the Convention).

The study provides the opportunity to reflect on the implicit assumptions that are still shared by much of the practitioners’ and scientific communities on how information systems are developed, should evolve and made interoperable to support services provision. Indeed, in the last decade, much progress has been done, understanding that technology is just one of the components to be considered. For example, in the Commission ‘European Interoperability Strategy for European public services’, it is recognized that “Interoperability issues are not only technological, but also cover a wide range of aspects, such as: lack of a cross-border and cross-sector legal basis for interoperability, insufficient awareness and political will, or lack of agreement on the governance structures required”. At the same time, the same vision shows how information systems and interoperability between systems are still perceived as positivistic objectives to reach. Indeed, the European Interoperability Framework definition of interoperability, “the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems”, in its generality and inclusiveness, miss the messiness of a reality populated by objectives multiplicity and conflict, unintended effects, and time bounded decisions. SIS story shows the relevance of all these elements when the temporal dimension is added to the equation. More importantly, it shows how a

---

9 European Commission, “European Interoperability Strategy (EIS) for European public services”, Bruxelles, le 16.12.2010 COM(2010) 744 final Annex 1 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services'.


---
system with all this messiness managed to support the EAW while the attempt to develop a more tidy second generation system resulted in a never ending sequences of accidents, delays and postponements.
0. Introduction

The European Arrest Warrant (EAW) and the surrender procedures between Member States is a mechanism designed to replace, simplifying and speeding up, the pre-existing “extradition system by requiring each national judicial authority (the executing judicial authority) to recognise, ipso facto, and with a minimum of formalities, requests for the surrender of a person made by the judicial authority of another Member State (the issuing judicial authority)”.11 Through the introduction of the European Arrest Warrant “the whole political and administrative phase is replaced by a judicial mechanism”.12

From a different perspective, the EAW mechanism can be described as a normative, technological and organizational assemblage13 allowing interoperability of judicial decision issued by a EU Member State in relation to the arrest and surrender by another EU Member State of a requested person, for the purposes of conducting a criminal prosecution, executing a custodial sentence or a detention order.

In spite of the difficulties which characterized both the adoption of the EAW Framework Decision both its initial implementation (of consistency between national norms, lack of operative practices, and of a shared understanding of roles and competences of the relevant actors), legal interpretations have progressively stabilized, and organizational and inter-organizational learning


13 The concept of assemblage, derived by the definition provided by Lanzara (2009), allows evoking the heterogeneous and loosely integrated nature of the EAW. A system characterized by the presence of distinct components of normative, technological and organizational nature. A system that is constituted by -and at the same time is the result of- a multiplicity of actors and authority structures that emerge and define their role over time, none of which is exercising full control over the system or its development. It is a net of situated interventions and design activities which are bounded in space and time; of intervention and activities which tend to be ‘local’ and fragmented, focused on maintaining, updating adapting and patching together one or more technological, organizational legal components, confronting unexpected events, drifts and derives. Its components have been often designed for other scopes and that are still performing other tasks. Its essence is continuously defined and redefined in a process, which takes place through mediation and negotiation, in which governance structures are explored, experimented and temporarily adopted. In the assembling, existing administrative routines, interfaces and jurisdictions are more or less intentionally redesigned to reach a technical, functional and institutional compatibility.
both of national and of other Member States norms and practices has taken place. At the same time, during the implementation process, both national norms and EAW Framework Decision have been amended to support the long term functioning of the EAW mechanism and smoothen some of the tensions it introduced. Indeed, a high level of legal, organizational and technological adaptation has been required to align, and keeping aligned, the components of the assemblage. The result is a system that is technically and organizationally sound, and that has proved to be a quite effective tool of criminal cooperation.

The analysis of the EAW in action has highlighted how one of the constitutive components, which allow the mechanism to function, is the Schengen Information System. The latter is an EU Large Scale Information System which became operational in 1995\textsuperscript{14} and which was “created as a compensatory measure following the abolition of controls at internal borders within the Schengen area”. The SIS allows competent authorities in Member States to exchange information that is used for performing controls on persons and objects at the external borders or on the territory, as well as for the issuance of visas and residence permits”.\textsuperscript{15}

As a consequence, this report focuses on three aspects of the SIS as a component of the EAW assemblage: 1) The institutional context, including the creation of the Schengen Area and the rise of the European Arrest Warrant; 2) the Schengen Information System’s features and its long evolution as the information infrastructure backbone which enables the EAW to operate; and 3) the SIS in action throughout the EAW procedure in one Member State, Italy. Some preliminary reflections on the SIS case study lessons for interoperability at EU level are provided in the conclusions.

The report builds on the results of a research carried out by IRSIG-CNR (Research Institute on Judicial Systems of the Italian National Research Council) researchers within the research project “The European Arrest Warrant in Law and in Practice: a comparative study for the consolidation of


the European law-enforcement area”. The research focused on the analysis of the normative framework, the case law, organizational practices, in depth EAW case files, and judicial actors’ perceptions. Within the Building interoperability for European civil proceedings online project this initial research effort has been integrated with further research and analysis of EU official documents related to SIS and SIS II and of the literature on the subject which has begun to be published in the last years. Indeed, the fact that several working documents have been recently declassified has been quite helpful. Contacts have also been renewed and communication exchanged with the Italian SIRENE Bureau, which, within the security and limits imposed by the nature of the task and by the existing laws and regulations, had already supported the European Arrest Warrant in Law and in Practice research with a very positive attitude. More difficult has been the attempt to contact the Italian N-SIS unit, which at present is still ongoing.

I have to state that the findings and interpretations expressed in this report are entirely those of the author and should not be attributed in any manner to the above mentioned people and institutions.

---

16 The project was coordinated by the Center for Social Studies at the University of Coimbra, with the participation of the Montaigne Center of the University of Utrecht, the Spanish Association Judges for Democracy and the Portuguese Judges' Association. The research project, which effectively ran from June 2008 to June 2010, has been co-funded by the European Commission (Directorate D -Internal security and criminal justice- of the Directorate-General Justice, Freedom and Security).

17 Thanks go to all the experts and practitioners who have provided the data and the information for the research. Special thanks go to Guido Coppola, Giuseppe Lanzillotti and Andrea Lievre of the Italian SIRENE Bureau for the additional data and information provided within the Building interoperability for European civil proceedings online preliminary investigation, which helped writing up the EAW-SIS introductory report.

18 A special thanks goes to Daniele Maria Marcoaldi of the Italian SIRENE Bureau for the support provided to the Building interoperability for European civil proceedings online research effort.
1. Institutional Background

1.1 European Union: integration, security and criminal Justice Cooperation

The European Union (EU), with its components, evolutions and dynamics, provides the institutional context in which the EAW and its technological backbone, SIS, have been created and have evolved. In particular, focus is posed on the situation and events that took place starting from the ‘90s as they more directly affected the EAW and SIS, with just a glance at previous relevant happenings.

The EU is the result of a long process, which has taken place in over 60 years. It traces its origins from the Treaty of Paris (1951), where France, West Germany, Italy, Belgium, Luxembourg and the Netherlands established the European Coal and Steel Community; and from the Treaty of Rome (1957), where the same six States created the European Atomic Energy Community (EURATOM) and the European Economic Community (EEC). In 1967, the Merger Treaty (1965) entered into force and rationalised the institutional structure of the three Communities, establishing a single Council and a Single Commission. As a results, “under the Treaty, the Communities shared the same institutions, although they remain legally independent”.

In the following years, the EU grew in size by the accession of new Member States, with UK, Ireland and Denmark joining in 1973, Greece in 1981 and Portugal and Spain in 1986; and in competences, with the addition of new policy areas. In 1993, the Maastricht Treaty, which established the European Union under its current name, provided for “an institutional change, establishing the ‘three pillar’ structure for what was henceforth to be the European Union”. The first pillar grouped the three European communities and was “subject to the normal supranational methods of decision-making, characterised by the central role of the Commission and European Court of Justice”. “The second and the third Pillars concerned important and sensitive areas of policy hitherto considered to be at the core of national sovereignty”; for this reason “member States devised a

---

19 In particular, the purpose of the EEC was to promote economic growth and stability through the establishment of a common market and a progressive approximation of the economic policies of its member states.
22 Paul P. Craig, Gráinne De Búrca, EU law: text, cases, and materials, 2008, p.15
23 Paul P. Craig, Gráinne De Búrca, EU law: text, cases, and materials, 2008, p.15
decision-making structure that was more intergovernmental”, “setting up ad hoc meetings to discuss such matters is the cumbersome, time consuming, and involves heavy transaction costs, more especially as the number of players expands”.24

The number of Member States has kept raising first from twelve to fifteen in 1995, to 25 in 2004 to the actual 27 in 2007. At the same time, also the constitutional basis of the EU has kept changing, with the Treaties of Amsterdam in 1997, Nice in 2001 and the Treaty of Lisbon, which came into force in 2009.

Figure 1 EU Evolution Timeline, source: http://en.wikipedia.org/wiki/Template:EU_evolution_timeline

In the period in question the EU operated “through a hybrid system of supranational independent institutions and intergovernmentally made decisions negotiated by the member States”.25 Key EU institutions include the European Commission, the Council of Ministers of the European Union (the Council),26 the European Council,27 the European Parliament, the Court of Justice of the European Union, and the European Central Bank.

1.1.1. European Union Law

The structure of EU law sources provides the Institutional background for understanding the normative components of the EU assemblage. “The EU law is divided into ‘primary’ and ‘secondary’ legislation. The treaties (primary legislation) are the basis or ground rules for all EU action. Secondary binding legislation – which includes regulations, directives and decisions – are derived from the principles and objectives set out in the treaties. The EU’s standard decision-making procedure is known as

24 Paul P. Craig, Gráinne De Búrca, EU law: text, cases, and materials, 2008, p.15
25 http://en.wikipedia.org/wiki/European_Union
26 representing the executives of member states
27 Including the President of the European Commission, the President of the European Council and the heads of state or government of the EU member states
'codecision' [(or "ordinary legislative procedure" after the entry into force of the Lisbon Treaty)]. This means that the directly elected European Parliament has to approve EU legislation together with the Council. The Commission drafts and implements EU legislation. The Treaty of Lisbon increased the number of policy areas where 'codecision' is used. The European Parliament also has more power to block a proposal if it disagrees with the Council”.28

The EU decision-making mechanisms changed during the time-period analyzed in the study. This has implications for the legislation activity concerning the normative component of the assemblage. “Between 1993 and 2009, the European Union (EU) legally consisted of three pillars. This structure was introduced with the Treaty of Maastricht on 1 November 1993, and was eventually abandoned on 1 December 2009 with the entry into force of the Treaty of Lisbon, when the EU obtained a consolidated legal personality.”29

The three Pillars were: the Community pillar, corresponding to the three Communities (first pillar); the common foreign, defence and security policy (second pillar); and the justice and Home affairs pillar, devoted to police and judicial cooperation in criminal matters (third pillar).30

The three pillars worked on the basis of two different decision-making procedures: “the Community procedure for the first pillar, and the intergovernmental procedure for the second and third pillars. In the case of the first pillar, only the Commission could submit proposals to the Council and Parliament, and a qualified majority was sufficient for a Council act to be adopted. In the case of the second and third pillars, this right of initiative was shared between the Commission and the Member States, and unanimity in the Council was generally necessary”.31

The Treaty of Lisbon, “amending the Treaty on European Union and the Treaty establishing the European Community was signed in the Portuguese capital on 13 December 2007 by the representatives of the twenty-seven Member States. It entered into force on 1 December 2009, after being ratified by all the Member States.”32

Relevant changes introduced by the treaty includes “the move from required unanimity to double majority voting in several policy areas in the...”

28 Source: http://europa.eu/about-eu/basic-information/decision-making/index_en.htm
29 http://en.wikipedia.org/wiki/Three_pillars_of_the_European_Union
30 “The Treaty of Amsterdam transferred some of the fields covered by the third pillar to the first pillar (free movement of persons)” http://europa.eu/legislation_summaries/glossary/eu_pillars_en.htm
31 http://europa.eu/legislation_summaries/glossary/eu_pillars_en.htm
Council of Ministers; a more powerful European Parliament as its role of forming a bicameral legislature alongside the Council of Ministers becomes the ordinary procedure; a single legal personality formally given to the EU and the creation of a long-term President of the European Council and a High Representative of the Union for Foreign Affairs and Security Policy. The Treaty also made the Union's bill of rights, the Charter of Fundamental Rights, legally binding.”

1.1.2. The Area of freedom, security and justice

“The creation of the area of freedom, security and justice is based on the Tampere (1999-04), Hague (2004-09) and Stockholm (2010-14) programmes. It derives from Title V of the Treaty on the Functioning of the European Union, which regulates the ‘Area of freedom, security and justice’ ”.

In practice, the AFSJ “is a collection of European Union (EU) policies designed to ensure security, rights and free movement within the EU”. On the one hand, internal borders were removed within the EU, increasing freedom of movement but also security risks. On the other hand cross-border judicial and police cooperation were increased, to tackle cross-border crime and terrorism and to make it easier to identify, arrest and transfer suspected criminals from the country where they were arrested to the country where they were wanted for questioning or to stand trial, reducing such security risk increment.

From an EU institutional perspective, “the area comes under the purview of the European Commissioner for Justice, Fundamental Rights and Citizenship and the European Commissioner for Home Affairs”. The relevant European Commission departments are the DG for Justice and DG Home Affairs. However there is also Eurojust and Europol, which develop judicial and police cooperation respectively. Related to the latter there is also the European Police College, the European Police Chiefs Task Force and Frontex.

“The area of freedom, security and justice … covers policy areas that range from the management of the European Union’s external borders to judicial cooperation in civil and criminal matters. It includes asylum and immigration policies, police cooperation, and the fight against crime

33 http://en.wikipedia.org/wiki/Lisbon_Treaty
(terrorism, organised crime, trafficking in human beings, drugs, etc.)”. 39
“Some notable projects related to the area are the European Arrest Warrant, the Schengen Area and Frontex patrols”. 40

1.2. The Schengen Agreement, Convention and Schengen Area

“The Schengen area is based on a body of rules (the Schengen acquis) which encompasses not only the abolition of border control at internal borders and common rules on the control of external borders but also a common visa policy, police and judicial cooperation, common rules on the return of irregular migrants and the establishment of common data-bases such as the Schengen Information System (SIS)”. 41 The Schengen Implementation Agreement (SIA), which may be considered as a “laboratory” for the European Internal Market (Art. 7A EC) became operative on the 26 March 1995, 42 ten years after the Schengen Agreement was signed (14 June 1985). With this step, the decades-old vision of a Europe without internal border controls was brought to life. In fact, since its entry into force, the common borders of the active signatory States can be crossed at any point (also) by citizens of any third country within the Schengen territory, without any form of identity control (art. 2.1 SIA) 43 At the same time, it should be noted that the focus of the Schengen Agreement and of the Convention implementing the Schengen Agreement are quite different. The Schengen Agreement can be seen as “an expression of the will to create a common area of circulation of goods and persons, in order to avoid a remake of incidents that had occurred a year earlier due to overzealous action of Italian customs officers (foreign trucks stopped at the border, protest road blocks set up in France, the entire European road network disrupted)”. 44 Its “priority was a gradual elimination of customs checks at common frontiers of the signatory States. As a matter of fact, only 7 out of the agreement's 33 articles concern police cooperation and the struggle against immigration. On the opposite, the Schengen Convention of

41 European Commission (2011) “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Schengen governance – strengthening the area without internal border control” 14357/11 p.2
44 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
the Schengen agreement, signed on June 19, 1990 by the same contracting parties, developed police, customs and judicial cooperation for purposes of common outer frontier control”. 45 The Schengen Convention was created to provide a counterbalance to the reduction of checks to the movement in the ‘common area’ and address insecurity and immigration issues, which had increased in Schengen Agreement signatory States public debates. One of the fundamental components of this increased cooperation “was the creation of a common computerized information system, the Schengen Information System (title IV of the Convention)”.

1.2.1. The Schengen Area expansion

An important element to consider looking at the SIS story is the growth of the Schengen Area. The first agreement between creating a Schengen area was signed in 1985 by its five original members (France, Germany, Belgium, Luxembourg and the Netherlands). From there, the Schengen area gradually expanded to include Italy on 27 November 1990, Spain and Portugal on 25 June 1991, Greece on 6 November 1992. Austria joined on 28 April 1995 and Denmark, Finland and Sweden on 19 December 1996. Iceland and Norway (non-UE Member States but members of the Nordic Passport Union) also joined on 19 December 1996.

The United Kingdom, while declining to join Schengen Convention in relation to passport controls, in 1999 expressed its intention to commence the implementation of the parts of the Schengen acquis related to Judicial cooperation, Drugs cooperation, Article 26 and Article 27 of the Schengen Convention, and Police cooperation. This request was approved by a Council Decision of 29 May 2000 (2000/365/EC) 47 and put into effect by a 2004 Council Decision (2004/926/EC) 48 from 1 January 2005. In 2002 Ireland also submitted a request for partial participation in the Schengen acquis with the exclusion of the provisions concerning passport controls. The request was approved by the Council Decision 2002/192/EC, 49 but the decision has not yet been put into effect.

45 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
46 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
47 Council Decision (2000/365/EC) of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis
48 Council Decision (2004/926/EC) of 22 December 2004 on the putting into effect of parts of the Schengen acquis by the United Kingdom of Great Britain and Northern Ireland
49 COUNCIL DECISION (2002/192/EC) of 28 February 2002 concerning Ireland’s request to take part in some of the provisions of the Schengen acquis
The Czech Republic, Estonia, Latvia, Lithuania, Hungary, Malta, Poland, Slovenia and Slovakia joined on 21 December 2007 while the non-UE Switzerland joined on 12 December 2008. A protocol on the participation of Liechtenstein in the Schengen area was signed on 28 February 2008. In May 2012, “Bulgaria, Cyprus and Romania also apply only parts of the Schengen acquis, as a decision of the Council of the European Union is still required before controls at their borders can be lifted”. Specifically, for what regards Cyprus, the implementation of the Schengen Agreement in this country has been delayed because of the Cyprus dispute. Finally, Liechtenstein joined the Schengen Area in December 2011.

1.3. The European Arrest Warrant Framework Decision

Describing the rise of the European Arrest Warrant from a normative perspective, this section provides also an insight on the complex interplay that characterized the governance of this process. As mentioned in the introduction, the EAW was introduced with the purpose of replacing the extradition procedure between EU countries with a faster and simpler surrender procedure that removes the political and administrative phases of decision-making. “Until the adoption of the EAW, extradition between EU member states was based on several different intergovernmental measures, themselves based on international law (Peers 2001) — for example, the 1957 Council of Europe European Convention on Extradition, the 1975 and 1978 protocols to the convention, the 1977 Council of Europe European Convention on terrorism, the Schengen Implementing Convention of 1990, a convention in 1995 [on simplified extradition procedure between the Member States of the European Union] supplementing the aforementioned


An interesting element: the integration of Switzerland in the Schengen area had repercussion on previously well-established border policy with Liechtenstein “Until Liechtenstein joins the Schengen Area, however, Liechtenstein’s only border crossing with Austria is still the subject of systematic border controls. In contrast Liechtenstein’s borders with Switzerland are only subject to video surveillance in a measure the Liechtenstein government have described as a "pragmatic interim solution" in order to prevent the re-establishment of controls along a border which has been open since 1923.” http://en.wikipedia.org/wiki/Schengen_Area
conventions, as well as a 1996 convention relating to extradition between the Member States of the European Union.

The EAW stands on the assumption of a high level of mutual trust and cooperation between EU countries and of the existence of common minimum standards of rule of law. This is provided, for the European Commission, by the fact that “Member States and national courts have to respect the provisions of the European Convention on Human Rights and to ensure that it is respected. Anyone arrested under an EAW may have a lawyer and, if necessary, an interpreter, as provided by the law of the country where he or she has been arrested. If judgement was given in his absence against anyone later arrested under an EAW, he has to be retried in the country requiring his return”. At the same time, much still needs to be done if National authorities involved in EAW activities stress keeping the “need to introduce a new judicial culture based on mutual trust, as a condition for the EAW system to deploy all its potential”.  

An EAW can be issued by a national issuing judicial authority for the purposes of conducting a criminal prosecution (for offences carrying a maximum penalty of at least 12 months) or enforcing a custodial sentence (for sentences of four months or more). At the same time, an EAW can not be issued for investigation purposes.

In relation to EAW cases, the double criminality principle is abolished for 32 serious categories of offences. This means that for those 32 categories of offences (as defined by the issuing country) the alleged action does not need to be a crime in the surrendering country but only in the issuing one.

In the Commission EAW FD evaluation report, issued on the 23.2.2005 (COM(2005)63, the Commission “provisionally estimated that, as a result of the entry into force of the Framework Decision, the average time taken to execute a warrant has fallen from more than nine months to 43 days. This does not include those frequent cases where the person consents to his surrender, for which the average time taken is 13 days”. 

---

To sum up, here is a list of the functional simplifications introduced through the EAW FD in comparison with the previous extradition system.58

- the EAW is issued and executed directly by judicial authorities – the role of the executive branch (ministries, etc.) has been abolished or reduced to that of a transmission facilitator;
- the EAW is issued on the same simple form in all Member States, so that it is easy to use and translate;
- the EAW effectively addresses the issue of dual criminality for a list of 32 categories of specified serious crimes under certain conditions, thereby overcoming the problems stemming from different criminal codes in Member States;
- grounds for refusal are strictly limited by the Framework Decision that distinguishes between mandatory and optional grounds. The surrender of Member States' citizens can, for instance, no longer be refused on the grounds of their citizenship. However some Member States have added some grounds for refusal when implementing the Framework Decision into their national law.
- the time-limits for deciding on and executing an EAW are explicit, making the surrender procedure much faster than the previous extradition procedure;
- a SIS alert has the same status as the original EAW, thereby simplifying the distribution of the warrants.

The practical application of the European Arrest Warrant and corresponding surrender procedures between Member States has in previous years been the subject of in-depth mutual evaluations,59 pursuant to Article 8(5) of the Joint Action of 5 December 1997 establishing a mechanism for evaluating

---


59 See for example the “Final report on the fourth round of mutual evaluations - The practical application of the European Arrest Warrant and corresponding surrender procedures between Member States” 8302/4/09 REV 4 LIMITE CRIMORG 55, COPE 68, EJ 24, EUROJUST 20; also see:
the application and implementation at national level of international undertakings in the fight against organised crime”. 60
The information gathered during the evaluation exercise shows that, “in general, the EAW is operating efficiently. The basis for this conclusion is the increasing volume of requests, the percentage of them that result in effective surrender and the fact that the surrender deadlines are generally met. The improvement is even more striking when these variables are compared with those existing under the previous extradition regime”. 61

1.3.1. The EAW Roadmap
The first relevant event in the rise of the EAW can be considered the European Council special meeting held in Tampere on 15 and 16 October 1999 on the creation of an area of freedom, security and justice in the European Union. In this meeting it was declared that the formal extradition procedures were to be abolished among the Member States “as far as persons are concerned who are fleeing from justice after having been finally sentenced...” and for other cases (i.e. prosecution of crimes) it was expressed the need for “fast track extradition procedures, without prejudice to the principle of fair trial”. 62 The following step was the Programme of measures to implement the principle of mutual recognition of judicial decisions in criminal matters, adopted by the Council on 30 November 2000,63 addressing the mutual enforcement of arrest warrants, as envisaged in point 37 of the Tampere European Council Conclusions.
The events of 11 September 2001 are turnaround point for a process that was moving only slowly forward. The need to support the war against terrorism increased the peer pressure on EU member States to go toward a deeper integration in the criminal area. 64 Just a few days after, the conclusions and plan of action of the extraordinary European Council meeting on 21 September 2001 states: “the European Council signifies its agreement to the introduction of a European arrest warrant and the adoption of a common definition of terrorism. The warrant will supplant the

60 “Final report on the fourth round of mutual evaluations - The practical application of the European Arrest Warrant and corresponding surrender procedures between Member States” 8302/4/09 REV 4 LIMITE CRIMORG 55, COPE 68, EJ 24, EUROJUST 20 p.4
62 Tampere European Council Conclusions
current system of extradition between Member States. Extradition procedures do not at present reflect the level of integration and confidence between Member States of the European Union. Accordingly, the European arrest warrant will allow wanted persons to be handed over directly from one judicial authority to another. In parallel, fundamental rights and freedoms will be guaranteed”.65 In his speech of the 4 October 2001 to the Parliament, Tony Blair, refers to the firm action taken by the European Union: “Transport, interior, finance and foreign ministers have all met to concert an ambitious and effective European response: enhancing police cooperation; speeding up extradition; putting an end to the funding of terrorism; and strengthening air security”.66

Some countries initially opposed parts of the EAW proposal. The strongest opposition came from Italy. The Italian position was in particular aimed to reduce the extensive list of crimes (32) specifically addressed by the new legal instrument and not requiring double criminality check to six. “The same six descriptions were contained in the Treaty of extradition recently signed by Italy and Spain, namely terrorism, organized crime, drug trafficking, arms smuggling, people trafficking and sexual abuse of minors”.67 After an intense political and media struggle, and under the mounting pressure coming from the other EU Member States, the Italian government dropped this position at the Laeken Summit on December 11 2001.68 The agreement on the introduction of the European Arrest Warrant reached at the Laeken Summit resulted in the adoption of the Framework Decision on 13 June 2002. The Framework Decision then entered into force on 7 August 2003, with a 31 December 2003 deadline for the Member States to comply with its provisions.

At the same time though, while all EU governments ratified the Framework Decision, some of the tension at the basis concerning fundamental rights protection and mutual trust were still unresolved. Indeed, “The Framework Decision was the outcome of the climate created by the terrorist attacks of 11 September 2001, with emotion and the need to send a strong signal to the public taking the place of measured reflection, and it was signed in

66 Tony Blair’s speech to parliament - The full text of the prime minister’s statement to parliament concerning the terrorist attacks in the US. The Guardian 04 October 2001 http://www.guardian.co.uk/world/2001/oct/04/september11.usa3
68 Black, I. “Italy agrees to EU arrest warrant” The Guardian 12 December 2001 http://www.guardian.co.uk/world/2001/dec/12/september11.usa
record time. However, one crucial aspect that is often overlooked is that this Framework Decision is not just about terrorism, it is about all criminal offences punishable under the criminal laws of the 25 Member States”. 69

As a consequence, the implementation laws introducing and regulating the EAW in the MSs systems were often complex processes and took longer than anticipated. Only half Member states complied with the time limit laid down in the FD (BE, DK, ES, IE, CY, LT, HU, PL, PT, SI, FI, SE, UK). The remaining MSs, with the exception of Italy, implemented the FD within an 8 months delay. 70 The Italian implementation law was approved last on April 22 2005 71 and published in the Gazzetta Ufficiale N. 98 of 29 April 2005. It entered into force on 14 May 2005.

Time delay was not the only issue. Several Member States had to revise their constitutions in order to adopt specific legislation transposing the Framework Decision. 72 Furthermore, although Member States largely implemented properly the Framework Decision, in some cases national implementing law failed to fully transpose it. In some cases implementing laws have been amended by parliaments and Constitutional Courts have been required to intervene (i.e. Belgium, Germany, Poland and Cyprus, Italy). In others courts jurisprudence have found viable compromises.

Not all problems and tension have been solved, though. An indication of the partially unsolved issues generated by the EAW and of the ongoing struggle to solve them can be read, for example, in the Council observation that, during the EAW mutual evaluations, “No small number [of National authorities involved in EAW activities] ... stressed the need to take further steps to approximate legislation and identify common procedural standards as a means of enhancing mutual trust”. 73

Another indication comes from the still ongoing adjustments to the EAW Framework Decision, such as the Framework Decision 2009/299/JHA of 26 February 2009 which, revising part of it, states that the "solution provided by the EAW Framework decision was not deemed satisfactory as regards cases where the person could not be informed of the proceedings". 74

---

71 http://www.camera.it/parlam/leggi/05069l.htm
74 Point 3 of the Preamble of the Framework Decision 2009/299/JHA
2. The Schengen Information System

As mentioned in the introduction, the Schengen Information System (SIS) can be considered the information infrastructure that allowed the EAW to be relatively swiftly implemented from an operational perspective. From a normative perspective, after the EAW FD has been implemented within the Schengen area, if a person is “wanted for arrest for extradition or surrender purposes (Schengen Convention, Art. 95) - the alert in SIS is equivalent to a European Arrest Warrant or a request for provisional arrest pursuant to the European Convention on Extradition”.75 At the same time, until the SIS will be capable of transmitting all the information described in Article 8 of the EAW FD,76 the alert is the equivalent to a European arrest warrant only “pending the receipt of the original in due and proper form by the executing judicial authority”.77

While the Schengen Information System is an integral part of the European Arrest Warrant, SIS predates the EAW and has a broader field of application. SIS is the European “largest shared database on maintaining public security, support police and judicial co-operation and managing

76 Article 8 of the EAW Framework Decision:
Content and form of the European arrest warrant
1. The European arrest warrant shall contain the following information set out in accordance with the form contained in the Annex:
(a) the identity and nationality of the requested person;
(b) the name, address, telephone and fax numbers and e-mail address of the issuing judicial authority;
(c) evidence of an enforceable judgment, an arrest warrant or any other enforceable judicial decision having the same effect, coming within the scope of Articles 1 and 2;
(d) the nature and legal classification of the offence, particularly in respect of Article 2;
(e) a description of the circumstances in which the offence was committed, including the time, place and degree of participation in the offence by the requested person;
(f) the penalty imposed, if there is a final judgment, or the prescribed scale of penalties for the offence under the law of the issuing Member State;
(g) if possible, other consequences of the offence.
2. The European arrest warrant must be translated into the official language or one of the official languages of the executing Member State. Any Member State may, when this Framework Decision is adopted or at a later date, state in a declaration deposited with the General Secretariat of the Council that it will accept a translation in one or more other official languages of the Institutions of the European Communities.
77 Art. 9 EAW FD, 2002/584/JHA: Council Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States - Statements made by certain Member States on the adoption of the Framework Decision
external border control. Participating States provide entries, called "alerts", on wanted and missing persons, lost and stolen property and entry bans". From a normative perspective, the Schengen Information System finds its roots in the Convention on the Implementation of the Schengen Agreement signed on 19 June 1990. When it took effect in 1995, the Convention on the Implementation of the Schengen Agreement “abolished checks at the internal borders of the signatory states and created a single external border where immigration checks for the Schengen area are carried out in accordance with identical procedures. Common rules regarding visas, right of asylum and checks at external borders were adopted to allow the free movement of persons within the signatory states without disrupting law and order.” The abolition of obstacles to the free movement of goods, persons, services and capital between Schengen States was coupled with the introduction of ‘compensatory measures’ -increased cross border cooperation and coordination- in order to uphold security, fight against organized crime and ensure justice. Accordingly, the Schengen Implementing Convention of 1990 “created a multinational database [the Schengen Information System] for the use of immigration, border control, judicial and police authorities in any of the States which fully apply the Schengen Convention”. SIS contains data (alerts) on certain categories of people (wanted, to be controlled or with refusal of entry) and goods, with the objectives ranging from border control, to “issuing of visas, residence permits, driver's licenses, customs regime, police and judicial activities, and also to guarantee public order, national and European security”. While initially SIS was created only for alerting authorities of other Schengen countries on certain categories of people and goods in order for them to take ‘concrete measures’ and ‘compensate’ for the removal of internal borders, with time, its nature and scope began to shift. Especially after the 9/11, Madrid and London terrorist attacks, the system started to change in order to seize its investigation support functions potentials. Indeed, already in 2002, a note from the Presidency of the Council of the European Union to the Working Party on SIS stated that “the idea of using

---

81 HOUSE OF LORDS, (2007) "Schengen Information System II (SIS II)", Report with Evidence
82 https://www.privacyinternational.org/article/austria-privacy-profile
the SIS data for other purposes than those initially foreseen, and especially for police information purposes in a broad sense, is now widely agreed upon and even follows from the Council conclusions after the events of 11 September 2001.83 This idea included both the proposals to extend the access to SIS to other authorities than those initially foreseen, both the proposals for new functionalities.84 The shift generated by this idea resulted in changes both in the rules regulating the use of the database, both in the modification of the database and of the information infrastructure (i.e. Council Regulation (EC) No 871/2004 and Council Decision 2005/451/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism).

2.1. SIS Legal Basis

From an EU legal perspective, SIS was established both on the first and the third pillar.85 The first-pillar aspects of SIS cover alerts for refusal of entry as well as access by Member States’ services responsible for issuing vehicle registration certificates. The third-pillar aspects of SIS cover all the alerts falling under Title VI of the EU Treaty, i.e. provisions on police and judicial cooperation in criminal matters.86 One of the results of this double nature was the need to have parallel EU norms regulating the (same) aspects of SIS pertaining to each pillar. As described in Section 1, changes introduced by the treaty of Lisbon in 2009 eliminated this dualism.

The 1990 Convention on the Implementation of the Schengen Agreement dedicates twenty-eight out of 142 articles to the Schengen information system in its Title IV. Going into quite some detail, the Schengen Convention provides for SIS establishment (Art. 92-93), operation and use (Art. 94-101), for protection of personal data and security of data contained in it (Art. 102-1118) and for the apportionment for the costs (Art.119). In particular, “Articles 94 to 100 divide the data entered in the SIS into a number of different categories of ‘alerts’”.87 An alert is a set of data entered in SIS allowing the competent authorities to identify a person or an object/vehicle with a view to taking specific action.

The six alert categories, corresponding with the specific article are:

83 Presidency of the Council of the European Union “Requirements for SIS” note 5968/02 LIMITE - SIS 6 COMIX 78
84 Presidency of the Council of the European Union “Requirements for SIS” note 5968/02 LIMITE - SIS 6 COMIX 78
85 See Section 1.1.1.
1. (Article 95) persons wanted for extradition to a Schengen State;
2. (Article 96) a list of non-EU citizens ("third-country nationals") who should in principle be denied entry to any of the Schengen States;
3. (Article 97) missing persons or persons to be placed under police protection;
4. (Article 98) persons wanted as witnesses, or for the purposes of prosecution or the enforcement of sentences;
5. (Article 99) persons or vehicles to be placed under surveillance or subjected to specific checks;
6. (Article 100) objects sought for the purpose of seizure or use in criminal proceedings.

With the years the articles of Title IV of the Convention on the Implementation of the Schengen Agreement have undergone a number of amendments (not all of them applicable given the two pillars nature of the Convention). Furthermore, some provisions will be replaced only once SIS II will become operational.

### 2.2 Some Governance elements

This section presents some information on a few of the bodies which played an active role in the development of SIS I and SIS II.

---


89 In particular, "The provisions of the Title IV, with the exception of Article 102A, will be replaced by Regulation (EC) No 1987/2006 of the European parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II) and Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) once they come into force. Article 102A will be replaced by Regulation (EC) No 1986/2006 of the European parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates from the same date." CONVENTION IMPLEMENTING THE SCHENGEN AGREEMENT Consolidated version June 2009 p.48
2.2.1. SIS I

For the implementation of the Schengen Convention, contracting parties/States created two bodies: Art. 131 establishes an Executive Committee, consisting of one Minister in charge of the Convention’s implementation in each party/State. The Executive Committee has “the general mission of supervising the correct implementation of the Convention and has specific additional competencies”. Art. 115 establishes a Joint Supervisory Authority (JSA) with “the task of verifying the good execution of the Convention’s provisions with respect to the function of the technical medium of the SIS”, and consisting of two representatives from each parties/States National Supervisory Authority. Furthermore, the JSA has also ”a number of more general competencies in the field of data protection”.

Beside these two bodies, “the Schengen organization is structured around a Central Group, with the subordinate SIS Steering committee and various working groups, some of which have been set up by the Convention”. The Schengen bodies are assisted by a secretariat, a task initially “fulfilled by the General Secretariat of the Economic Union of Benelux, based in Brussels”. Following the Protocol of the Treaty of Amsterdam (1997) integrating of the Schengen acquis into the framework of the European Union, “With its Decision 1999/307/EC of 1 May 1999, the Council established a procedure for incorporating the Schengen Secretariat into the General Secretariat of the Council”.

Coordination between the various bodies has not been always smooth, as shown by JSA reports, for example: “On several occasions ... with increasing insistence ... the JSA has requested a number of documents essential to its knowledge of the Convention's implementation and of the operation of the SIS, so that it could carry out its mission effectively. It often encountered

---

90 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
91 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
92 Art. 115 Schengen Convention
93 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
94 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
95 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
difficulties in obtaining these in due time and, in spite of its complaints, did not succeed yet in becoming an addressee of some of these documents as they are being worked out, in particular documents from the Steering committee and the Permanent Working Party (PWP).” 97

2.2.2. SIS II
Council Regulation (EC) 2424/2001 and the Council Decision 2001/886/JHA on the development of the second generation Schengen Information System (SIS II) entrusted the competence for the development of SIS II to the European Commission with the assistance of a regulatory committee composed of the representatives of the Member States and chaired by a representative of the Commission. This committee in particular is involved on issues such as the design of the physical architecture of the system, technical aspects that have a bearing on personal data protection, serious financial implications for the budgets or for the national systems of the Member States; and for the development of security requirements. At the same time, “During the past decade, a complex arrangement of groups, committees, boards and task forces have emerged within the governance framework of SIS II. These groups consist of members of police boards, national technical experts, civil servants representing national ministries of interior and security bodies, and provide a platform on which a network of expertise has been constructed on SIS II.” 98

According to the legal instruments governing the various versions of SIS, the Commission is entrusted with the operational management of SIS II during a transitional period. “This period should be no longer than five years from the date from which the SIS II legal instruments apply. The Commission currently entrusts the operational management of SIS II to national public-sector bodies in France. It is, however, not the Commission’s core task to operate such large-scale IT system. Hence, the need to establish a Management Authority in the long term, mainly to ensure continuity and operational management of the respective systems and the permanent flow of data”. 99 The new Regulatory Agency should carry out the

97 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
tasks of the ‘Management Authority’ not only for SIS II, but also for the Visa Information System (VIS)\textsuperscript{100} and EURODAC.\textsuperscript{101}

\textsuperscript{100} The Visa Information System has been created to support the exchange of visa data between the European Union (EU) countries and associated countries applying the common visa policy. The system has been established by Council Decision 2004/512/EC of 8 June 2004. “It consists of a central information system, the ‘Central Visa Information System’ (CS-VIS), of an interface in each Member State, the ‘National Interfaces’ (NI-VIS) that provide the connection to the relevant central national authorities of the respective Member States, and of a communication infrastructure between the Central Visa Information System and the National Interfaces”.

\textsuperscript{101} Eurodac is an information system created to support the comparison of fingerprints of asylum applicants and illegal immigrants. It was established by Council Regulation 2725/2000 of 11 December 2000 to facilitate the effective application of the Dublin Convention (the Dublin Convention has been replaced by Regulation (EC) No 343/2003 of 18 February 2003 and Commission Regulation (EC) No 1560/2003 of 2 September 2003), which aims to determine the State responsible for examining an asylum application (Secretariat of the Eurodac Supervision Coordination Group "Coordinated Supervision Of Eurodac: Activity Report 2008-2009" Brussels, 8 March 2010 ). “The system consists of a central unit, a computerised central database for comparing the fingerprint data of asylum applicants, and means of data transmission between the Member States and the central database”
2.3. Some technical and organizational features

From a technical perspective, the countries participating in the 1990 Schengen Convention “adopted a data-processing star architecture made up of a central site containing the reference database”, the technical support function of the Schengen Information System, known as C-SIS, and national sections, known as N-SIS, containing a copy of the database. The French Republic is responsible for C-SIS, which is located in Strasbourg. At the same time, C-SIS set up and maintaining costs are shared by the Schengen member States, as is liability. N-SIS are set up and maintained

---

103 http://en.wikipedia.org/wiki/SIRENE
104 Art.92.3. of the Convention Implementing the Schengen Agreement
individually by each State. In theory, the national data file should be “materially identical to the data files of the national sections of each of the other contracting parties”. 105 When setting up its national section, each State must observe the protocols and procedures which have been jointly established for the C-SIS. Each national section’s data file is used for searches in the territory of each State. It is not possible to search the data files of other N-SIS. 106 Maintenance and service level commitments for hardware and software must be provided for by each State to ensure the 24/7 operation of N-SIS and to guarantee data integrity both of N-SIS. Similar performance levels and guarantees needs to be provided for any national copies, where these exist (including real-time synchronisation of copies and regular database comparisons). 107

“All national systems are connected on-line with the central system via a secured communication network”.108 The system conceived with an architecture that should ensure that national databases contain identical information.109 All together, C-SIS, N-SISes and the linking Network, constitute the SIS. The system became fully operational by the end of 1994, with the first technical link between the then seven participant States taking place the 30 November 1994.110

So, for example, in case of escape of a prisoner, the competent authority immediately report that a SIS alert need to be issued on that specific individual and the relevant data is entered in the National SIS database. The N-SIS in turn transmits immediately the data to C-SIS. The central

105 Art.92.2. of the Convention Implementing the Schengen Agreement
106 Art.92.2. of the Convention Implementing the Schengen Agreement
107 European Union, SCHENGEN INFORMATION SYSTEM, SIRENE: Recommendations and Best Practices, EU Schengen catalogne Volume 2, December 2002
109 In particular, according to art 92.3. of the Convention Implementing the Schengen Agreement, C-SIS comprises a data file which will ensure via on-line transmission that the data files of the national sections contain identical information.
system will then send this data to the other N-SIS so that all N-SIS are updated in real time and (almost) simultaneously.\(^{111}\)

“The SIS operates on the principle that the national systems cannot exchange computerised data directly between themselves, but instead only via the central system (C.SIS). However, it is necessary for the Member States to be able to exchange supplementary information, either on a bilateral or multilateral basis, as required for implementing certain provisions of the Schengen Convention, and to ensure full application of Title IV of the Schengen Convention for the SIS as a whole”.\(^{112}\) This supplementary information, which cannot be inserted in SIS records but needs to be exchanged for allowing the appropriate action to be taken in case people and objects are found as a result of a search on SIS, is provided by a network of Member States central authorities known as SIRENE Bureaux,\(^{113}\) which are the human interface of the SIS.\(^{114}\) SIRENE Bureaux (see par. 2.4) were not foreseen in the initial version of the Convention Implementing the Schengen Agreement but have been established later. Article 92.4. of the Schengen Convention, which took effect according to Article 1.1. of Council Regulation (EC) No 871/2004\(^{115}\) and Art. 2.1. of Council Decision 2005/211/JHA,\(^{116}\) provides that “Member States shall, in accordance with national legislation, exchange through the authorities designated for that purpose (Sirene) all supplementary information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this system.”\(^{117}\)

While in theory everything should run smoothly and as provided for by the normative framework, this is not always the case. For example, in its first

\(^{113}\) SIRENE stands for Supplementary Information Request at the National Entry
\(^{115}\) Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism.
\(^{116}\) Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism
\(^{117}\) Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism
control mission in 1996, the Schengen Convention Joint Supervisory Authority (JSA) discovered that the databases of the N-SISs were not identical\textsuperscript{118} as provided for in Art. 92.2. of the Convention and that due to design feature could never be; the procedure for detecting differences currently followed was too infrequent\textsuperscript{119} and too long; the technical measures necessary to safeguard established security standards were not always applied; that the set rules were too vague and had not been properly issued; too many people were granted super user access to the system,\textsuperscript{121} tracing functions\textsuperscript{122} were not satisfactorily applied; and security for the management and transport of the magnetic media containing the SIS data was lacking.\textsuperscript{123}

The next subsection focuses on specific elements of SIS and in particular on the data, the forms and the network.

2.3.1. The Data
Creation, update and deletion
The feeding of new data into the SIS (EAWs, stolen vehicles, wanted persons etc.), and their update and deletion is done in a decentralized manner. Each Member State supplies the SIS freely within the definitions and limits established by the Convention on the Implementation of the Schengen Agreement,\textsuperscript{124} and in accordance to the indications of the SIRENE Manual.\textsuperscript{125}

\textsuperscript{118} A large number of disparities were detected between the databases of France and Luxembourg and those of other countries; these differences date back to April 1996 and had not been rectified six months later (Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97)
\textsuperscript{119} Approximately once every six months (Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97)
\textsuperscript{120} Taking up several months to be carried out (Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97)
\textsuperscript{121} “enabling them to access and change the contents of any file in the computer system (operating system, database and network) and to erase any trace of their action” (Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97)
\textsuperscript{122} “to verify in retrospect the operations carried out by the users, regardless of priority (date, time, terminal, user ID, type of operation)” (Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97)
\textsuperscript{123} Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
According to the SIRENE Manual, "Automatic transfer to N.SIS of the national alerts that fulfil the criteria for introduction into the SIS shall be the preferred way to introduce SIS alerts. This automatic transfer, including data quality checks, should also be transparent and not require additional action from the authority entering the alert ... [Furthermore,] where the national system enables the automatic transfer of national alerts to SIS, ... the deletion of a SIS-related alert in the national database should also lead to an automatic deletion of its SIS equivalent".126

While other alerts can be entered by authorised personnel at nationally decentralized level, given the relevance of the issues at stake, Article 95 alerts (EAWs) are entered, modified and deleted by SIRENE bureaux personnel. In relation to “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”.127 In theory, every national alert that is "Schengen-relevant" should “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.”128 At the same time, “Each Schengen State decides which of its law enforcement and immigration control authorities are to have access to some or all categories of SIS alerts, and for which purposes. If a national authority finds that a particular individual or object is listed in the SIS, this is known as a “hit””.129

According to Art.106.1. of the Convention Implementing the Schengen Agreement, only the State issuing the alert is authorised to modify, add to, correct or delete data which it has entered. The SIRENE Manual specify that an alert can be deleted by the service that entered it once the condition to maintain it no longer apply or by C.SIS once its expiry date has passed.130

127 European Union, SCHENGEN INFORMATION SYSTEM, SIRENE: Recommendations and Best Practices, EU Schengen catalogue Volume 2, December 2002
128 European Union, SCHENGEN INFORMATION SYSTEM, SIRENE: Recommendations and Best Practices, EU Schengen catalogue Volume 2, December 2002
The Convention provides for different life time-spans for different data categories. Personal data should be kept only for the time required to meet the purposes for which they were supplied. The need for continued storage of such data must be reviewed by the issuing Member State no later than three years after they were entered, or one year in the case of the alerts referred to in Article 99. C.SIS automatically informs N.SISs of scheduled deletion of data from the system one month in advance. The issuing authority can decide to keep the alert should this prove necessary for the purposes for which the alert was issued. Any extension of the alert must be communicated to the C.SIS. Other data can be kept for a maximum of three years if they concern motor vehicles, trailers and caravans five years if they concern issued identity papers and suspect banknotes and 10 years for other categories.

If an authority of another State has evidence suggesting that an item of data is incorrect or has been unlawfully stored according it should inform the issuing State as soon as possible; and the latter is legally “obliged to check the communication and, if necessary, correct or delete the item in question immediately”. C.SIS keep deleted for one year for checks on accuracy and lawfully data enter, after which period they must be destroyed.

**Access**

The Convention Implementing the Schengen Agreement regulates access to SIS data. According to Art. 101.1 of the original version of the Convention, access to data entered in the SIS and the right to search such data directly is reserved to the Schengen States authorities responsible for border checks and other police and customs checks carried out within the country, and the coordination of such checks. These end-users may only search data which they require for the performance of their tasks (Art. 101.3).

To have an example and an order of magnitude, in France at the beginning of 2005 there were about 15000 computer terminals allowing access to SIS data to authorized officers distributed among the national police,

---

131 Art.112 of the Convention Implementing the Schengen Agreement
132 Art.112 of the Convention Implementing the Schengen Agreement
133 Art.106.2. of the Convention Implementing the Schengen Agreement
134 Art.113 of the Convention Implementing the Schengen Agreement
135 In addition, access to data entered in accordance with Article 96 and the right to search such data directly may be exercised by the authorities responsible for issuing visas, the central authorities responsible for examining visa applications and the authorities responsible for issuing residence permits and for the administration of legislation on aliens in the context of the application of the provisions of this convention relating to the movement of persons. Access to data shall be governed by the nationall aw of each contracting party. (Art. 101.2.).
gendermerie, customs, consulates and prefectures. Furthermore, in 2005 SIS was consulted by French users nearly 35 million times.136

As to the modality of access by end users, “the system is based on a ‘hit/no hit’ query function which indicates whether information on a person or object exists within the system, thus alerting police officers, border guards and customs officials across the Schengen area to persons and items that may pose an immigration or security risk”.137 Furthermore, SIS data138 can be used only for the purposes laid down for each category of alert referred to in the articles 95 to 100. Furthermore, as a general rule, SIS data may not be used for administrative purposes.139

The SIS is a daily tool in the performance of police forces, custom officers and consulates.

Council Regulation (EC) No 871/2004 and Council Decision 2005/451/JHA concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism add to Art.101.1. that “access to data entered in the SIS and the right to search such data directly may also be exercised by national judicial authorities, inter alia, those responsible for the initiation of public prosecutions in criminal proceedings and judicial inquiries prior to indictment, in the performance of their tasks, as set out in national legislation.” They also set up a legal framework for the European Police Office (Europol) and for the European Union's Judicial Cooperation Unit (Eurojust) access to SIS. In particular, according to Art.101A “The European Police Office (Europol) shall within its mandate and at its own expense have the right to have access to, and to search directly, data entered into the Schengen Information System in accordance with Articles 95, 99 and 100 ...”, and according to Art.101B “The national members of Eurojust and their assistants shall have the right to have access to, and search, data entered in accordance with Articles 95 and 98 into the Schengen Information System...”

138 Provided for in Articles 95 to 100 of the Convention implementing the Schengen Agreement.
139 Art 102 of the Convention implementing the Schengen Agreement. The use of SIS for the ‘administrative’ purposes of issuing visas, residence permits and the administration of legislation on aliens in the context of the application of the provisions of the Convention implementing the Schengen Agreement relating to the movement of persons is provided for in art.96 of the Convention
Volumes
The number of SIS records greatly increased since its launch in March 1995 and during the over 15 years of activity of the system, from almost 3,9 millions "alerts" (record entries) in 1995\textsuperscript{140} to over 35 millions in 2010. These figures are simply based on the total number of "alerts" held in the SIS on a single day, they do not reflect the numbers deleted or added during the course of a year (see analysis below). "Alerts" held on the SIS include "persons" (for example, those wanted for arrest, extradition, to be refused entry, for discrete surveillance) and "objects" (vehicles, arms, documents including passports and identity cards, bank notes).

In January 2005, the SIS database contained over 13 million valid records divided approximately as follows: 1,2 millions concerning people (of which about \(\frac{3}{4}\) main records and \(\frac{1}{4}\) aliases) of which about 15 thousands were Art. 95 requests.\textsuperscript{141} By December 2010 data, the volume of valid records (not expired including aliases) reached over 35 millions. Of these, 1.2 millions concerned wanted persons (of which about \(\frac{3}{4}\) main records and \(\frac{1}{4}\) aliases) and over 31 thousands were Art. 95 requests (persons wanted for extradition to a Schengen State). As to 2011, according to the Council of the European Union website, “the number of alerts is rising by approximately 3\% per month”.\textsuperscript{142}

2.3.2. The Forms
Data is entered in SIS through several forms. The main forms used in EAW cases are four: A, M, F and G. The EAW correspond to a SIS alert 95\textsuperscript{143} and

\textsuperscript{140} http://database.statewatch.org/article.asp?aid=2662
\textsuperscript{141} HOUSE OF LORDS, (2007) "Schengen Information System II (SIS II)", Report with Evidence
\textsuperscript{143} According to Art. 95 of the Convention Implementing the Schengen Agreement (Chapter on Operation And Use Of The Schengen Information System):
Art. 95
1. Data on persons wanted for arrest for extradition purposes shall be entered at the request of the judicial authority of the requesting Contracting Party.
2. Before issuing an alert, the Contracting Party shall check whether the arrest is authorised under the national law of the requested Contracting Parties. If the Contracting Party issuing the alert has any doubts, it must consult the other Contracting Parties concerned. The Contracting Party issuing the alert shall send the requested Contracting Parties by the quickest means possible both the alert and the following essential information relating to the case:
(a) the authority which issued the request for arrest;
(b) whether there is an arrest warrant or other document having the same legal effect, or an enforceable judgment;
requires the filing of A+M SIS Forms. Form A corresponds to "Supplementary information (Article 95(2)). Form M corresponds to "Miscellaneous information". Schengen alerts take precedence over Interpol alerts and "Interpol alert should include a note for the Schengen States indicating the Schengen IDnumber of the alert". It is important to note that if a person is "wanted for arrest for extradition or surrender purposes (Schengen Convention, Art. 95) - the alert in SIS is equivalent to a European Arrest Warrant or a request for provisional arrest pursuant to the European Convention on Extradition". The M Form can be used also to exchange further information following a hit, for example to inform the SIRENE Bureau of the issuing Member State on whether the surrender may take place.

The F Form, Flag, can be filled by a SIRENE Bureau to which an Alert is addressed. It is a request to the issuing SIRENE Bureau to ‘flag’ the alert for that specific country. A flagged Art 95 Alert is considered as being issued for

---

(c) the nature and legal classification of the offence;  
(d) a description of the circumstances in which the offence was committed, including the time, place and the degree of participation in the offence by the person for whom the alert has been issued;  
(e) in so far as is possible, the consequences of the offence.

3. A requested Contracting Party may add to the alert in the data file of its national section of the Schengen Information System a flag prohibiting arrest on the basis of the alert until the flag is deleted. The flag must be deleted no later than 24 hours after the alert has been entered, unless the Contracting Party refuses to make the requested arrest on legal grounds or for special reasons of expediency. In particularly exceptional cases where this is justified by the complex nature of the facts behind the alert, the above time limit may be extended to one week. Without prejudice to a flag or a decision to refuse the arrest, the other Contracting Parties may make the arrest requested in the alert.

4. If, for particularly urgent reasons, a Contracting Party requests an immediate search, the requested Contracting Party shall examine whether it is able to withdraw its flag. The requested Contracting Party shall take the necessary steps to ensure that the action to be taken can be carried out immediately if the alert is validated.

5. If the arrest cannot be made because an investigation has not been completed or because a requested Contracting Party refuses, the latter must regard the alert as being an alert for the purposes of communicating the place of residence of the person concerned.

6. The requested Contracting Parties shall carry out the action as requested in the alert in accordance with extradition Conventions in force and with national law. They shall not be obliged to carry out the action requested where one of their nationals is involved, without prejudice to the possibility of making the arrest in accordance with national law.

144 European Union, SCHENGEN INFORMATION SYSTEM, SIRENE: Recommendations and Best Practices, EU Schengen catalogue Volume 2, December 2002
the purpose of communicating the place of residence of the person concerned in the Countries for which it has been flagged. 146 147 The G Form, Matching an Alert (hit) is filled by the SIRENE Bureau personnel in the executing Country when the requested person has been identified/arrested in order to inform the issuing country that the alert is matched.

"before a country is incorporated actively into the Schengen area, one of the requirements is to review the SIRENE "A" forms of the operational countries to provide for the requesting of validity flags". 148

---

147 Article 25 of the Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) -Flagging related to alerts for arrest for surrender purposes- provides that : "1. Where Framework Decision 2002/584/JHA applies, a flag preventing arrest shall only be added to an alert for arrest for surrender purposes where the competent judicial authority under national law for the execution of a European Arrest Warrant has refused its execution on the basis of a ground for non-execution and where the addition of the flag has been required.
2. However, at the behest of a competent judicial authority under national law, either on the basis of a general instruction or in a specific case, a flag may also be required to be added to an alert for arrest for surrender purposes if it is obvious that the execution of the European Arrest Warrant will have to be refused".
148 “Connection of new States to SISNET” Note 12465/04 LIMITE SIRIS 92 COMIX 557
### A. Supplementary Information (Article 95)(a)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE</td>
<td>Date of Incident</td>
</tr>
<tr>
<td>MESSAGE REF NO.</td>
<td>Incident Reference Number</td>
</tr>
<tr>
<td>GENDER</td>
<td>Gender</td>
</tr>
<tr>
<td>AGENT ADDRESS</td>
<td>Agent's Address</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>STATURE NAME</td>
<td>Stature Name</td>
</tr>
<tr>
<td>PLACE OF BIRTH</td>
<td>Place of Birth</td>
</tr>
<tr>
<td>SEX</td>
<td>Sex</td>
</tr>
<tr>
<td>NATURALITY</td>
<td>Nationality</td>
</tr>
<tr>
<td>AUTHORITY ORDERING THE APPEAL</td>
<td>Authority Ordering the Appeal</td>
</tr>
<tr>
<td>NAME OF THE APPEAL</td>
<td>Name of the Appeal</td>
</tr>
<tr>
<td>PLACE OF ISSUE</td>
<td>Place of Issue</td>
</tr>
<tr>
<td>DATE OF ISSUE</td>
<td>Date of Issue</td>
</tr>
<tr>
<td>PLACE OF HEARING</td>
<td>Place of Hearing</td>
</tr>
<tr>
<td>DATE OF DECISION</td>
<td>Date of Decision</td>
</tr>
<tr>
<td>AGE OF APPEAL</td>
<td>Age of Appeal</td>
</tr>
<tr>
<td>SEX OF APPEAL</td>
<td>Sex of Appeal</td>
</tr>
<tr>
<td>NATURALITY OF APPEAL</td>
<td>Nationality of Appeal</td>
</tr>
<tr>
<td>VEHICLE NAME</td>
<td>Vehicle Name</td>
</tr>
<tr>
<td>VEHICLE NUMBER</td>
<td>Vehicle Number</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Description</td>
</tr>
<tr>
<td>CATEGORY OF INCIDENT DOCUMENT</td>
<td>Category of Incident Document</td>
</tr>
<tr>
<td>NARRATIVE OF INCIDENT</td>
<td>Narrative of Incident</td>
</tr>
<tr>
<td>IDENTITY DOCUMENT NUMBER</td>
<td>Identity Document Number</td>
</tr>
<tr>
<td>ARMS TYPE</td>
<td>Arms Type</td>
</tr>
<tr>
<td>ARMS CARRIER</td>
<td>Arms Carrier</td>
</tr>
<tr>
<td>ARMS MODEL</td>
<td>Arms Model</td>
</tr>
<tr>
<td>NATIONALITY OF ARMS</td>
<td>Nationality of Arms</td>
</tr>
<tr>
<td>CONTRACTOR</td>
<td>Contractor</td>
</tr>
<tr>
<td>FACTS CONCERNING THE APPEAL</td>
<td>Facts Concerning the Appeal</td>
</tr>
</tbody>
</table>

### B. Matching an Alert (Ref)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE OF MESSAGE</td>
<td>Date of Message</td>
</tr>
<tr>
<td>MESSAGE REF NO.</td>
<td>Message Reference Number</td>
</tr>
<tr>
<td>GENDER</td>
<td>Gender</td>
</tr>
<tr>
<td>AGENT ADDRESS</td>
<td>Agent's Address</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>VEHICLE NAME</td>
<td>Vehicle Name</td>
</tr>
<tr>
<td>VEHICLE NUMBER</td>
<td>Vehicle Number</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Description</td>
</tr>
<tr>
<td>CATEGORY OF INCIDENT DOCUMENT</td>
<td>Category of Incident Document</td>
</tr>
<tr>
<td>NARRATIVE OF INCIDENT</td>
<td>Narrative of Incident</td>
</tr>
<tr>
<td>IDENTITY DOCUMENT NUMBER</td>
<td>Identity Document Number</td>
</tr>
<tr>
<td>ARMS TYPE</td>
<td>Arms Type</td>
</tr>
<tr>
<td>ARMS CARRIER</td>
<td>Arms Carrier</td>
</tr>
<tr>
<td>ARMS MODEL</td>
<td>Arms Model</td>
</tr>
<tr>
<td>NATIONALITY OF ARMS</td>
<td>Nationality of Arms</td>
</tr>
<tr>
<td>CONTRACTOR</td>
<td>Contractor</td>
</tr>
<tr>
<td>FACTS CONCERNING THE APPEAL</td>
<td>Facts Concerning the Alert</td>
</tr>
</tbody>
</table>

### C. Matching an Alert (Ref)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE OF MESSAGE</td>
<td>Date of Message</td>
</tr>
<tr>
<td>MESSAGE REF NO.</td>
<td>Message Reference Number</td>
</tr>
<tr>
<td>GENDER</td>
<td>Gender</td>
</tr>
<tr>
<td>AGENT ADDRESS</td>
<td>Agent's Address</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>VEHICLE NAME</td>
<td>Vehicle Name</td>
</tr>
<tr>
<td>VEHICLE NUMBER</td>
<td>Vehicle Number</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Description</td>
</tr>
<tr>
<td>CATEGORY OF INCIDENT DOCUMENT</td>
<td>Category of Incident Document</td>
</tr>
<tr>
<td>NARRATIVE OF INCIDENT</td>
<td>Narrative of Incident</td>
</tr>
<tr>
<td>IDENTITY DOCUMENT NUMBER</td>
<td>Identity Document Number</td>
</tr>
<tr>
<td>ARMS TYPE</td>
<td>Arms Type</td>
</tr>
<tr>
<td>ARMS CARRIER</td>
<td>Arms Carrier</td>
</tr>
<tr>
<td>ARMS MODEL</td>
<td>Arms Model</td>
</tr>
<tr>
<td>NATIONALITY OF ARMS</td>
<td>Nationality of Arms</td>
</tr>
<tr>
<td>CONTRACTOR</td>
<td>Contractor</td>
</tr>
<tr>
<td>FACTS CONCERNING THE APPEAL</td>
<td>Facts Concerning the Alert</td>
</tr>
</tbody>
</table>

### D. Miscellaneous Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE OF MESSAGE</td>
<td>Date of Message</td>
</tr>
<tr>
<td>MESSAGE REF NO.</td>
<td>Message Reference Number</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>GENDER</td>
<td>Gender</td>
</tr>
<tr>
<td>AGENT ADDRESS</td>
<td>Agent's Address</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>VEHICLE NAME</td>
<td>Vehicle Name</td>
</tr>
<tr>
<td>VEHICLE NUMBER</td>
<td>Vehicle Number</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Description</td>
</tr>
<tr>
<td>CATEGORY OF INCIDENT DOCUMENT</td>
<td>Category of Incident Document</td>
</tr>
<tr>
<td>NARRATIVE OF INCIDENT</td>
<td>Narrative of Incident</td>
</tr>
<tr>
<td>IDENTITY DOCUMENT NUMBER</td>
<td>Identity Document Number</td>
</tr>
<tr>
<td>ARMS TYPE</td>
<td>Arms Type</td>
</tr>
<tr>
<td>ARMS CARRIER</td>
<td>Arms Carrier</td>
</tr>
<tr>
<td>ARMS MODEL</td>
<td>Arms Model</td>
</tr>
<tr>
<td>NATIONALITY OF ARMS</td>
<td>Nationality of Arms</td>
</tr>
<tr>
<td>CONTRACTOR</td>
<td>Contractor</td>
</tr>
<tr>
<td>FACTS CONCERNING THE APPEAL</td>
<td>Facts Concerning the Alert</td>
</tr>
</tbody>
</table>

### E. Flag

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE OF MESSAGE</td>
<td>Date of Message</td>
</tr>
<tr>
<td>MESSAGE REF NO.</td>
<td>Message Reference Number</td>
</tr>
<tr>
<td>GENDER</td>
<td>Gender</td>
</tr>
<tr>
<td>AGENT ADDRESS</td>
<td>Agent's Address</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>VEHICLE NAME</td>
<td>Vehicle Name</td>
</tr>
<tr>
<td>VEHICLE NUMBER</td>
<td>Vehicle Number</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Description</td>
</tr>
<tr>
<td>CATEGORY OF INCIDENT DOCUMENT</td>
<td>Category of Incident Document</td>
</tr>
<tr>
<td>NARRATIVE OF INCIDENT</td>
<td>Narrative of Incident</td>
</tr>
<tr>
<td>IDENTITY DOCUMENT NUMBER</td>
<td>Identity Document Number</td>
</tr>
<tr>
<td>ARMS TYPE</td>
<td>Arms Type</td>
</tr>
<tr>
<td>ARMS CARRIER</td>
<td>Arms Carrier</td>
</tr>
<tr>
<td>ARMS MODEL</td>
<td>Arms Model</td>
</tr>
<tr>
<td>NATIONALITY OF ARMS</td>
<td>Nationality of Arms</td>
</tr>
<tr>
<td>CONTRACTOR</td>
<td>Contractor</td>
</tr>
<tr>
<td>FACTS CONCERNING THE APPEAL</td>
<td>Facts Concerning the Alert</td>
</tr>
</tbody>
</table>

### F. Flag

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATE OF MESSAGE</td>
<td>Date of Message</td>
</tr>
<tr>
<td>MESSAGE REF NO.</td>
<td>Message Reference Number</td>
</tr>
<tr>
<td>GENDER</td>
<td>Gender</td>
</tr>
<tr>
<td>AGENT ADDRESS</td>
<td>Agent's Address</td>
</tr>
<tr>
<td>VENUE</td>
<td>Location</td>
</tr>
<tr>
<td>NARRATION</td>
<td>Narrative</td>
</tr>
<tr>
<td>VEHICLE NAME</td>
<td>Vehicle Name</td>
</tr>
<tr>
<td>VEHICLE NUMBER</td>
<td>Vehicle Number</td>
</tr>
<tr>
<td>DESCRIPTION</td>
<td>Description</td>
</tr>
<tr>
<td>CATEGORY OF INCIDENT DOCUMENT</td>
<td>Category of Incident Document</td>
</tr>
<tr>
<td>NARRATIVE OF INCIDENT</td>
<td>Narrative of Incident</td>
</tr>
<tr>
<td>IDENTITY DOCUMENT NUMBER</td>
<td>Identity Document Number</td>
</tr>
<tr>
<td>ARMS TYPE</td>
<td>Arms Type</td>
</tr>
<tr>
<td>ARMS CARRIER</td>
<td>Arms Carrier</td>
</tr>
<tr>
<td>ARMS MODEL</td>
<td>Arms Model</td>
</tr>
<tr>
<td>NATIONALITY OF ARMS</td>
<td>Nationality of Arms</td>
</tr>
<tr>
<td>CONTRACTOR</td>
<td>Contractor</td>
</tr>
<tr>
<td>FACTS CONCERNING THE APPEAL</td>
<td>Facts Concerning the Alert</td>
</tr>
</tbody>
</table>

---

**42**
2.3.3. The Network

At present SIS is connected through a virtual private network with TCP/IP protocol\(^{149}\) called SISNET, which was introduced between 2001 and 2002 to substitute the previous network, the SIRENE Network Phase II, based on X.25.

**SIRENE Network Phase II** installation, management and related supplying services were regulated by an agreement concluded in August 1996 between the Secretary-General of the Benelux Economic Union (replaced by the Secretary-General of the Council of the European Union in 1999) on behalf of these Member States concerned and France Telecom Network Services Belgium (afterword become Global One Belgium).\(^{150}\) The contract terminated on August 2001.\(^{151}\) The network lines were leased by the French Government between C.SIS and the French border and by each Member State from the French border to the Member State. At the same time, each Member State had purchased and was the owner of the crypto devices (Kryptoguards) used on the network.\(^{152}\)

**SISNET** - The decision to introduce a new network was formally taken at the end of 1999 with the Council Decision 1999/870/EC authorising the Deputy Secretary-General of the Council of the European Union to execute a call for tenders and conclude contracts for the development installation and management of a communication infrastructure for the Schengen environment, ‘SISNET’, and to manage such contracts. SISNET budget, based on the financial contributions of the concerned States, is regulated by Council Decision 2000/265/EC\(^{153}\) and following amendments.\(^{154}\)

---

\(^{149}\) “Connection of new States to SISNET” Note 12465/04 LIMITE SIRIS 92 COMIX 557

\(^{150}\) See: Council Decision of 3 May 1999 authorising the Secretary-General of the Council of the European Union in the context of the integration of the Schengen acquis into the framework of the European Union to act as representative of certain Member States for the purposes of concluding contracts relating to the installation and functioning of the ‘Help Desk Server’ of the Management Unit and of the Sirene Network Phase II and to manage such contracts (1999/322/EC).

\(^{151}\) Council Decision of 17 December 1999 authorising the Deputy Secretary-General of the Council of the European Union to act as representative of certain Member States for the purpose of concluding contracts relating to the installation and the functioning of the communication infrastructure for the Schengen environment, ‘SISNET’, and to manage such contracts (1999/870/EC).

\(^{152}\) SIS-TECH Working Group -EU/Iceland and Norway Mixed Committee- (2002) “Information about the SISNET” Note 12436/1/02 REV 1 LIMITE SIS-TECH 137 COMIX 539

\(^{153}\) Council Decision of 27 March 2000 on the establishment of a financial regulation governing the budgetary aspects of the management by the Deputy Secretary -General of the Council, of contracts concluded in his name, on behalf of certain Member States, relating to the installation and the functioning of the communication infrastructure for the Schengen environment, ‘Sisnet’.
The introduction of the new network was not without problems. When on 13th of September 2002 the Council Secretariat (SISNET Project Team) gave Final Acceptance of the Network to the supplier, some problems such as a number of un-availabilities of the network service and a high failure rate of the new crypto-devices had been recorded. The issue was monitored by the SIS-TECH WG “in close cooperation with the suppliers”. Furthermore, problems emerged in relation to SISNET Service Level Agreement (SLA) which needed to be renegotiated (with Belgacom) as LSA definitions and actual network statistics did not correspond. The contract for SISNET was stipulated to terminate automatically on 13 November 2008 and could not be renewed or extended through direct negotiation with the contractor. This deadline was conceived as for that time SIS II (See Section 2.5.2.) and its network were supposed to be operational. As SIS II was not, the States concerned had to authorise the Deputy Secretary-General of the Council to the execution of a call for tender for the provision of services concerning the communication infrastructure for the Schengen environment, pending its migration to a communication infrastructure at the charge of the European Community; and the conclusion and management of the contracts for the provision of such services (including budget issues). The possibility to migrate SIS and SIRENE onto the s-TESTA network by 13 November 2008 was considered, and taken as a fall back options given the inherent risks involved in the tendering for a

(2000/265/EC)  
154 SISNET 2011 estimated expenditure are about 4 Million Euros (16963/10 SIRIS 172 COMIX 785)  
155 SIS-TECH Working Group -EU/Iceland and Norway Mixed Committee- (2002) “Information about the SISNET” Note 12436/1/02 REV 1 LIMITE SIS-TECH 137 COMIX 539  
156 “Service credits SISNET agreement” Note 5066/1/04 REV 1 LIMITE SIS-TECH 1 COMIX 5  
157 Council Decision of 5 March 2007 authorising the Deputy Secretary-General of the Council of the European Union to act as representative of certain Member States for the purpose of concluding and managing contracts relating to the provision of services concerning a communication infrastructure for the Schengen environment, pending its migration to a communication infrastructure at the charge of the European Community (2007/149/EC)  
158 s-TESTA is the European Community’s own private, IP-based network dedicated to inter-administrative requirements and providing guaranteed performance levels. s-TESTA has been created to offer a telecommunications interconnection platform that responds to the growing need for secure information exchange between European public administrations. s-TESTA build on the experience of a preceding network (TESTA). Its kick-off was in mid 2007, and full migration was achieved by end of April 2008. http://ec.europa.eu/idabc/en/document/2097/5644.html  
159 The Council of the European Union of 15 February 2007 asked “the Commission to make proposals as soon as possible to provide for the possibility of migrating the SIS, Sirene and Vision onto the s-TESTA network by 13 November 2008, under its responsibility” (Council Decision (2007/149/EC))
new SISNET contract. These events intertwined with the Portugal proposal to extend SIS (and therefore SISNET) to the new EU Member States (See Section 2.5.4.). Concerns for possible delays in SIS II as a result of changing the topology of SISNET were expressed. Changes were nevertheless introduced. As to 2011, the extended SISNET is still operating, providing the communication infrastructure for the still growing SIS and SIRENE.

Additional Services on SISNET:
Indeed, in its ten years of life, SISNET showed characteristics of a service enabling and experimenting system. Here are two cases:

**SISNET e-mail system** "On 1 June 2004 the SISNET e-mail system, for use among Schengen entities, N-SISes and SIRENEs, came into operation. It also provides the possibility of secure exchanges of information which hitherto circulated through traditional channels such as fax, mail or internet. Types of information exchange possible include the exchange of photographs, prints or background documents for court decisions. Countries were allowed to decide between setting up their own server or use a server managed by C.SIS."  

**SIS II tests** while in the end not actually carried out, there have been ongoing discussion of experimenting C-SIS II and N-SIS II data transmission on SISNET.  

2.4. SIRENE Bureau
The SIRENE Bureaux (Supplementary Information Requested to the National /Entry Supplément d’Informations Requis à l’Entrée Nationale) is a creation of the Schengen States that was “not explicitly foreseen by the Convention. Charged with the exchange of complementary information within each Schengen State, they also act as intermediaries in the course of various State to State consultations on the attitude to adopt in the event of

---


161 “Connection of new States to SISNET” Note 12465/04 LIMITE SIRIS 92 COMIX 557

162 “E-mail on SISNET: summary of the proposal” Note 11546/03 LIMITE SIS-TECH 73 COMIX 466

163 “Connection of new States to SISNET” Note 12465/04 LIMITE SIRIS 92 COMIX 557
the execution of a SIS entry”. 164 Indeed, SIRENE Bureaux were created responding to an organizational and coordination need and affirmed themselves as “an essential feature of the SIS system, without which it could scarcely function.” 165

According to a research carried out by the Schengen Convention provisional Joint Supervisory Authority (PJSA) 166 in the initial stages of the Schengen Convention implementation, with exception of Belgium, the States then “enforcing the Convention (Germany, Spain, France, Luxembourg, the Netherlands, Portugal) did not allocate the central competency for the N.SIS to their SIRENE Bureau on the grounds of article 108, but rather created it on the grounds of a national text (France, the Netherlands, Portugal) or considered that a number of national texts on police matters or texts in relation with the Schengen Convention were sufficient to establish its juridical existence (Germany, Spain, Luxembourg)”. 167 Furthermore, the PJSA reported that, with only two exceptions, “Belgium (where the SIRENE office, as an instance with central competency for the N.SIS, is linked to the Ministry of Justice) and of Portugal (where the central instance is distinct from the SIRENE office and linked to the Ministerial Department of foreigners and frontiers of the Ministry of the Interior), the other Schengen States had entrusted the central competency for the N.SIS to their police or gendarmerie (state police corps) departments and linked their SIRENE office to these departments”. 168

Only ten years after the Schengen Convention implementation Art. 92.4 was added to it, providing a common legal basis for the SIRENE Bureaux to all Schengen States. 169 According to Art. 92.4, "Member States shall in

---

164 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
166 "The Joint Supervisory Authority was officially established upon enforcement of the Convention on March 26, 1995. Its composition is attached as an enclosure. However, under the impulse of Mr. Faber, data protection commissioner of Luxembourg and first chairman of the JSA, a provisional Joint Supervisory Authority was set up as early as the month of June, 1992 with the agreement of the Schengen ministers” (Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97).
167 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
168 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
169 Art 92.4 of the Schengen convention was added through Article 1.1. of Council Regulation (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism and Art. 2.1. of Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction
accordance with national legislation exchange through the authorities designated for that purpose (Sirene) all supplementary information necessary in connection with the entry of alerts and for allowing the appropriate action to be taken in cases where persons in respect of whom, and objects in respect of which, data have been entered in the Schengen Information System, are found as a result of searches made in this System. Such information shall be used only for the purpose for which it was transmitted”.

In practice, the SIRENE Bureaux act as the human interfaces of the Schengen Information System\textsuperscript{170}. They are “set up and designated as the single point of contact for each Schengen State in respect of SIS alerts and post-hit procedure”,\textsuperscript{171} reducing the complexity of cross border communication and coordination. In particular, the SIRENE network of national contact points carries out the exchange of additional information not included in the SIS after a “hit” has taken place. More in general, these activities “consist in consultations prior to the creation of a SIS entry, exchanges of information, surveillance of multiple entries and setting up priority orders”.\textsuperscript{172} In other terms, “The SIRENE bureau is responsible for holding supplementary information in relation to all its own national entries and making it available to the bureau of other Schengen States”.\textsuperscript{173} In this way, all offices responsible for international police co-operation, can “be accessed through a single point of contact, be contained within the same management structure and located at the same site”.\textsuperscript{174} Such contact point must be fully operational on a 24/7 basis.\textsuperscript{175} The SIRENE bureau has also the responsibility “to perform the role of data quality assurance coordinator for the information that is introduced in the SIS”.\textsuperscript{176}

\textsuperscript{170} Schengen Information System, Sirene: Recommendations and Best Practices - December 2002 -EU Schengen catalogue Volume 2, p.12
\textsuperscript{171} European Union, SCHENGEN INFORMATION SYSTEM, SIRENE: Recommendations and Best Practices, EU Schengen catalogue Volume 2, December 2002
\textsuperscript{172} Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
\textsuperscript{173} HOUSE OF LORDS, (2007) “Schengen Information System II (SIS II)”, Report with Evidence
\textsuperscript{174} European Union, SCHENGEN INFORMATION SYSTEM, SIRENE: Recommendations and Best Practices, EU Schengen catalogne Volume 2, December 2002
SIRENE Bureaux “missions and acts are defined in a concrete way in a common manual designated as ‘SIRENE manual’ ”. 177 The SIRENE Manual is an important element of coordination in the performance of SIRENE bureaux activities. It consists of a set of instructions to operators in the SIRENE bureaux of each Member State, describing “in detail the rules and procedures governing the bilateral or multilateral exchange of the supplementary information which is required to implement correctly certain provisions of the Convention of 1990 implementing the Schengen Agreement”.178 It is interesting to note that the document has needed to be frequently updated and has been only recently fully declassified (in its last version of 2011).

In the Italian case, for example, the SIRENE Bureau is part of the Service for International Cooperation, within the Central Directorate of Criminal Police of the Public Security Department of the Ministry of Interior. It is a multi-agency office, manned by personnel of the three main Italian Police Forces: Carabinieri, Polizia di Stato and Guardia di Finanza. Its main task “is to reduce the time needed for the information exchange between the Member Countries’ law enforcement agencies, without prejudice to the competence of the Interpol Service regarding the Countries which are not party to the Schengen Agreement”.179

177 Schengen Convention Joint Supervisory Authority (JSA), First Annual Activity Report, March 95-March 97
2.5. A long evolution path

While in 1995 SIS began officially to perform its tasks, this date should be seen more as a beginning of a long process of development than an end of it. This is due to several factors, including new contracting parties (States) to the Schengen Convention, changes in the political context (such as the rise of the terrorism issue in the European political agenda) and in the EU law framework, evolution of technologies, misalignments between components that needed to be worked on. The following paragraphs try to describe some of the main steps that characterized this process of development.

<table>
<thead>
<tr>
<th>SIS geographical calendar:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995: France, Germany, Luxembourg, Belgium, Netherlands, Spain and Portugal</td>
</tr>
<tr>
<td>1997: Italy (July), Greece and Austria (December)</td>
</tr>
<tr>
<td>2001: Denmark, Finland, Iceland, Norway and Sweden</td>
</tr>
<tr>
<td>2007: Czech Republic, Estonia, Hungary, Latvia, Lithuania, Malta, Poland, Slovakia, Slovenia</td>
</tr>
<tr>
<td>2008: Switzerland</td>
</tr>
<tr>
<td>2011 Liechtenstein</td>
</tr>
</tbody>
</table>

2.5.1. The first step, from SIS I to SIS I+

Starting from 1998 a more up-to-date version of the SIS was developed (SIS 1+) to allow the Nordic countries joined Schengen (Denmark, Sweden, Finland, Norway and Iceland). SIS 1+ “included the possibility of linking two or three additional countries to the system. The upgrade was also meant to improve the performance of the SIS and make it easier to manage and maintain”.

SIS1+ become operational in 2001, at the end of the SIRENE Network Phase II phase. JSA considered SIS1+ to be an improvement on the previous system in so far as compliance with the relevant data protection principles was concerned.

2.5.2. SIS II

Given some design limitations -the initial design of the SIS had not provided for the participation of more than 18 States-, and as the Schengen Area kept growing, it emerged the need for a new version of the SIS to

---

181 Schengen Convention Joint Supervisory Authority (JSA), Sixth report, January 2002 - December 2003
accommodate the inclusion of the EU’s new Member States. According to Hayes "The Schengen Executive took the decision to create SIS II in late 1996 after Italy, Austria and Greece joined the SIS. This took the number of participating state to ten – two more than originally planned – and with the prospect of up to 25 countries eventually joining it was agreed that the existing SIS simply could not cope".  

This need was also seen as an opportunity to benefit from the developments in the field of information technology and to allow for the introduction of new functionalities such as the inclusion of biometric data. 

---

182 Hayes B. “Statewatch analysis - From the Schengen Information System to SIS II and the Visa Information (VIS): the proposals explained” STATEWATCH REPORT, FEBRUARY 2004
The preparatory work on the concept of SIS II was carried out by the SIS Steering Committee and the Permanent Working Party (PWP) at the end of the 90s and the preliminary study was carried out by IBM. The JSA became involved in it by mid 1998. Following this initial work, on 6 December 2001 the Council adopted two legislative instruments (the Council Regulation (EC) No 2424/2001 and the Council Decision 2001/886/JHA), making the Commission responsible for developing SIS II and providing for the related expenditure to be covered by the general budget of the EU. The Commission published a communication [COM(2001) 720] on 18 December 2001 examining ways of creating and developing SIS II.

“The Commission launched the technical implementation in October 2004 by signing a contract with a budget of up to 40 million EUR for the development of the SIS II and the VIS (Visa Information System), which shares the same technical platform. The target date set for the delivery of the SIS II was March 2007. In parallel to the technical implementation, discussions on new requirements of the SIS have been on the agenda of the Council, which adopted a number of conclusions on the functionalities of the SIS II in 2003 and 2004. The European Parliament contributed also to the debate and expressed its views at the end of 2003”.  

To provide an appropriate legal framework describing SIS II operation and use, following studies and discussions relating to the architecture and functionalities of the future system, the Commission presented three

---

184 Schengen Convention Joint Supervisory Authority (JSA), Third Annual Activity Report, March 98 – February 99
185 These instruments were modified in 2006, extending the period of their validity until 31 December 2008.
proposals for legislative instruments in 2005. Two of the instruments in this package (Regulation (EC) No 1987/2006 of the European parliament and of the Council of 20 December 2006 on 1st pillar aspects of the establishment, operation and use of SIS II and Regulation (EC) No 1986/2006 on access to SIS II by the services responsible for issuing vehicle registration certificates) were adopted on 20 December 2006. The third instrument, Council Decision 2007/533/JHA determining 3rd pillar aspects of the establishment, operation and use of SIS II) was adopted on 12 June 2007. As a consequence, the provisions of the Schengen acquis governing SIS I+, with the exception of Article 102A of the Schengen Convention, will be replaced by Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA once they come into force. Article 102A will be replaced by Regulation (EC) No 1986/2006. In particular, in the EAW perspective, Article 31 of Council Decision 2007/533/JHA – Execution of action based on an alert on a person wanted for arrest with a view to surrender or extradition- foresee that “1. An alert entered in SIS II in accordance with Article 26 in conjunction with the additional data referred to in Article 27, shall constitute and have the same effect as a European Arrest Warrant issued in accordance with Framework Decision 2002/584/JHA where this Framework Decision applies”. In other words, while after an arrest based on an Art. 95 alert on SIS I a paper copy of the EAW must be sent from the issuing Country to the executing one, this will not be necessary any more for an Art. 95 alert on SIS II as the electronic one will be sufficient.

**SIS II Technical architecture**

SIS II high level architecture is similar to that of SIS I. Such architecture has been normatively regulated in quite some detail since an early stage of development. According to Art 4 of Regulation (EC) No 1987/2006 and of Council Decision 2007/533/JHA, SIS II is composed of a central system (Central SIS II), a national system (the ‘N.SIS II’) in each of the Schengen Member States, and a communication infrastructure connecting them. Central SIS II is composed of a technical support function (CS-SIS) containing a database (SIS II database) and a uniform national interface (NI-SIS which include a Local National Interface in each Member State and a Central National Interface securing access to CS-SIS with separate logical

187


52
access points for each State\textsuperscript{188}); CS-SIS performs technical supervision and administration functions. It is located in Strasbourg (France) and a backup CS-SIS, capable of ensuring all functionalities of the principal CS-SIS in the event of failure of this system, is located in Sankt Johann im Pongau (Austria). CS-SIS should provide the services necessary for the entry and processing of SIS II data, including searches in the SIS II database. For the Member States which use a national copy, CS-SIS should provide the online update of the national copies; ensure the synchronisation of and consistency between the national copies and the SIS II database; provide the operations for initialisation and restoration of the national copies.\textsuperscript{189}

N.SISs II consist of a national data systems which communicate with Central SIS II. An N.SIS II may contain a data file (a ‘national copy’), containing a complete or partial copy of the SIS II database. SIS II data is entered, updated, deleted and searched via the various N.SIS II systems. A national copy should be available for the purpose of carrying out automated searches in the territory of each of the Member States using such a copy. It should not be possible to search the data files of other Member States’ N.SIS II.\textsuperscript{190}

Network – Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA provide a first description of SIS II network as a Communication Infrastructure between CS-SIS and NI-SIS “that provides an encrypted virtual network dedicated to SIS II data and the exchange of data between SIRENE Bureaux”.\textsuperscript{191} The Annexes to Commission Decision 2007/170/EC\textsuperscript{192} and 2007/171/EC\textsuperscript{193} further specify that SIS II secured private communications infrastructure should be provided by the Secured Trans-European Services for Telematics between Administrations (s-TESTA). The delivery and management of such services is provided for under a Framework Contract concluded by the Commission on its own behalf and on


\textsuperscript{192} Commission Decision 2007/170/EC of 16 March 2007 laying down the network requirements for the Schengen Information System II (1st pillar)

\textsuperscript{193} Commission Decision 2007/171/EC of 16 March 2007 laying down the network requirements for the Schengen Information System II (3rd pillar)
behalf of the Council, EUROPOL and the European Railway Agency. SIS II network SOC (network operation centre) in Bratislava.

**Budget** - The cost of developing SIS II is a charge on the budget of the EU. By 2007, according to the House of Lords, a total of over €26 million had been committed to this project from the EU budget. At the time, “according to the Commission’s proposed SIS II legislation, the EU budget will be charged a further €114 million between 2007 and 2012 to get SIS II up and running.” By December 2010 the total budgetary commitments made by the Commission on the SIS II project (2002-2010) amounted to over 133 million Euros.

### 2.5.3 Some new functions for SIS I+

While SIS II began to be developed, SIS I was not static. In fact, following the security emergency related to the terrorist attacks the Spanish Government proposed important changes to increase the scope of SIS I without waiting for the roll out of SIS II. The Spanish proposal resulted in the Council Regulation (EC) No 871/2004 of 29 April 2004 and Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism. In light of the possibility to use SIS to support the fight against terrorism, existing Schengen Convention provisions were modified and new SIS functions were introduced “with respect to the current version of the SIS, in particular as far as concerns the provision of access to certain types of data entered in the SIS for authorities the proper performance of whose tasks would be facilitated were they able to search these data, including Europol and the national members of Eurojust, the extension of the categories of missing objects about which alerts may be entered and the recording of transmissions of personal data”. While not evident from changes in the system nomenclature, this step “amounted to a

---

194 (SEC(2007) 810)
197 Report from the Commission to the European Parliament and the Council progress report on the development of the second generation Schengen information system (SIS II) - July 2010 - December 2010, Note 12470/11 CATS 60 SIS-TECH 73 SIRIS 65 COMIX 434
198 COUNCIL REGULATION (EC) No 871/2004 of 29 April 2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism
fundamental departure from the basic principles of Article 102 of the Schengen Convention, which limits the use of Schengen data to the purposes laid down in each category of alert”.

2.5.4. SIS One4All

After the introduction of new functions in SIS I, and due to delay in the SIS II development and its implementation (including, in October 2006, Portugal put forward a proposal for a temporary solution to allow the SIS to be adapted to allow the participation of more than 18 States, so enabling the new EU Member States (Slovak Republic, Slovenia, Estonia, Hungary, Latvia, Lithuania, Malta, Poland and Czech Republic) to join Schengen by October 2007. “The proposal involved the ‘cloning’ of the Portuguese national system, its integration in the new Member States and subsequently their connection to the central system already in use”. The system was called SIS One4All. “The Commission believed that it would add nine months to the planning of SIS II. Nevertheless on 5 December 2006 the Justice and Home Affaire Council, after re-affirming that “the development of the SIS II remains the absolute priority”, decided to implement SIS one4all ..., and invited the Commission to present yet another revised timetable for SIS II by February 2007”. The successful implementation of SISone4all, and the positive Schengen evaluations of the new MS, allowed the lifting of internal border controls with these new countries at the end of 2007 for land and sea borders and in March 2008 for air borders. The lifting of internal border controls paved the way for implementing alternative and less risky approaches for migrating from SIS1+ to SIS II”. At the same time, “Following requests by the Member States to allow more time for testing the system and to adopt a less risky strategy for migration from the old system to the new one, the Commission presented proposals for a regulation and a decision defining the tasks and responsibilities of the various parties involved in preparing for the migration to SIS II (including testing and any further development work

199 Schengen Convention Joint Supervisory Authority (JSA), Sixth report, January 2002 - December 2003
200 http://www.epractice.eu/cases/SISone4ALL
needed during this phase). These proposals were adopted by the Council on 24 October 2008.\(^{203}\)

As time went by, though, further delay characterized SIS II development and implementation. As a consequence, “in June 2009, during JHA Council, Romania and Bulgaria presented a joint declaration regarding the common intention to connect to SIS through SISOne4ALL solution”\(^{204}\) while continuing the parallel development of national SIS II systems in order to be ready to migrate from SIS1+ to SIS II together with the other migrating Member States.\(^{205}\)

The Council decision on the application of the provisions of the Schengen acquis relating to the Schengen Information System in the Republic of Bulgaria and Romania was adopted on the 29th of June 2010, during the reunion of the UE Council on Agriculture (AGRI). The adoption of the Decision enabled the Romanian and Bulgarian authorities to enter data into the SIS.\(^{206}\)

As a consequence, both Romania and Bulgaria are now connected to the SIS and enter, update and delete national alerts in SIS as well as undertake the necessary activities in order to execute the alerts entered in SIS by other states.\(^{207}\)


\(^{204}\) http://www.schengen.mai.gov.ro/English/index07_01.htm

\(^{205}\) http://www.mvr.bg/en/Shengen/sis.htm

\(^{206}\) http://www.schengen.mai.gov.ro/English/index09.htm

2.5.5. SIS II and SIS I+R(evolution)

In parallel to the changes taking place to the functioning SIS I, The work on developing SIS II kept going. At the same time, while absolute priority to the development of SIS II was reaffirmed in several occasions by JHA\textsuperscript{208} the implementation of the SISone4ALL project impacted on SIS II schedule. As a consequence, and following invitation by the Council, the Commission drew up a revised timetable in consultation with Member States' technical experts from the Council's informal SIS II Task Force and with the Member States' delegations in the SIS II Committee. According to this new schedule, the operational date for SIS II for Member States using the SIS I+ was moved to December 2008. Only then the integration process for Member States not connected to the SIS I+ could commence.\textsuperscript{209}

As described in Section 2.5.2., by the end of 2007, provisions for the establishment, operation and use of SIS II (Regulation (EC) No 1987/2006;

\textsuperscript{208} Revised Global SIS II schedule in light of the SISone4ALL implementation, 5780/07 LIMITE SIRIS 17 COMIX 98 Brussels, 29 January 2007
\textsuperscript{209} Revised Global SIS II schedule in light of the SISone4ALL implementation, 5780/07 LIMITE SIRIS 17 COMIX 98 Brussels, 29 January 2007
Council Decision 2007/533/JH) and for the network requirements (Commission Decisions 2007/170/EC and 2007/170171/EC) under 1st and 3rd pillars had been adopted. At the same time, a comprehensive test of SIS II needed to be set out, conducted by the Commission together with the Member States, and validated by the preparatory bodies of the Council, confirming that the level of performance of SIS II is at least equivalent to that achieved with SIS 1+. The test scope and organisation were specified by Council Decision 2008/173/EC211 and Council Regulation (EC) No 189/2008,212 which foresaw also the obligation for the commission to draw up interim and final test status reports. Furthermore, a legal instrument to govern the migration from SIS I+ to SIS II environment was also required. This instrument, provided in October 2008 by Council Regulation (EC) No 1104/2008213 and by Council Decision 2008/839/JHA214 required that an ‘interim migration architecture’ for the Schengen Information System were to be established and tested in order to better manage the potential difficulties brought about by the migration from SIS 1+ to SIS II. The interim migration architecture was to have no impact on the operational availability of SIS 1+. A converter (a technical tool to allow consistent and reliable communication between C.SIS and Central SIS II) was to be provided and kept updated by the Commission. The migration legal instrument had an expiration date on 30 June 2010.

While this normative implementation framework was being developed, the technological development encountered significant problems, in particular in the development of SIS II central system.215 This resulted in a delay of the schedule and the need to prevent the expiry of the migration legal provisions.

212 Council Regulation (EC) No 189/2008 of 18 February 2008 on the tests of the second generation Schengen Information System (SIS II)
213 Council Regulation (EC) No 1104/2008 of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)
214 Council Decision 2008/839/JHA of 24 October 2008 on migration from the Schengen Information System (SIS 1+) to the second generation Schengen Information System (SIS II)
Furthermore, “failure of the main development contractor to pass the Operational Systems Test (OST) in December 2008”\textsuperscript{216} triggered both an analysis-and-repair period and comprehensive architectural review (which pointed out that the system components were “over-engineered and capable of simplification”\textsuperscript{217}), both the exploration of “an alternative technical scenario for developing SIS II based on SIS 1+, known as ‘SIS 1+ renewal and evolution’ (SIS 1+ RE)”.\textsuperscript{218}

In order to improve the involvement of the Member States, “as the project moved into a new phase, a global SIS II programme management approach was introduced in January 2009, as recognised by the Council on 26-27 February”.\textsuperscript{219} Furthermore, the Council on 26-27 February 2009 requested the Presidency and the Commission\textsuperscript{220} to submit a report containing an in-depth assessment and comparison of both scenarios. As both project were judged technically feasible the Council concluded on 4-5 June that the development of SIS II was to continue on the basis of SIS II project and that SIS 1+ RE was going to be retained as the contingency plan. The Council also agreed to two project milestones to test the stability, reliability and performance of the central SIS II and the proper functioning of vital core functionalities after significant development phases of SIS II project.\textsuperscript{221} Contracts with SIS II contractors had to be renegotiated to

\textsuperscript{216} Report from the Commission to the European Parliament and the Council on the development of the second generation Schengen Information System (SIS II) - Progress Report January 2009 - June 2009
\textsuperscript{218} Report from the Commission to the European Parliament and the Council on the development of the second generation Schengen Information System (SIS II) - Progress Report January 2009 - June 2009
\textsuperscript{219} Report from the Commission to the European Parliament and the Council on the development of the second generation Schengen Information System (SIS II) - Progress Report July 2009 - December 2009. Furthermore, “the Council of 4-5 June invited the Commission to build upon the experience and lessons learned from this management structure and develop it further. These management changes have been consolidated in the legislative proposal for a Regulation to amend the migration instruments” (ibidem).
\textsuperscript{220} in close cooperation with the SIS II Task Force, and in consultation with the appropriate instances (Report from the Commission to the European Parliament and the Council on the development of the second generation Schengen Information System (SIS II) - Progress Report January 2009 - June 2009)
\textsuperscript{221} Report from the Commission to the European Parliament and the Council on the development of the second generation Schengen Information System (SIS II) - Progress Report January 2009 - June 2009
include milestones non-compliance as resolutive conditions. Furthermore, France negotiated a contract for the replacement of obsolete components of SIS 1+ (and optionally extendable for SIS 1+RE), which could not be used beyond September 2010.

Another element that needed to be considered was the significant increase in the number of alerts. In 2009, “From the 22 million alerts originally foreseen, the latest estimates predict[ed] 73 million alerts in the foreseeable future” and in 2010 an estimated size SIS II at go live of 52 million alerts. This required new system capacity specification, an intensive work on requirements and the redefinition of SIS II schedule. A new expiry date was therefore introduced by Council Regulation (EU) 541/2010 amending Regulation (EC) no 1104/2008 and Council Regulation (EU) 542/2010 amending Decision 2008/839/JHA. At the same time, “process of refining the requirements did not modify the core obligations stemming directly from the SIS II legal instruments”.

This further delay resulted also in secondary repercussions such as the temporary suspension of the back-up local national interfaces (to be re-activated at a later stage, prior to go-live) to reduce costs.

---

By the end of 2010, the Commission states that “the significant technical and political uncertainties over the future of the SIS II project that characterised the beginning of 2010 have progressively been addressed in the course of the year. This intensive work culminated with the successful outcome of the first milestone test, the consensual definition of final requirements for the system to go live and the conclusion of the corresponding contractual framework. These positive developments all contributed to bringing the SIS II project back on track with a clear and shared vision on the remaining phases of the project, as well as a realistic schedule and an adequate budgetary plan to complete the work outstanding”.228

On a final note, Regulation (EU) No 1077/2011 of the European Parliament and of the Council of 25 October 2011 established a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice to be responsible for the operational management of Central SIS II and certain aspects of the communication infrastructure.

**UK SIS Experience**

When the Schengen acquis was integrated into the legal framework of the EU by a Protocol to the Amsterdam Treaty in 1999, the United Kingdom gained the possibility to request participation in all or part of that acquis, subject to approval by the unanimous consent of the Schengen states. To that end, the United Kingdom requested and gained approval in 2000 to participate in all of the Schengen acquis provisions concerning criminal law and policing (except for cross-border hot pursuit by police officers). This also entailed participation in the SIS, as regards criminal law and policing information, but not the SIS immigration data, concerning the list of persons to be denied entry into the Schengen States. The Schengen provisions in which the United Kingdom had been given permission to participate were put into effect for this country from 1 January 2005. The United Kingdom should have been ready to be linked to the SIS database by late 2004, however, it failed to connect to the system. According to Home Office officials, the connection proved impossible due to technical difficulties and “acts of God”, such as a fire which destroyed some equipment.

---

228 Report from the commission to the European Parliament and the Council progress report on the development of the second generation Schengen information system (SIS II) - July 2010 - December 2010 - 12470/11 CATS 60 SIS-TECH 73 SIRIS 65 COMIX 434
The Home Office assessment in October 2005 was that SIS I connection for the United Kingdom would not have been achieved by the time SIS II would have been delivered for the rest of the Member States. Ministers decided that efforts should be concentrated on delivering SIS II to a properly robust programme and timetable. The United Kingdom's aspiration was to join SIS II in 2009. As a consequence, and due to the SIS II delays, still in 2011 the United Kingdom does not participate in the current SIS.

(Source: HOUSE OF LORDS, (2007) "Schengen Information System II (SIS II)", Report with Evidence)

2.6. Outside of the box: e-CODEX EAW and Secure communication in cross border criminal matters

The following paragraphs briefly address two deficit sources in the EAW-SIS supported assemblage: National level ICT tools not always adequate and lack of justice sector technologies for cross border cooperation in the criminal sector.

As to the first point, important deficits have been detected in some of the EAW mutual evaluation visits "with regard to the use of database equipment and IT tools adapted to the EAW. The exercise reveals that a centralised reliable system able to provide complete, up-to-date and easily accessible dedicated information on the operation of the EAW does not exist in a number of Member States. This flaw extends on occasion to other kinds of information relevant to EAW procedures (e.g. pending criminal proceedings). Examples of the introduction of case management systems adapted to the specific needs of EAW procedures were recorded during the evaluation, although this does not seem to be general practice. The positive impact of those tools on the functioning of the system as a whole (production of reliable statistics, improvement of analytical capabilities) and on the management of EAW cases (monitoring of deadlines, compliance with undertakings, provision of information to foreign counterparts, operation of the speciality rule) was constantly highlighted by the experts". 229.

As to the second point, during the EAW evaluation exercise many of the judicial "authorities interviewed stressed the lack of appropriate communications with their foreign counterparts throughout the EAW procedure. Complaints were repeatedly recorded that the level of communication regarding the progress of EAW proceedings is unsatisfactory.

229 "Final report on the fourth round of mutual evaluations - The practical application of the European Arrest Warrant and corresponding surrender procedures between Member States” 8302/4/09 REV 4 LIMITE CRIMORG 55, COPE 68, EJ 24, EUROJUST 20 p.23
... According to some evaluation reports, these flaws often extend to the timely communication of the surrender dates, and to the requirement to provide, at the time of the surrender, precise information on the total period of detention served by the requested person in the executing Member State on the basis of the EAW". 230 It should be noted that, while supporting a judicial procedure, the SIS is not managed by judicial authorities but by police and security authorities.

While the National level ICT tools adequacy issue needs to be addressed primarily at Member State level, the lack of justice sector technologies for cross border cooperation in the criminal sector is presently been addressed within the first European Large Scale Pilot in the domain of e-Justice, e-CODEX (e-Justice Communication via Online Data Exchange).231 The goal of e-CODEX is to improve the cross-border access of citizens and businesses to legal means in Europe as well as to improve the interoperability between legal authorities within the EU. More in detail, the project aims to develop true operational electronic services supporting cross border legal procedures in five use cases: European Payment Order (EPO) and Small Claims, European Arrest Warrant (EAW), Secure cross-border exchange of sensitive data, and Mutual recognition of financial penalties.

European Arrest Warrant and Secure cross-border exchange of criminal data use cases, in particular, are aimed at providing a technological

---

230 “Final report on the fourth round of mutual evaluations - The practical application of the European Arrest Warrant and corresponding surrender procedures between Member States” 8302/4/09 REV 4 LIMITE CRIMORG 55, COPE 68, EJ 24, EUROJUST 20 p.20

231 [http://www.e-codex.eu/](http://www.e-codex.eu/) e-CODEX is an EU co-funded project (Ref. CIP-ICT PSP 2010 no 270968). The project started in December 2010 and will end in December of 2013. The project is carried out by 18 partners either being or representing their national ministries of justice of 15 European countries, plus the Council of Bars and Law Societies of Europe (CCBE) and the Conseil des Notariats de l’Union Européenne (CNUE). More in detail, The project is coordinated by the Justizministerium des Landes Nordrhein-Westfalen (JM NRW) GERMANY, and sees the participation of: Bundesministerium für Justiz Österreich (BMJ Austria) AUSTRIA; Federal Public Service Justice (MoJ Belgium) BELGIUM; Fedict Belgium (Fedict Belgium) BELGIUM; Ministry of Justice of the Czech Republic (MoJ Czech Republic) CZECH REPUBLIC; Ministry of Justice (MoJ Estonia) ESTONIA; Ministry of Justice France (MoJ France) FRANCE; Aristotelio Panepistimio Thessalonikis (AUTH Greece) GREECE; Italian Ministry of Justice - Directorate General for IT (MoJ Italy) ITALY; Malta Information Technology Agency (MJHA/MITA Malta) MALTA; Ministerie van Justitie (MoJ Netherlands) NETHERLANDS; Instituto das Tecnologias de Informação na Justiça (MJ - ITIJ Portugal) Portugal; Ministry of Communications and Information Society (MCSI Romania) ROMANIA; Spanish Ministry of Justice - Directorate General for Modernization of Justice Administration (MJU Spain) SPAIN; Ministry of Public Administration and Justice (KIM Hungary) HUNGARY; IT Department of the Ministry of Justice of Turkey (MoJ Turkey) TURKEY; Council of Bars and Law Societies of Europe (CCBE) BELGIUM; Conseil des Notariats de l’Union Européenne (CNUE) BELGIUM
infrastructure to support judicial cooperation activities in criminal matters that so far have been decoupled from SIS (even if occasionally supported by it) as pertaining to the domain of cross-border judicial authority to judicial authority data, information and document exchange and not to the one of police and security. The systems are conceived as operating separately from SIS. The European Arrest Warrant pilot focuses on the transmission between executing and issuing judicial authorities of 1) electronic European Arrest Warrant requests and documents related to the surrender decision and 2) the information for the actual surrender of the subject to the issuing Member State. It is considered that if the experience is successful, in the future it could be extended to the exchange of other judicial sensitive documents. Secure cross-border exchange of criminal data is addressed more in general to support judicial cross-border data exchange (as provided for by the Council Decision 2005/671/JHA).  

High level and common functional requirements (what the ICT systems are supposed to do) and non functional requirements (how they are supposed to be), and overall systems specifications have been identified through a process of negotiation between the project partners and with the support of national subject matter experts (both in the ICT field, both in the formal and actual judicial procedures). Key external actors such as Eurojust have been involved in the process. Test scenarios for the piloting of each use case have been designed.  

From a governance perspective, the project has been so far quite challenging. While finding alternative technical solution has not so far being problematic, their implications in relation to national and EU norms and their interpretation create complex entanglements, which need to be solved. High-level architectural decisions have required much negotiation and discussion, both the creation of specialized sub-groups focusing on specific issues. Furthermore, quite some effort was required in order to bringing together the right people, with the needed technical, legal and organizational competences (ranging from specific branches of National and EU law, to XML, to the empirical functioning of the selected cross border procedures).

### 2.6.1. e-CODEX High Level Architecture

Member States have already established ICT solutions in the justice domain, solutions that respond to specific requirements of national legal systems,

---

233 From e-CODEX D7.3 High Level Architecture Definition V0.2
and which implied considerable investments in terms of financial and human resources. As “these national solutions ... cannot simply be replaced in favour of new, centralised approaches”\textsuperscript{234} e-CODEX builds on the idea of creating an interoperability layer for the electronic exchange of data and documents between the existing European national information systems and infrastructures. Accordingly, “e-CODEX ... should not be a new centralised approach or duplication of any national solution at the European level”.\textsuperscript{235} Furthermore, given the size, complexity, cost and independent evolution of such national systems, feasibility and evolvability reasons suggested to avoid, wherever possible, attempting their modification in order to fit e-CODEX needs.\textsuperscript{236} What e-CODEX wants to create, therefore, is an e-Delivery platform based on a multilateral solution in which all parties agree to common e-CODEX interoperability standards.\textsuperscript{237} The choice of a multilateral solution avoids the need to implement bilateral arrangements as this would “create the need for the maintenance of a multitude of solutions and agreements” \textsuperscript{238} and increase complexity. In practice, the e-Delivery platform exchanges data and documents that are translated from sending national format to e-CODEX format and then again to receiving national format.

One of the key concepts adopted by E-CODEX to achieve such simplification is the creation of a ‘circle of trust’ between the judicial authorities involved. This circle of trust should provide the basis for the Judicial authorities to trust the information provided through e-CODEX. In other words, E-CODEX works on each Member State trust of other Member States on issues such as confidentiality, eIdentification, eSignature, eDocuments, ePayment and transport.\textsuperscript{239} So, for example, “through the use of the ‘circle of trust’ the responsibility of verifying the signature lies with the sending country. The process does not have to be repeated in the receiving country”.\textsuperscript{240} As e-CODEX analysis has shown, without such circle

\textsuperscript{234} e-CODEX Technical Annex V.1.1 p.11
\textsuperscript{235} e-CODEX Deliverable 4.2 Concept for Implementation of WP4 (Pilots authentication and signature specifications) p-13
\textsuperscript{236} e-CODEX Deliverable 7.1 Governance and Guidelines Definition p.10
\textsuperscript{238} e-CODEX Deliverable 7.1 Governance and Guidelines Definition p.30
\textsuperscript{239} e-CODEX Deliverable 7.1 Governance and Guidelines Definition p.10
\textsuperscript{240} e-CODEX D7.3 High Level Architecture Definition V0.2 p.20
of trust, the complexity of the task would be too high to be managed in order to produce a working solution. 

In line with its exchange nature, and quite differently from SIS, the e-CODEX system is not designed for the storage of data and documents but only for the transport of messages. As a consequence, after a successful message transmission, the message is deleted and only the log information is stored for statistical purposes. \(^{241}\)

---

241 e-CODEX D7.3 High Level Architecture Definition V0.2 p.16

---

Figure 5 – e-CODEX High level architecture schema Source: e-CODEX D7.3

The above picture provides a simplified representation of e-CODEX high-level architecture, including the main actors, components and of their interconnections. In essence, e-CODEX allows the electronic exchange of data and documents between the main actors of cross border judicial activities (e-CODEX users). The representation applies to all use cases that have been selected for the piloting phase of the project.

E-CODEX infrastructure allows an e-CODEX user to submit files, data and documents. The e-CODEX users for civil cases are typically the claimant, the defendant, their lawyers and the court of origin. While for simplicity claimant and defendant (and respective lawyers) in Figure 4 appears to be
in the same Country (A), this is not usually the case. In the criminal cases users can be public prosecutors, judges, lawyers or even members of the police forces.

The e-CODEX includes four main building blocks: the e-CODEX Service Provider, the e-CODEX Connector, the e-CODEX Gateway and the e-CODEX Transport Infrastructure.

An e-CODEX user creates, submits and receives his/her files though his/her national system (i.e. the national solution which allows e-filing of national cases which has been adapted to satisfy e-CODEX requirements or an ad-hoc solution) or through the e-Justice portal. Such systems, for the purpose of e-CODEX are defined and act as e-CODEX Service Providers. In order to be an e-CODEX service provider a system must be able to deliver a service in conformity with e-CODEX standards (security standards, privacy...) in the field of e-justice and be connected to an e-CODEX gateway through an e-CODEX Connector of an e-CODEX member. An e-CODEX Service Provider can be a governmental solution or a private solution (the figure below provides an example of the Austrian governmental solution). In other words, depending on the use case, or on the role of the user, these e-CODEX service provider can be a national application maintained by the participating country’s government, the e-Justice portal or another application used by legal professionals.\(^{242}\) In order to be connected, the system must undergo an audit from the MS owner of the gateway.\(^{243}\)

---

**Figure 6 - Example of Backend Integration (Austrian case).** In the representation eCODEX Gateway represent both e-CODEX Gateway and Connector. Source: e-CODEX D5.3

The e-CODEX Connector performs two main functions: 1) the e-CODEX Connector transform the outgoing documents received from the e-CODEX

---

\(^{242}\) D3.3 Documented System Requirements and Specifications

\(^{243}\) Cf. D7.2 Requirements Finalisation & D3.2 Described Test Scenarios
Service Provider from the national standard to the e-CODEX standard and add a trust-ok token to the documents. The trust-ok token provides the results of electronic signature verification or a statement guaranteeing that the document was issued by a system that is capable of identifying the user and that ensures that the document is uniquely linked to the user and is created using means that the user can maintain under his control and any subsequent change of the data is detectable. According to the principle of the circle of trust, the responsibility for the implementation and the control of those characteristics lies with the Member State whose party to a procedure uses the system. The receiving country can then trust the documents and is not required to validate them again. 2) The e-CODEX Connector transforms the incoming documents received by the national e-CODEX gateway from the e-CODEX standard to the national standard, and it verifies the trust-ok token. The e-CODEX Connector is to be built by each piloting Member State.

The e-CODEX Gateways are national (and the e-Justice portal) “channels” or systems for data transmission between two communication partners. The gateways are required to fulfil specific security requirements within their operation but also for the communication with others. They perform different functionalities, such as establishing a connection to other gateways and connectors, format the content of a message to be sent to the eBMS3.0 standard and extract the contents of a received eBMS3.0 message, providing a transport signature and providing a timestamp for outgoing messages and checking of the transport signature, providing of a timestamp and sending of an acknowledgment of receipt for incoming messages. Each e-CODEX member is responsible for its e-CODEX Gateway. The standard e-CODEX Gateway component is in the process of being built up by e-CODEX Work Package 5 (Transportation) “on an already existing open source product called Holodeck, consisting of a list of AXIS Modules and some basic functionalities on top […]. Additionally there will be some extensions provided by e-CODEX”. The e-CODEX Transport Infrastructure is responsible for the secure and reliable transport of data and files from one e-CODEX gateway to another. It has been decided to adopt a decentralized architecture. If a technical need will emerge in the future, a central hub will then be introduced. To

244 D3.3 Documented System Requirements and Specifications
245 e-CODEX Deliverable 5.3 Concept of Implementation v0.9, p.
246 The e-CODEX Connector might perform protocol and semantic translations. Member States are free to decide at what stage in their infrastructure they will perform these actions if they are necessary at all.
247 D 4.2: Concept for Implementation of WP4
248 e-CODEX Deliverable 5.3 Concept of Implementation v0.9, p.64
allow access to all potential users, the system will use the Internet with encryption to ensure a secure connection. Further investigations on s-Testa from legal and technical perspective should be done. The final solution should be able to run over any IP network including s-Testa. In principle, the e-CODEX Transport Infrastructure will be “content agnostic, however it remains to be discussed if delivery evidences are business documents and therefore part of the content (the payload) or if they are rather an integral part of the transport infrastructure”.  

From a technical perspective, e-CODEX transport solution is based on ebMS V3.0, extended by the convergence concept that has been developed by e-CODEX together with other Large Scale Pilots, in particular SPOCS and PEPPOL. Evidences and evidence format necessary for the data exchange are based on ETSI REM standard. For the addressing of the gateways, the possibility to use a dynamic system to discover the corresponding gateway and its capabilities along the concept developed in PEPPOL has been considered. However, as a short-term solution for the piloting, e-CODEX will use a static addressing solution “as is available in out-of the box ebMS messaging products (e.g. in the OS solution Holodeck), while working on the topic of dynamic discovery in parallel”.  

According to the initial planning, the identification of the competent court was supposed to take place through the European Court Atlas provided by the EU e-Justice Portal. However, due to the un-readiness European Court Atlas, it has been decided to provide national web-services for identify the competent court for the pilot proceedings.  

---

249 D5.2 Reusable Assets  
250 ebMS stands for Electronic Business using eXtensible Markup Language (ebXML) Messaging Services. ebXML is commonly known as e-business XML. The ebMS specification defines the technical interconnection, including security standards and the message structure (e-CODEX D7.3 High Level Architecture Definition V0.2 p.14).  
251 Simple Procedures Online for Cross- Border Services (http://www.eu-spocs.eu/)  
252 Pan-European Public Procurement Online (http://www.peppol.eu/)  
253 The gateways communicate in a peer-to-peer like model across the internet and discover partner gateways and their routing addresses via the SML/SMP infrastructure (e-CODEX Deliverable 5.3 Concept of Implementation v0.9, p.45)  
254 e-CODEX Deliverable 5.3 Concept of Implementation v0.9, p.14  
255 e-CODEX Deliverable 5.3 Concept of Implementation v0.9, p.48  
256 e-CODEX Deliverable 5.3 Concept of Implementation v0.9 p.15
As payment of court or other fees can be required by the procedure, e-CODEX addresses the issue. While apparently simple, also this aspect is a source of complexity as the various Member States have different ways to handle e-payment. To cope with this complexity, pilot solutions will "vary from direct debit handling outside the e-CODEX process to online payment done with a national system parallel to the e-CODEX process and handing over the payment receipt to the e-CODEX process". 257

A representation of the electronic cross border judicial communication exchange process supported by e-CODEX is provided in the swim lane diagram below:

---

257 e-CODEX Deliverable 5.3 Concept of Implementation v0.9 p.14
Figure 8 – High level use cases scenario. Source: D7.2 Requirements Finalisation & D3.2 Described Test Scenarios
3. The EAW in action in Italy

3.1. Issuing an EAW in Italy

In Italy in order to issue an EAW both for the prosecution of a crime and for the enforcement of a sentence, there should be evidence that the requested person is, resides, or is domiciled in the territory of one of the EU Member States. The *Vademecum* drafted by the Ministry of Justice to support the EAW implementation suggests the application of the *principle of proportionality* to issue an EAW. The judge or the public prosecutor should assess the gravity of the crime, the personality of the perpetrator, the amount of the punishment and the duration of the precautionary measure, also in consideration of the expiry of the terms of the phase. They should also consider the large amount of resources that the enforcement of the arrest warrant requires.

The competent authority to issue an EAW during the investigation and trial phases is the judge who issued the domestic arrest warrant (precautionary measure of prison custody or house arrest). According to our interviews (and in line with the EAW FD) EAWs are not issued for investigative purposes. In general, the request/draft of the EAW is prepared by the public prosecutor of the public prosecutor offices attached to the first instance Court or to the Court of Appeal who is following the case and who has all the required information to fill the EAW. In prosecution cases, the issue of an EAW requires the existence of a domestic arrest warrant, which, according to art. 280.2 of the Code of Criminal Procedure, can be imposed only for offences which are punishable with maximum imprisonment of four years or more. If the request is approved and signed by the judge, copy of the EAW (with eventual additional documents attached to it) is sent to the Ministry of Justice and, frequently, also directly to SIRENE and INTERPOL. While according to Art 9 of the EAW FD, “When the location of the requested person is known, the issuing judicial authority may transmit the European arrest warrant directly to the executing judicial authority”,\(^{258}\) also in this case the EAW is usually transmitted through the Ministry of Justice. After receiving the EAW, the Ministry of Justice faxes the EAW to SIRENE for issuing a SIS Alert 95 and to INTERPOL for the diffusion to “EAW Countries” which are not included in SIS. In a few occasions in the past it happened that the request of issuing a SIS Alert 95 was sent by the issuing judicial

\(^{258}\) Art 9 of the EAW Framework Decision
authority to the SIRENE Bureau without informing the Ministry of Justice. For this reason the SIRENE Bureau now alerts the Ministry of such events. The competent authority to issue an EAW for the enforcement of a sentence is the public prosecutor attached to the court that issued the arrest order (Ordine di Esecuzione e Carcerazione). According to the Vademecum, an EAW is issued when there is a sentence of at least one year of actual imprisonment. In practice, given the Italian suspension regimen, the sentence must be of at least 3 years imprisonment. Article 656 of the Italian code of criminal procedure describes three tracks to be followed for the execution of detention sentences: the first track includes cases with a remaining sentence to be served of more than three years (six years in some specific cases). In these cases the public prosecutor issues the arrest order. The second track includes cases with a remaining sentence to be served of less than three years (six years in some specific cases), for which the public prosecutor issues the arrest order with suspension (Ordine di Esecuzione Carceraria con Sospensione). Finally, the third track includes all cases sentences of less than three years for which the suspension is not issued (these are the cases included in art. 656.9).

Again, if an EAW is issued, a copy of the EAW is usually sent/faxed to the Ministry of Justice and to the SIRENE Bureau (and to INTERPOL). As this is not always the case, as a rule the Ministry of Justice faxes the EAW to the SIRENE Bureau for issuing a SIS Alert 95 (and to INTERPOL for the diffusion to “EAW Countries” which are not included in SIS). At the same time, the SIRENE Bureau keeps informed the Ministry of justice of requests received directly by the issuing judicial authority.

If the requested person is wanted for the execution of more than one sentence, the public prosecutor must fill one EAW form for each sentence and inform the SIRENE Bureau about which sentence to use in order to issue the Alert, as SIS allows the entry of just one Alert per person. In general, it is inserted the “main” sentence. When the requested person is localized/arrested, the SIRENE Bureau informs the executing Member State of the existence of more than one sentence and of a plurality of EAWs. As a

---

259 the public prosecutor through the judge indicated in article 665 of the code of criminal procedure who issued the order to execute the custodial sentence of at least one year mentioned in article 656 of the same code, provided that its execution is not suspended (i.e. first offence); the public prosecutor identified in accordance with article 658 of the code of criminal procedure as far as the execution of detention orders is concerned

consequence of the principle of speciality, when more than one EAW exists for the same person, it is necessary that the executing judicial authority decides for the surrender on each one of them. When the surrender takes place, only the sentences for which the EAW has been approved can be enforced. It is still possible, though, to ask to the person surrendered to renounce to the speciality clause or, to submit/resubmit an EAW to the executing Member State for the sentences for which surrender has not been granted.\(^{261}\)

As a consequence of both normative restraints and *Vademecum* persuasive reasoning, Italian judges and public prosecutors, typically issue EAWs only in “serious cases” such as terrorism, organised crime, murder, rape, large drug smuggling etc. The existence of other EAWs issued by Italian courts is not checked by the Italian authority issuing an EAW. Checks are made both by the Ministry of Justice and by the SIRENE unit. The SIRENE unit and the Ministry of Justice alert each other that the EAW has already been issued for the same person.

The task to assist the competent judicial authorities and the responsibilities for the administrative transmission and reception of European arrest warrants, as well as for all other official correspondence related, is delegated by the Minister of Justice (designed as the central authority by the Italian Law 69/05 Art 4. transposing Art. 7 of the Framework Decision, see section 1.2.2 of the present report) to the Directorate for International cooperation (Ufficio II) within the Directorate General for Criminal Justice.\(^{262}\)

The *Ufficio II* keeps records of all incoming and outgoing EAWs sent from the courts. When an EAW is received from an Italian court (generally the first communication takes place by post or by fax) a case file is created. This file will collect all the documents related to the case sent or received by the *Ufficio II* from then on.

If the location of the person is not known and there is not a suspicion that the person is outside the Italian border, often a SIS Alert 98\(^{263}\) (or SIS Alert


\(^{262}\) The Directorate for International cooperation is located in Rome within the Ministry of Justice building. Directorate is organized in 4 units: EAW, rogatory assistance, extradition and transfer of prisoners and bilateral negotiations.

\(^{263}\) According to Art. 98 of the Schengen Agreement (Chapter on Operation And Use Of The Schengen Information System):

Art. 98
1. Data on witnesses, persons summoned to appear before the judicial authorities in connection with criminal proceedings in order to account for acts for which they are being prosecuted, or persons who are to be served with a criminal judgment or a summons to report in order to serve a penalty involving deprivation of liberty shall be entered, at the request of the competent judicial authorities, for the purposes of communicating their place of residence or domicile.

2. Information requested shall be communicated to the requesting Party in accordance with national law and the Conventions in force on mutual assistance in criminal matters.

264 According to Art. 99 of the Schengen Agreement (Chapter on Operation And Use Of The Schengen Information System):

Art. 99
1. Data on persons or vehicles shall be entered in accordance with the national law of the Contracting Party issuing the alert, for the purposes of discreet surveillance or of specific checks in accordance with paragraph 5.

2. Such an alert may be issued for the purposes of prosecuting criminal offences and for the prevention of threats to public security:
   (a) where there is clear evidence that the person concerned intends to commit or is committing numerous and extremely serious criminal offences; or
   (b) where an overall assessment of the person concerned, in particular on the basis of past criminal offences, gives reason to suppose that that person will also commit extremely serious criminal offences in the future.

3. In addition, the alert may be issued in accordance with national law, at the request of the authorities responsible for national security, where there is clear evidence that the information referred to in paragraph 4 is necessary in order to prevent a serious threat by the person concerned or other serious threats to internal or external national security. The Contracting Party issuing the alert shall be obliged to consult the other Contracting Parties beforehand.

4. For the purposes of discreet surveillance, all or some of the following information may be collected and communicated to the authority issuing the alert when border checks or other police and customs checks are carried out within the country:
   (a) the fact that the person for whom or the vehicle for which an alert has been issued has been found;
   (b) the place, time or reason for the check;
   (c) the route and destination of the journey;
   (d) persons accompanying the person concerned or occupants of the vehicle;
   (e) the vehicle used;
   (f) objects carried;
   (g) the circumstances under which the person or the vehicle was found.
   During the collection of this information steps must be taken not to jeopardise the discreet nature of the surveillance.

5. During the specific checks referred to in paragraph 1, persons, vehicles and objects carried may be searched in accordance with national law for the purposes referred to in paragraphs 2 and 3. If the specific check is not authorised under the law of a Contracting Party, it shall automatically be replaced, for that Contracting Party, by discreet surveillance.

6. A requested Contracting Party may add to the alert in the data file of its national section of the Schengen Information System a flag prohibiting, until the flag is deleted, performance of the action to be taken on the basis of the alert for the purposes of discreet surveillance or
an Alert 95 are then issued. While a SIS Alert 98 (99) is filed at local level, Alerts 95 are issued only by the SIRENE unit. When receiving an EAW issued by an Italian judicial authority, the SIRENE Bureau in Rome (Italy) provides to fill the A+M forms and enter the data in SIS translating the needed information from Italian to English. The translation is typically made by the operator entering the data. All SIRENE personnel typically speak English at a fair-good level. During the interviews, it was noted though that the task of translating is both delicate and time-consuming, and this may generate problems with the growing number of cases that the division is facing. Direct interaction between the public prosecutor/judge following the case and SIRENE may take place in order to better respond to the requirements of the case (i.e. particularly urgent, missing relevant information, ambiguities to be solved to allow a correct translation and the issuing of the Alert etc.). While “an EAW can be issued for several offences at the same time, as long as they are covered by the same domestic arrest warrant or conviction”, 265 the SIS alert 95 must refer only to the main offence. This may generate problems in the data enter. All incoming and outgoing messages and documents are recorded in a secure electronic repository.

If the decision at the basis of the EAW is reviewed or retracted, the EAW and the SIS Alert should be retired. It happens though that SIRENE is not notified. As a consequence of the missed notification, the Alert originally inserted in the SIS appears as being valid. This may give rise to substantial problems. For example, as also noted during the Italian EAW Council of EU peer review, “a person who has been apprehended in Italy and who is subsequently put on trial, without this being communicated to SIRENE, may after his or her release again be detained in a different locality or in a different Member State. Police and/or judicial time is thus wasted, and it could also give rise to possible allegations of breaches of the law by the executing authority with regard to incorrect data being inserted in the SIS”. 266

---


266 Council of the European Union (2009) Evaluation report on the fourth round of mutual evaluations “the practical application of the European arrest warrant and corresponding surrender procedures between member states” Report on Italy, 5832/1/09 REV1 p.20
Foreign SIRENE Bureaux may ask to flag the Art.95 alert in relation to their State. As previously mentioned, a flagged alert is considered as being issued for the purpose of communicating the place of residence of the person concerned. An issue that has arisen in the EAW evaluation reports “is the scrutiny and flagging in the SIS of alerts for arrest for surrender purposes without the matter being put before the competent executing judicial authority for consideration. This is a major issue for the operation of the EAW, since the flagging of an alert may de facto amount to non-execution of the underlying EAW”.  

After a person has been localized/apprehended in another EU country, the SIRENE Bureau is typically alerted through a Form G sent by the national SIRENE Unit of the Country in which the person has been localized/apprehended. Additional information may be required by the foreign authority. If available, the Office directly provides it through the use of L and M forms. Furthermore, the SIRENE Bureau inform the Ministry of Justice and the issuing authority about the need to provide the translation of the EAW within the required time limit, as well as to provide for eventual additional information asked form the foreign authority. The Ministry of Justice or the issuing judicial authority may also be contacted directly by the foreign authority once the requested person has been apprehended in one of the EU countries. The translation of the EAW is made by the Ufficio II of the Ministry of Justice. English, French, German and Spanish translators are available internally. For other languages the Ufficio II must resort to the services of external translators. As it was noted during the interviews at the ministry personnel, this may generate problems, especially in case of countries with very tight deadlines for the transmission of the official translation. Additional information may be requested by the foreign authority, both in order to evaluate the need for detention measures and to decide on the surrender.

If the surrender is granted, Interpol organizes the transfer of the person, who is arrested by the Frontier Police when passing the border or at the national airport. The Alert 95 is revoked out. In case the surrender is not granted, the foreign authority requires the Italian SIRENE unit to Flag the Alert for that country. The Alert though is still valid for all other SIS countries. Furthermore, the issuing authority may issue a new EAW.

267 “Final report on the fourth round of mutual evaluations - The practical application of the European Arrest Warrant and corresponding surrender procedures between Member States” 8302/4/09 REV 4 LIMITE CRIMORG 55, COPE 68, EJ 24, EUROJUST 20 p.17
268 Matching an alert (HIT)
269 Form L corresponds to “Supplementary information on a person’s identity”
concerning the same person which results in a new Alert for the same person which is valid also in that country. Provisional detention time limits, ranging in general between three months and one year (calculated including the detention period matured abroad) may result in the person being released just after the surrender or even in the retirement of the surrender request, while the procedure is being decided in the executing country. In one of the interviews emerged how three persons requested for participation in terrorist acts were physically surrendered just the day before the provisional detention time limit of the phase of the proceeding.

3.2. Executing an EAW
Typically the execution of an EAW begins with the localization/apprehension of the requested person by a local police unit following a check based on an Alert 95 (or on the basis of an Interpol alert -diffusion or red notice) or on a routine check from which the existence of an alert is discovered (i.e. passport control at the airport). If an Alert 95 result when a control is made, the person is immediately taken into custody. The local police immediately contacts the SIRENE Bureau which verifies the consistency of the Alert, sends a G form (HIT) to the SIRENE Bureau of the issuing country and, if needed, requests additional information. This is particularly important in order to notice cases in which identity thefts have occurred or
in which details are so vague that no exact identification is possible (i.e. an Alert for Mr. John Brown, no birth date, somatic or other data available). Form M is used for this exchange of information between national SIRENE Bureaux.

The Italian SIRENE unit provides the local police office a “support kit” for the procedure the local police office has to follow according to the Italian implementation law (L 69/05) and the Court of cassation adjourned case law. This kit has been specifically designed to be easy to use and contain both indications on the activities to carry out and electronic forms to fill out the documents the local police office needs to produce.

The local police office then proceeds with the arrest of the person. This is not necessarily an easy task as the person being arrested should be informed in a language which he or she understands about the EAW and its content, about the possibility of consenting to surrender, about the right to legal counsel and to be assisted by an interpreter. A local office may not have, for example, the availability of a translator with the right competences. The police then informs all the authorities interested providing copy of the report of the procedural steps followed (including the steps taken to identify the requested person) and of the Model A+M to the Court of Appeal of the District, the Public Prosecutor Office General attached to it, the Ministry of Justice and the SIRENE unit.

The Ministry of Justice then notifies the requesting Member State of the arrest, requesting the transmission of the arrest warrant and eventual additional documentation (in general the issuing country has already been unofficially notified by SIS) translated in Italian as according to Article 6.7. Law 69/05 Italy accepts EAWs only in Italian. Although in cases of urgency the Ufficio II has provided to the translation through its internal translators. A formal certification is not required. The Ufficio II, upon reception of the EAW, makes a check of the EAW and in case of evident problems such as missing parts or the EAW not being translated into Italian, contacts the issuing authority asking it to make the appropriate corrections/integrations. It should be noted that the lack of translation of the EAW into Italian is a common reason for the rejection of an EAW execution on formal grounds.270

When the Ufficio II receives the EAW from the issuing authority, it then submits it to the Court of Appeal with territorial jurisdiction, which is the court in charge of the decision about the execution of the EAW.

270 Council of the European Union (2009) Evaluation report on the fourth round of mutual evaluations "the practical application of the European arrest warrant and corresponding surrender procedures between member states" Report on Italy, 5832/1/09 REV1 p.25
Within 24 hours the person held in custody must be made available by the police to the judges of the Court of Appeal in whose district the arrest has been made. Within forty-eight hours after receiving the report of arrest, the arrest must be validated by the Court of Appeal. If it is evident that the wrong person was arrested or the person was arrested on grounds other than those pursuant to the law, the release of the person is ordered (If the SIS alert is not modified, the person may be arrested again). Also, if the competent issuing authority does not provide an Italian translation of the EAW (or the SIS alert) to the Italian Ministry of Justice or to the competent Judicial Authority within ten days of the validation of the arrest by the Court of Appeal, the order imposing the coercive measures is null and void. In case of problems concerning the content or the authenticity of the documents transmitted by the issuing judicial authority, the Court of Appeal can contact directly, or through the Ufficio II of the Ministry of Justice, the issuing authority. If the EAW in Italian is delivered and there is still danger that the person may abscond, new coercive measures can be ordered. The order can be challenged before the Supreme Court of Cassation. The appeal may be lodged by the legal counsel of the requested person or by the public prosecutor general of the Court of Appeal in the interest of the law.

After the first examination by a judge of the Court of Appeal to validate the arrest, a panel of three judges of the Court of Appeal holds a hearing for the discussion of the surrender. This hearing is always held even if the requested person has expressed her or his consent to surrender. However in this case the hearing must take place within ten days from the date in which the consent to surrender has been given (Art.14.4. of the Italian implementing law).

Additional information is often requested by the Italian executing judicial authority to the issuing authority to comply with Art. 6.3. and 6.4. of the Italian implementing law. One important piece of information is the date in which the crime has been committed. As the Italian implementation law provides that the EAW surrender procedure does not apply to offences committed before 7 August 2002, the lack of indication of the date the offence was committed is a common formal ground for refusal. As already mentioned, according to Art. 6.3. surrender is permitted only if a copy of the detention order of personal freedom or custodial sentence that has given rise to the EAW is attached.

According to to Art. 6.4. of the Italian EAW law, the following clarification are also requested: a report on the offences with evidence of the sources of proof, the time and place in which the offences happened and their legal classification; the text of the legal provisions applicable, with an indication
of the type and duration of the penalty, physical description or other information that could help ascertain the identity and nationality of the requested person. If relevant information is missing from the EAW, the executing authority may request it directly or through the Ufficio II.

However, given the case law of the Court of Cassation, while all this information is always requested, failure to receive the report on the offences and the text of the legal provisions applicable or documentation concerning the identification of the requested person does not preclude anymore the surrender.

The request of the court of Appeal is submitted to the Ufficio II, specifying the date of the hearing in camera for which it should be available (Art.6.5). The Ufficio II translates the request in the language requested by the issuing Country and submits it to the issuing authority. Ufficio II has a practice to submit such request also to INTERPOL/SIRENE, asking it to inform the corresponding service in the issuing Member State in order to ensure the transmission and reduce the possibility of errors through redundancy.271

If the issuing authority does not provide such information within 30 days since receiving the request, the court decides anyway on the case. While initially this was considered reason for automatic refusal, the case law of the Court of Cassation has pointed out that a favourable decision may be taken if enough information is available.

The Court of Appeal holds a hearing in the presence of the general prosecutor, the legal counsel of the requested person and the requested person if wants to be present. Immediately following the hearing, the Court of Appeal discusses "in camera" the decision regarding the execution of the EAW. At the conclusion of this discussion, the decision is read out immediately. The reading is considered as notification to the parties, whether present or not. The parties are entitled to receive a copy of the decision (Art. 17.6.).272

The decision should be issued within sixty days from the execution of the precautionary measures related to the EAW request. The decision is

271 Council of the European Union (2009) Evaluation report on the fourth round of mutual evaluations "the practical application of the European arrest warrant and corresponding surrender procedures between member states" Report on Italy, 5832/1/09 REV1 p.29
272 See also: Council of the European Union (2009) Evaluation report on the fourth round of mutual evaluations "the practical application of the European arrest warrant and corresponding surrender procedures between member states" Report on Italy, 5832/1/09 REV1 p.31
transmitted immediately to the Ufficio II, who informs the competent authorities of the issuing Member State also through SIRENE. In the case of a positive surrender decision, INTERPOL is informed by the Ufficio II, in order to organize the physical surrender. From the interviews emerged that in the cases in which it was not possible for the foreign executing authority to arrange surrender within the 10-day deadline, the person is typically released and then re-apprehended for the physical execution of the surrender.

If the Court of Appeal refuses the surrender request, it immediately revokes the eventual precautionary measure related to the EAW procedure and order the release of the requested person.

The decision of the Court of Appeal on the surrender request may be challenged before the Court of Cassation. The appeal may be lodged by the legal counsel of the requested person or by the public prosecutor general of the Court of Appeal. An appeal is possible also against a surrender decision in a case where the requested person concerned has given her or his consent to the surrender. The appeal must be lodged within 10 days of notification of the decision of the Court of Appeal and suspends the execution of the surrender decision. Lawyers have criticized the short span of time available, as in their opinion it does not provide enough time to prepare the documents.

EAW cases are typically allocated to the sixth penal section of the Court of Cassation. The Court of Cassation holds a hearing within fifteen days from receiving the documents of the case. The public prosecutor office and the legal counsel are notified at least five days in advance. Also in this case, lawyers have criticized the short span of time available, as in their opinion it is not enough to prepare the case. Within the general public prosecutor office attached to the Court of Cassation there is not a functional specialization as EAW is concerned and cases are allocated considering the hearing calendar of the public prosecutors. At the same time, some public prosecutors possess a specific expertise in dealing with such cases.

The Court of Cassation does not decide only on points of law, as it usually does in other cassation procedures, but also on substance of the case. Also, contrary to the typical Court of Cassation procedure, the requested person can be present and is allowed to speak to the court. This, though, takes place quite seldom. At the conclusion of the hearing the Court of Cassation [decides in chamber and immediately afterwards] reads out its decision. The written decision of the Court of Cassation at the conclusion of the hearing should be accompanied by a specific statement containing the grounds underlying it. If it is not possible to immediately deliver this
statement, the Court of Cassation should deliver the statement within five
days from reaching the decision.
A copy of the decision is immediately transmitted to the Ministry of Justice
(Ufficio II). The procedures that follow in case of surrender decision or
acquittal are analogue to those described for a decision of the Court of
Appeal. The Court of cassation can also quash a decision with remittal, in
which case the documents are transmitted by the Court of cassation to the
Court of Appeal where the remittal judge should decide the case within
twenty days of receiving them.

There is a contact point for EAW matters at the Court of Cassation. The aim
of the contact point is, on the one hand, to function as a centre of expertise
for the benefit of the members of the Court of Cassation (and, as
appropriate, for members of Courts of Appeal that may need information or
assistance in EAW matters), and on the other hand to facilitate contacts
with issuing authorities in the other Member States. 273

---

273 See also: Council of the European Union (2009) Evaluation report on the fourth round of
mutual evaluations "the practical application of the European arrest warrant and
corresponding surrender procedures between member states" Report on Italy, 5832/1/09
REV1 p.32
4. Preliminary conclusions

The report has attempted to provide a flavour of the complexity ingrained in the main EAW information infrastructure: the Schengen Information System. It is a complexity that is embedded in the heterogeneous and loosely integrated nature of the assemblage, which, once “in action”, manages to perform its tasks. At the same time, the reconstruction of the SIS and SIS II stories allows to see how, under the surface, the assemblage components (normative, technological and organizational) change with time. It allows to see how the trajectories these components follows are not always convergent. Also, it shows how external events and the broader political context (i.e. terrorism attacks, new EU Members accession) indeed play a relevant, if ex-ante unpredictable, role in determining the direction of a change. Indeed, while the system as a whole is still there after almost twenty years from its implementation, its components have radically changed.

The case study shows how, while all these changes have taken place, the capability of the Schengen information System to perform its functions has been kept and maintained. At the same time, it shows also how the same has not been true for the second generation of the Schengen information System. In this case, the same kinds of changes have resulted in a never-ending normative and technological development phase.

The SIS story provides therefore the opportunity to reflect on the implicit assumptions that are still shared by much of the practitioners’ and scientific communities on how information systems are developed, should evolve and made interoperable to support services provision. Indeed, in the last decade, much progress has been done, understanding that technology is just one of the components to be considered. For example, in the Commission ‘European Interoperability Strategy (EIS) for European public services’, it is recognized that “Interoperability issues are not only technological, but also cover a wide range of aspects, such as: lack of a cross-border and cross-sector legal basis for interoperability, insufficient awareness and political will, or lack of agreement on the governance structures required”. At the same time, the same vision shows how

---

274 European Commission, "European Interoperability Strategy (EIS) for European public services", Bruxelles, le 16.12.2010 COM(2010) 744 final Annex 1 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services'.

84
information systems and interoperability between systems are still perceived as positivistic objectives to reach. Indeed, the European Interoperability Framework (EIF) definition of interoperability, “the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems”, \(^{275}\) in its generality and inclusiveness, miss the messiness of a reality populated by objectives multiplicity and conflict, unintended effects, and time bounded decisions. SIS story shows the relevance of all these elements when the temporal dimension is added to the equation. More importantly, it shows how a system with all this messiness managed to support the EAW while the attempt to develop a more tidy second generation system resulted in a never ending sequences of accidents, delays and postponements.

5. Some lessons for the creation and evolution of an EU scale interoperability infrastructure

While the previous section pointed out some of the limits of the present EU vision in relation to European Interoperability, it nevertheless stands true that "Interoperability between public administrations is crucial for achieving European integration and concerns core aims of the European Union". In this perspective, the Schengen Information System story provides a number of lessons to support the creation and evolution of an EU scale interoperability infrastructure, in order to better understand which are the elements and the dynamics (normative, organizational, technological, semantic and governance) which have allowed the system to perform.

5.1. About Norms

When dealing with large-scale interoperability infrastructures, agreements need to be ratified and norms and contracts created. The story of SIS is full of examples of Council Decisions and Regulations defining technical, organizational and functional features of the system, allowing contracts to be ratified and by which authorities, and imposing time limits to their validity. In this way, the norms that are introduced shape not only the features, but also the development path of the system. At the same time, norms (and contracts) reveal themselves to be time bounded and sometime time-limited. As a consequence of escalating complexity, unforeseen derives and delays, norms need to be changed and new contracts stipulated. This process does not take place in a linear and well ordinated manner. It produces effects which are not considered when observing an information system performing its functions in one point in time, but which are a fundamental component of the life of the system and a key element to understand it. Indeed, the juridical maze that is needed to assemble a large-scale information system requires constant attention and cultivation. Indeed, SIS story points out how legal interpretations can progressively stabilize trough recursive interactions between the various actors and component that constitute the ‘performative assemblage’. At the same time, the Schengen Manual example, which keeps being updated and adapted


86
over time, shows how this stabilization is not in the direction of a static asset but of a dynamic one.
The story also shows how the assemblage is capable of performing its functions tolerating (at least for a time) some discrepancies between the normative layer and its technological and organizational components. As an example, while the Schengen Convention Joint Supervisory Authority (JSA) in 1996 discovered that the databases of the N-SISs were not identical as provided for by the Schengen Convention, the system remained functional. In some cases such discrepancies are resolved ex post recognising for example roles and functions that have imposed in the practice, as for the SIRENE Bureaux, formally introduced in the Schengen convention by Council Regulation (EC) No 871/2004 of 29 April 2004 and Council Decision 2005/211/JHA of 24 February 2005, ten years after they started to perform their essential tasks.  

5.2. About Organization

While some organizational structures are conceived ex-ante, i.e. N-SIS units, other impose themselves as a functional requirement and are only afterward formally recognized as in the SIRENE Bureaux case. Indeed, SIRENE Bureaux, adding one layer of organization, reduced the complexity in several other layers of the system. It provided a single gateway/interfaces at national level capable of reducing and translating meanings and actions between different organizations such as the various Police forces. The role of the SIRENE Bureaux has provided to be paramount not only in the everyday functioning of SIS, supporting cross-training, standardization and shearing of practices, but also in its extension to new Member States, with the training and assessment of the new units before they were connected. It is indeed due to the existence of the SIRENE Bureaux that has provided the competences and resources needed to interface the existing SIS with the somewhat different requirements of the EAW FD. Indeed, SIRENE Bureaux have also absorbed part of the complexity of the EAW procedure, supporting communications between issuing and executing authorities or, as in the Italian example, providing a regularly updated “support kit” for the EAW arrest procedure to the local police offices.

SIS story shows also how in the long run, organizations involved may change, their role may change, and new organizations can be created and begin to play a role. Eurojust and Europol are two examples from the ‘user’

perspective, but the changes in the governance component as EU governance structure changed over time is even more relevant.

5.3. About Technology

Perfect fit is not always required in order for the technology to be performative. Predating the EAW, SIS is not perfectly aligned with it (i.e. it does not provide for the 32 categories of crimes for which the double criminality principle does not apply). At the same time, SIS perform its function ‘well enough’ for the EAW FD to be successfully implemented.

As already mentioned in the section on norms, problems of compatibility between technology an norms may emerge. The SIS showed to be able to tolerate some inconsistencies and still performing its functions.

Size both from a databases growth both from a geographical extension provided to be a non irrelevant technical issue. SIS updates such as SIS I+ and SIS One4All were triggered by such needs. Between the results of this need to extend and keep SIS operational, there has been on the one hand a reduction in the resources that could be allocated SIS II, and on the other hand a growing misalignment between the SIS II technological and organizational components, which caused additional delay in the development and implementation of the system.

5.4. About Semantic

The way in which semantic issues have found solutions in SIS case provides some useful hints for the development of other interoperability infrastructures. The key role of SIRENE Bureaux in the translation of meanings and actions. Furthermore, the capability of the system of allowing some flexibility on ‘where’ the translation takes place increases the ability of the system to perform. The presence in the SIS Bureaux of personnel speaking several languages allow the system to perform also in many cases in which SIS alerts not in English. Furthermore, their specialized competences and their understanding of other states EAW FD implementation laws and practices have also reduced the complexity of communication and finding a common understanding between issuing and executing authorities, helping solving semantic impasses which are generated not only by the use of different languages, but from seeing and understanding the world from different, nationally bound, legal perspectives.

A last aspect, also related to semantic is that the definition of what SIS is, and therefore which procedures and practices can support has shifted with time. While initially SIS was created only for alerting authorities of other
Schengen countries on certain categories of people and goods in order for them to take ‘concrete measures’ and ‘compensate’ for the removal of internal borders, with time, its nature and scope has shifted in order to support new instruments such as the EAW, but also include investigative functions.

5.5. About Governance

Not only governance structures needs to be created and equilibriums need to be achieved. As time goes by they need to be able to change. It is the case of the events related to the decision to adopt SIS One4All, but also to the one related to SIS I+RE alternative to SIS II.

Another element worth considering is that at least one “great pressure source” seems to be linked to each relevant policy action/change. Such pressures have gone on the one hand in the direction of making SIS I evolve to remain operational and “do more”. On the other hand they seems to have resulted in a greater delay in SIS II development and implementation. As SIS II experience shows, tighter the coupling attempted, stronger become derives, time delays and greater the level of coordination required. Given all these elements it looks like the governance capability and drive was not enough for the complexity of SIS II project.